



Caméras PTZ Spectra Enhanced et Spectra Pro Operations Manual

Caméras Spectra Enhanced PTZ et Spectra Pro PTZ :

- Spectra Enhanced 8 Series PTZ
- Spectra Enhanced IR Look Up 7 Series PTZ
- Spectra Professional 2 Series PTZ
- Spectra Professional 2 Series PTZ

Numéro du document : C6775M

Date de publication : 2026-02-02

Caméras PTZ Spectra Enhanced et Spectra Pro Manuel d'utilisation

© 2026, Pelco Corporation. Tous droits réservés. MOTOROLA, MOTO, MOTOROLA SOLUTIONS et le logo M stylisé sont des marques commerciales ou des marques déposées de Motorola Trademark Holdings, LLC et sont utilisées sous licence. Toutes les autres marques de commerce sont la propriété de leurs détenteurs respectifs. Sauf mention explicite et écrite, aucune licence n'est accordée en ce qui concerne les droits d'auteur, les dessins industriels, les marques commerciales, les brevets ou autres droits de propriété intellectuelle de Pelco Corporation ou de ses concédants de licence.

Ce document a été compilé et publié en utilisant les spécifications et descriptions de produit disponibles au moment de la publication. Le contenu de ce document et les spécifications des produits présentés ci-après sont modifiables sans préavis. Pelco Corporation se réserve le droit d'apporter des modifications sans avis préalable. Ni Pelco Corporation ni aucune de ses sociétés affiliées : (1) ne garantit l'exhaustivité ou l'exactitude des informations contenues dans ce document ; ou (2) n'est responsable de l'utilisation que vous faites de ces informations ou de la confiance que vous leur accordez. Pelco Corporation ne peut être tenue responsable des pertes ou dommages (y compris les dommages indirects) causés par la confiance accordée aux informations présentées ici.

Pelco Corporation
pelco.com

C6775M
Révision : 4 - EN
2026-02-02

Contenu

Caméra Manuel d'utilisation	9
Configuration système requise	10
Initialisation d'une caméra	10
Live Preview	10
Téléchargement des images enregistrées	10
Amélioration de la qualité d'image de la caméra	11
Utilisation des caméras PTZ avec des tours de garde et des paramètres prédéfinis	11
Ajout de paramètres prédéfinis PTZ	11
Activation de superpositions d'analyse	12
General	13
Modification du nom et de l'emplacement de la caméra	13
Modification de l'état d'alimentation de la caméra	13
Mode de la caméra	13
Time settings	14
GPS settings	14
Network & Security	15
Changer le Hostname	15
Désactivation de DHCP	15
Activation du protocole IPv6	15
Désactivation de WS Discovery	16
Configuration des paramètres de recherche DNS	16
Configuration des ports de contrôle	17
Configuration du serveur NTP	17
Réglage de MTU size	17
Modification des paramètres Ethernet	18
Modification des paramètres de sécurité	18
Configuration de SNMP	18
Available traps	19
Configuration de DSCP	20
Restaurer les paramètres par défaut	21
Configuration des paramètres de pare-feu	21
Ajout de nouveaux agents MQTT	21
Configuration des paramètres SMTP	28
Gestion de l'accès au réseau via des filtres IP	28
Restaurer les paramètres par défaut	29
Configuration de WebRTC	29

Suppression de serveurs	30
Configuration des profils 802.1x	30
Gestion des configurations 802.1x enregistrées	30
Changer le Encryption Engine	32
Licence FIPS	32
Gestion de l'accès aux caméras ou dispositifs via des certificats	33
Informations relatives au certificat	33
Ajouter un nouveau certificat	33
Téléchargement d'un certificat auto-signé	33
Téléchargement d'un certificat client-serveur via une demande de signature	34
Téléchargement d'un certificat client-serveur via PKCS#12	34
Téléchargement d'un certificat client-serveur via PKCS8	35
Téléchargement d'un certificat CA	35
Téléchargement des demandes de signature de certificat	36
Chemins de validation des certificats	36
Ajout d'un nouveau chemin de validation de certificat	37
Gestion des chemins de validation des certificats	37
Ajout et gestion des règles de validation des certificats	37
Gestion des règles de validation des certificats	38
Configuration des profils 802.1x	38
Gestion des configurations 802.1x enregistrées	39
Modification des chemins de validation des certificats	39
Authentification unique (SSO)	39
Compatibilité	39
Exigences en matière d'authentification	39
Configuration de l'authentification unique dans l'interface Web de la caméra	40
Image & Display	42
Live Preview	42
Réglage de Image Settings	42
Configuration de Auto Focus Zone	43
Day/Night Settings	43
Modification du Day / Night mode	43
Activation des LED infrarouges	44
Réglage du Seuil Jour/Nuit (EV)	44
Activation de la compensation IR adaptative	44
Activation du contrôle de visibilité nocturne	44
Réglage de Exposure Settings	45
Utilisation de Flicker Control	45

Modification de l'exposition	45
Réglage d'un niveau d'exposition maximal	45
Réglage du gain maximal	45
Modification du Priority	46
Passage au mode Diaphragme	46
Utilisation de WDR	46
Utilisation de Backlight Compensation Mode	46
Utilisation de Priorité diaphragme	46
Advanced Filters	47
Désembuage numérique	47
Stabilisation électronique de l'image (EIS = Electronic Image Stabilization)	47
Adjustment	47
Image Rotation	47
Réglage de base Image Settings	48
Zoom & Focus	48
White Balance	48
Temporal Filter Strength	49
Overlays	49
Ajouter Overlays	49
Compression & Image Rate	51
Considérations relatives à la configuration des paramètres Compression & Image Rate	51
Configuration des paramètres Compression & Image Rate	51
Configuration des paramètres de multidiffusion pour la vidéo	52
Activation de la résolution maximale du flux secondaire	52
Activation du flux quaternaire recadré	53
Paramètres avancés de Compression & Image Rate	53
Utilisation de HDSM SmartCodec	53
Désactivation de Mode Scène inactive	54
Utilisation de Mode Scène inactive	54
Affichage de la transmission directe via l'URI de flux RTSP	54
Streaming Settings	55
Analytics	56
Motion Detection	56
Activation de l'événement d'alarme de mouvement ONVIF	57
Sabotage Detection	57
Configuration de Classified Object Motion Detection	57
Création d'événements d'analyse de mouvement	58
Activation de superpositions d'analyse	59

Utilisation de Self Learning	60
Suspendre et réinitialiser Self Learning	61
Suspend Self Learning	61
Reset Self Learning	61
Modification du Scene Mode	61
Modification de la zone d'inclusion	61
Test en cours Analytics Events	62
Types d'événements d'analyse	63
Analyse vidéo	63
Analyse audio	63
Camera Automation	65
Créer des règles et affecter des actions	65
Gestion des règles	67
Ajout de nouvelles séquences	67
Gestion des séquences	67
Ajouter de nouveaux courriels d'actions	68
Configuration des informations du serveur SMTP	68
Gestion des informations du serveur STMP	68
Ajouter un courriel d'action	68
Ajout de nouvelles actions FTP	69
Configuration des informations du serveur FTP	69
Gestion des informations du serveur FTP	69
Ajouter une action FTP	69
Cloud Connection	70
Paramètres étendus	70
Privacy Zones	71
Création de Privacy Zones	71
Gestion des Privacy Zones	71
Storage	73
Informations sur Storage	73
Formatage de la carte SD	73
Informations carte SD	73
Chiffrement de carte SD	74
Configuration de Recording Mode	74
Télécharger les enregistrements depuis l'interface Web	75
Téléchargement des vidéos enregistrées depuis la carte SD	75
ONVIF Profile G	76
Dépannage de carte SD	76
Réactivation de la carte SD	76

System	77
Mise à jour de Firmware	77
Redémarrage de la caméra	77
Suppression de tous les paramètres	78
Device Logs	79
Mise à jour de Device Logs	79
Téléchargement du journal	79
PTZ	79
PTZ Patterns	80
Création de PTZ Patterns	80
Gestion des PTZ Patterns	80
PTZ Scans	81
Création de PTZ Scans	81
Gestion des PTZ Scans	81
PTZ Zones	82
PTZ Tours	82
Ajout de PTZ Presets	82
Création de PTZ Tours	83
Ajouter des PTZ Presets aux PTZ Tours	83
Gestion des PTZ Tours enregistrés	84
PTZ Limits	84
Audio	85
Configuration de Device Speaker	85
Configuration de Device Microphone	86
Configuration des paramètres Multicast pour l'audio	86
Users	87
Ajouter Users	87
Gestion des Users	87
Conservation des comptes utilisateurs lors de la restauration du micrologiciel	88
Modification du Password Complexity Requirements	88
Security group	89
About	90
Compte	91
Modifier votre Password	91
Se déconnecter	91
Déconnexion après utilisation de l'authentification unique	91
Plus d'informations et d'assistance	92

Caméra Manuel d'utilisation

Ce Manuel d'utilisation fournit des instructions pour installer Caméras PTZ Spectra Enhanced et Spectra Pro et configurer ses paramètres. Les instructions contenues dans ce Manuel d'utilisation renvoient à l'interface Web de la caméra pour effectuer les différentes étapes. Vous aurez besoin de l'adresse IP de la caméra pour accéder à l'interface Web à partir d'un navigateur Web.

L'interface Web ne vous permet de travailler que sur une seule caméra à la fois. Si vous installez ou configurez plusieurs caméras à la fois, utilisez plutôt l'outil CCT (Camera Configuration Tool). Voir le [Manuel de l'utilisateur CCT](#) pour obtenir des instructions.

Les paramètres et fonctions disponibles dans l'interface Web dépendent du dispositif spécifique et de la version du micrologiciel. Les informations contenues dans ce guide concernent Caméras PTZ Spectra Enhanced et Spectra Pro qui utilise la dernière version du micrologiciel. Vous pouvez télécharger le dernier micrologiciel à l'adresse <https://www.pelco.com/updates>.

Configuration système requise

Vous pouvez accéder à l'interface Web depuis n'importe quel appareil Windows, Mac ou mobile via l'un des navigateurs suivants :

- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Configurez votre navigateur Web pour qu'il accepte les cookies, sinon l'interface Web ne fonctionnera pas correctement.

D'autres navigateurs peuvent fonctionner, mais cela n'a pas été vérifié.

Initialisation d'une caméra

Lors de votre première connexion à une caméra, cette dernière se trouve dans son état d'usine par défaut. À l'état d'usine par défaut, les caméras n'ayant ni nom d'utilisateur, ni mot de passe par défaut, vous serez invité à créer un compte. Vous pouvez également utiliser un VMS tiers ou CCT pour initialiser la caméra et créer le premier compte administrateur.

Pour initialiser la caméra et créer un compte administrateur, procédez comme suit :

1. Entrez l'adresse IPS de la caméra dans votre navigateur Web. Le système vous redirigera vers la page *Add user* pour créer un compte.
2. Entrez un nouveau **Username** ou conservez le nom d'administrateur par défaut.
3. Entrez un nouveau **Username** pour l'utilisateur. Nous vous recommandons d'utiliser un mot de passe sécurisé et complexe.
4. Confirmez le nouveau **Password** en le saisissant à nouveau.
5. Assurez-vous que **User name (Security group)** est sur Administrator.
6. Cliquez sur **Save**.

Vous pouvez désormais vous connecter à la caméra.

Live Preview

La page *Live Preview* vous permet d'avoir un aperçu de la vidéo en direct, de vérifier l'état du stockage, de télécharger les enregistrements de la carte SD et de modifier les paramètres de base de la caméra afin d'améliorer la qualité d'image.

Téléchargement des images enregistrées

Si une carte SD est installée dans la caméra et que le stockage sur carte SD est activé, vous pouvez télécharger les images enregistrées à partir de la page *Live Preview*.

- Cliquez sur **Download** dans la zone *Download Still from Camera*.

Le système télécharge les fichiers au format .JPG.

Amélioration de la qualité d'image de la caméra

La page *Live Preview* permet aux utilisateurs d'améliorer la qualité d'image globale. Pour plus de paramètres d'image, voir [Image & Display sur la page 42](#).

Pour utiliser les commandes d'image, procédez comme suit :

1. Pour zoomer, déplacez le curseur **Zoom** vers la droite.
2. Pour dézoomer, déplacez le curseur **Zoom** vers la gauche.
3. Cliquez sur **Auto Focus** pour que la caméra fasse la mise au point automatiquement.
4. Pour faire la mise au point, déplacez le curseur **Focus** vers la droite ou vers la gauche.

Les modifications sont enregistrées automatiquement.

Utilisation des caméras PTZ avec des tours de garde et des paramètres prédéfinis

La page *Live Preview* vous permet d'exécuter des tours de garde PTZ et des paramètres prédéfinis. Vous pouvez également revenir à la position de départ ou définir la position de départ.

1. Pour lancer un tour de garde PTZ, sélectionnez-le dans la liste déroulante **Tours** et cliquez sur **Start**.
2. Pour ajouter un préréglage, entrez un nom dans le champ **Add Preset** et cliquez sur **Add**.
3. Pour utiliser un préréglage, sélectionnez-le dans la liste déroulante **Presets** et cliquez sur **Go**.
4. Pour supprimer un préréglage, sélectionnez-le dans la liste déroulante **Presets** et cliquez sur **Remove**.
5. Pour ramener la caméra à sa position de départ, cliquez sur **Go**.
6. Pour régler la position de départ de la caméra, positionnez la caméra et cliquez sur **Set**.

Les modifications sont enregistrées automatiquement.

Ajout de paramètres prédéfinis PTZ

La page *Live Preview* vous permet créer des paramètres prédéfinis PTZ pour enregistrer certaines positions de panoramique/inclinaison et certains niveaux de zoom.

1. Pour ajouter un nouveau paramètre prédéfini PTZ, utilisez les commandes **Zoom** et **Focus** pour positionner la caméra.
2. Entrez un nom de préréglage dans le champ **Add Preset**.
3. Cliquez sur **Add**.

Les caméras PTZ peuvent utiliser des fonctions d'analyse à domicile et des positions prédéfinies. Assurez-vous d'avoir mis à jour le micrologiciel minimum requis pour utiliser l'analyse sur des positions prédéfinies.

Activation de superpositions d'analyse

La page *Live Preview* vous permet d'activer les superpositions d'analyse pour faciliter la visualisation des règles d'analyse. Lorsque les superpositions d'analyse sont activées, des superpositions apparaissent autour des objets répondant aux critères définis par les règles d'analyse.

- Pour activer les superpositions d'analyse, activez l'option **Analytics Overlays**. Les modifications sont enregistrées automatiquement.



NOTE

Pour pouvoir activer les superpositions d'analyse, vous devez activer les métadonnées XML d'analyse sur la page *Paramètres étendus*. Pour plus d'informations, voir [Paramètres étendus sur la page 70](#).

General

Les paramètres *General* permettent aux administrateurs de configurer les paramètres s'appliquant à l'identité et aux fonctions essentielles de la caméra, telles que le nom de la caméra, son emplacement, son état d'alimentation, et de modifier le mode de la caméra.

Voir [Mode de la caméra en dessous](#) pour obtenir des instructions sur la modification du mode de la caméra.

Modification du nom et de l'emplacement de la caméra

La page *General* vous permet de modifier le nom et l'emplacement de la caméra. Cela permet d'identifier les différentes caméras présentes sur le réseau. Vous pourrez utiliser un filtre pour filtrer les caméras par emplacement dans des outils tels que CCT ou VMS. Le nom et l'emplacement de la caméra apparaîtront dans le VMS lorsque la caméra déclenche des événements d'analyse et envoie des notifications.

1. Accédez à la page *General* dans l'interface Web de la caméra.
2. Entrez un nouveau nom pour la caméra dans le champ **Name**.
3. Entrez un nouvel emplacement dans le champ **Location**.
4. Cliquez sur **Save**.

Les informations relatives à la caméra seront modifiées afin de refléter le nouveau nom et l'emplacement.

Modification de l'état d'alimentation de la caméra

La page *General* vous permet de modifier l'état d'alimentation de la caméra de Aux à PoE.

Si la caméra est connectée à la fois à une alimentation PoE et à une alimentation auxiliaire externe, elle sera alimentée par l'alimentation auxiliaire. Si vous préférez que la caméra utilise une alimentation PoE, vous pouvez modifier manuellement l'état d'alimentation pour utiliser PoE.

- Pour modifier l'état d'alimentation de la caméra, sélectionnez l'option **Force PoE** dans la liste déroulante **Device Power State**. Cliquez sur **Save**.

La caméra passera sur une alimentation PoE au lieu de l'alimentation auxiliaire.

Mode de la caméra

La page *General* vous permet modifier le mode de la caméra afin de privilégier différentes fonctions pour chaque caméra. Par exemple, si vous souhaitez augmenter la fréquence d'images d'une caméra, vous pouvez la régler en mode Fréquence d'image élevée. Cependant, le mode Fréquence d'images élevée désactive d'autres fonctions.

Vous ne pouvez modifier le mode de la caméra que sur les caméras utilisant une bande passante plus élevée. Cette fonction ne s'affiche pas si le modèle de caméra ne la prend pas en charge.

1. Accédez à la page *General* dans l'interface Web de la caméra.
2. Dans la zone *Settings*, cliquez sur la liste déroulante **Mode** et sélectionnez un autre mode de caméra :
 - a. Full feature : propose les fonctionnalités complètes de la caméra. Le mode Complète est le mode par défaut de la caméra.
 - b. High Frame Rate : utilise le débit d'images le plus élevé possible, mais peut désactiver certaines fonctions de la caméra.
 - c. No Video Analytics : désactive l'analyse vidéo. Cette option est destinée aux déploiements où l'analyse vidéo par caméra interfère avec d'autres intégrations d'analyse.
 - d. Dynamic Privacy Masks : active les masques de confidentialité dynamiques. Les masques de confidentialité dynamiques peuvent détecter le moment où l'objet, p. ex. une personne ou un véhicule, se déplace et s'ajuster de sorte que l'objet reste masqué.
3. Cliquez sur **Save**.

La caméra redémarre dès que vous changez le mode.

Actualisez le navigateur et reconnectez-vous lorsque la caméra a fini de redémarrer.

Time settings

La page *General* vous permet de modifier le fuseau horaire de la caméra, afin qu'il corresponde à sa situation géographique. Cela garantit que la caméra peut se synchroniser avec d'autres dispositifs sur le réseau. Pour que le site fonctionne efficacement, les horloges doivent être synchronisées entre toutes les caméras, tous les dispositifs et tous les serveurs du réseau.

1. Accédez à la page *General* dans l'interface Web de la caméra.
2. À partir de la zone *Time settings*, cliquez sur la liste déroulante **Fuseau horaire** et sélectionnez le fuseau horaire approprié.
3. Vous pouvez désactiver **Automatically adjust clock for Daylight Savings Time** si nécessaire. Cependant, nous vous recommandons de laisser cette option activée.
4. Cliquez sur **Save**.

L'horloge de la caméra affiche alors l'heure de son fuseau horaire.

GPS settings

La page *General* donne accès au champ GPS settings permettant de saisir les informations de géolocalisation de la caméra sous forme de valeurs décimales. Les informations GPS peuvent être utiles pour la carte et d'autres applications basées sur la localisation.

1. Accédez à la page *General* dans l'interface Web de la caméra.
2. À partir de la zone *GPS settings* entrez une valeur dans le champ **Latitude** (-90-90).
3. Entrez une valeur dans le champ **Longitude** (-180-180).
4. Entrez une valeur dans le champ **Elevation (meters above sea level)**, qui est calculée en mètres au-dessus du niveau de la mer. N'accepte que des valeurs positives.
5. Cliquez sur **Save**.

La caméra modifie alors ses coordonnées GPS pour s'aligner sur sa position géographique.

Network & Security

Les paramètres *Network & Security* permettent aux administrateurs de modifier la manière dont la caméra se connecte au réseau du serveur et le comportement de synchronisation de l'heure de la caméra.

Changer le Hostname

La page *Network & Security* permet aux administrateurs de modifier le nom d'hôte de la caméra.

1. Accédez à la page *Network & Security* dans l'interface Web de la caméra.
2. Modifiez le texte dans le champ **Hostname**.
3. Cliquez sur **Save**.

Le nom d'hôte de la caméra est mis à jour.

Désactivation de DHCP

La page *Network & Security* permet aux administrateurs d'activer ou de désactiver le protocole DHCP. Le protocole DHCP est activé par défaut.

1. Accédez à la page *Network & Security* dans l'interface Web de la caméra.
2. Cliquez sur le **DHCP** pour le désactiver.
3. Cliquez sur **Save**.

La caméra désactivera le DHCP.

Activation du protocole IPv6

La page *Network & Security* permet aux administrateurs d'activer le protocole IPv6, afin d'accueillir davantage de dispositifs sur le réseau.



NOTE

L'activation d'IPv6 ne désactive pas les paramètres IPv4.

Pour activer IPv6, procédez comme suit :

1. Accédez à la page *Network & Security* dans l'interface Web de la caméra.
2. À partir de la zone **IPv6 Settings**, cochez la case **Enable** et cliquez sur **Apply**. Des paramètres supplémentaires apparaîtront.
3. La case **Accept Router Advertisements** doit rester cochée si vous utilisez l'état DHCPv6 Auto.
4. Sélectionnez l'état DHCPv6 dans le menu déroulant :

- a. Auto : l'état de DHCPv6 est déterminé par les publications du routeur (AR). Le paramètre Accepter les annonces de routeur est nécessaire pour que ce paramètre fonctionne comme prévu.
 - b. Stateless : la caméra reçoit uniquement les informations relatives au DNS et au NTP depuis le serveur DHCPv6. Les adresses IP du serveur DHCPv6 ne sont pas acceptées.
 - c. Stateful
 - d. Off
5. Entrez les adresses IPv6 statiques.
 6. Entrer le Default Gateway.
 7. Cliquez sur **Save**.

La caméra activera IPv6 et utilisera les nouveaux paramètres DHCPv6.

Désactivation de WS Discovery

La page *Network & Security* permet aux administrateurs de désactiver WS Discovery. WS Discovery est nécessaire pour la communication multidiffusion et la détection. WS Discovery est activé par défaut afin que les caméras puissent être détectées par CCT ou certains VMS dès leur ajout dans le réseau.

1. Accédez à la page *Network & Security* dans l'interface Web de la caméra.
2. Pour désactiver la détection WS, décochez la case **Enable WS Discovery Protocol**.
3. Cliquez sur **Save**.

La caméra ne sera plus détectable sur le réseau.



TIP

Désactivez WS Discovery après avoir ajouté la caméra au réseau afin d'empêcher des personnes malintentionnées de détecter la caméra et d'accéder à la transmission directe.

Configuration des paramètres de recherche DNS

Les paramètres *Network & Security* permettent aux administrateurs de modifier l'adresse du serveur DNS de la caméra ou d'affecter un autre serveur DNS à la caméra.

Par défaut, les caméras obtiennent automatiquement une adresse de serveur DNS.

1. Accédez à la page *Network*.
2. Sélectionnez **Use the following DNS server address** pour affecter les serveurs DNS manuellement.
3. Entrez l'adresse du serveur pour Preferred DNS server. C'est le premier serveur DNS auquel la caméra tente de se connecter.
4. Entrez l'adresse du serveur pour Alternative DNS server 1. C'est le premier serveur de secours.
5. Entrez l'adresse du serveur pour Alternative DNS server 2. C'est le deuxième serveur de secours.
6. Cliquez sur **Save**.

La caméra utilisera le nouveau serveur DNS et les nouveaux paramètres DNS.

Configuration des ports de contrôle

La page *Network & Security* permet aux administrateurs de configurer les paramètres du port de contrôle afin d'affecter certains types de connexions à certains ports.

Pour configurer les ports de contrôle, procédez comme suit :

1. Accédez à la page *Network & Security* dans l'interface Web de la caméra.
2. Assurez-vous que la case **Enable HTTP connections** est cochée.
3. Vous pouvez modifier les ports si nécessaire (1..65534). Voici les ports par défaut :
 - a. HTTP port : 80
 - b. HTTPS port : 443
 - c. RTSP port : 554
 - d. RTSP replay port : 555
 - e. WebRTC port : 9090
4. Cliquez sur **Save**.

La caméra utilise alors les nouveaux paramètres du port de contrôle.

Configuration du serveur NTP

La page *Network & Security* permet aux administrateurs de configurer les paramètres de configuration du serveur NTP externe, afin que la caméra se synchronise avec le serveur NTP. Cela permet de d'assurer que la caméra conservera la date et l'heure correctes, évitant ainsi tout problème de synchronisation horaire.

Pour configurer le serveur NPT, procédez comme suit :

1. Accédez à la page *Network & Security* dans l'interface Web de la caméra.
2. Sélectionnez le **Manual** pour affecter un serveur NTP manuellement.
3. Entrez l'adresse du serveur NTP pour affecter le serveur.
4. Cliquez sur **Save**.

La caméra utilise alors le nouveau serveur NPT et les nouveaux paramètres.

Réglage de MTU size

La page *Network & Security* permet aux administrateurs de régler la taille maximale du paquet (MTU = Maximum Transmission Unit), afin de décongestionner le réseau.

1. Accédez à la page *Network & Security* dans l'interface Web de la caméra.
2. Pour régler MTU size, entrez une valeur (576 - 1500) dans le champ **MTU size**. La valeur par défaut est de 1500.
3. Cliquez sur **Save**.



TIP

Si le réseau est lent, vous pouvez réduire MTU size pour améliorer les performances du réseau.

Modification des paramètres Ethernet

La page *Network & Security* permet aux administrateurs de modifier les paramètres Ethernet pour activer le mode duplex et régler la tolérance de liaison.

Pour régler les paramètres Ethernet, procédez comme suit :

1. Accédez à la page *Network & Security* dans l'interface Web de la caméra.
2. Sélectionnez le menu déroulant **Speed/Duplex** et choisissez **100M full duplex** pour activer le mode duplex.
Le paramètre de négociation automatique est préférable pour la plupart des caméras. Il négociera la vitesse optimale et le paramètre duplex pour votre connexion réseau.
3. Sélectionnez le menu déroulant **Link tolerance** et modifiez le pourcentage de tolérance des liens.
Augmenter la tolérance de liaison signifie que le réseau peut tolérer un éventail plus large de variations avant qu'une erreur ne se produise.
4. Cliquez sur **Save**.

La caméra utilisera les nouveaux paramètres Ethernet.

Modification des paramètres de sécurité

La page *Network & Security* permet aux administrateurs de modifier la version TLS minimale et d'ajuster le délai d'expiration de la session de connexion.

Pour modifier les paramètres de sécurité de la caméra, procédez comme suit :

1. Accédez à la page *Network & Security* dans l'interface Web de la caméra.
2. Sélectionnez la liste déroulante **Minimum TLS version** et choisissez TLS 1.3 si vous souhaitez limiter la caméra à l'utilisation d'une version minimale de TLS.
 - a. **TLS 1.3** est recommandé pour une sécurité accrue.
 - b. **TLS 1.2** peut être sélectionné si cela est nécessaire pour la rétrocompatibilité.
3. Entrez la durée maximale d'inactivité avant déconnexion d'un utilisateur (en minutes), dans le champ **Login session timeout**. Cela permet d'éviter tout accès non autorisé.
4. Cliquez sur **Save**.

La caméra utilisera la nouvelle version TLS ou le délai d'expiration de session.

Configuration de SNMP

La page *SNMP* permet aux administrateurs de configurer les paramètres SNMP du dispositif et de choisir les informations d'état qui sont envoyées à la page du poste de gestion. L'activation du protocole SNMP facilite la gestion des dispositifs connectés au réseau.

Pour plus d'informations sur les informations d'état ou les interruptions qui seront envoyées, voir le fichier MIB (Management Information Base) du dispositif sur le site Web de Pelco : www.pelco.com/updates.

Pour activer et configurer SNMP, procédez comme suit :

1. Accédez à *Network & Security* > *SNMP* dans l'interface Web de la caméra.
2. Cliquez sur **Activer SNMP** pour l'activer.
3. Sélectionnez une autre version SNMP dans la liste déroulante **Version** si nécessaire :
 - a. SNMP v2c : utilisez SNMP v2c pour envoyer une requête au dispositif, afin d'obtenir des informations sur son état via une requête SNMP Get, et recevoir des notifications d'interruption du dispositif.
 - b. SNMP v3 : utilisez SNMP v2c pour envoyer une requête à la caméra, afin d'obtenir des informations sur son état via une requête SNMP Get, et recevoir des notifications d'interruption de la caméra. SNMP v3 assure une sécurité accrue en vous permettant de définir un nom d'utilisateur et un mot de passe pour la caméra. Cette caméra utilise l'authentification de type SHA-1 et le chiffrement de type AES.
4. Si vous avez sélectionné SNMP v2c, renseignez les champs suivants :
 - a. Lecture communauté : entrez le nom de la communauté en lecture pour le dispositif. Ce nom sert à authentifier le trafic SNMP. Seuls les postes de gestion SNMP ayant le même nom de communauté en lecture recevront une réponse du dispositif.
 - b. Écriture communauté : entrez l'adresse IP du poste de gestion où les interruptions seront envoyées. Dans la zone *Available traps*, sélectionnez les interruptions qui seront envoyées. Pour plus d'informations sur les différents types d'interruptions, voir [Available traps en dessous](#).
 - c. IP de destination interruption : entrez l'adresse IP du poste de gestion auquel les interruptions seront envoyées.
5. Si vous avez sélectionné SNMP v3, renseignez les champs obligatoires :
 - a. Nom d'utilisateur : entrez le nom d'utilisateur devant être utilisé par le poste de gestion lors de l'envoi de la requête SNMP Get à la caméra.
 - b. Mot de passe : entrez le mot de passe que le poste de gestion doit utiliser avec le nom d'utilisateur choisi.
6. Cliquez sur **Save**.

Available traps

Les interruptions disponibles sont les suivantes :

- Temperature alert : un avis d'interruption sera envoyé lorsque la température de la caméra passe au-dessus ou en dessous du seuil de prise en charge. Un avis sera également envoyé lorsque la température de la caméra retournera à la normale.
- The camera will alert you when it is being tampered with. : notification d'interruption envoyée lorsque la caméra détecte une action de vandalisme humain.
- The camera will alert you when its out of storage space. : un avis d'interruption sera envoyé lorsque l'état de la carte SD change.

Configuration de DSCP

La page *DSCP* permet aux administrateurs d'activer ou de désactiver la fonction DSCP, de choisir des valeurs pour les types de trafic répertoriés ci-dessous et de restaurer les valeurs par défaut. Cela permet de gérer le trafic réseau et d'assurer la qualité de service (QoS) sur les réseaux IP modernes. DiffServ peut être utilisé pour réduire la latence du trafic réseau critique, tel que la voix ou la diffusion en direct, tout en fournissant un service simplifié au mieux aux services non critiques, tels que le trafic Web ou les transferts de fichiers.

Pour les flux principaux, secondaires, tertiaires et de relecture, il est très important de préparer et de configurer le trafic de flux. Dans le cas d'un flux sur TCP (une prise commune avec RTSP), la valeur DSCP est prise à partir du flux principal et propagée aux autres flux. La configuration d'un flux via UDP permet à l'utilisateur de spécifier différentes valeurs de DSCP pour tous les flux.

Pour configurer DSCP, procédez comme suit :

1. Accédez à *Network & Security > DSCP* dans l'interface Web de la caméra.
2. Appuyez sur **Activer la fonction** si elle n'est pas déjà activée. DSCP est activée par défaut.
3. Dans le menu déroulant **Onvif protocol**, cliquez pour sélectionner l'une des options suivantes :
 - a. DF (0)
 - b. CS2 (16) (option par défaut)
4. Dans le menu déroulant **Web interface**, cliquez pour sélectionner l'une des options suivantes :
 - a. DF (0)
 - b. AF21 (18) (option par défaut)
5. Dans le menu déroulant **SNMP**, cliquez pour sélectionner l'une des options suivantes :
 - a. DF (0)
 - b. CS2 (16) (option par défaut)
6. Dans le menu déroulant **Primary stream**, cliquez pour sélectionner l'une des options suivantes :
 - a. CS3 (24)
 - b. AF31 (26)
 - c. CS4 (32)
 - d. AF41 (34) (option par défaut)
7. Dans le menu déroulant **Secondary stream**, cliquez pour sélectionner l'une des options suivantes :
 - a. CS3 (24)
 - b. AF31 (26)
 - c. CS4 (32)
 - d. AF41 (34) (option par défaut)
8. Dans le menu déroulant **Tertiary stream**, cliquez pour sélectionner l'une des options suivantes :
 - a. CS3 (24) (option par défaut)
 - b. AF33 (30)
9. Dans le menu déroulant **Replay stream**, cliquez pour sélectionner l'une des options suivantes :

- a. CS3 (24) (option par défaut)
 - b. AF33 (30)
 - c. CS4 (32)
 - d. AF43 (38)
10. Cliquez sur **Save**.

Restaurer les paramètres par défaut

- Les administrateurs peuvent utiliser l'option **Restore Defaults** si vous devez restaurer les paramètres par défaut. Cliquez sur **Save**.

Configuration des paramètres de pare-feu

La page *Firewall* permet aux administrateurs d'autoriser ou de refuser l'accès à certaines adresses IP.

- Accédez à *Network & Security > Firewall* dans l'interface Web de la caméra.
- Le pare-feu est désactivé par défaut. Pour autoriser l'accès à certaines adresses IP, sélectionnez **Allow**.
- Pour refuser l'accès à certaines adresses IP, sélectionnez **Deny**.
- Entrez une adresse IP dans le champ.
- Cliquez sur **Add new address** pour ajouter d'autres adresses IP.
- Cliquez sur **Save**.

Les paramètres de pare-feu s'activent alors immédiatement.

Ajout de nouveaux agents MQTT

La page *MQTT Brokers* permet aux administrateurs d'ajouter de nouveaux agents MQTT. L'utilisation d'agents MQTT est utile dans les environnements contraints où plusieurs capteurs sont connectés aux caméras.

Pour ajouter un nouveau courtier, procédez comme suit :

- Accédez à *Network & Security > MQTT Brokers* dans l'interface Web de la caméra.
- Cliquez sur **Add new broker**.
- Pour **AddressAddress** : entrez l'adresse réseau de l'agent d'événement. Le format `scheme://host:port` indique le protocole à utiliser (p.ex. : `mqtt://`, `mqtt://`), le nom d'hôte ou l'adresse IP de l'agent, et le numéro de port pour la connexion.



IMPORTANT

wss/ws (les sockets Web ne sont actuellement pas pris en charge). Vous devez utiliser le protocole mqtt/mqtts.

4. Pour **Topic prefix** : entrez la chaîne préfixe de tous les sujets pour les événements publiés sur l'agent. Cela facilite le filtrage et la gestion des sujets sur l'agent, en particulier dans les environnements comportant plusieurs dispositifs ONVIF. Par exemple, si le préfixe est onvif/device1, un événement avec le sujet VideoSource/MotionAlarm est publié sur onvif/device1/VideoSource/MotionAlarm.
5. Pour **Username et Password** : utilisé pour l'authentification auprès de l'agent d'événement. Si l'agent requiert un nom d'utilisateur et un mot de passe pour que les clients puissent se connecter, ceux-ci doivent être saisis ici.
6. Pour **Certificate ID** : spécifie l'identifiant d'un certificat côté client à utiliser pour l'authentification TLS avec l'agent. Cette option est utilisée lorsque l'agent requiert que les clients présentent un certificat pour établir une connexion sécurisée.



IMPORTANT

Les certificats sont sélectionnés dans la liste des certificats enregistrés sous *Network & Security > Identity & Trust*.

7. Pour **QoS** : QoS signifie Quality of Service (qualité de service) et désigne un paramètre qui détermine la garantie de délivrabilité des messages. Il comporte généralement les niveaux suivants : 0 (au maximum une fois) : le message est envoyé une seule fois, sans confirmation de réception. C'est le niveau le plus rapide, mais aussi le moins fiable. 1 (au moins une fois) : le message est garanti d'être délivré au moins une fois, mais il peut être délivré plusieurs fois. 2 (une seule fois exactement) : le message est garanti d'être délivré une seule fois. C'est le niveau le plus fiable, mais aussi le plus lent.
8. Pour **Filtre de publication** : vous permet de sélectionner les catégories d'événements qui seront envoyés à l'agent. En cochant les cases en regard des sources d'événements, telles que Moteur de chiffrement, Dispositif, Source vidéo, etc. vous pouvez contrôler le flux des messages d'événements et réduire le trafic réseau inutile.
9. Pour **Règle de validation du chemin d'accès au certificat** : spécifie l'identifiant de règle à utiliser pour valider la chaîne de certificats de l'agent d'événement. Ceci est important pour garantir que le client se connecte à un agent fiable et authentique. Important : l'interface utilisateur vous permet de sélectionner des règles de validation à partir de la liste des règles créées/ajoutées sur l'interface utilisateur via la page des certificats.
10. Cliquez sur **Ajouter**.

Le nouvel agent apparaît dans la liste. Vous pouvez consulter l'adresse, l'état et les actions dans la liste *Agents*.

Publier des filtres

Élément	Description
Moteur de chiffrement	Composant central responsable de l'exécution des opérations de chiffrement/déchiffrement.
Mise à jour du moteur de chiffrement	Événement ou processus indiquant une mise à jour du micrologiciel ou du logiciel du module de chiffrement.
Modes de chiffrement disponibles	Liste des protocoles de chiffrement pris en charge (p. ex. : AES, versions TLS).
Dispositif	Représentation générale de l'unité physique elle-même.
Déclencheur	Entrée ou signal déclenchant une action ou un événement spécifique.
Relais	Sortie électrique utilisée pour contrôler des dispositifs externes (p. ex. : lumières, serrures de porte).
Entrée numérique	Entrée électrique utilisée pour détecter des signaux externes (p. ex. : contact de porte, capteur d'alarme).
Entrée numérique	(entrée en double) Autre exemple d'entrée numérique.
Éclairage	Paramètres ou état liés aux sources lumineuses (p. ex. : LED infrarouges, lumière blanche).
Mise à jour de la configuration des utilisateurs	Mécanisme utilisé pour spécifier les événements et modifications de configuration publiés (envoyés) aux abonnés/clients externes. Cela évite tout trafic de données inutile.
Journaux	Enregistrements des activités, des erreurs et des événements du système.
Configuration	Paramètres généraux ou paramètres du dispositif.
Planification	Périodes définies pour des actions spécifiques (p. ex. : enregistrement, activation d'un événement).
Modifié	Notification générale indiquant qu'un paramètre ou un état a été modifié.
Supprimé	Notification générale indiquant qu'un élément ou une configuration a été supprimé(e).
Planification	(entrée en double) Périodes définies pour des actions spécifiques.
État	État opérationnel actuel (p. ex. : en cours d'exécution, inactif, erreur).
Actif	Indique qu'une fonction, un processus ou un paramètre est actuellement opérationnel.
Contrôleur PTZ	Composant gérant les mouvements de panoramique, d'inclinaison et de zoom d'une caméra.
Tours de garde PTZ prédéfinis	Séquence définie de positions prédéfinies de la caméra pour un tour de garde automatique.
Configuration	(entrée en double) Paramètres ou réglages généraux.
Source vidéo	Canal physique ou logique fournissant les données vidéo (objectif de la caméra).
Alarme de mouvement	Événement déclenché par la détection d'un mouvement dans le flux vidéo.
Changement de scène globale	Événement indiquant un changement important et global dans le champ de visibilité de la caméra (p. ex. : déplacement de la caméra).
Service d'analyse	Sous-système chargé de l'analyse du contenu vidéo (p. ex. : détection, suivi).
Support	Fait référence aux flux vidéo et sonores eux-mêmes.
Profil modifié	Notification indiquant qu'un ensemble de paramètres enregistrés (profil) a été modifié.

Élément	Description
Configuration modifiée	Envoie les informations modifiées de configuration aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Contrôle des médias	Envoie les informations de contrôle des médias aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de profils	Publie la mise à jour de la configuration de profils aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de paramètres prédéfinis	Envoie les informations d'interdiction de direction aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de tours de garde prédéfinis	Publie les informations relatives à la mise à jour de tours de garde prédéfinis aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de protocoles réseau	Envoie les informations relatives à la mise à jour de la configuration de protocoles réseau aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Led Enabled	Envoie les informations relatives à la mise à jour de la configuration de Led Enabled aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Ir Led Allowed	Envoie les informations relatives à la mise à jour de la configuration de Ir Led Allowed aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Ip Cam Mode	Envoie les informations relatives à la mise à jour de la configuration de Ip Cam Mode aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Profile	Envoie les informations relatives à la mise à jour de la configuration de Profile aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Video Src	Envoie les informations relatives à la mise à jour de la configuration de Video Src aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Video Src Cfg	Envoie les informations relatives à la mise à jour de la configuration de Video Src Cfg aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Video Src Cfg Options	Envoie les informations relatives à la mise à jour de la configuration de Video Src Cfg Options aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Video Enc Cfg	Envoie les informations relatives à la mise à jour de la configuration de Video Enc Cfg aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Video Enc Cfg Options	Envoie les informations relatives à la mise à jour de la configuration de Video Enc Cfg Options aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Audio Src	Envoie les informations relatives à la mise à jour de la configuration de Audio Src aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Audio Src Cfg	Envoie les informations relatives à la mise à jour de la configuration de Audio Src Cfg aux abonnés/clients externes, limitant ainsi le trafic de données inutile.

Élément	Description
Src Cfg	
Mise à jour de la configuration de Audio Src Cfg Options	Envoie les informations relatives à la mise à jour de la configuration de Audio Src Cfg Options aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Audio Enc Cfg	Envoie les informations relatives à la mise à jour de la configuration de Audio Enc Cfg aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Audio Enc Cfg Options	Envoie les informations relatives à la mise à jour de la configuration de Audio Enc Cfg Options aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Audio Out	Envoie les informations relatives à la mise à jour de la configuration de Audio Out aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Audio Out Cfg	Envoie les informations relatives à la mise à jour de la configuration de Audio Out Cfg aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Audio Out Cfg Options	Envoie les informations relatives à la mise à jour de la configuration de Audio Out Cfg Options aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Audio Dec Cfg	Envoie les informations relatives à la mise à jour de la configuration de Audio Dec Cfg aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Audio Dec Cfg Options	Envoie les informations relatives à la mise à jour de la configuration de Audio Dec Cfg Options aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Metadata Cfg	Envoie les informations relatives à la mise à jour de la configuration de Metadata Cfg aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration des options Metadata Cfg	Envoie les informations relatives à la mise à jour de la configuration des options Metadata Cfg aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Video Analytics Cfg	Envoie les informations relatives à la mise à jour de la configuration de Video Analytics Cfg aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Ptz Cfg	Envoie les informations relatives à la mise à jour de la configuration de Ptz Cfg aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Ptz Cfg Options	Envoie les informations relatives à la mise à jour de la configuration de Ptz Cfg Options aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Scopes	Envoie les informations relatives à la mise à jour de la configuration de Scopes aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Digital Input	Envoie les informations relatives à la mise à jour de la configuration de Digital Input aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Relay	Envoie les informations relatives à la mise à jour de la configuration de Relay Output aux abonnés/clients externes, limitant ainsi le trafic de données inutile.

Élément	Description
Output	
Mise à jour de la configuration de Imaging Settings20	Envoie les informations relatives à la mise à jour de la configuration de Imaging Settings20 aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Imaging Options20	Envoie les informations relatives à la mise à jour de la configuration de Imaging Options20 aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Thermal Cfg	Envoie les informations relatives à la mise à jour de la configuration de Thermal Cfg aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de protocole réseau	Envoie les informations relatives à la mise à jour de la configuration de protocole réseau aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de modèles	Envoie les informations relatives à la mise à jour de la configuration de modèles aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Serial Port Options	Envoie les informations relatives à la mise à jour de la configuration de Serial Port Options aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Serial Port Settings	Envoie les informations relatives à la mise à jour de la configuration de Serial Port Settings aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Video Src Ptz Settings	Envoie les informations relatives à la mise à jour de la configuration de Video Src Ptz Settings aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Preset Tour Options	Envoie les informations relatives à la mise à jour de la configuration de Preset Tour Options pour les mises à jour de configuration aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mise à jour de la configuration de Radiometric Rule Overlay Cfg	Envoie les informations relatives à la mise à jour de la configuration de Radiometric Rule Overlay Cfg aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Configuration enregistrement	Paramètres définissant le mode d'enregistrement de la vidéo/audio (p. ex. : qualité, conservation).
État tâche	État actuel d'une tâche définie, telle qu'une session d'enregistrement.
Configuration de l'enregistrement	(entrée en double) Paramètres pour l'enregistrement.
Configuration piste	Paramètres pour la gestion et l'indexation des segments de données enregistrés (pistes).
Configuration de la tâche d'enregistrement	Configuration détaillée pour une tâche d'enregistrement automatisée.
Supprimer données de piste	Commande permettant de supprimer un segment de données enregistrées.
Créer enregistrement	Commande permettant de lancer un nouveau travail ou une nouvelle session d'enregistrement.
Supprimer enregistrement	Commande permettant de supprimer une tâche d'enregistrement ou les données qui y sont associées.

Élément	Description
Créer piste	Commande permettant de définir ou de démarrer un nouveau segment de piste enregistrée.
Supprimer piste	Commande permettant de supprimer une piste enregistrée spécifique.
Moteur de règles	Composant central traitant les événements et déclenchant les actions correspondantes en fonction de règles définies.
Direction inhabituelle de l'objet	Envoie des événements Direction inhabituelle de l'objet aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Détection de mouvements	Envoie des événements Détection de mouvements aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Vitesse inhabituelle de l'objet	Envoie des événements Vitesse inhabituelle de l'objet aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Emplacement inhabituel de l'objet	Envoie des événements Emplacement inhabituel de l'objet aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Suivi automatique d'objets dans la zone	Envoie des événements Suivi automatique d'objets dans la zone aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Mouvement intelligent	Envoie des événements Mouvement intelligent aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Direction interdite	Envoie des événements Direction interdite aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Arrêt objet	Envoie des événements Arrêt objet aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Objet rôdeur	Envoie des événements Objet rôdeur aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Apparition d'objet	Envoie des événements Apparition d'objet aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Disparition d'objet	Envoie des événements Disparition d'objet aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Franchissement d'objet	Envoie des événements Franchissement d'objet aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Présence d'objets	Envoie des événements de Présence d'objets aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Détecteur de ligne	Envoie des événements Détecteur de ligne aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Franchi	Envoie des événements Franchi aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Sabotage	Envoie des événements Sabotage aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Sortie d'objet	Envoie des événements Sortie d'objet aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Entrée d'objet	Envoie des événements Entrée d'objet aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Détecteur rôdeur	Envoie des événements Détecteur rôdeur aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Objet rôdeur en cours	Envoie des événements Objet rôdeur en cours aux abonnés/clients externes, limitant ainsi le trafic de données inutile.

Élément	Description
Objet absent	Envoie des événements Objet absent aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Détecteur champ	Envoie des événements Détecteur champ aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Objets à l'intérieur	Envoie des événements Objets à l'intérieur aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Filtre IP	Règle définie pour autoriser ou refuser le trafic réseau en fonction de l'adresse IP.
Tentative d'accès non autorisé	Envoie des événements liés aux tentatives d'accès non autorisées aux abonnés/clients externes, limitant ainsi le trafic de données inutile.
Advancedsecurity	Composant général ou paramètres liés aux fonctions de sécurité renforcées.
Keystore	Un référentiel pour les clés de chiffrement et les certificats.
État clé	État actuel d'une clé de chiffrement (p. ex. : active, révoquée, expirée).

Configuration des paramètres SMTP

La page *SMTP* permet aux administrateurs de configurer les paramètres SMTP.

Pour configurer les paramètres SMTP, procédez comme suit :

1. Accédez à *Network & Security > SMTP* dans l'interface Web de la caméra.
2. Entrez Server URL au format suivant : `smtps://smtp.gmail.com:465`, p. ex. : `smtps://server.company.com:465`.
3. Saisissez le Username et le Password.
4. Entrez l'adresse électronique de l'expéditeur, p. ex. : `<utilisateur@exemple.com>`.
5. Cliquez sur **Save**.

Les paramètres du serveur SMTP sont alors modifiés.

Gestion de l'accès au réseau via des filtres IP

La page *IP Filter* permet aux administrateurs de contrôler les adresses IP autorisées à se connecter à votre caméra. Le filtre IP limite l'accès à certaines adresses IP, soit en refusant, soit en restreignant l'accès à certaines adresses IP. Vous pouvez également inclure le refus ou l'autorisation d'accès à des plages d'adresses IP.



IMPORTANT

Si vous choisissez de filtrer l'accès IP à l'aide du Allow access, assurez-vous que vous configurez les adresses correctes pour être autorisées ou vous risquez d'être verrouillé hors de votre caméra.

Les administrateurs peuvent configurer l'authentification basée sur le port 802.1x afin de définir les informations d'identification appropriées pour la caméra, de sorte que le flux vidéo ne soit pas bloqué par le commutateur.

Pour utiliser le filtre IP, procédez comme suit :

1. Accédez à *Network & Security > IP Filter* dans l'interface Web de la caméra.
2. Cliquez sur le bouton **Enable IP filter** pour activer le filtre IP.
3. Sélectionnez l'option **Allow access** pour autoriser l'accès à un nombre limité d'adresses IP.
4. Sélectionnez l'option **Deny access** pour refuser l'accès à un nombre limité d'adresses IP.
5. Dans la zone des entrées du filtre IP, cliquez sur l'icône **+** pour ajouter des adresses IP.
6. Entrez l'adresse IP dans le champ.
7. Continuez à cliquer sur l'icône **+** pour ajouter des adresses IP. Vous pouvez ajouter jusqu'à 256 IP filter entries.
8. Vous pouvez sélectionner l'icône **–** pour supprimer des adresses IP de la liste des entrées.
9. Cliquez sur **Save**.

Restaurer les paramètres par défaut

- Les administrateurs peuvent utiliser l'option **Restore Defaults** si vous devez restaurer les paramètres par défaut. Cliquez sur **Save**.

Configuration de WebRTC

La page *WebRTC* permet aux administrateurs d'activer WebRTC via les serveurs STUN ou TURN. Vous pouvez configurer WebRTC en ajoutant des serveurs STUN ou TURN. En règle générale, on utilise des serveurs STUN, sauf si les adresses IP des clients ou les numéros de port des serveurs sont masqués sur le réseau (pare-feux, p. ex.).

Pour configurer WebRTC, procédez comme suit :

1. Accédez à *Network & Security > WebRTC* dans l'interface Web de la caméra.
2. À partir de la zone *General Settings*, sélectionnez le type de serveur que vous souhaitez utiliser :
 - a. STUN servers : utilise une communication directe entre les clients WebRTC via les adresses IP publiques et de ports.
 - b. TURN servers : fournit une solution de secours en cas d'absence de communication directe.



NOTE

Pour gérer et utiliser des serveurs TURN, vous devez désactiver les connexions HTTP.

3. Si vous utilisez STUN servers, entrez l'adresse du serveur STUN au format : `stun[s] : <host> [ :<port>]`
4. Si vous utilisez TURN servers, entrez l'adresse du serveur STUN au format : `turn[s]: <host> [:<port>] [?transport =<protocol>]`
5. Utilisez le bouton **Add STUN Server** ou **Add TURN Server** pour continuer à ajouter des adresses de serveur.
6. Cliquez sur **Save**.

Le nouveau serveur sera ajouté à la liste.

Suppression de serveurs

- Les administrateurs peuvent supprimer un serveur en sélectionnant l'icône . Cliquez sur **Save**.

Configuration des profils 802.1x

La page *802.1x* permet aux administrateurs de configurer des profils et de gérer les configurations 802.1x enregistrées. Vous pouvez configurer l'authentification basée sur le port 802.1x afin de définir les informations d'identification appropriées pour la caméra, de sorte que le flux vidéo ne soit pas bloqué par le commutateur. Cela permet aux administrateurs de gérer l'accès au flux vidéo.

Pour configurer les profils 802.1x, procédez comme suit :

1. Accédez à *Network & Security > 802.1x* dans l'interface Web de la caméra.
2. Dans la zone *Configurer les profils 802.1X*, cliquez sur la liste déroulante **Protocole** et sélectionnez un autre protocole :
 - a. PEAP : pour l'authentification par nom d'utilisateur et mot de passe.
 - b. EAP-TLS : pour l'authentification par certificat.
3. Si vous avez sélectionné PEAP, renseignez les champs obligatoires :
 - a. Configuration name : donnez un nom au profil.
 - b. Identité : entrez le nom d'utilisateur qui sera utilisé pour authentifier la caméra.
 - c. Password : saisissez le mot de passe qui sera utilisé pour authentifier la caméra.
 - d. Authentifier serveur : cochez cette case si vous devez ajouter un certificat.
4. Si vous avez sélectionné EAP-TLS, renseignez les champs obligatoires :
 - a. Configuration name : donnez un nom au profil.
 - b. Identité : entrez le nom d'utilisateur qui sera utilisé pour authentifier la caméra.
 - c. certTLS : sélectionnez le fichier de certificat codé PEM pour authentifier la caméra.
 - d. Private key : sélectionnez le fichier de clé privée encodé au format PEM pour authentifier la caméra.
 - e. Private key password : si la clé privée est dotée d'un mot de passe, tapez ce mot de passe ici.
5. Cliquez sur **Upload File** et le certificat client TLS et la clé privée sont téléchargés sur la caméra. Les fichiers téléchargés sont utilisés afin de générer un certificat unique capable d'authentifier la caméra. Ce certificat unique s'affiche dans le champ **Uploaded certificate**.
6. Cliquez sur **Save**.

S'il s'agit du premier profil que vous ajoutez à la caméra, il sera automatiquement activé.

Les configurations enregistrées sont répertoriées sous *Saved 802.1X configurations*. Pour basculer entre les profils d'authentification ou les supprimer, voir [Gestion des configurations 802.1x enregistrées en dessous](#).

Gestion des configurations 802.1x enregistrées

Les administrateurs peuvent gérer vos profils d'authentification dans la zone *Configure 802.1X profiles* :

- Pour sélectionner un autre profil d'authentification, sélectionnez la configuration enregistrée, puis cliquez sur **Enable**.
- Pour supprimer l'un des profils d'authentification, sélectionnez la configuration enregistrée puis cliquez sur **Remove**.

Ces modifications seront enregistrées automatiquement.

Changer le Encryption Engine

La page *Encryption Engine* permet aux administrateurs de modifier les méthodes de chiffrement afin d'activer la conformité FIPS ou NXP TPM.

Pour changer le moteur de chiffrement, procédez comme suit :

1. Accédez à *Network & Security > Encryption Engine* dans l'interface Web de la caméra.
2. À partir de la zone *Security*, sélectionnez une option dans la liste déroulante **Encryption Engine** :
 - a. Network : FIPS n'est pas activé. OpenSSL est activé par défaut.
 - b. FIPS 140-2 : FIPS 140-2 est activé.
 - c. FIPS 140-3 : FIPS 140-3 niveau 1 est activé en mettant la bibliothèque OpenSSL en mode FIPS.
 - d. TPM NXP : FIPS 140-2 niveau 3 est activé via le TPM. Pour les caméras plus récentes équipées de FIPS 140-3 TPM, cette option active à la place FIPS 140-3 niveau 3.



NOTE

En cas d'erreur TPM, le message suivant s'affiche : "Erreur sabotage module Trusted Platform". Cette caméra n'est pas fiable. Cycle d'alimentation requis." Vous devez redémarrer la caméra pour résoudre le problème. La caméra peut encore enregistrer des images jusqu'au redémarrage. Voir [System sur la page 77](#) pour obtenir des instructions.

3. Cliquez sur **Save**.



IMPORTANT

La modification de ce paramètre sur votre caméra nécessitera le redémarrage de votre caméra et vous perdrez le flux vidéo pendant cette période. Nous vous recommandons d'appliquer ce paramètre pendant les périodes d'exploitation non sensibles.

Licence FIPS

Pour pouvoir utiliser ces moteurs de chiffrement FIPS, vous devez acheter une licence FIPS :

- FIPS 140-2 de niveau 1
- FIPS 140-2 niveau 3 sur les caméras équipées d'un module TPM intégré
- FIPS 140-3 niveau 3 sur les caméras équipées d'un module TPM intégré

Contactez le représentant commercial à l'adresse Pelco pour obtenir des licences supplémentaires.

Gestion de l'accès aux caméras ou dispositifs via des certificats

La page *Identity & Trust* permet aux administrateurs d'ajouter et de télécharger des certificats, d'afficher des informations ou de télécharger une demande de signature de certificat (CSR = Certificate Signing Request). Certains certificats ne peuvent pas être supprimés, tels que les certificats préchargés fournis avec des bibliothèques tierces ou ceux portant le préfixe "preloaded" de MPI (à l'avenir).

Informations relatives au certificat

La page *Certificates* répertorie tous les certificats présents sur la caméra, accompagnés des informations suivantes :

- Nom : nom du certificat.
- Type : type de certificat, c.-à-d. approuvé ou non.
- Date d'expiration : date d'expiration du certificat.

Ajouter un nouveau certificat

La page *Certificates* permet aux administrateurs de créer de nouveaux certificats pour l'authentification.

Téléchargement d'un certificat auto-signé

Vous pouvez télécharger un certificat auto-signé pour l'authentification.

1. Accédez à *Network & Security > Certificates* dans l'interface Web de la caméra.
2. Cliquez sur **Add new certificate**.
3. Pour créer un certificat auto-signé, cliquez sur **Next**.
 - a. Entrer le nom : nom du certificat. Ce champ est obligatoire.
 - b. Entrer le nom commun : nom de l'hôte principal du serveur. Ce champ est obligatoire.
 - c. Entrer la durée de validité (en années) : nombre d'années de validité du certificat.
 - d. Saisir le pays : pays où se trouve l'organisation.
 - e. État ou province : État (États-Unis) ou province (Canada) associé(e) à l'organisation.
 - f. Entrer la ville ou la localité (si nécessaire) : localisation géographique de l'organisation.
 - g. Entrer le nom de l'organisation (si nécessaire) : nom de l'organisation demandant les certificats.
 - h. Entrer l'unité organisationnelle (si nécessaire) : nom de l'unité au sein de l'organisation demandant les certificats.
 - i. Sélectionner un type de clé : sélectionnez-le dans la liste des types de clés.
4. Cliquez sur **Next**.
5. Si vous souhaitez créer un nouveau chemin de validation en n'utilisant que ce certificat, cochez la case **Oui, créer un nouveau chemin de validation lors de l'enregistrement**.



NOTE

Si vous souhaitez créer un chemin de validation de certificat avec des certificats supplémentaires, passez à la page *Chemin de validation de certificat*. Voir [Chemins de validation des certificats sur la page 36](#) pour obtenir des instructions.

6. Cliquez sur **Save**.

L'activation du nouveau certificat désactivera tous les certificats qui étaient utilisés par le même service.

Téléchargement d'un certificat client-serveur via une demande de signature

Les administrateurs peuvent télécharger un certificat client-serveur à des fins d'authentification.

1. Cliquez sur **Ajouter un nouveau certificat**.
2. Pour créer un certificat auto-signé, cliquez sur **Next**.
3. Pour télécharger un certificat client-serveur créé via une demande de signature, sélectionnez **Télécharger un certificat client-serveur créé via une demande de signature**, puis cliquez sur **Next**.
 - a. Entrer le nom : nom du certificat. Ce champ est obligatoire.
 - b. Entrer le nom commun : nom de l'hôte principal du serveur. Ce champ est obligatoire.
 - c. Entrer la durée de validité (en années) : nombre d'années de validité du certificat.
 - d. Saisir le pays : pays où se trouve l'organisation.
 - e. État ou province : État (États-Unis) ou province (Canada) associé(e) à l'organisation.
 - f. Entrer la ville ou la localité (si nécessaire) : localisation géographique de l'organisation.
 - g. Entrer le nom de l'organisation (si nécessaire) : nom de l'organisation demandant les certificats.
 - h. Entrer l'unité organisationnelle (si nécessaire) : nom de l'unité au sein de l'organisation demandant les certificats.
 - i. Sélectionner un type de clé : sélectionnez-le dans la liste des types de clés.
4. Cliquez sur **Suivant**.
5. Si vous souhaitez créer un nouveau chemin de validation en n'utilisant que ce certificat, cochez la case **Oui, créer un nouveau chemin de validation lors de l'enregistrement**.



NOTE

Si vous souhaitez créer un chemin de validation de certificat avec des certificats supplémentaires, utilisez la page *Chemin de validation de certificat*. Voir [Chemins de validation des certificats sur la page 36](#) pour obtenir des instructions.

6. Cliquez sur **Save**.

L'activation du nouveau certificat désactivera tous les certificats qui étaient utilisés par le même service.

Téléchargement d'un certificat client-serveur via PKCS#12

Les administrateurs peuvent télécharger un certificat client-serveur pour l'authentification via PKCS#12.

1. Cliquez sur **Ajouter un nouveau certificat**.
2. Pour télécharger un certificat client-serveur avec clé privée via PKCS#12, sélectionnez **Télécharger un certificat client-serveur avec clé privée via PKCS#12**, puis cliquez sur **Suivant**.
3. Entrer le nom : nom du certificat. Ce champ est obligatoire.
4. Sélectionnez **Cliquer pour télécharger le fichier de certificat** et choisissez un fichier sur l'ordinateur local.
5. Cliquez sur **Suivant**.
6. Cliquez sur le bouton **Cliquer pour télécharger le fichier de certificat** et sélectionnez le fichier .p12 ou .pfx sur votre ordinateur local.
7. Entrez le mot de passe si nécessaire. Si aucun mot de passe n'est requis, décochez le bouton **Mot de passe**.
8. Cliquez sur **Suivant**.
9. Cliquez sur **Save**.

L'activation du nouveau certificat désactivera tous les certificats qui étaient utilisés par le même service.

Téléchargement d'un certificat client-serveur via PKCS8

Les administrateurs peuvent télécharger un certificat client-serveur pour l'authentification via PKCS8 :

1. Cliquez sur **Ajouter un nouveau certificat**.
2. Pour télécharger un certificat client-serveur avec clé privée via PKCS8, sélectionnez **Télécharger un certificat client-serveur avec clé privée via PKCS8**, puis cliquez sur **Suivant**.
3. Entrer le nom : nom du certificat. Ce champ est obligatoire.
4. Sélectionnez **Cliquer pour télécharger le fichier de certificat** et choisissez un fichier sur l'ordinateur local.
5. Sélectionnez **Cliquez pour télécharger un fichier clé** et choisissez un fichier sur l'ordinateur local.
6. Entrez le mot de passe si nécessaire.
7. Si aucun mot de passe n'est requis, décochez la case **Mot de passe**.
8. Cliquez sur **Suivant**.
9. Cliquez sur le bouton **Cliquer pour télécharger le fichier de certificat** et sélectionnez le fichier .pem, .crt, .cer ou .der sur votre ordinateur local.
10. Cliquez sur le bouton **Cliquer pour télécharger le fichier de clé** et sélectionnez le fichier .key, .pem ou .rsa sur votre ordinateur local.
11. Entrez le mot de passe si nécessaire. Si aucun mot de passe n'est requis, décochez le bouton **Mot de passe**.
12. Cliquez sur **Next**.
13. Cliquez sur **Save**.

L'activation du nouveau certificat désactivera tous les certificats qui étaient utilisés par le même service.

Téléchargement d'un certificat CA

Les administrateurs peuvent télécharger un certificat CA pour l'authentification.

1. Cliquez sur **Ajouter un nouveau certificat**.
2. Pour télécharger un certificat CA, sélectionnez **Certificat CA** et cliquez sur **Next**.
3. Entrer le nom : nom du certificat. Ce champ est obligatoire.
4. Sélectionnez **Cliquer pour télécharger le fichier de certificat** et choisissez un fichier sur l'ordinateur local.
5. Cliquez sur **Next**.
6. Cliquez sur le bouton **Cliquer pour télécharger le fichier de certificat** et sélectionnez le fichier .pem, .crt, .cer ou .der sur votre ordinateur local.
7. Cliquez sur **Next**.
8. Cliquez sur **Save**.

L'activation du nouveau certificat désactivera tous les certificats qui étaient utilisés par le même service.

Téléchargement des demandes de signature de certificat

La page *Identity & Trust* permet aux administrateurs de télécharger des demandes de signature de certificat.

1. Accédez à *Network & Security > Identity & Trust* dans l'interface Web de la caméra.
2. Cliquez sur **Télécharger le CSR** et saisissez les informations suivantes :
 - Nom commun : nom d'hôte principal du serveur. Ce champ est obligatoire.
 - Nom alternatif du sujet (DNS) : valeurs alternatives associées au certificat, telles que l'adresse électronique, les adresses IP, les URI, les noms DNS.
 - Unité organisationnelle : nom de l'unité au sein de l'organisation demandant les certificats.
 - Organisation : nom de l'organisation demandant les certificats.
 - Localité: localité géographique de l'organisation.
 - État ou province : État (États-Unis) ou province (Canada) associé(e) à l'organisation.
 - Pays : pays de l'organisation.
3. Cliquez sur le bouton **Download** pour télécharger la demande de signature de certificat.
4. Cliquez sur **Save**.

La demande de signature de certificat est alors téléchargée sous forme de fichier .CSR.

Chemins de validation des certificats

La page *Chemins de validation des certificats*, permet aux administrateurs d'ajouter de nouveaux chemins et de gérer les chemins enregistrés. Les administrateurs peuvent sélectionner parmi les chemins de validation de certificats enregistrés sur la page *TLS*. Pour plus d'informations, voir [Modification des chemins de validation des certificats sur la page 39](#). Accès à la page *Chemins de validation des certificats* de la page *Identity & Trust*.

Ajoutez les nouveaux chemins de validation de certificats dans l'ordre suivant :

- Placez le certificat racine en premier
- Placez un certificat intermédiaire entre les deux (facultatif)
- Placez l'entité finale en dernier

Ajout d'un nouveau chemin de validation de certificat

Les administrateurs peuvent télécharger un nouveau chemin de validation de certificat.

1. Accédez à *Network > Identity & Trust > Chemins de validation des certificats* dans l'interface Web de la caméra.
2. Cliquez sur **Ajouter un nouveau chemin**.
3. Entrez un nom pour le chemin dans les détails du chemin.
4. Effectuez une recherche dans la liste des certificats disponibles et sélectionnez ceux que vous souhaitez ajouter.
5. Utilisez le bouton **>** pour déplacer les certificats vers la zone *Ordre du chemin d'accès aux certificats*, à droite.
6. Utilisez le bouton **<** pour replacer des certificats dans la zone *Certificats disponibles*, à gauche.
7. Cliquez et faites glisser l'icône **::** pour réorganiser la liste des certificats.
8. Cliquez sur **Save**.

Le nouveau chemin de validation du certificat est ajouté à la liste.

Gestion des chemins de validation des certificats

Les administrateurs peuvent gérer les chemins de validation des certificats via les options de la liste :

- Pour afficher les chemins de validation des certificats, cliquez sur l'icône **:** et sélectionnez **Vue**.
- Pour supprimer un chemin de validation de certificat, cliquez sur l'icône **:** et sélectionnez **Supprimer**.

Les administrateurs ne peuvent pas supprimer de chemin de validation de certificat actuellement utilisé par la caméra.

Ajout et gestion des règles de validation des certificats

La page *Règles de validation des certificats* vous permet d'ajouter de nouvelles règles et de gérer les règles enregistrées. Vous pouvez accéder à l'onglet *Accès* à la page *Chemins de validation des certificats* depuis la page *Identity & Trust*.

Pour ajouter une nouvelle règle, procédez comme suit :

1. Accédez à *Network > Identity & Trust > Règles de validation des certificats* dans l'interface Web de la caméra.
2. Cliquez sur **Ajouter une règle**.
3. Entrez un nom de chemin d'accès dans *Détails règle*.
4. Effectuez une recherche dans la liste des certificats disponibles et sélectionnez ceux que vous souhaitez ajouter.
5. Utilisez le bouton **>** pour déplacer les certificats vers la zone *Certificat sélectionné*, à droite.
6. Utilisez le bouton **<** pour replacer des certificats dans la zone *Certificats disponibles*, à gauche.
7. Cliquez et faites glisser le bouton **::** pour réorganiser la liste des certificats.
8. Cliquez sur **Save**.

La nouvelle règle de validation des certificats est ajoutée à la liste.

Gestion des règles de validation des certificats

Vous pouvez gérer les règles de validation des certificats via les options de la liste :

- Pour afficher une règle de validation des certificats, cliquez sur l'icône : et sélectionnez **Vue**.
- Pour supprimer une règle de validation de certificat, cliquez sur l'icône : et sélectionnez **Supprimer**.

Vous ne pourrez pas supprimer de règle de validation de certificat actuellement utilisée par la caméra.

Configuration des profils 802.1x

La page *802.1x* permet aux administrateurs de configurer des profils et de gérer les configurations 802.1x enregistrées. Vous pouvez configurer l'authentification basée sur le port 802.1x afin de définir les informations d'identification appropriées pour la caméra, de sorte que le flux vidéo ne soit pas bloqué par le commutateur. Cela permet aux administrateurs de gérer l'accès au flux vidéo.

Pour configurer les profils 802.1x, procédez comme suit :

1. Accédez à *Network & Security > 802.1x* dans l'interface Web de la caméra.
2. Dans la zone *Configurer les profils 802.1X*, cliquez sur la liste déroulante **Protocole** et sélectionnez un autre protocole :
 - a. PEAP : pour l'authentification par nom d'utilisateur et mot de passe.
 - b. EAP-TLS : pour l'authentification par certificat.
3. Si vous avez sélectionné PEAP, renseignez les champs obligatoires :
 - a. Configuration name : donnez un nom au profil.
 - b. Identité : entrez le nom d'utilisateur qui sera utilisé pour authentifier la caméra.
 - c. Password : saisissez le mot de passe qui sera utilisé pour authentifier la caméra.
 - d. Authentifier serveur : cochez cette case si vous devez ajouter un certificat.
4. Si vous avez sélectionné EAP-TLS, renseignez les champs obligatoires :
 - a. Configuration name : donnez un nom au profil.
 - b. Identité : entrez le nom d'utilisateur qui sera utilisé pour authentifier la caméra.
 - c. certTLS : sélectionnez le fichier de certificat codé PEM pour authentifier la caméra.
 - d. Private key : sélectionnez le fichier de clé privée encodé au format PEM pour authentifier la caméra.
 - e. Private key password : si la clé privée est dotée d'un mot de passe, tapez ce mot de passe ici.
5. Cliquez sur **Upload File** et le certificat client TLS et la clé privée sont téléchargés sur la caméra. Les fichiers téléchargés sont utilisés afin de générer un certificat unique capable d'authentifier la caméra. Ce certificat unique s'affiche dans le champ **Uploaded certificate**.
6. Cliquez sur **Save**.

S'il s'agit du premier profil que vous ajoutez à la caméra, il sera automatiquement activé.

Les configurations enregistrées sont répertoriées sous *Saved 802.1X configurations*. Pour basculer entre les profils d'authentification ou les supprimer, voir [Gestion des configurations 802.1x enregistrées sur la page suivante](#).

Gestion des configurations 802.1x enregistrées

Les administrateurs peuvent gérer vos profils d'authentification dans la zone *Configure 802.1X profiles* :

- Pour sélectionner un autre profil d'authentification, sélectionnez la configuration enregistrée, puis cliquez sur **Enable**.
- Pour supprimer l'un des profils d'authentification, sélectionnez la configuration enregistrée puis cliquez sur **Remove**.

Ces modifications seront enregistrées automatiquement.

Modification des chemins de validation des certificats

La page *TLS* permet aux administrateurs de sélectionner parmi une liste de chemins de validation de certificats enregistrés.

1. Accédez à *Network > TLS* dans l'interface Web de la caméra.
2. Sélectionnez une configuration Certificate Validation Path enregistrée, dans la liste déroulante.
3. Cliquez sur **Save**.



NOTE

Pour que le chemin de validation du certificat soit apparaisse dans la liste, vous devez le créer dans *Identity & Trust > Certificate Validation Path*. Pour plus d'informations, voir [Chemins de validation des certificats sur la page 36](#).

Authentification unique (SSO)

L'authentification unique (SSO) permet aux administrateurs système de configurer les caméras, afin de n'utiliser qu'un seul jeu d'identifiants pour la connexion. Cela simplifie l'accès en confiant l'authentification des utilisateurs à un fournisseur d'identité externe. La mise en œuvre repose sur un fournisseur d'autorisation conforme à OpenID Connect qui utilise des jetons d'accès JWT et prend en charge une demande de rôles ONVIF.

Compatibilité

La caméra peut être configurée avec la plupart des fournisseurs d'autorisation conformes à OpenID Connect, à condition qu'ils utilisent des jetons d'accès JWT et prennent en charge une demande de rôles ONVIF. Bien que la compatibilité ait été vérifiée avec Keycloak, Ping One, Microsoft Entra ID et Okta, d'autres fournisseurs conformes devraient également être compatibles.

Exigences en matière d'authentification

La configuration initiale du SSO implique des étapes similaires sur toutes les plateformes, bien que certaines étapes spécifiques puissent varier. Les caméras nécessitent ces paramètres pour authentifier les utilisateurs :

1. Enregistrer les caméras en tant qu'applications clientes : la caméra doit être enregistrée en tant qu'application cliente auprès du service d'autorisation tiers.
2. Configurer les paramètres : vous devrez configurer des paramètres tels que l'adresse du serveur d'autorisation, l'ID client, la clé secrète client, le scope, la règle de validation du chemin d'accès au certificat, les audiences, la méthode de vérification de la signature JWT et les revendications personnalisées (facultatif).
3. Validation des jetons : la caméra valide les jetons d'identification et d'accès, en vérifiant leur signature, leur émetteur, leur audience, leur date d'expiration et les éventuelles revendications personnalisées. Pour les jetons d'identification, une valeur "nonce" unique est utilisée afin de prévenir les risques de sécurité tels que les attaques par rejeu.
4. Rôles ONVIF pour l'autorisation : l'autorisation des utilisateurs est gérée en associant l'identité de l'utilisateur à un niveau utilisateur ONVIF (p. ex. : onvif:Administrator, onvif:Operator, onvif:User). Ce mappage s'effectue via une revendication "roles" dans le jeton d'accès. Si cette revendication est manquante ou invalide, l'accès est refusé.

Configuration de l'authentification unique dans l'interface Web de la caméra

Les administrateurs peuvent configurer l'authentification unique (SSO) dans l'interface Web de la caméra avec des fournisseurs d'autorisation OpenID Connect tiers. Les autorisations du compte administrateur sont requises à la fois pour la caméra et pour le fournisseur d'autorisation tiers.

Les étapes de configuration de l'authentification unique pour les caméras dépendent de la configuration et des spécifications d'autorisation des tiers. En général, les caméras doivent être configurées comme des applications clientes avec le service d'autorisation. Les caméras valideront les identifiants et les jetons d'accès, et le jeton d'accès doit prendre en charge les revendications de rôles ONVIF.



IMPORTANT

Pour configurer les paramètres d'authentification unique, vous devez accéder à l'interface Web via HTTPS.

Pour configurer l'authentification unique, procédez comme suit :

1. Accédez à *Network > Authentification unique* dans l'interface Web de la caméra.
2. Si nécessaire, cliquez sur **Rediriger vers HTTPS** et saisissez à nouveau vos identifiants de connexion à la caméra.
3. Dans la zone *Serveur d'autorisation OIDC*, entrez l'adresse du serveur d'autorisation.
4. Dans la zone *Configuration du flux du code d'autorisation*, entrez les paramètres suivants :
 - a. ID client
 - b. Secret client
 - c. Scope
5. Dans la zone *Validation du certificat serveur*, sélectionnez une **Règle de validation du chemin d'accès au certificat** dans la liste déroulante.
6. Dans la zone *Validation JWT*, cliquez sur **Ajouter** pour ajouter les règles requises :

- a. Audiences prises en charge
 - b. Revendications personnalisées
 - c. Valeurs prises en charge
7. Sélectionnez une **méthode de vérification de signature JWT** dans la liste déroulante.
 8. Cliquez sur **Save**.

Une fois ces conditions remplies, vous pouvez revenir à cette section pour terminer la configuration côté caméra.

Image & Display

Les paramètres *Image & Display* vous permettent de modifier les paramètres généraux de l'image, les paramètres Jour/Nuit, les paramètres d'exposition, et d'activer les filtres avancés, tels que le désembuage numérique et la stabilisation de l'image.

Live Preview

La page Live Preview affiche les enregistrements en direct provenant de la caméra. La page Live Preview présente les informations suivantes sur la caméra :

- **Current Exposure** : niveaux d'exposition actuels à la lumière de la caméra, mesurés en millisecondes (ms).
- **Current Iris** : l'ouverture actuelle du diaphragme de la caméra est indiquée par un nombre F (f/#). Le nombre F mesure la distance focale de l'objectif par rapport au diamètre de l'ouverture. Plus le nombre F est petit, plus l'ouverture est grande par rapport à la distance focale, ce qui signifie que davantage de lumière peut pénétrer dans l'objectif.
 - Un petit nombre F signifie que les objets éloignés sont flous tandis que la mise au point reste sur le sujet.
 - Un nombre F élevé signifie une meilleure profondeur de champ, ce qui signifie qu'une plus grande partie de la scène sera mise au point.
- **Current Gain** : le gain actuel de la caméra contrôle l'amplification du signal provenant du capteur de la caméra, mesurée en décibels (dB).
- **Last Known Light Level** : valeur d'exposition (EV) de la caméra à un point culminant récent.



TIP

La zone de mise au point automatique est utilisée pour mettre au point la caméra automatiquement dès que la température fluctue. Assurez-vous que le contraste de la zone d'intérêt est suffisant, autant pendant la journée que pendant la nuit.

Réglage de Image Settings

La page *Image & Display* permet aux administrateurs et aux utilisateurs de régler les paramètres d'image via des options disponibles sous Live Preview. Vous pouvez également déplacer et configurer l'Auto Focus Zone.

Pour régler les paramètres d'image, procédez comme suit :

1. Accédez à *Image & Display* dans l'interface Web de la caméra.
2. Pour zoomer, déplacez le curseur **Zoom** vers la droite.
3. Pour dézoomer, déplacez le curseur **Zoom** vers la gauche.
4. Cliquez sur **Auto Focus** pour que la caméra fasse la mise au point automatiquement.
5. Pour faire la mise au point, déplacez le curseur **Focus** vers la droite ou vers la gauche.

6. Pour utiliser Image Rotation, sélectionnez le menu déroulant **Image Rotation** et sélectionnez une option.
7. Pour utiliser la fonction Temperature Refocus, ACTIVEZ l'option **Enable Temperature Refocus**.
8. Cliquez sur **Save**.

La caméra se réglera en fonction des commandes d'image.

Configuration de Auto Focus Zone

Vous pouvez modifier la forme et l'emplacement de Auto Focus Zone via Live View.

1. Si vous ne voyez pas Auto Focus Zone sur Live View, basculez le bouton Show Auto Focus Zone sur la position **Actif**. Un cadre bleu doit apparaître au milieu de Live View.
2. Pour déplacer Auto Focus Zone, cliquez et faites glisser le cadre bleu.
3. Pour redimensionner Auto Focus Zone, cliquez sur le cadre bleu pour le mettre en surbrillance, puis cliquez et faites glisser ses quatre coins pour en modifier sa forme.
4. Cliquez sur **Save**.

Day/Night Settings

La page *Day/Night Settings* vous permet de configurer le comportement de la caméra lors de la commutation entre les paramètres de jour et de nuit.

Modification du Day / Night mode

Vous pouvez modifier Day / Night mode de la caméra afin de déterminer la manière dont celle-ci commutera entre les paramètres d'image claire et sombre. Cela améliore l'image pour une visibilité 24 heures sur 24.

1. Accédez à *Image & Display > Day/Night Settings* dans l'interface Web de la caméra.
2. Sélectionnez une option dans la liste déroulante *Day / Night mode* :
 - a. **Automatic** : lorsque le niveau de luminosité est supérieur au seuil jour/nuit, l'image vidéo est en couleur. Lorsque le niveau de lumière passe sous le seuil jour/nuit, la caméra ouvre automatiquement le filtre de coupure IR et passe en mode monochrome. Pour les caméras sans IRCF, la caméra commutera simplement en mode monochrome. Si les illuminateurs IR sont activés, ils sont également mis en marche.
Lorsque le paramètre Day / Night mode est défini sur Automatic, vous pouvez utiliser le curseur pour définir le seuil jour/nuit. Déplacez le curseur pour définir le niveau de luminosité lorsque la caméra passe entre le mode jour et le mode nuit. La valeur du curseur est dans Valeurs de l'exposition (EV).
En mode jour, le dernier niveau de luminosité connu s'affiche sous le volet d'image et apparaît également sous la forme d'une barre bleue sur le curseur Seuil Jour/Nuit.
 - b. **Color** : l'image vidéo sera toujours en couleur.
 - c. **Monochrome** : l'image vidéo sera toujours en monochrome.
 - d. **External** : la caméra ouvrira le filtre anti-infrarouge et passera en mode monochrome, selon l'état du circuit d'entrée numérique. Pour les caméras sans IRCF, la caméra commutera simplement en mode monochrome.



NOTE

Vous pouvez définir l'état de circuit d'entrées numériques par défaut, sur la page E/S numérique. Pour plus d'informations, consultez [Digital Inputs and Outputs](#) [Digital Inputs & Outputs](#).

3. Cliquez sur **Save**.

Activation des LED infrarouges

Cette fonction vous permet d'activer ou de désactiver manuellement les projecteurs infrarouges installés sur la caméra.

- Pour activer les LED infrarouges en mode nuit, cliquez sur le bouton **Activation infrarouge**. Cliquez sur **Save**.

Réglage du Seuil Jour/Nuit (EV)

Pour régler le Seuil Jour/Nuit (EV), utilisez le curseur pour augmenter ou diminuer le seuil minimum requis pour que la caméra change de mode. Vous pouvez également saisir une valeur (-8 et 8) dans le champ EV.

- Déplacer le curseur vers la droite diminue le seuil requis pour que la caméra commute vers les paramètres de jour.
- Déplacer le curseur vers la gauche diminue le seuil requis pour que la caméra passe en mode nuit.

Activation de la compensation IR adaptative

L'activation des réglages infrarouges automatiques via la compensation IR adaptative permet à la caméra de régler automatiquement l'image vidéo en fonction de la saturation causée par l'éclairage infrarouge.

- Pour activer la compensation IR adaptative, cliquez sur le bouton **IR adaptatif**. Cliquez sur **Save**.

Activation du contrôle de visibilité nocturne

Le contrôle de visibilité nocturne, lorsqu'il est activé, effectue un test périodique en basculant entre le mode jour / nuit pour vérifier si le niveau de lumière est suffisant pour passer du mode nuit au mode jour. Lorsque cette fonction est désactivée, la caméra utilise une méthode moins optimale pour déterminer si le niveau de luminosité est suffisant pour commuter en mode jour.

- Pour activer le contrôle de visibilité nocturne, cliquez sur le bouton **Contrôle de visibilité nocturne**. Cliquez sur **Save**.



NOTE

La désactivation de la vérification de la visibilité nocturne peut retarder la transition de la caméra entre les modes nuit et jour et rendre le temps de transition moins optimal. Par exemple, la caméra reste en mode nuit 30 minutes de plus que nécessaire.

Réglage de Exposure Settings

La page *Exposure Settings* vous permet de régler les paramètres d'exposition de la caméra, afin d'optimiser la visibilité dans des environnements très lumineux ou très sombres. Vous pouvez trouver *Exposure Settings* en accédant à *Image & Display > Exposure Settings* dans l'interface Web de la caméra.

Utilisation de Flicker Control

Utilisez la fonction Anti-scintillement dans les scènes où l'image de la caméra semble scintiller. Le scintillement est souvent causé par les lumières fluorescentes. Vous pouvez réduire l'effet de scintillement en réglant la fonction Anti-scintillement sur la même fréquence que les lumières. En général, l'Europe est à 50 Hz et l'Amérique du Nord est à 60 Hz.

- Cliquez sur la liste déroulante **Flicker Control** et sélectionnez une fréquence (Hz). Cliquez sur **Save**.

La caméra commencera à utiliser la nouvelle fréquence.

Modification de l'exposition

L'exposition détermine la quantité de lumière qui atteint le capteur de la caméra. L'exposition est réglée par défaut sur Automatique, ce qui permet à la caméra de contrôler l'exposition. Vous pouvez modifier le temps d'exposition afin de laisser entrer davantage de lumière dans le capteur de la caméra, et d'éclaircir ainsi l'image. Vous pouvez également réduire l'exposition pour assombrir l'image. L'augmentation manuelle de la durée d'exposition peut affecter le débit d'image.

- Cliquez sur la liste déroulante **Exposure** et sélectionnez une valeur (en millisecondes). Cliquez sur **Save**.

La caméra règle alors le capteur selon le nouveau niveau d'exposition.

Réglage d'un niveau d'exposition maximal

L'exposition maximale limite l'exposition lorsque la caméra est sur Automatique. Dans des conditions de faible luminosité, réglez un niveau d'exposition maximal afin de pouvoir contrôler manuellement le temps d'exposition de la caméra sans générer d'images floues.

La liste déroulante Exposition maximale n'est disponible que lorsque le paramètre Exposition est sur Automatique.

- Cliquez sur la liste déroulante **Maximum Exposure** et sélectionnez une valeur (en millisecondes). Cliquez sur **Save**.

La caméra appliquera le réglage d'exposition maximal afin d'éviter les images floues.

Réglage du gain maximal

L'option Gain maximal restreint le paramètre de gain automatique avec un niveau de gain maximal. Dans des conditions de faible luminosité, appliquez un gain maximal, afin d'optimiser les détails sans créer de bruit excessif dans les images.

- Cliquez sur la liste déroulante **Maximum Gain** et sélectionnez un niveau de gain maximal (en millisecondes). Cliquez sur **Save**.

La caméra appliquera le paramètre de gain maximal afin d'éviter un bruit numérique excessif dans l'image.

Modification du Priority

La fonction Priorité vous permet de donner la priorité au débit d'images ou à l'exposition. Lorsque la priorité est sur Débit d'images, la caméra maintient le débit d'images défini comme priorité et ne règle pas l'exposition au-delà de ce qui peut être enregistré pour le débit d'images défini. Lorsque la priorité est sur Exposition, la caméra conserve le réglage d'exposition comme priorité, en ignorant le débit d'images défini, afin d'obtenir la meilleure image possible.

- Cliquez sur la liste déroulante **Priority** et sélectionnez soit Débit d'images, soit Exposition. Cliquez sur **Save**.

La caméra appliquera la priorité de l'option sélectionnée, soit Débit d'images, soit Exposition.

Passage au mode Diaphragme

Le mode Iris détermine le mode de commande du diaphragme de la caméra. Vous pouvez autoriser la caméra à contrôler le diaphragme en sélectionnant l'option Auto. Si vous souhaitez contrôler manuellement le diaphragme, sélectionnez Ouvert ou Fermé.

- Si vous souhaitez que la caméra contrôle le diaphragme pendant que vous contrôlez d'autres paramètres, sélectionnez **Auto**.
- Si vous souhaitez ouvrir le diaphragme, afin de pouvoir le fermer manuellement, sélectionnez **Ouvert**.
- Si vous souhaitez fermer le diaphragme afin de pouvoir l'ouvrir manuellement, sélectionnez **Fermer**.

Utilisation de WDR

La fonction WDR (Wide Dynamic Range) permet à la caméra de régler l'image vidéo afin de s'adapter aux scènes où la lumière vive et les ombres sombres sont clairement visibles.

- Cliquez sur le bouton **WDR** pour l'activer. Cliquez sur **Save**.

La caméra commencera alors à utiliser la fonction WDR.

Utilisation de Backlight Compensation Mode

La compensation de contre-jour permet d'éclaircir les zones sombres lorsqu'il y a un fort éclairage en arrière-plan, par exemple une grande fenêtre à l'arrière-plan. Vous pouvez activer la compensation de contre-jour pour éclaircir les zones sombres et obtenir une image bien exposée.

- Cliquez sur le bouton **Backlight Compensation Mode** pour l'activer. Cliquez sur **Save**.

La caméra commencera à utiliser la compensation de contre-jour.

Utilisation de Priorité diaphragme

Le mode Priorité diaphragme vous permet de contrôler manuellement l'ouverture de la caméra (diaphragme) pour un réglage fixe. Cela signifie que vous déterminez le degré d'ouverture ou de fermeture du diaphragme de l'objectif, ce qui a un impact direct sur la profondeur de champ. Lorsque l'ouverture reste constante, la caméra règle automatiquement la vitesse d'obturation et le gain afin de maintenir une exposition correcte.

Les fonctions telles que WDR (Wide Dynamic Range) et Compensation du contre-jour ne sont pas disponibles lorsque le mode Priorité diaphragme est activé.

- Cliquez sur le bouton **Priorité diaphragme** pour l'activer. Cliquez sur **Save**.

Si vous essayez d'activer le mode Priorité diaphragme via un appel ONVIF tout en activant simultanément le WDR, l'exposition automatique ou la compensation de contre-jour, ces derniers paramètres seront prioritaires et le mode Priorité diaphragme sera ignoré.

Advanced Filters

La page *Advanced Filters* permet d'activer les fonctions de désembuage numérique et de stabilisation de l'image, afin d'améliorer la visibilité. Vous pouvez trouver *Advanced Filters* en accédant à *Image & Display* > *Advanced Filters* dans l'interface Web de la caméra.

Désembuage numérique

Si la caméra est installée dans un environnement brumeux, vous pouvez utiliser la fonction Désembuage numérique pour augmenter le contraste vidéo, afin de rendre les objets plus visibles dans la scène.

1. Cliquez sur le bouton **Activer désembuage numérique** pour activer le désembuage numérique.
2. Dans la liste déroulante **Niveau de désembuage**, sélectionnez l'une des options disponibles : Faible, Moyen, Élevé.
3. Cliquez sur **Save**.

La caméra appliquera la fonction de désembuage pour rendre les images floues plus nettes.

Stabilisation électronique de l'image (EIS = Electronic Image Stabilization)

Si la caméra est montée sur mât ou toute autre surface susceptible de trembler ou de vibrer, vous pouvez utiliser la stabilisation de l'image. La fonction de stabilisation de l'image intégrée à la caméra permet de compenser les mouvements, améliorant ainsi l'enregistrement.

- Cliquez sur le bouton **Stabilisation de l'image** pour activer la stabilisation de l'image. Cliquez sur **Save**.

La caméra appliquera une stabilisation de l'image, afin de compenser les mouvements du dispositif.

Adjustment

La zone *Adjustment* vous permet de régler les paramètres de l'image afin de l'ajuster et d'optimiser la visibilité. Vous pouvez trouver la zone Adjustment en accédant à *Image & Display* > *Adjustment* dans l'interface Web de la caméra.

Image Rotation

Image Rotation fait pivoter l'image de la caméra lorsque celle-ci est installée à l'envers ou sur le côté.

- Pour utiliser Image Rotation, sélectionnez le menu déroulant **Image Rotation** et choisissez une option. Cliquez sur **Save**.

Vous pouvez faire pivoter l'image de 90°, 180° et 270°.

Réglage de base Image Settings

La zone *Basic Settings* vous permet de contrôler les paramètres d'image de la caméra.

1. Utilisez les curseurs pour régler les paramètres suivants :
 - a. Sharpness : augmenter la netteté permet de clarifier les détails fins.
Le réglage de la netteté rend l'image floue au début. Refaites la mise au point de la caméra après avoir réglé la netteté.
 - b. Saturation : augmenter la saturation renforce l'intensité des couleurs. Réduire la saturation diminue l'intensité.
 - c. Contrast : augmenter le contraste permet de mettre en valeur certains aspects de l'image. Réduire le contraste permet d'adoucir l'image. Le niveau de contraste approprié dépend des sujets que vous souhaitez voir clairement, ainsi que des paramètres.
 - d. Brightness : augmenter la luminosité permet de faciliter la visualisation des scènes sombres. Si l'augmentation de la luminosité rend les zones sombres plus difficiles à voir, en raison d'un fort contre-jour par exemple, vous pouvez utiliser à la place l'option Backlight Compensation Mode. Voir [Réglage de Exposure Settings sur la page 45](#) pour obtenir des instructions.
2. Cliquez sur **Save**.

Zoom & Focus

La zone *Zoom & Focus* vous permet de zoomer et de faire la mise au point de la caméra.

1. Pour zoomer, déplacez le curseur **Zoom** vers la droite.
2. Pour dézoomer, déplacez le curseur **Zoom** vers la gauche.
3. Cliquez sur **Auto Focus** pour que la caméra fasse la mise au point automatiquement.
4. Pour faire la mise au point, déplacez le curseur **Focus** vers la droite ou vers la gauche.
5. Cliquez sur **Save**.

White Balance

La zone *White Balance* vous permet d'affecter un mode de White Balance afin de compenser la décoloration de l'image. Par exemple, les lumières fluorescentes peuvent donner une teinte verte à la scène. La balance des blancs corrige cet effet et rend les objets dans le champ de visibilité tels qu'ils apparaissent normalement.

1. Cliquez sur la liste déroulante *White Balance* et sélectionnez l'un des modes suivants :
 - a. Automatic : permet à la caméra de contrôler automatiquement les canaux de couleur rouge, vert et bleu afin de neutraliser la dominante de couleur et d'obtenir un blanc plus précis.
 - b. Manual : permet de régler manuellement les niveaux de rouge et de bleu.
2. Vous pouvez cocher la case Dominant Color Compensation si elle est disponible. Sélectionnez cette option lorsque la scène contient une grande zone monochrome dans le champ de visibilité. Par exemple, une grande zone de pelouse contient beaucoup de vert.
3. Si vous avez sélectionné Manual comme mode White Balance, utilisez les curseurs de rouge et de bleu pour compenser manuellement la décoloration de l'image.
4. Cliquez sur **Save**.

Temporal Filter Strength

Temporal Filter Strength réduit le bruit numérique, en calculant la moyenne du bruit sur plusieurs images. Cela peut réduire le flou et diminuer l'utilisation de la bande passante.



TIP

Commencez par effectuer de légers réglages, car toute modification radicale est susceptible de dégrader la qualité d'image globale.

- Déplacez le curseur Temporal Filter Strength vers la droite pour réduire le bruit visuel dans la scène.
- Déplacez le curseur Temporal Filter Strength vers la gauche pour réduire le filtre de force temporelle. Cela permet de restaurer la qualité d'image lorsque l'intensité du filtre est trop élevée, mais réintroduit du bruit visuel dans l'image.

Overlays

La page *Overlays* vous permet d'ajouter et de personnaliser des superpositions et d'activer ou désactiver l'affichage du réticule.

Qu'est-ce que Overlays ?

Overlays sont des textes ou des symboles qui s'affichent directement sur le flux vidéo en direct de la caméra. Ils sont utilisés pour ajouter des informations utiles aux enregistrements, telles que la date et l'heure. Une caractéristique importante est que lorsque vous téléchargez des images fixes depuis la caméra, les fichiers d'image obtenus incluent les informations superposées affichées.

Ajouter Overlays

La page *Overlays* vous permet de créer et configurer plusieurs types de superposition en même temps.

1. Accédez à *Image & Display > Overlays* dans l'interface Web de la caméra.
2. Cliquez sur **Add new Overlay**.
3. Sélectionnez le menu déroulant **Location** et choisissez un emplacement de l'écran où la superposition doit apparaître.
4. Sélectionnez le menu déroulant **Overlay Type** et choisissez une ou plusieurs options :
 - a. Custom Text : ajoutez un champ de texte et saisissez le texte à afficher.
 - b. Date : ajoutez la date.
 - c. Time : ajoutez l'heure.
 - d. Camera Name : ajoutez le nom de la caméra. Le nom de la caméra est défini dans la page Général, sous Paramètres.
 - e. Location : ajoutez l'emplacement.
 - f. Compass : ajoutez la superposition de la boussole. Voir [Étalonnage de PTZ CompassPTZ Compass](#) pour connaître les étapes supplémentaires.
 - g. PTZ Preset Name : ajoutez le nom du paramètre prédéfini PTZ à la superposition. Le texte apparaît à l'écran dès l'exécution du paramètre prédéfini PTZ.

- h. Nom de la zone PTZ : ajoutez le nom de la zone PTZ à la superposition. Le texte apparaît à l'écran dès l'apparition du nom de la zone dans le champ de visibilité de la caméra PTZ.
 - i. Position PTZ : ajoutez le nom de la position PTZ à la superposition. La superposition de la position PTZ affiche des informations de position en temps réel. Cela signifie qu'elle est toujours présente et affiche les données de panoramique, d'inclinaison et de zoom.
- 5. Si vous choisissez Custom Text, entrez le texte dans le champ **Overlay Text**. La limite est de 64 caractères en texte brut.
- 6. Si vous choisissez Date, vous pouvez sélectionner un autre format de date dans le menu déroulant **Date Format**.
- 7. Si vous choisissez Time, vous pouvez sélectionner un autre format d'heure dans le menu déroulant **Time Format**.
- 8. Pour modifier Font size, modifiez la valeur de la police (entre 12 et 80 pt) dans le champ **Font size**. La taille de police par défaut est de 24.
- 9. Pour modifier Text Color, sélectionnez le menu déroulant **Text Color** et choisissez une autre couleur.
- 10. Pour modifier Background Color, sélectionnez le menu déroulant **Background Color** et choisissez une autre couleur.
- 11. Cliquez sur **Save**.

La superposition apparaît sur l'écran d'aperçu en direct.

Compression & Image Rate

Les paramètres *Compression & Image Rate* vous permettent de modifier les paramètres de compression et de qualité d'image de la caméra.

Considérations relatives à la configuration des paramètres Compression & Image Rate

- Qualité d'image vs bande passante : la modification des paramètres de fréquence d'images et de taux de compression pour améliorer la qualité d'image est susceptible d'augmenter l'utilisation de la bande passante. En règle générale, les paramètres améliorant la qualité d'image augmentent l'utilisation de la bande passante, en raison de l'augmentation de la taille des fichiers. L'objectif est d'optimiser la qualité d'image sans provoquer de congestion du réseau.
- Analyse vidéo par auto-apprentissage : la mise à jour des paramètres de débit d'images et de taux de compression peut entraîner la réinitialisation automatique de la progression de Self Learning.

Configuration des paramètres Compression & Image Rate

La page Compression & Image Rate vous permet de configurer les paramètres de streaming de la caméra afin d'optimiser la qualité vidéo en fonction des contraintes réseau. La caméra règle automatiquement la qualité de compression afin de respecter la limite de bande passante spécifiée.

Les caméras peuvent avoir des flux principaux, secondaires, tertiaires et quaternaires. Certains modèles de caméras ne disposent pas de flux quaternaires. Se référer aux [Fiches techniques des caméras Pelco](#) pour connaître les spécifications de votre caméra.

Pour configurer un flux vidéo, sélectionnez le flux et modifiez les paramètres suivants :

1. Dans la liste déroulante **Compression Standard**, sélectionnez le format de streaming préféré pour compresser les fichiers vidéo.
Si vous utilisez le stockage intégré, veillez à sélectionner **H.264**.



NOTE

Le changement de format de streaming vers H.264 ou H.265 n'affectera que les enregistrements du VMS. Vous ne verrez aucune différence dans Live Preview de l'interface Web de la caméra.

2. Pour les caméras prenant en charge Rate control, sélectionnez l'une des options suivantes dans la liste déroulante :
 - a. CVBR : utilise le VBR pour régler le débit binaire en fonction de la complexité de la scène.
 - b. CBR : utilise un débit binaire fixe pour produire des fichiers vidéo plus petits.
3. Sélectionnez la liste déroulante **Resolution**, puis sélectionnez la résolution de l'image.
4. Sélectionnez la liste déroulante **Frame rate**, puis sélectionnez la fréquence d'image. Choisissez une valeur comprise entre 1 et 30 secondes. Ceci détermine le nombre d'images par seconde pour le streaming de la caméra sur le réseau. La fréquence d'image par défaut est de 30.

5. Dans la liste déroulante **Quality**, sélectionnez la qualité d'image souhaitée. Régler la qualité d'image sur 1 produira une vidéo de la plus haute qualité, mais nécessitera la plus grande bande passante.
6. Dans le champ **Max Bitrate**, saisissez la bande passante maximale que la caméra peut utiliser. Vous pouvez entrer n'importe quel nombre compris entre 200 et 12000 kbps.
7. Dans le champ **Keyframe Interval**, saisissez le nombre de trames présentes entre chaque image clé. Vous pouvez entrer n'importe quel nombre compris entre 2 et 64.
8. Pour configurer les paramètres de multidiffusion, voir [Configuration des paramètres de multidiffusion pour la vidéo en dessous](#).
9. Vous pouvez vérifier les URL de diffusion RTSP ou les URI d'images fixes sur la page Compression & Image Rate, mais vous ne pouvez pas modifier ces valeurs. Pour utiliser l'URI de flux RTSP afin de visionner le flux vidéo de la caméra, voir [Affichage de la transmission directe via l'URI de flux RTSP sur la page 54](#).
10. Cliquez sur **Save**.

Cela applique les paramètres de fréquence d'image et de taux de compression au flux de la caméra.

Vous pouvez configurer ces paramètres individuellement pour les flux principaux, secondaires, tertiaires et quaternaires, s'ils sont disponibles. Voir [Activation du flux quaternaire recadré sur la page suivante](#) pour accéder au flux quaternaire.

Configuration des paramètres de multidiffusion pour la vidéo

Pour configurer le comportement Multicast pour le flux de la caméra, procédez comme suit :

1. Pour configurer Multicast, entrez les informations requises dans les champs suivants :
 - a. Address : entrez l'adresse du serveur.
 - b. Port : entrez le numéro de port du serveur (1024...65534). N'accepte que les valeurs paires.
 - c. Time to live : entrez le nombre de secondes (1-255).
2. Cliquez sur **Save**.

La caméra transmet le flux vidéo au serveur spécifié ci-dessus et les images de la caméra sont alors visibles sur le(s) client(s) connecté(s) à ce serveur, via le numéro de port spécifié.

Si vous souhaitez configurer le streaming en multidiffusion pour l'audio, voir [Configuration des paramètres Multicast pour l'audio sur la page 86](#).

Activation de la résolution maximale du flux secondaire

La page Compression & Image Rate vous permet d'activer la résolution maximale du flux secondaire.

- Cochez la case **Activer la résolution maximale du flux secondaire** pour l'activer. Cliquez sur **Save**.

La caméra va redémarrer.

Le flux secondaire de la caméra utilisera la fréquence d'image maximale prise en charge par la caméra. La fréquence d'image maximale dépend du modèle de caméra.

Activation du flux quaternaire recadré

La page Compression & Image Rate vous permet d'activer Quaternary Stream de la caméra. Cela vous permet de générer un quatrième flux vidéo spécialisé (le flux quaternaire) à partir de la sortie de votre caméra. Ce flux est recadré, ce qui signifie qu'il se concentre sur une zone spécifique plus petite de l'image vidéo originale à pleine résolution.

Pourquoi activer le flux quaternaire recadré ?

- Amélioration des détails : en se concentrant sur une zone d'intérêt (ROI) plus petite, la caméra peut allouer davantage de puissance de traitement et de bande passante à cette zone spécifique. Cela vous permet de transmettre un flux recadré avec une résolution effective plus élevée ou des détails plus fins que le flux en plein écran, en particulier lors d'un zoom numérique.
- Réduction de la bande passante et du stockage : le flux recadré contient beaucoup moins de données pixel que le flux en pleine résolution. Cela permet d'enregistrer ou de visionner le quatrième flux en utilisant moins de bande passante et en consommant moins d'espace de stockage, ce qui est très avantageux pour la surveillance à distance ou pour économiser des ressources lorsqu'une petite zone seulement nécessite une vision continue et très détaillée.
- Confidentialité : bien que le masquage de confidentialité soit une option, un flux recadré peut remplir une fonction similaire en ne réalisant que la diffusion en direct de la zone nécessaire, excluant ainsi efficacement tout contenu dispositif sensible de la transmission ou de l'enregistrement sur ce flux particulier.

Le flux quaternaire recadré n'est disponible que sur les caméras prenant en charge un quatrième flux. Cependant, les paramètres du flux quaternaire sont masqués jusqu'à ce que vous activiez le flux quaternaire recadré.

1. Accédez à la page Compression & Image Rate.
2. Cochez la case **Activer le flux quaternaire recadré** pour l'activer.
3. Cliquez sur **Save**.

La caméra redémarrera et vous devrez vous reconnecter.

Sélectionnez la page **quaternaire** pour accéder aux paramètres de flux quaternaire. Vous pouvez régler ces paramètres de la même manière que pour les flux principal, secondaire et tertiaire. Voir [Configuration des paramètres Compression & Image Rate sur la page 51](#) pour obtenir des instructions.

Paramètres avancés de Compression & Image Rate

La page *Advanced* vous permet de configurer des paramètres plus avancés pour la diffusion en direct et le Débit d'image, tels que Smart Codec et Mode Scène inactive. En modifiant le comportement de la diffusion en direct pendant les périodes de faible activité, ces paramètres permettent de réduire l'utilisation de la bande passante.

Utilisation de HDSM SmartCodec

Vous pouvez activer et configurer les paramètres de HDSM SmartCodec à la page Configuration vidéo. HDSM SmartCodec permet d'isoler les objets des zones d'arrière-plan. Cela réduit l'utilisation de la bande passante de la caméra en se concentrant sur les sujets d'intérêt.

HDSM SmartCodec est désactivée par défaut.

1. À partir de la zone *HDSM SmartCodec* cliquez sur le bouton **HDSM SmartCodec** pour l'activer.
2. Cliquez sur **Save**.

L'activation de HDSM SmartCodec activera Mode Scène inactive. Voir [Utilisation de Mode Scène inactive en dessous](#) pour obtenir des instructions.

Désactivation de Mode Scène inactive

Si vous souhaitez continuer à utiliser HDSM SmartCodec sans Mode Scène inactive, vous pouvez le désactiver.

- Re-cliquez sur le bouton **Mode Scène inactive** pour désactiver cette fonction.

Utilisation de Mode Scène inactive

Après avoir activé HDSM SmartCodec Mode Scène inactive, le mode Scène inactive s'active automatiquement. Le mode Scène inactive économise la bande passante en réduisant les fonctions d'analyse pendant les périodes d'inactivité. Vous pouvez configurer Mode Scène inactive pour définir les normes de qualité d'image en l'absence d'activité dans la scène.

1. Dans la zone Scènes immobiles, vous pouvez configurer les paramètres suivants :
 - a. Min Image Rate : fréquence d'image d'encodage (images par seconde) en l'absence de mouvement dans la scène.
 - b. Keyframe Interval : nombre d'images entre chaque image clé en l'absence de mouvement dans la scène (entre 1 et 254 images).
 - c. Post Motion Delay : délai (en secondes) après la fin du mouvement avant que la caméra passe en mode veille (entre 5 et 60).
 - d. Quality : qualité de compression en l'absence de mouvement dans la scène (entre 6 et 20).
 - e. Max Bitrate : nombre maximal de kilo-octets par seconde en l'absence de mouvement dans la scène.
2. Cliquez sur **Save**.

Affichage de la transmission directe via l'URI de flux RTSP

Vous pouvez visionner la transmission directe du flux vidéo de la caméra à partir de n'importe quelle application prenant en charge les diffusions RTSP, y compris les lecteurs vidéo, en utilisant l'adresse RTSP (Real Time Streaming Protocol = Protocole de streaming en temps réel).

1. Pour visionner la transmission directe du flux vidéo de la caméra à partir d'un lecteur vidéo externe, cliquez sur le bouton **Générer l'URI de flux RTSP**. Si ce bouton n'est pas disponible, l'URI est généré automatiquement.
2. Dans la zone URI de flux RTSP, l'adresse générée s'affiche en bas de la section. Si les URI sont générés automatiquement, ils s'affichent également ici.
3. Sélectionnez Unicast si vous prévoyez de visionner le flux vidéo à partir d'un seul lecteur vidéo à la fois.
4. Sélectionnez Multicast si vous prévoyez de visionner la vidéo à partir de plusieurs lecteurs vidéo simultanément.

5. Copiez et collez l'adresse générée dans votre lecteur vidéo. N'ouvrez PAS le flux vidéo en direct pour le moment.
6. Ajoutez votre nom d'utilisateur et votre mot de passe au début de l'adresse au format suivant :
rtsp://<nom d'utilisateur>:<mot de passe>@<URI de flux RTSP générée>/.
Exemple : rtsp://admin:admin@192.168.1.79/defaultPrimary?streamType=u.
7. Ouvrez le flux vidéo en direct.

La transmission directe montrera le flux vidéo en direct de la caméra.

Streaming Settings

La page *Streaming Settings* vous permet de définir le profil multimédia ONVIF et de configurer les paramètres du profil.

1. Sélectionnez un profil média ONVIF dans le menu déroulant **Profiles**.
2. Sélectionnez un profil dans le menu déroulant **Video Source**.
3. Sélectionnez un profil dans le menu déroulant **Audio Source**.
4. Pour activer les métadonnées, sélectionnez métadonnées0 dans le menu déroulant **Metadata**.
5. Pour désactiver les métadonnées, sélectionnez Aucune dans le menu déroulant **Metadata**.
6. Sélectionnez un profil dans le menu déroulant **Video Encoder**.
7. Cliquez sur **Save**.

Analytics

Les paramètres *Analytics* vous permettent de créer et gérer des événements d'analyse.

Motion Detection

La page *Motion Detection* vous permet de configurer Motion Detection en deux étapes : définir d'abord les zones de détection de mouvements, puis régler les niveaux de sensibilité et de seuil. La sensibilité détermine l'ampleur du changement que chaque pixel doit subir avant que l'analyse ne détecte un mouvement.

Pour configurer la détection de mouvements, procédez comme suit :

1. Pour ajouter des zones Motion Detection :
 - a. Assurez-vous que l'option **Sélectionner la zone** est sélectionnée.
 - b. Cliquez sur une zone de Live Preview et faites glisser votre curseur pour générer un carré vert. Ce carré vert est une zone de détection de mouvements. Tout mouvement dans cette zone déclenchera un événement.
 - c. Continuez à cliquer et à faire glisser votre curseur pour générer des zones de détection de mouvements.
 - d. Si vous souhaitez recommencer, vous pouvez cliquer sur **Sélectionner tout** pour restaurer les zones de détection de mouvements.
2. Pour supprimer des zones dans les zones Motion Detection :
 - a. Sélectionnez l'option **Supprimer zone**.
 - b. Cliquez sur une zone de Live Preview où vous voyez des carrés verts, puis faites glisser votre curseur pour supprimer la zone. Cela génère un trou dans la zone Motion Detection. Les mouvements dans la zone supprimée ne déclencheront pas d'événement.
 - c. Continuez à cliquer et à faire glisser votre curseur pour désactiver les zones où vous ne souhaitez pas que le mouvement soit un déclencheur d'événement.
 - d. Si vous souhaitez recommencer, vous pouvez cliquer sur **Supprimer toutes les zones** pour supprimer les zones de détection de mouvements.
3. Pour configurer Sensitivity :
 - a. Cliquez sur **Sensitivity** et faites glisser le curseur pour augmenter Sensitivity(0-100). Plus la valeur de Sensitivity est élevée, plus la quantité de pixels à modifier avant que le mouvement ne soit détecté est faible. Sensitivity détermine le nombre de pixels qui doivent changer avant que l'image ne soit considérée comme ayant un mouvement. La valeur par défaut est 50.
4. Pour configurer Threshold :
 - a. Cliquez sur **Threshold** et faites glisser le curseur pour augmenter le seuil (0-100). Plus le seuil est élevé, plus le nombre de pixels devant changer avant que l'image ne soit considérée comme étant en mouvement est élevé. La valeur par défaut est 20.
5. Vous pouvez activer l'option **Afficher le mouvement dans la vidéo** pour afficher le mouvement dans Live Preview.
6. Cliquez sur **Save**.

7. Si vous souhaitez tester l'événement, cliquez sur le bouton ►**Test** situé en haut à droite de l'écran. Cela enverra un événement "Test" au système de gestion vidéo VMS (Video Management System). Accédez au VMS pour vérifier que l'événement a bien été reçu.

L'événement d'analyse est alors enregistré et la caméra déclenche un événement dès que l'activité est détectée dans la ou les zones d'intérêt. Pour obtenir des instructions sur la modification de la zone d'inclusion, voir [Modification de la zone d'inclusion sur la page 61](#).

Activation de l'événement d'alarme de mouvement ONVIF

Activez les événements d'alarme de mouvement ONVIF afin que la caméra puisse envoyer des événements ONVIF. De nombreux systèmes de gestion vidéo tiers nécessitent le protocole ONVIF pour traiter les événements.

- Cliquez sur **Activer alarme de mouvement ONVIF** pour activer le protocole d'événement d'alarme de mouvement ONVIF.

La caméra se met alors à envoyer des événements d'alarme de mouvement ONVIF.

Sabotage Detection

Les paramètres Sabotage Detection vous permettent de créer et de modifier des événements Sabotage Detection.

Sabotage Detection détecte le vandalisme humain, en détectant les mouvements brusques ou les secousses latérales caractéristiques du vandalisme humain. L'activation de Sabotage Detection permet au système de transmettre les notifications d'événements à un système intégré et d'envoyer des alarmes aux utilisateurs.

Configuration de Classified Object Motion Detection

La fonction Détection de mouvement des objets classifiés analyse les enregistrements vidéo, mais ne signale que les mouvements de véhicules ou de personnes. Cette option n'est disponible que pour les dispositifs d'analyse vidéo par auto-apprentissage Avigilon. L'événement Détection de mouvement des objets classifiés est répertorié sur la page *Événements* de la page Analyse. Le nom par défaut est Règle de mouvement intelligente. Vous ne pouvez pas modifier le nom de cette règle.

Pour modifier l'événement Détection de mouvement des objets classifiés, procédez comme suit :

1. Accédez à *Analytics* dans l'interface Web de la caméra.
2. Cliquez sur l'icône ✎ en regard de Classified Object Motion Detection pour modifier l'événement.
3. Sélectionnez Object types que vous souhaitez détecter dans l'analyse :
 - a. Personne
 - b. Véhicule
4. Si vous avez sélectionné Personne dans Object types, vous pouvez choisir la Person settings à surveiller :
 - a. Hard Hat : détecte la présence ou l'absence d'une personne portant un casque de sécurité.
 - b. High-visibility Vest : détecte la présence ou l'absence d'une personne portant un gilet haute visibilité.

5. Si vous avez sélectionné Véhicule dans Object types, vous pouvez sélectionner le Vehicle settings à surveiller :
 - a. Bicycle
 - b. Car
 - c. Motorcycle
 - d. Bus
 - e. Large Truck
 - f. Pickup Truck
 - g. Van
6. Cliquez et faites glisser le curseur **Sensitivity** pour régler le niveau de Sensibilité. L'abaissement de la sensibilité augmente les risques de faux négatifs.
7. Pour configurer **No. of objects**, entrez le nombre d'objets requis pour détecter une alarme.
8. Pour configurer **Threshold Time**, entrez la durée minimale requise avant que l'événement ne se déclenche.
9. Cliquez sur **Save**.
10. Si vous souhaitez tester l'événement, cliquez sur le bouton ►**Test** situé en haut à droite de l'écran. Cela enverra un événement "Test" au système de gestion vidéo VMS (Video Management System). Accédez au VMS pour vérifier que l'événement a bien été reçu.

L'événement d'analyse est alors enregistré et la caméra déclenche un événement dès que l'activité est détectée dans la ou les zones d'intérêt. Pour obtenir des instructions sur la modification de la zone d'inclusion, voir [Modification de la zone d'inclusion sur la page 61](#).

Création d'événements d'analyse de mouvement

La page *Analytics* permet aux administrateurs et aux utilisateurs de créer, modifier et tester des événements d'analyse de mouvement.

Pour créer un nouvel événement d'analyse, procédez comme suit :

1. Accédez à *Analytics* dans l'interface Web de la caméra.
2. Cliquez sur **Add Event** pour ajouter un événement d'analyse de mouvement.
3. Entrez un nom pour l'événement d'analyse. Le nom de l'événement apparaîtra dans le VMS lorsqu'il sera détecté ; veillez donc à ce qu'il soit descriptif.
4. Pour créer un événement basé sur Object Activity, sélectionnez l'un des types de détection suivants :
 - a. Objects crossing beam : l'événement se déclenche lorsque le nombre spécifié d'objets a traversé le faisceau directionnel configuré dans le champ de visibilité de la caméra. Le faisceau peut être unidirectionnel ou bidirectionnel.
 - b. Objects enter area : l'événement est déclenché dès lors que le nombre d'objets indiqué a pénétré dans la zone d'intérêt.
 - c. Objects leave area : déclenchement d'un événement dès lors que la limite spécifiée a été atteinte concernant le nombre d'objets sortant de la zone d'intérêt.

- d. Object loitering : l'événement se déclenche lorsque le type d'objet sélectionné se déplace dans la zone d'intérêt, puis s'immobilise pendant une période prolongée.
 - e. Objects not present in area : l'événement est déclenché quand aucun objet n'est présent dans la zone d'intérêt.
 - f. Object appears or enters area : l'événement se déclenche dès pénétration des objets dans la zone d'intérêt. Les objets peuvent apparaître ou pénétrer dans la zone d'intérêt.
 - g. Objects in area : l'événement se déclenche dès présence des objets dans la zone d'intérêt.
 - h. Object stops in area : l'événement se déclenche lorsque l'objet s'arrête.
 - i. Direction violated : déclenchement d'un événement dès qu'un objet suit une direction interdite.
 - j. Objects too close : l'événement se déclenche lorsque les objets sont trop proches.
5. Pour créer un événement basé sur Behavior Anomaly, sélectionnez l'un des types de détection suivants :
- a. Unusual Crowd Growth : cet événement se déclenche lorsque la taille d'une foule augmente de manière inattendue.
 - b. Unusual Crowd Size : cet événement se déclenche lorsqu'une affluence inhabituelle est détectée.
 - c. Crowd size : cet événement se déclenche lorsque le nombre de personnes est dépassé pendant une durée configurable.
6. Cliquez et faites glisser le curseur **Sensitivity** pour régler le niveau de Sensibilité. L'abaissement de la sensibilité augmente les risques de faux négatifs.
7. Pour configurer **No. of objects**, entrez le nombre d'objets requis pour déclencher une alarme.
8. Pour configurer **Threshold Time**, entrez la durée minimale requise avant que l'événement ne se déclenche.
9. Pour configurer **Timeout**, entrez le laps de temps imparti avant qu'un autre événement ne se déclenche.
10. Cliquez sur **Save**.
11. Si vous souhaitez tester l'événement, cliquez sur le bouton ►**Test** situé en haut à droite de l'écran. Cela enverra un événement "Test" au système de gestion vidéo VMS (Video Management System). Accédez au VMS pour vérifier que l'événement a bien été reçu.

L'événement d'analyse est alors enregistré et la caméra déclenche un événement dès que l'activité est détectée dans la ou les zones d'intérêt. Pour obtenir des instructions sur la modification de la zone d'inclusion, voir [Modification de la zone d'inclusion sur la page 61](#).

Activation de superpositions d'analyse

La page *Analytics* vous permet d'activer les superpositions d'analyse. Les superpositions d'analyse affichent des informations d'analyse utiles à l'écran lorsque des événements se déclenchent.



NOTE

Pour pouvoir afficher les superpositions d'analyse, vous devez activer les métadonnées XML d'analyse, dans *Paramètres étendus*. Voir [Paramètres étendus sur la page 70](#) pour obtenir des instructions.

Pour activer les superpositions d'analyse, procédez comme suit :

1. Accédez à *Analytics* dans l'interface Web de la caméra.
2. Cliquez sur le bouton **Afficher fiabilité de l'objet** pour inclure les informations relatives à la fiabilité de l'objet dans la superposition.
3. Cliquez sur le bouton **Afficher ID de l'objet** pour inclure l'ID de l'objet dans la superposition.
4. Cliquez sur **Save**.

Les informations d'analyse s'affichent à l'écran lorsqu'un événement se déclenche.

Utilisation de Self Learning

La page *Analytics* vous permet de configurer l'analyse par auto-apprentissage. L'auto-apprentissage permet à la caméra d'apprendre la scène et d'effectuer des réglages automatiques en fonction de l'activité de cette dernière. L'auto-apprentissage améliore considérablement la précision de détection des objets classés.

Les scènes avec moins d'activité nécessiteront une mise en scène pendant la phase d'apprentissage. La mise en scène consiste à diriger l'activité afin d'indiquer à la caméra quelle activité détecter. Un exemple de mise en scène consisterait à faire passer une personne dans la zone d'intérêt pendant l'apprentissage.

Pour activer l'auto-apprentissage, procédez comme suit :

1. Accédez à *Analytics* dans l'interface Web de la caméra.
2. Cochez la case **Enable Self Learning** pour activer l'analyse par auto-apprentissage.
3. Cochez la case **Suspend Self Learning** pour suspendre l'auto-apprentissage.
4. Si vous souhaitez réinitialiser l'auto-apprentissage, cliquez sur le bouton **Reset Self Learning**. Cela supprime l'auto-apprentissage précédent.



IMPORTANT

Cette action est irréversible.

5. Cliquez sur **Save**.

L'auto-apprentissage progressera en fonction de l'activité détectée dans le champ de visibilité de la caméra.

Suspendre et réinitialiser Self Learning

Suspend Self Learning

La suspension de l'analyse vidéo par auto-apprentissage afin que la caméra continue à reconnaître correctement les objets sur la base des apprentissages précédents et ne dégrade pas sa détection d'objets lorsqu'elle est laissée à elle-même dans des scènes clairessemées.

Les exemples de scénarios suivants illustrent le cas où l'auto-apprentissage doit être suspendu :

- Vous n'attendez pas de personnes ou de véhicules dans le champ de vision du dispositif.
- Les objets se déplacent à différentes hauteurs. Par exemple, passerelles aériennes, quais de gare, collines et passages souterrains.

Reset Self Learning

Lorsque la progression de l'apprentissage est réinitialisée, toutes les données d'apprentissage sont effacées et l'appareil doit réapprendre la scène. Ceci empêche les détections fausses et manquées en fonction des données antérieures.



NOTE

L'auto-apprentissage doit être systématiquement réinitialisé après un déplacement physique ou un réglage de la caméra, ou une modification du niveau de mise au point ou de zoom.

Modification du Scene Mode

La zone *Scene Mode* vous permet de modifier le type de scène d'analyse. Un type de scène optimisé améliorera les résultats de l'analyse.

1. Accédez à *Analytics* dans l'interface Web de la caméra.
2. Cliquez sur la liste déroulante *Scene Mode* et sélectionnez l'une des options suivantes :
 - a. Grande zone intérieure
 - b. Extérieur
3. Cliquez sur **Save**.

La caméra changera le mode des scènes d'analyse.

Pour connaître les meilleures pratiques en matière d'optimisation de l'analyse vidéo, voir le [Conception d'un site avec analyse vidéo Pelco](#)

Modification de la zone d'inclusion

Vous pouvez modifier la zone d'inclusion afin d'exclure les zones qui n'ont pas besoin d'être surveillées pour un événement spécifique.

La zone d'inclusion apparaît sous la forme d'un cadre vert dans l'aperçu en direct. Utilisez votre curseur pour modifier la forme et la taille de la zone d'inclusion afin de vous assurer que toutes les régions que vous souhaitez surveiller pour l'événement sont bien surveillées. Après avoir modifié la zone d'inclusion, vous pouvez ajouter une ou plusieurs zones d'exclusion afin d'ignorer les petites régions dans le champ de visibilité de la caméra.

Pour modifier la zone d'inclusion, procédez comme suit :

1. Pour modifier la zone d'inclusion :
 - a. Cliquez et faites glisser le milieu du cadre vert sur l'écran pour déplacer la zone d'inclusion.
 - b. Cliquez et faites glisser les nœuds bleus pour reformer la zone d'inclusion.
 - c. Cliquez et faites glisser les nœuds verts pour créer des nœuds bleus et verts supplémentaires.
2. Pour ajouter des zones d'exclusion :
 - a. Cliquez sur **+ Ajouter une zone d'exclusion** pour ajouter une nouvelle zone d'exclusion. Les zones d'exclusion génèrent des trous dans la zone d'inclusion. Les événements de la zone d'exclusion ne déclenchent pas d'événement.
 - b. Cliquez et faites glisser le centre du carré vert sur l'écran pour déplacer la zone d'exclusion.
 - c. Reformez la zone d'exclusion de la même manière que vous avez formé la zone d'inclusion.
 - d. Continuez à cliquer et à faire glisser pour exclure les zones où vous ne souhaitez pas que l'activité déclenche un événement.
 - e. Cliquez sur **Supprimer la zone d'exclusion** pour supprimer la zone d'exclusion sélectionnée.
3. Si vous souhaitez recommencer, cliquez sur **Réinitialiser les zones** et sélectionnez l'une des options suivantes :
 - a. Réinitialiser une zone d'exclusion : réinitialise la zone d'exclusion pour couvrir l'ensemble du champ de visibilité.
 - b. Réinitialiser les zones d'exclusion : supprime les zones d'exclusion.
 - c. Réinitialiser toutes les zones : réinitialise la zone d'inclusion et supprime les zones d'exclusion. Vous ne pouvez pas supprimer la zone d'inclusion requise.
4. Cliquez sur **Save**.

Cela met à jour l'événement afin que seuls les événements détectés dans les zones d'inclusion déclenchent cette configuration d'événement particulière.

Test en cours Analytics Events

Il existe deux façons de tester les événements d'analyse :

- Après avoir enregistré l'événement, vous pouvez le tester en sélectionnant le bouton ►**Test** situé en haut à droite de l'écran.
- Vous pouvez également rechercher la règle d'analyse dans la page *Événements* et cliquer sur le bouton ►.

Cliquez sur le bouton **Test** pour envoyer un événement "Test" au système de gestion vidéo VMS (Video Management System). Accédez au VMS pour vérifier que l'événement a bien été reçu.

Types d'événements d'analyse

Analyse vidéo

Événements de mouvement

Objets dans la zone	Déclenchement d'un événement dès qu'il y a un mouvement du type d'objet sélectionné dans la zone d'intérêt
Objets franchissant un faisceau	Déclenchement d'un événement dès lors que la limite spécifiée a été atteinte concernant le nombre d'objets ayant traversé le faisceau directionnel configuré au niveau du champ de vision de la caméra. Le faisceau peut être unidirectionnel ou bidirectionnel.
Entrée d'objets dans la zone	L'événement est déclenché dès lors que le nombre d'objets indiqué a pénétré dans la zone d'intérêt.
Sortie d'objets de la zone	Déclenchement d'un événement dès lors que la limite spécifiée a été atteinte concernant le nombre d'objets sortant de la zone d'intérêt.
Objet rôdeur	L'événement se déclenche lorsque le type d'objet sélectionné se déplace dans la zone d'intérêt, puis s'immobilise pendant une période prolongée.
Objet non présent dans la zone	L'événement est déclenché quand aucun objet n'est présent dans la zone d'intérêt.
Un objet apparaît ou entre dans la zone	L'événement se déclenche dès pénétration des objets dans la zone d'intérêt. Cet événement peut être utilisé pour compter des objets.
Arrêt de l'objet dans la zone	Déclenchement d'un événement dès lors qu'un objet pénètre, puis demeure immobile dans la zone d'intérêt pendant la durée définie.
Objets trop proches	L'événement se déclenche lorsque deux objets sont trop proches l'un de l'autre, en fonction de la distance spécifiée pour l'événement. Modèles de caméras récents uniquement.
Violation de direction	Déclenchement d'un événement dès qu'un objet suit une direction interdite.
Taille de foule inhabituelle	Cet événement se déclenche lorsqu'une affluence inhabituelle est détectée.
Croissance de foule inhabituelle	Cet événement se déclenche lorsque la taille d'une foule augmente de manière inattendue.
Taille de la foule	Cet événement se déclenche lorsque le nombre de personnes est dépassé pendant une durée configurable.

Analyse audio

Événements audio

Cri	Cet événement se déclenche lorsqu'un être humain crie.
Bris de verre	Cet événement se déclenche lorsqu'un verre se brise.
Alarme voiture	Cet événement se déclenche lorsqu'une alarme de voiture se déclenche.
Alarme incendie	Cet événement se déclenche lorsqu'une alarme incendie se déclenche.
Aboiement de chien	Cet événement se déclenche lorsqu'un chien aboie.
Crissement de pneu	Cet événement se déclenche lorsque des pneus crissent.
Choc de métal	Cet événement se déclenche en cas de chute de métal.
Bruit fort	Cet événement se déclenche lorsqu'un son fort est détecté.

Caméras PTZ Spectra Enhanced et Spectra Pro Manuel d'utilisation

Ultrason	Cet événement se déclenche lorsqu'un son à haute fréquence est détecté.
Coup de feu	Cet événement se déclenche lorsqu'un coup de feu est détecté. Nécessite une licence premium.

Camera Automation

Les paramètres *Camera Automation* permettent aux administrateurs de créer des règles et d'affecter des actions que la caméra exécutera automatiquement en réponse à des déclencheurs spécifiques.

Chaque règle spécifie une action que la caméra doit effectuer chaque fois que le déclencheur spécifié s'active lorsqu'une condition spécifiée est vraie. Certaines actions sont prédéfinies et peuvent être utilisées dans les règles, tandis que d'autres doivent être définies par l'utilisateur pour pouvoir être utilisées dans les règles.



IMPORTANT

Toute modification apportée aux actions aura une incidence sur toutes les règles de caméra qui les utilisent.

Créer des règles et affecter des actions

Les règles définissent le déclencheur et les conditions requises pour déclencher des actions. Les administrateurs peuvent créer des règles basées sur l'analyse des caméras, les entrées numériques, le comportement PTZ et l'état du système. Vous pouvez créer des actions définies par l'utilisateur lors de la création de règles ou celles-ci peuvent créer les actions en premier.

Pour créer une nouvelle règle, procédez comme suit :

1. Accédez à *Camera Automation* dans l'interface Web de la caméra.
2. Cliquez sur le bouton **+ Ajouter** pour créer une nouvelle Règle.
3. Entrez les informations requises dans la fenêtre contextuelle **Automatisation de la caméra** :
 - a. Entrez un nom de règle dans le champ **Nom règle**.
4. Définissez le déclencheur dans la zone *Lorsque le déclencheur suivant s'active*, en sélectionnant une option dans la liste déroulante :
 - a. Analytics : crée une règle d'analyse.
 - b. DigitalInput : crée une règle Digital input.
 - c. SystemStatus : crée une règle d'état du système.
5. Si vous avez choisi Analytics comme déclencheur, sélectionnez l'un des types d'analyse enregistrés dans la liste. Si vous avez créé d'autres événements d'analyse, ceux-ci apparaîtront également dans la liste.
 - a. Règle de mouvement intelligente : lorsque la caméra détecte un événement de mouvement spécifique, par exemple des objets classés dans la scène. Vous pouvez effectuer la sélection dans la liste des règles de mouvements que vous avez créées à la page *Analyse*.
 - b. Règle de sabotage de la caméra : lorsque la caméra détecte une personne sabotant la caméra elle-même.
 - c. Détecteur de mouvements : lorsque la caméra détecte un mouvement dans la scène.

6. Si vous avez choisi SystemStatus comme Déclencheur, sélectionnez l'un des types SystemStatus suivants :
 - a. PTZInitialized : déclenche une action lorsque la caméra bouge.
 - b. SystemBooted : active un déclencheur lorsque la caméra redémarre.



TIP

Si vous souhaitez que la caméra revienne à sa position de départ lors du redémarrage, utilisez PTZInitialized et sélectionnez **GoHome** comme action.

7. Cliquez sur le bouton **Simuler déclencheur** si vous souhaitez tester les règles que vous avez déjà définies avec ce déclencheur.



NOTE

Simuler déclencheur entraîne uniquement l'exécution par le moteur de règles des règles dépendant du déclencheur choisi. Cela ne simule pas l'événement sous-jacent qui activerait le déclencheur dans la vie réelle.

8. Définissez la condition dans la zone *Et la condition suivante est vraie*, en sélectionnant une option dans la liste déroulante :
 - a. Toujours : la règle effectuera l'action chaque fois que le déclencheur sélectionné se déclenche.
 - b. Jamais : la règle n'effectuera jamais l'action, même si le déclencheur sélectionné se déclenche. Cette option permet de désactiver temporairement une règle.
9. Cliquez sur le bouton **Évaluer** si vous souhaitez vérifier si la condition sélectionnée est vraie ou fausse.
10. Définissez l'action dans la zone *Effectuer ensuite cette action*, en sélectionnant une option dans la liste déroulante :
 - a. Sortie numérique : déclenche une sortie numérique. DigitalOutput n'apparaît que sur les caméras disposant d'une ou plusieurs sorties numériques.
 - b. Courriel : envoie un courriel lorsque le déclencheur sélectionné se déclenche et que la condition est vraie.
 - c. FTP : déclenche une action FTP envoyée à un sous-répertoire.
 - d. Séquence : lance une séquence d'actions lorsque le déclencheur sélectionné se déclenche et que la condition est vraie.
11. Après avoir sélectionné les catégories d'actions disponibles dans la liste, vous pouvez soit choisir parmi les actions disponibles, soit en créer une nouvelle. Sélectionnez **+ Ajouter** et remplissez les champs comme décrit dans la section intitulée *Créer et gérer des séquences* sous .
12. Cliquez sur le bouton **Invoquer** si vous souhaitez tester l'action.
13. Cliquez sur **Save**.

La nouvelle règle apparaît alors dans la liste des règles.

Gestion des règles

Les administrateurs peuvent modifier les règles existantes via des opérations disponibles à la page *Règles*:

- Cliquez sur l'icône  pour modifier une règle.
- Pour supprimer une règle, cliquez sur l'icône .

La modification ou la suppression de règles affecte toutes les caméras utilisant une règle actuellement.

Ajout de nouvelles séquences

Les séquences de caméra automatisent une série d'actions. Ces actions comprennent les sorties numériques, l'envoi de courriels ou le transfert de fichiers via FTP. Vous pouvez créer et personnaliser des séquences, et même définir des délais entre chaque étape. Vous pouvez utiliser ces séquences lors de la création de règles pour la caméra.

Pour ajouter une nouvelle séquence, procédez comme suit :

1. Accédez à *Camera Automation > User-Defined Actions* dans l'interface Web de la caméra.
2. Sélectionnez **Sequence** pour afficher la zone des paramètres.
3. Cliquez sur le bouton **Add sequence**.
4. Saisissez un nom pour le Sequence.
5. Sélectionnez une action dans la liste ou cliquez sur Add action pour en créer une.
6. Saisissez les informations requises à la page Sequence :
 - a. Delay : entrez le nombre de minutes pendant lesquelles vous souhaitez que la séquence attende avant d'effectuer l'action.
 - b. Category : spécifie une catégorie, par exemple "PTZ".
 - c. Name— spécifie l'action spécifique dans la catégorie, par exemple "GoHome".
7. Cliquez sur le bouton **Test** pour tester la séquence.
8. Cliquez sur **Save**.

La nouvelle séquence apparaîtra dans la zone Sequence et sera répertoriée comme option lors de la création ou de la modification de règles.

Gestion des séquences

Pour modifier une séquence, utilisez les opérations de la page :

- Cliquez et faites glisser l'icône  pour réorganiser la séquence.
- Cliquez sur l'icône  pour supprimer une séquence.

La modification ou la suppression de séquences affectera toutes les règles des caméra utilisant actuellement la séquence.

Ajouter de nouveaux courriels d'actions

Les courriels d'actions automatisent l'envoi de courriels en réponse aux règles de la caméra, via le serveur SMTP. Les courriels d'actions peuvent être utilisés comme actions définies par l'utilisateur lors de la création de règles. Pour pouvoir créer des courriels d'actions, vous devez configurer les informations du serveur SMTP.



IMPORTANT

Toute modification apportée aux informations du serveur SMTP aura une incidence sur les règles utilisant déjà ce courriel.

Configuration des informations du serveur SMTP

Si vous ajoutez le serveur SMTP pour la première fois, le bouton s'intitule Configurer SMTP. Pour pouvoir accéder à l'onglet **Accès**, vous devez configurer SMTP.

Pour configurer les informations du serveur SMTP pour la première fois, procédez comme suit :

1. Vous y accédez à partir de *Camera Automation > Courriels d'actions* dans l'interface Web de la caméra.
2. Cliquez sur le bouton **Configurer SMTP**.
3. Saisissez les informations suivantes :
 - a. Saisissez l'URL du serveur SMTP.
 - b. Saisissez le nom d'utilisateur sur l'URL du serveur que vous avez fournie.
 - c. Saisissez le mot de passe de l'utilisateur ou le mot de passe de l'application pour le nom d'utilisateur
 - d. Saisissez une adresse électronique pour l'adresse électronique de l'expéditeur.
4. Cliquez sur **Enregistrer**.

Vous pouvez alors ajouter des adresses électroniques via cette configuration du serveur SMTP.

Gestion des informations du serveur SMTP

Vous pouvez gérer les paramètres SMTP existants dans la zone Courriel :

- Cliquez sur le bouton **Modifier SMTP** pour modifier les informations du serveur SMTP, puis cliquez sur **Appliquer**.

Les informations relatives au serveur SMTP affichent alors la nouvelle configuration.

Ajouter un courriel d'action

Une fois le serveur SMTP configuré, le bouton Configurer SMTP devient **Modifier SMTP** et le bouton **Ajouter courriel** s'active.

Pour créer un nouveau courriel d'action, procédez comme suit :

1. Cliquez sur le bouton **Ajouter courriel**.
2. Saisissez un nom pour le courriel d'action.
3. Saisissez l'adresse électronique du destinataire dans le champ **Courriel à**.
4. Vous pouvez saisir une autre adresse électronique dans le champ **Courriel Cc**, le cas échéant.
5. Saisissez le texte que vous souhaitez utiliser pour la ligne d'objet du courriel dans le champ **Objet courriel**.
6. Saisissez le texte de courriel souhaité, dans la section **Corps courriel**.
7. Cliquez sur **Enregistrer**.

Le nouveau courriel d'action apparaîtra comme option lorsque les utilisateurs créeront ou modifieront des règles.

Ajout de nouvelles actions FTP

Vous pouvez créer des actions FTP à utiliser lors de l'affectation d'actions au moteur de règles. Sélectionnez la ligne **FTP** pour afficher la zone FTP. Vous pouvez activer FTP en configurant les informations du serveur FTP.

Configuration des informations du serveur FTP

Si vous ajoutez le serveur FTP pour la première fois, le bouton s'intitule **Configurer FTP**. Pour pouvoir accéder à l'onglet **Accès**, vous devez configurer un serveur FTP.

Pour configurer les informations du serveur FTP, procédez comme suit :

1. Accédez à *Camera Automation > User-Defined Actions* dans l'interface Web de la caméra.
2. Cliquez sur **Configurer le serveur FTP**.
3. Entrez l'URL du serveur.
4. Entrez le nom d'utilisateur pour l'URL du serveur que vous avez fourni.
5. Entrez le mot de passe FTP associé au nom d'utilisateur.
6. Cliquez sur **Enregistrer**.

Vous pouvez ajouter des actions FTP avec cette configuration de serveur FTP.

Gestion des informations du serveur FTP

Vous pouvez gérer les paramètres FTP existants dans la zone FTP :

- Cliquez sur le bouton **Modifier FTP** pour modifier les informations relatives au serveur FTP, puis cliquez sur **Appliquer**.

Les informations du serveur FTP afficheront la nouvelle configuration.

Ajouter une action FTP

Après avoir ajouté les informations relatives au serveur FTP et activé FTP, vous pouvez créer une nouvelle action FTP.

1. Cliquez sur **Ajouter une action FTP**.
2. Entrez un nom pour l'action FTP.
3. Entrez le sous-répertoire.
4. Entrez le modèle de nom de fichier.
5. Sélectionnez un type de fichier dans le menu déroulant :
 - a. Snapshot : envoie une image JPEG depuis la caméra vers le serveur FTP.
 - b. hiResSnapshot : envoie une image plus grande et à plus grande résolution que l'image réduite produite par l'option Snapshot.
6. Cliquez sur **Enregistrer**.

La nouvelle action FTP apparaît alors sous forme d'option lorsque les utilisateurs créent ou modifient des règles.

Cloud Connection

La page *Cloud Connection* vous permet de connecter la caméra à Elevate soit via le code QR de l'interface Web de la caméra, soit en entrant le numéro de série de la caméra.

Pour connecter des caméras, vous devez vous connecter à votre compte Elevate.

Pour connecter une caméra Pelco à Elevate, procédez comme suit :

1. Accédez à Cloud Connection dans l'interface Web de la caméra.
2. Cliquez sur **Turn on provisioning mode**.
3. Les caméras utiliseront par défaut la méthode Code QR pour se connecter. Si vous souhaitez connecter la caméra via le numéro de série, sélectionnez **Numéro de série** dans le menu déroulant.
4. Connectez-vous à votre compte [Pelco Elevate](#).
5. Sélectionnez le bouton **Ajouter une caméra**.
6. Si vous utilisez la méthode Code QR :
 - a. Choisissez la méthode Code QR dans votre compte Elevate.
 - b. Scannez le code QR ci-dessous avec votre caméra pour vous connecter.
7. Si vous utilisez la méthode Numéro de série :
 - a. Choisissez la méthode Numéro de série dans votre compte Elevate.
 - b. Entrez le numéro de série de la caméra et cliquez sur **Confirmer**.
8. La caméra se connecte alors à Elevate.

L'indicateur d'état de la connexion s'actualise pour indiquer que la connexion est établie.

Paramètres étendus

La page *Paramètres étendus* vous permet de configurer les paramètres ONVIF. Les paramètres ONVIF vous permettent d'activer certaines fonctions et fonctionnalités nécessitant des configurations ONVIF spécifiques.

1. Cliquez sur le bouton **Activer les documents XML multipaquets** pour réduire la taille des métadonnées. Uniquement pour les systèmes de gestion vidéo prenant en charge les documents XML multipaquets.
2. Cliquez sur le bouton **Activer les requêtes d'options d'analyse** pour activer les requêtes GetAnalyticsModuleOptions et GetRuleOptions.
3. Cliquez sur le bouton **Activer les métadonnées XML d'analyse** pour activer les métadonnées XML. Ceci est nécessaire pour activer les cadres de sélection.
4. Cliquez sur le bouton **Activer l'encodage RLE du masque de mouvement** pour activer l'encodage RLE du masque de mouvement. Uniquement pour les systèmes de gestion vidéo ne nécessitant pas de masque non codé.
5. Cliquez sur le bouton **Activer les événements supplémentaires** pour envoyer des événements supplémentaires non définis par ONVIF susceptibles d'être utiles à certains systèmes de gestion vidéo.
6. Cliquez sur le bouton **Activer les événements d'analyse Singleton** pour envoyer des événements d'analyse Singleton au lieu des événements de propriété.
7. Cliquez sur **Save**.

Privacy Zones

La page *Privacy Zones* vous permet créer jusqu'à 64 zones de confidentialité. Les zones de confidentialité peuvent être appliquées à des emplacements sensibles, tels que les zones résidentielles, les toilettes ou les bureaux privés, afin d'empêcher toute observation ou tout enregistrement non autorisé des personnes se trouvant dans ces espaces.

Création de Privacy Zones

Pour créer Privacy Zones, procédez comme suit :

1. Accédez à *Privacy Zones* dans l'interface Web de la caméra.
2. Pour ajouter une zone de confidentialité, cliquez sur **Ajouter**. La zone de confidentialité apparaît sous forme de cadre bleu sur Live Preview.
3. Pour définir la zone privée, procédez d'une des manières suivantes :
 - a. Cliquez et faites glisser le cadre bleu pour déplacer la zone de confidentialité.
 - b. Sélectionnez le cadre bleu pour afficher les nœuds à chaque angle. Cliquez et faites glisser l'angle du cadre pour redimensionner la zone de confidentialité. Privacy Zones ne peut être que de forme rectangulaire. Plusieurs zones privées peuvent être utilisées pour obscurcir d'autres formes.
4. Pour un réglage précis, vous pouvez utiliser le curseur **Zoom** pour agrandir ou réduire l'image.
5. Cliquez sur **Save**.

Les zones de confidentialité apparaissent dans des zones désignées.

Gestion des Privacy Zones

Vous pouvez gérer les Privacy Zones enregistrées dans la liste *Privacy Zones* :

- Si vous souhaitez qu'une zone de confidentialité apparaisse floutée plutôt qu'opaque, cochez la case **Blur**.
- Si vous souhaitez supprimer une zone de confidentialité, cliquez sur l'icône .

Storage

La page *Storage* vous permet d'activer le stockage intégré et de télécharger les vidéos enregistrées directement depuis la caméra. Le stockage intégré n'est disponible que sur les caméras équipées d'un emplacement pour carte SD ou microSD. La carte SD enregistrera en flux plein écran, avec la plus haute résolution. En règle générale, le meilleur flux à enregistrer est le flux principal de la caméra.

Insérez la carte SD dans la caméra afin de pouvoir utiliser la fonction de stockage intégrée. Se référer au [guide d'installation de la caméra](#) pour connaître l'emplacement du logement pour carte SD. Pour les caméras avec 2 fentes pour carte microSD, la caméra enregistrera la vidéo sur des cartes SD dans les deux fentes. La capacité de stockage totale du système est la capacité de stockage combinée de chacune des deux cartes individuelles.



IMPORTANT

Les défaillances de la carte SD peuvent entraîner le redémarrage continu de la caméra. Pour éviter cela, la carte SD sera désactivée si des défaillances persistantes sont détectées. Pour plus d'informations, voir [Dépannage de carte SD sur la page 76](#).

Informations sur Storage

La zone *Stockage intégré* vous permet d'afficher les informations relatives au dispositif et de formater la carte SD.

Informations sur le stockage intégré :

- État : état de stockage de la caméra. Par exemple : enregistrement, enregistrement en cas de perte de connexion au serveur, etc.
- Capacité totale : capacité de stockage totale (Go) avec une ou plusieurs cartes SD installées.
- Utilisation actuelle : utilisation actuelle de l'espace de stockage (Go).
- Capacité restante : capacité de stockage restante (en heures).

Formatage de la carte SD

La page *Storage* vous permet de formater la carte SD pour la réinitialiser à son état d'usine par défaut. Cela efface toutes les données et configure un nouveau système de fichiers.

- Cliquez sur **Format Card** dans la zone *Onboard Storage*.

La caméra redémarrera et les enregistrements enregistrés sur la carte seront supprimés.

Informations carte SD

La page *Storage* vous permet d'afficher les informations de carte SD suivantes :

- Modèle : numéro de modèle de la carte SD.
- Numéro de série : numéro de série de la carte SD.
- Capacité : capacité de stockage de la carte SD (Go).
- Espace libre : espace de stockage disponible sur la carte SD (Mo).
- Vitesse d'écriture mesurée : vitesse d'écriture de la carte (Mo/s).

Chiffrement de carte SD

La page *Storage* vous permet d'activer le chiffrement de la carte SD afin de chiffrer les fichiers vidéo à titre de mesure de sécurité.



IMPORTANT

L'activation ou la désactivation du chiffrement formatera toutes les cartes insérées et effacera tous les fichiers s'y trouvant.

- Cochez la case **Card Encryption** dans la zone *Onboard Storage* pour activer le chiffrement de la carte. Cliquez sur **Save**.

La ou les cartes SD seront reformatées et les fichiers qui y sont stockés seront supprimés.

Configuration de Recording Mode

La page *Storage* vous permet d'activer Onboard Storage et de configurer le mode d'enregistrement, ainsi que la durée de conservation.

Pour configurer le mode d'enregistrement, procédez comme suit :

1. Cliquez sur le bouton **Enable Onboard Storage**.
2. Cliquez sur le bouton **Recording when server connection is lost** pour que la caméra enregistre la vidéo à la fois sur le VMS et sur la carte SD. Par défaut, la caméra n'enregistre sur la carte SD que lorsqu'elle est déconnectée du VMS.
3. Sélectionnez l'un des modes d'enregistrement suivants :
 - a. Continuous : la caméra enregistre en continu sur la carte SD, sans interruption.
 - b. On Motion : la caméra n'enregistre qu'en cas de mouvement dans la scène. La vidéo enregistrée est divisée en fichiers ne dépassant pas cinq minutes ou une taille de 100 Mo. Si vous configurez une caméra d'analyse vidéo, le paramètre On Motion enregistre soit les changements de pixels dans la scène, soit les événements de mouvement analysés, selon la configuration de la caméra dans le VMS.
4. Cliquez sur le bouton **Enable Recording Retention** pour conserver les enregistrements pendant une durée déterminée (de 5 minutes à 2 ans). Vous pouvez affecter le nombre de jours, d'heures et de minutes de conservation des enregistrements.
5. Cliquez sur **Save**.

Après avoir configuré le mode d'enregistrement, vérifiez les paramètres Compression and Image Rate pour vous assurer que le format est réglé sur **H.264** ou **H.265**, afin d'optimiser la capacité d'enregistrement et les performances de la carte SD.

Télécharger les enregistrements depuis l'interface Web

La page *Storage* vous permet de visionner et de télécharger les enregistrements sur la ou les cartes SD.

Si deux cartes SD sont installées dans la caméra, sélectionnez la carte SD à partir de laquelle vous souhaitez télécharger la vidéo. Vous devrez peut-être vérifier les deux cartes SD pour l'enregistrement à télécharger. La caméra peut enregistrer de la vidéo sur l'une ou l'autre carte SD en fonction de la capacité restante des cartes SD.

Nous vous recommandons de télécharger les vidéos enregistrées à partir de l'interface Web. Si votre bande passante est limitée, vous pouvez choisir de télécharger la vidéo enregistrée, directement depuis la carte SD. Voir [Téléchargement des vidéos enregistrées depuis la carte SD en dessous](#) pour obtenir des instructions.

Pour télécharger une vidéo enregistrée à partir de l'interface Web, procédez comme suit :

1. Dans la liste d'enregistrement, cochez la case en regard de tous les fichiers vidéo à télécharger. Pour vous aider à trouver la vidéo que vous voulez, vous pouvez filtrer les vidéos par date et heure. Cochez la case **Filter**, puis sélectionnez la plage horaire.
2. Cliquez sur **Download**.

Les fichiers vidéo sélectionnés sont automatiquement téléchargés vers le dossier de téléchargements par défaut de votre navigateur. Autorisez le téléchargement si le navigateur vous y invite.



NOTE

Ne fermez pas la fenêtre du navigateur avant la fin du téléchargement, sinon le fichier ne pourra pas se télécharger correctement. C'est très important si vous téléchargez plusieurs fichiers vidéo, car le téléchargement est individuel.

Téléchargement des vidéos enregistrées depuis la carte SD

La page *Storage* vous permet de télécharger les vidéos enregistrées directement depuis la carte SD si la bande passante est insuffisante pour les télécharger depuis l'interface Web.

Pour télécharger les vidéos enregistrées directement depuis la carte SD, procédez comme suit :

1. Dans la zone *Settings*, décochez la case **Enable Onboard Storage** pour désactiver le stockage intégré, puis cliquez sur **Apply**.
2. Retirez la carte SD de la caméra.
3. Insérez la carte SD dans un lecteur de cartes.
4. Lorsque la boîte de dialogue Windows AutoPlay apparaît, sélectionnez **Open folder** (Ouvrir le dossier) pour afficher les fichiers.
5. Ouvrez l'application Enregistrement de la caméra. La fenêtre Enregistrement de la caméra affiche tous les fichiers vidéo stockés sur la carte SD.

- a. Pour télécharger toutes les vidéos enregistrées, cliquez sur **Download**.
 - b. Pour télécharger une vidéo spécifique, sélectionnez les fichiers vidéo souhaités, puis cliquez sur **Télécharger la sélection**.
6. Lorsque vous y êtes invité, choisissez un emplacement pour enregistrer les fichiers vidéo.
7. Les fichiers commencent à se télécharger à partir de la carte SD et sont sauvegardés à l'emplacement sélectionné.
8. Lorsque vous êtes prêt, éjectez la carte SD.
9. Réinsérez la carte SD dans la caméra, puis sélectionnez **Enable Onboard Storage**.

La carte SD recommence alors à enregistrer.

ONVIF Profile G

ONVIF Profil G permet aux systèmes de gestion vidéo de récupérer des vidéos à partir du stockage intégré en cas d'interruption de la vidéo VMS due à une panne réseau ou à un événement similaire.

- Sur les caméras équipées des versions 4.4.0.X ou ultérieures du micrologiciel, ONVIF Profile G est déjà activé.

Dépannage de carte SD

Une défaillance de la carte peut entraîner une défaillance de la caméra en provoquant son redémarrage continu. Si la caméra détecte des défaillances persistantes, la carte SD sera automatiquement désactivée.

Une fois la carte SD désactivée, la caméra et l'interface Web vous informeront du problème :

- L'enregistrement vidéo affichera le message suivant : `SD card has failed. Format or replace the card`
Vous pouvez désactiver les superpositions vidéo sur la page *Storage*, en décochant la case **Activer la superposition SD désactivée**.
- La page *Storage* affichera le message suivant : `Onglet Stockage SD désactivé`

Réactivation de la carte SD

Pour réactiver la carte SD, procédez comme suit :

1. Retirez la carte SD du logement de la caméra et remplacez-la par une carte SD en état de fonctionnement. Un test de vitesse sera effectué sur la nouvelle carte lorsqu'elle sera insérée afin de déterminer si elle fonctionnera sans problème.
2. Vous pouvez également forcer la réactivation de la carte SD dans l'interface Web, en sélectionnant **Forcer l'activation de la carte SD désactivée** à la page *Storage*.



IMPORTANT

Il n'est pas recommandé de forcer la réactivation de la carte SD, sauf si vous êtes sûr que la carte ne présente aucun problème. Si la carte continue à ne pas fonctionner, cela peut entraîner l'entrée de la caméra dans une boucle de redémarrage et après des défaillances persistantes, la carte SD sera à nouveau désactivée.

System

Les paramètres *System* permettent aux administrateurs de consulter les informations système, de mettre à jour manuellement le micrologiciel, de redémarrer le dispositif et de rétablir les paramètres d'usine de la caméra.

Vous pouvez afficher les informations *System* suivantes :

- **Firmware Version** : affiche la version du micrologiciel installée sur la caméra.
- **Model Number** : le numéro de modèle de la caméra indique si elle dispose de certaines fonctions, telles que des LED infrarouges.
- **Hardware Version** : le numéro de version du matériel peut être utile lorsque vous contactez le service d'assistance pour des questions relatives au micrologiciel.
- **Serial Number** : numéro de série unique de la caméra.

Mise à jour de Firmware

La page *System* permet aux administrateurs de mettre à jour le micrologiciel de la caméra.

Pour mettre à niveau manuellement le micrologiciel de la caméra, procédez comme suit :

1. Accédez à *System* dans l'interface Web de la caméra.
2. Téléchargez la dernière version du fichier .bin du micrologiciel sur le site Web Pelco à l'adresse www.pelco.com/updates.
3. Cliquez sur **Browse**, puis recherchez et localisez le fichier du micrologiciel sur votre ordinateur.
4. Cliquez sur **Firmware Update** et attendez que la mise à jour soit terminée.

La caméra redémarrera pendant 1 à 2 minutes.

Une fois le redémarrage de la caméra terminé, actualisez votre navigateur et reconnectez-vous.

Redémarrage de la caméra

Si la caméra fonctionne de manière inhabituelle, un administrateur peut utiliser la fonction Reboot pour résoudre le problème.

1. Accédez à *System* dans l'interface Web de la caméra.
2. Cliquez sur **Reboot** pour faire redémarrer la caméra.

La caméra redémarre alors. Cela peut prendre plusieurs minutes.



TIP

Une fois que la caméra a fini de redémarrer, actualisez votre navigateur. Vous devrez vous reconnecter.

Suppression de tous les paramètres

Les administrateurs peuvent supprimer tous les paramètres de la caméra, afin de rétablir les paramètres d'usine par défaut :

1. Accédez à *System* dans l'interface Web de la caméra.
2. Cochez la case **Preserve Network Configurations** pour que la configuration des paramètres réseau de la caméra ne soit pas réinitialisée.
3. Cliquez sur **Clear All Settings** pour réinitialiser les paramètres de la caméra.
4. Cliquez sur **Ok** dans la boîte de dialogue de confirmation.

La caméra effectue alors une réinitialisation selon les réglages d'usine.

Device Logs

La page *Device Logs* vous permet d'afficher, de mettre à jour ou de télécharger le journal du dispositif sur la page *Informations sur le dispositif*. Vous pouvez utiliser les filtres pour affiner les journaux affichés dans la page. Vous pouvez filtrer par type de journal, niveau minimum de journalisation et modifier le nombre de journaux affichés à la fois.

Mise à jour de Device Logs

Vous pouvez actualiser la liste des journaux de dispositifs.

- Pour actualiser la liste des journaux de dispositifs, cliquez sur **Mettre à jour**.

Tous les journaux enregistrés depuis la dernière actualisation seront ajoutés à la page.

Téléchargement du journal

Vous pouvez télécharger la liste actuelle des journaux de dispositifs.

- Pour télécharger les journaux, cliquez sur **Télécharger le journal**.



TIP

Assurez-vous d'avoir sélectionné les bons filtres avant le téléchargement.

PTZ

L'interface Web de la caméra propose quatre fonctions permettant d'automatiser le comportement de la caméra PTZ. Les caméras PTZ peuvent être programmées pour effectuer des mouvements spécifiques lorsqu'elles sont déclenchées par un événement ou actionnées manuellement. Par exemple, lorsqu'un mouvement est détecté sur la porte arrière après les heures d'ouverture, la caméra PTZ peut effectuer un panoramique, une inclinaison et un zoom sur la porte arrière avant de balayer le parking, puis zoomer sur la sortie des véhicules, etc. Ces comportements peuvent être programmés via les différentes fonctions de la caméra PTZ.

Il existe quatre types de fonctions pour les caméras PTZ :

- **PTZ Patterns** : enregistrez et reproduisez les mouvements de la caméra en temps réel. Vous pouvez les utiliser pour effectuer la surveillance automatique d'une zone spécifique en créant un modèle de mouvements panoramiques, d'inclinaison et de zoom.
- **PTZ Scans** : programmez une séquence de mouvements panoramiques, d'inclinaison et de zoom, et définissez un temps d'arrêt spécifique pour chaque mouvement. Cela permet d'enregistrer une trajectoire spécifique qui pourra être reproduite ultérieurement.
- **PTZ Zones** : affectez un nom à une région dans le champ de visibilité de la caméra.
- **PTZ Tours** : programmez la caméra pour qu'elle se déplace automatiquement à travers une série de positions avec des paramètres prédéfinis. Vous devez créer les préréglages avant de les ajouter à un tour de garde. Les tours de garde peuvent être ajoutés lors de la création de règles pour la caméra ou d'actions définies par les utilisateurs.

- **PTZ Limits** : limitez l'amplitude du mouvement de la caméra afin qu'elle ne montre pas d'obstacles et ne dépasse pas un certain niveau de zoom. Par exemple, vous pouvez définir des limites pour empêcher la caméra de montrer un mur proche.

PTZ Patterns

La page *PTZ Patterns* vous permet de créer et de gérer des PTZ Patterns. PTZ Patterns enregistre les mouvements PTZ de la caméra en temps réel et le système les lit.

Création de PTZ Patterns

Pour créer un PTZ Patterns, vous devez déplacer manuellement la caméra selon les mouvements de panoramique, d'inclinaison et de zoom souhaités, que le système enregistre puis reproduit.

Pour créer PTZ Patterns, procédez comme suit :

1. Positionnez la caméra via les commandes PTZ :
 - a. Faire glisser pour zoomer : cliquez et faites glisser sur l'écran pour zoomer. Un carré blanc apparaît au milieu de la visionneuse en direct.
 - b. Panoramique : cliquez dans le carré blanc et faites glisser dans la direction où vous souhaitez que la caméra effectue un panoramique.
 - c. Réglage précis : utilisez les commandes de zoom et de mise au point, situées sous la visionneuse en direct pour régler la qualité d'image avec précision.
2. Si nécessaire, sélectionnez **Commandes de mise au point et de zoom numérique** dans la liste déroulante **Type de commande**. La caméra utilise par défaut les commandes PTZ.
3. Cliquez sur **Create and Record** et utilisez les commandes Zoom et Mise au point pendant que le système enregistre le modèle.
4. Cliquez sur **Arrêter l'enregistrement** après avoir terminé.
5. Nommez le modèle dans le champ **Pattern name**.
6. Cliquez sur **Save**.

Le modèle PTZ peut désormais être lu pour effectuer la surveillance automatique d'une zone.

Gestion des PTZ Patterns

Pour gérer un modèle existant, sélectionnez un PTZ Patterns dans la liste déroulante.

1. Sélectionnez un modèle PTZ dans la liste déroulante.
2. Pour exécuter le modèle, cliquez sur **Run**.
3. Pour arrêter le modèle, cliquez sur **Stop**.
4. Pour réenregistrer le modèle, cliquez sur **Re-Record** et utilisez les commandes Zoom et Mise au point pour réenregistrer.
5. Pour supprimer le modèle, cliquez sur **Delete Pattern**.
6. Cliquez sur **Save**.

PTZ Scans

La page *PTZ Scans* vous permet de créer et gérer des PTZ Scans. Un balayage peut être utilisé pour enregistrer une trajectoire de panoramique/inclinaison/zoom qui peut être reproduite exactement telle qu'elle a été enregistrée.

Création de PTZ Scans

Pour créer PTZ Scans, procédez comme suit :

1. Positionnez la caméra via les commandes PTZ :
 - a. Faire glisser pour zoomer : cliquez et faites glisser sur l'écran pour zoomer. Un carré blanc apparaît au milieu de la visionneuse en direct.
 - b. Panoramique : cliquez dans le carré blanc et faites glisser dans la direction où vous souhaitez que la caméra effectue un panoramique.
 - c. Réglage précis : utilisez les commandes de zoom et de mise au point, situées sous la visionneuse en direct pour régler la qualité d'image avec précision.
2. Si vous devez utiliser le zoom numérique et la mise au point, sélectionnez **Commandes de mise au point et de zoom numérique** dans la liste déroulante **Control Type**. La caméra utilise par défaut les commandes PTZ.
3. Cliquez sur **New**.
4. Nommez le balayage dans le champ **Scan name**.
5. Sélectionnez un type de balayage dans la liste déroulante **Scan type**.
6. Pour définir des limites de balayage :
 - a. Pour définir la limite gauche, entrez une valeur pour la limite la plus à gauche, puis cliquez sur Définir limite gauche.
 - b. Pour définir la limite droite, entrez une valeur pour la limite la plus à droite, puis cliquez sur Définir limite droite.
 - c. Pour régler la vitesse de panoramique, entrez le pourcentage de la vitesse maximale (0,1-20) dans le champ Vitesse panoramique (%). Ce paramètre détermine la vitesse de panoramique de la caméra.
 - d. Pour définir le temps d'attente, entrez le nombre de secondes pendant lesquelles vous souhaitez que la caméra fasse une pause (0,1 à 60) dans le champ Temps d'attente (%).
7. Cliquez sur **Save**.

Le nouveau balayage PTZ apparaîtra dans la liste.

Gestion des PTZ Scans

Pour gérer les PTZ Scans enregistrés, vous pouvez utiliser les options suivantes :

1. Sélectionnez un PTZ Scans dans la liste déroulante **PTZ Scans**.
2. Cliquez sur **Run** pour lancer le balayage.
3. Cliquez sur **Stop** pour arrêter le balayage.
4. Cliquez sur **Re-Record** pour réenregistrer le balayage et utilisez les commandes Zoom et Mise au point pour recommencer le balayage.
5. Cliquez sur **Delete** pour supprimer le balayage.

PTZ Zones

PTZ Zones vous permettent de libeller des zones du champ de visibilité de la caméra. Lorsque la caméra est orientée vers une zone, le nom de cette zone apparaît sous forme de texte superposé.



NOTE

Vous devez activer les PTZ Zones pour qu'ils apparaissent à l'écran. Vous pouvez les activer à la page *Overlays*, en créant une nouvelle superposition et en utilisant Nom de la zone PTZ comme type de superposition.

Pour créer un fichier PTZ Zones, procédez comme suit :

1. Accédez à PTZ Zones dans l'interface Web de la caméra.
2. Entrez un nom dans le champ Nom de zone.
3. Cliquez sur **Create Zone**. La nouvelle zone sera ajoutée à la liste dans la zone *Selected Zone*.
4. Sélectionnez la zone dans la liste **Selected Zone**.
5. Utilisez les commandes PTZ pour effectuer un panoramique, une inclinaison ou un zoom sur une zone du champ de visibilité.
6. Cliquez sur **Set Zone Position**.

La superposition de texte à l'écran apparaîtra sur Live preview.

Si la superposition de texte à l'écran n'apparaît pas sur Live preview, cela signifie que les zones PTZ n'ont pas été activées. Accédez à *Image & Display > Overlays* et créez une nouvelle superposition de texte pour les noms de zones PTZ. Voir [Overlays sur la page 49](#) pour obtenir des instructions.

PTZ Tours

La page *PTZ Tours* permet aux administrateurs de créer de nouveaux tours de garde et de gérer les tours de garde enregistrés. Les PTZ Tours permettent à la caméra de se déplacer automatiquement selon divers paramètres prédéfinis.

Ajout de PTZ Presets

Vous devez créer les pré-réglage dont vous avez besoin avant de pouvoir les ajouter à un tour de garde.

Pour ajouter un pré-réglage PTZ, procédez comme suit :

1. Accédez à *PTZ Tours* dans l'interface Web de la caméra.
2. Positionnez la caméra via les commandes PTZ :
 - a. Faire glisser pour zoomer : cliquez et faites glisser sur l'écran pour zoomer. Un carré blanc apparaît au milieu de la visionneuse en direct.
 - b. Panoramique : cliquez dans le carré blanc et faites glisser dans la direction où vous souhaitez que la caméra effectue un panoramique.
 - c. Réglage précis : utilisez les commandes de zoom et de mise au point, situées sous la visionneuse en direct pour régler la qualité d'image avec précision.
3. Si nécessaire, sélectionnez **Commandes de mise au point et de zoom numérique** dans la liste déroulante **Control Type**. La caméra utilise par défaut les commandes PTZ.
4. Entrez un nom de préséglage dans le champ **Preset**.

Le nouveau paramètre prédéfini PTZ apparaîtra dans la liste.

Création de PTZ Tours

Vous pouvez créer de nouveaux tours de garde en sélectionnant et y ajoutant des PTZ Presets.

Pour ajouter un tour de garde PTZ, procédez comme suit :

1. Nommez le tour de garde dans le champ **Tour name**.
2. Sélectionnez un mode de tour de garde dans la liste déroulante **Tour mode** :
 - a. Sequential : la caméra passe à chaque paramètre prédéfini dans l'ordre spécifié.
 - b. Random : la caméra passe à chaque paramètre prédéfini dans un ordre aléatoire.
3. Si nécessaire, cochez la case **Set As Default Tour** pour exécuter le tour de garde automatiquement. Cela active le paramètre Default Tour Idle Start Time.
4. Si vous avez sélectionné **Set As Default Tour** et que vous souhaitez définir le temps d'attente, entrez le temps d'attente (en minutes) avant le début du tour de garde. C'est le temps d'attente de la caméra avant démarrage automatique du tour de garde.
5. Dans le champ **Tour Pause Duration**, saisissez la durée s'écoulant avant la répétition d'un tour de garde. Les tours de garde se répètent jusqu'à ce qu'ils soient arrêtés manuellement ou que d'autres commandes PTZ soient utilisées.
6. Cliquez sur **Save**.

Le nouveau tour de garde PTZ apparaît dans la liste.

Ajouter des PTZ Presets aux PTZ Tours

Vous pouvez ajouter les paramètres prédéfinis enregistrés aux tours de garde.

Pour ajouter des préséglage à un tour de garde PTZ, procédez comme suit :

1. Cliquez sur **Add Preset** pour ajouter un préséglage à la liste.
2. Sélectionnez un préséglage dans la liste déroulante.
3. Dans le champ **Move Speed**, entrez un pourcentage de la vitesse maximale définie à la page *PTZ Limits*. Cela détermine la vitesse à laquelle la caméra se déplace pendant le préséglage.

4. Dans le champ **View Time**, entrez la durée pendant laquelle vous souhaitez que la caméra reste sur cette position prédéfinie.
5. Ajoutez d'autres préréglages selon vos besoins.
6. Cliquez et faites glisser l'icône  pour réorganiser les préréglages.
7. Cliquez sur l'icône  pour supprimer un préréglage.

Le tour de garde sera mis à jour pour inclure les préréglages.

Gestion des PTZ Tours enregistrés

Pour gérer vos tours de garde enregistrés, vous pouvez utiliser les options suivantes :

- Pour modifier un tour de garde, sélectionnez-la, effectuez vos modifications, puis cliquez sur **Ok** pour enregistrer.
- Pour supprimer le tour de garde, cliquez sur l'icône , puis sur **Ok** pour confirmer.

PTZ Limits

La page PTZ Limits permet aux utilisateurs de définir *PTZ Limits* pour limiter l'amplitude du mouvement de la caméra afin qu'aucun obstacle ne soit jamais visible. Par exemple, si la caméra PTZ est installée près du côté d'un bâtiment, les utilisateurs peuvent définir des limites de mouvement, afin que la caméra PTZ ne montre pas le mur. Les utilisateurs peuvent également limiter le niveau de zoom dans les zones où tout est à portée de main.

Pour définir PTZ Limits, procédez comme suit :

1. Accédez à *PTZ Limits* dans l'interface Web de la caméra.
2. Positionnez la caméra via les commandes PTZ :
 - a. Faire glisser pour zoomer : cliquez et faites glisser sur l'écran pour zoomer. Un carré blanc apparaît au milieu de la visionneuse en direct.
 - b. Panoramique : cliquez dans le carré blanc et faites glisser dans la direction où vous souhaitez que la caméra effectue un panoramique.
 - c. Réglage précis : utilisez les commandes de zoom et de mise au point, situées sous la visionneuse en direct pour régler la qualité d'image avec précision.
3. Si nécessaire, sélectionnez **Commandes de mise au point et de zoom numérique** dans la liste déroulante **Control Type**. La caméra utilise par défaut les commandes PTZ.
4. Sélectionnez le type de commande dans la liste déroulante **Control Type** :
 - a. PTZ : contrôle le mouvement physique et le niveau de zoom optique.
 - b. Digital Pan and Zoom : contrôle le niveau de zoom numérique des caméras.
5. Pour définir une limite de zoom maximale, cliquez et faites glisser le curseur **Zoom** jusqu'à la valeur maximale souhaitée.
6. Pour définir la limite du panoramique :

- a. Saisissez les coordonnées (0-360 degrés) dans le champ **From** et une coordonnée (0-360 degrés) dans le champ **To**.
 - b. Cliquez sur l'icône , puis sur Live Preview pour définir les coordonnées.
 - c. Cliquez et faites glisser les icônes  sur la boussole pour définir la limite. La zone bleue représente l'amplitude de mouvement de la caméra. La flèche indique la position actuelle de la caméra.
7. Pour définir la limite d'inclinaison :
 - a. Saisissez les coordonnées (-20-91 degrés) dans le champ **From** et une coordonnée (-20-91 degrés) dans le champ **To**.
 - b. Cliquez sur l'icône , puis sur Live Preview pour définir les coordonnées.
 - c. Cliquez et faites glisser les icônes  sur la boussole pour définir la limite. La zone bleue représente l'amplitude de mouvement de la caméra. La flèche indique la position actuelle de la caméra.
8. Pour définir la limite de vitesse prédéfinie, saisissez la limite de vitesse maximale prédéfinie dans le champ **Preset speed limit** (0-300) en degrés par seconde.
9. Pour définir la limite de vitesse de panoramique/inclinaison, saisissez la limite maximale de vitesse de panoramique/inclinaison dans le champ **Pan/Tilt speed limit** (0-300) en degrés par seconde.
10. Cliquez sur le bouton **Digital zoom** pour activer le zoom numérique.
11. Cliquez sur **Save**.

Les mouvements PTZ sont alors limités aux régions que vous aurez sélectionnées.

Audio

La page *Audio* vous permet de régler divers paramètres du son afin d'optimiser la qualité audio et de définir le comportement du microphone et du haut-parleur intégrés à l'interphone vidéo.

Pour configurer les paramètres de son, procédez comme suit :

1. Accédez à *Audio* dans l'interface Web de la caméra.
2. Dans le champ **Audio Settings**, spécifiez l'encodeur audio à utiliser :
 - Opus : codec audio haute qualité par défaut produisant généralement un audio de qualité supérieure. À utiliser si vous utilisez la version 6.10 ou ultérieure du logiciel ou un système de gestion vidéo tiers prenant en charge le protocole Opus.
 - G.711 : pris en charge sur diverses plates-formes. À utiliser si votre version logicielle ou votre VMS tiers ne prend pas en charge Opus.
3. Cliquez sur **Save**.

Les paramètres audio seront mis à jour.

Configuration de Device Speaker

La page *Audio* vous permet de configurer le haut-parleur du dispositif.

Pour configurer le haut-parleur du dispositif, procédez comme suit :

- À partir de la zone *Device Speaker*, cliquez et faites glisser le curseur **Speaker volume** pour définir la valeur (0-31 dB). La valeur par défaut est 0. Cliquez sur **Save**.

Les paramètres Device Speaker sont alors mis à jour.

Configuration de Device Microphone

La page *Audio* permet de configurer le microphone du dispositif.

Pour configurer le microphone du dispositif, procédez comme suit :

- À partir de la zone *Device Microphone*, cliquez et faites glisser le curseur **Gain for microphone** pour définir la valeur (0-31 dB). La valeur par défaut est 0. Cliquez sur **Save**.

L'augmentation de la valeur Gain for microphone augmente le volume.

Configuration des paramètres Multicast pour l'audio

Pour configurer le comportement de Multicast pour l'audio d'un dispositif, procédez comme suit :

1. Pour configurer Multicast, entrez les informations requises dans les champs suivants :
 - a. Address— Entrez l'adresse du serveur.
 - b. Port— Entrez le numéro de port du serveur (1024...65534). N'accepte que les valeurs paires.
 - c. Time to live : entrez le nombre de secondes (1-255).
2. Cliquez sur **Save**.

La caméra transmet l'audio au serveur spécifié ci-dessus, le rendant ainsi accessible sur le(s) client(s) connecté(s) à ce serveur, via le numéro de port spécifié.

Pour configurer le streaming en multidiffusion pour la vidéo, voir [Configuration des paramètres de multidiffusion pour la vidéo sur la page 52](#).

Users

La page *Users* permet aux administrateurs d'ajouter de nouveaux comptes utilisateurs et de gérer les comptes utilisateurs existants. Vous pouvez choisir de conserver les comptes utilisateurs et les mots de passe lors d'une restauration du micrologiciel. Les administrateurs peuvent également modifier les exigences en matière de complexité des mots de passe, afin de s'assurer que les utilisateurs créent des mots de passe complexes.

Lorsque vous créez de nouveaux utilisateurs, vous devez affecter un rôle à Security group : utilisateur, opérateur ou administrateur. Les groupes de sécurité sont associés à différents niveaux d'accès aux paramètres de la caméra. Voir [Security group sur la page 89](#) pour obtenir des informations sur l'accès et les autorisations.

Ajouter Users

Pour ajouter un nouvel utilisateur, procédez comme suit :

1. Accédez à la page *Utilisateurs* dans l'interface Web de la caméra.
2. Cliquez sur le bouton **Ajouter un nouvel utilisateur**.
3. Entrez Username.
4. Entrez Password.



TIP

Le mot de passe doit comporter des lettres majuscules, des lettres minuscules, des chiffres et des symboles. Vérifiez l'indicateur **Relative password strength** pour déterminer la force du mot de passe.

5. Saisissez une nouvelle fois le mot de passe pour confirmer.
6. Sélectionnez un groupe de sécurité dans le menu déroulant **Security group**.
7. Activez **Use PTZ controls** pour accorder à l'utilisateur le droit d'utiliser les commandes de caméra PTZ.
8. Cliquez sur **Save**.

Le nouvel utilisateur apparaîtra dans la liste Users.

Gestion des Users

Vous pouvez modifier et supprimer des comptes utilisateurs à la page *Users*.

- Pour modifier le Username du compte, cliquez sur l'icône  et saisissez le nouveau Username dans le champ.
- Pour supprimer un compte, cliquez sur l'icône , puis sur **Delete** dans la boîte de dialogue de confirmation.

Conservation des comptes utilisateurs lors de la restauration du micrologiciel

La page *Users* permet aux administrateurs d'effectuer des restaurations du micrologiciel dans le cadre du dépannage des problèmes liés aux caméras. Lorsqu'on effectue une restauration du micrologiciel, les comptes utilisateurs et les mots de passe sont supprimés de la caméra.

Veillez à sélectionner cette option avant de terminer la restauration du micrologiciel. Les comptes utilisateurs et les mots de passe ne peuvent pas être restaurés après la suppression des paramètres de la caméra.

- Pour éviter que les comptes utilisateurs et les mots de passe ne soient supprimés, veillez à cocher la case **Do not clear usernames or passwords on firmware revert** avant de terminer la restauration du micrologiciel.

Après la restauration du micrologiciel, vous devriez pouvoir voir les comptes utilisateurs et les mots de passe.

Modification du Password Complexity Requirements

La page *Users* permet aux administrateurs de modifier les exigences de complexité du mot de passe.

1. Entrez la longueur minimale du mot de passe (0 à 128 caractères) dans le champ **Minimum Length:**.
2. Entrez le nombre minimum de caractères majuscules (0 à 128 caractères) dans le champ **Uppercase:**.
3. Entrez le nombre minimum de caractères numériques (0 à 128 caractères) dans le champ **Number:**.
4. Entrez le nombre minimum de symboles (0 à 128 caractères) dans le champ **Symbols:**.
5. Cochez la case **Lock Password Complexity configuration** pour empêcher les autres utilisateurs de le modifier.
6. Cliquez sur **Save**.

Les utilisateurs et les opérateurs devront satisfaire à ces exigences lorsqu'ils modifieront leurs mots de passe.

Security group

Autorisations	User	Operator	Administrator
Live Preview	Yes	Yes	Yes
PTZ Controls	Yes ¹	Yes	Yes
General Settings	Non	Non	Yes
Network Settings	Non	Non	Yes
Image and Display	Non	Yes	Yes
Compression and Image Rate	Non	Yes	Yes
Motion Detection	Non	Yes	Yes
Tamper Detection	Non	Yes	Yes
Analytics	Non	Yes	Yes
Camera Automation	Non	Non	Yes
Privacy Zones	Non	Yes	Yes
Digital Inputs and Outputs	Non	Yes	Yes
Audio Settings	Non	Yes	Yes
Storage	Non	Yes ²	Yes
Licensing	Non	Non	Yes
Users	Non	Non	Yes
System	Non	Non	Yes
Device Logs	Non	Non	Yes

¹ Les utilisateurs peuvent utiliser les commandes PTZ si l'administrateur leur en donne l'autorisation.

² Les utilisateurs peuvent configurer les paramètres de stockage intégré, mais ne peuvent pas supprimer les enregistrements vidéo ni formater la carte SD.

About

Device Information

Nom	Nom de la caméra.
Location	Emplacement de la caméra
Part Number	Référence/modèle de la caméra.
Orderable Part Number	Référence alternative de la caméra.
Serial Number	Numéro de série unique de la caméra.
Device UUID	Identifiant unique universel
Firmware Version	Version de micrologiciel exécutée sur la caméra
Vasys Version	Version du logiciel Val System sur la caméra.
Build hash	Empreinte numérique unique pour cette version spécifique du logiciel ou du micrologiciel.
MAC Address	Identifiant unique et codé en dur affecté à un contrôleur d'interface réseau (NIC) sur la caméra.
Licenses	Bibliothèque de licences tierces pour les composants tiers et informations associées.
ONVIF Conformance	Profils ONVIF pris en charge par la caméra.
Power Source	Source d'alimentation alimentant actuellement la caméra.
Operation mode	Mode de fonctionnement actuel de la caméra.

Compte

Les *Users* vous permettent de modifier votre mot de passe ou de vous déconnecter de l'interface Web de la caméra. Cliquez sur l'icône  pour accéder à la page *Users*.

Modifier votre Password

Si vous vous souvenez de votre mot de passe actuel, vous pouvez le modifier lorsque vous êtes connecté à l'interface Web de la caméra. Si vous ne vous souvenez pas de votre mot de passe, vous devrez contacter votre administrateur système.

1. Sélectionnez l'icône  en haut à droite de la fenêtre.
2. Entrez votre mot de passe actuel dans le champ **Old Password**.
3. Entrez un nouveau mot de passe dans le champ **New Password**.
4. Vérifiez l'indicateur de force relative du mot de passe pour vous assurer que votre mot de passe est suffisamment fort.
5. Saisissez à nouveau le nouveau mot de passe dans le champ **Re-type password**.
6. Cliquez sur **Save**.

Votre nouveau mot de passe sera effectif lors de votre prochaine connexion.

Se déconnecter

La déconnexion de l'interface Web est très simple.

1. Pour vous déconnecter de l'interface Web, cliquez sur l'icône  en haut à droite de la fenêtre.
2. Cliquez sur **Logout**.



NOTE

Les utilisateurs seront automatiquement déconnectés de l'interface Web au bout de 15 minutes d'inactivité.

Déconnexion après utilisation de l'authentification unique

Lorsque vous vous déconnectez, vous êtes déconnecté à la fois de la caméra et du service de connexion externe.

Plus d'informations et d'assistance

Pour obtenir de la documentation supplémentaire sur le produit et des mises à jour du logiciel et du micrologiciel, rendez-vous sur [.pelco.com](https://pelco.com).

Assistance technique

Contactez l'assistance technique Pelco sur support.pelco.com/s/contactsupport.