Guide de l'utilisateur de Security Center 5.9

Date: 2023-12-25

1. Présentation de Security Desk

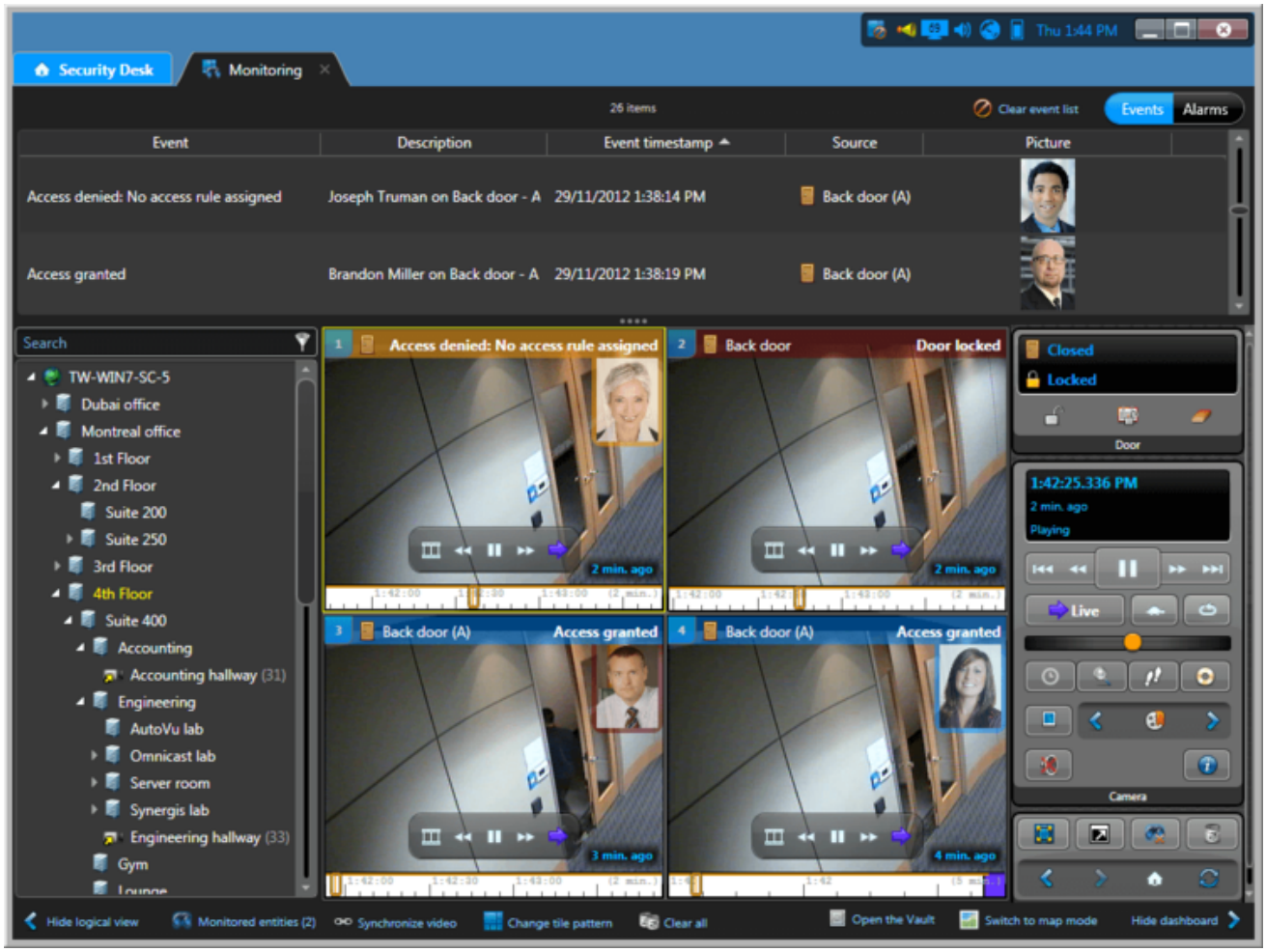
1 | Présentation de Security Desk

1.1 | Présentation rapide de Security Desk

1.1.1 | À propos de Security Desk

Security Desk est l'interface utilisateur unifiée de Security Center. Elle fournit un flux d'opérateurs cohérent à travers tous les systèmes principaux Security Center, Omnicast™, Synergis™, et AutoVu™. L'interface unique axée sur les tâches de Security Desk permet aux opérateurs de contrôler et de surveiller efficacement plusieurs applications de sécurité et de sûreté publique.

Au sein d'une même interface, vous pouvez suivre les événements et les alarmes en temps réel, créer des rapports, contrôler l'état des portes et suivre les titulaires de cartes ou encore visionner les flux vidéo en direct ou enregistrés. Lorsqu'il est connecté à une *Fédération* de plusieurs systèmes, Security Desk permet de gérer la surveillance, la création de rapports et les alarmes sur des dizaines ou des centaines de sites.



1.1.2 | Organisation de Security Center

Security Center est organisé par tâches. Les tâches peuvent être personnalisées et plusieurs tâches peuvent être effectuées en même temps. Vous ne verrez pas forcément toutes les tâches et commandes Security Center décrites dans ce guide, car leur disponibilité peut dépendre de votre licence et de vos privilèges d'utilisateur. Des privilèges d'utilisateur sont associés à chaque tâche et à de nombreuses commandes dans Security Center.

Les tâches sur la page d'accueil sont classées en trois catégories :

Administration
Config Tool seulement) Tâches de création et configuration des entités requises pour modéliser votre système.

Exploitation
Tâches liées aux opérations Security Center quotidiennes.

Investigation
Security Desk seulement) Tâches permettant de rechercher des informations dans les bases de données de Security Center ou des systèmes fédérés.

Maintenance
Tâches dédiées à la maintenance et au dépannage.
Chaque catégorie principale est divisée en sous-catégories comme suit :

Tâches communes
Tâches partagées par les trois modules logiciels de Security Center. Ces tâches sont toujours disponibles, quels que soient les modules pris en charge par votre licence logicielle.

Contrôle d'accès
Tâches dédiées au contrôle d'accès. Les tâches de contrôle d'accès ont des icônes soulignées en rouge. Elles ne sont disponibles que si *Synergis*™ est pris en charge par votre licence logicielle.

RAPI
tâches liées aux opérations de *Reconnaissance automatique de plaques d'immatriculation (RAPI)*. Les tâches de RAPI ont des icônes soulignées en orange. Elles ne sont disponibles que si *AutoVu*™ est pris en charge par votre licence logicielle.

Vidéo
Tâches dédiées à la gestion de la vidéo. Les tâches vidéo ont des icônes soulignées en vert. Elles ne sont disponibles que si *Omnicast*™ est pris en charge par votre licence logicielle.

1.1.3 | Se connecter à Security Center via Security Desk

Pour vous connecter à Security Center, vous devez ouvrir l'application Security Desk et vous connecter au Répertoire Security Center.

Avant de commencer

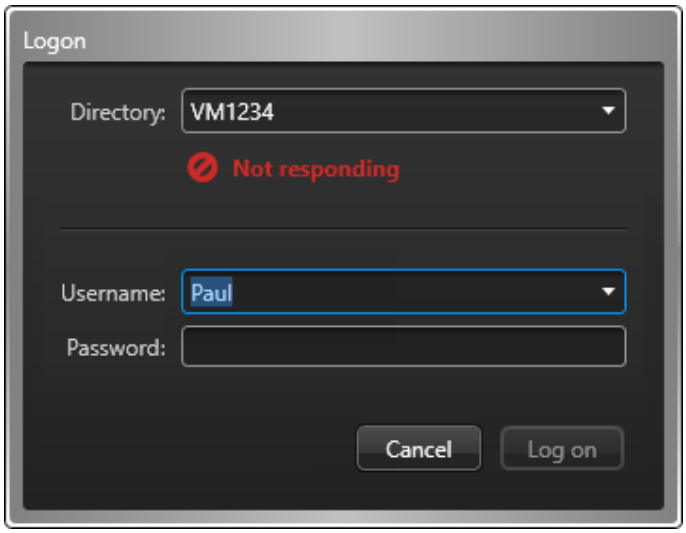
Vous devez disposer de votre nom d'utilisateur et mot de passe et du nom du *Directory* auquel vous voulez vous connecter.

À savoir

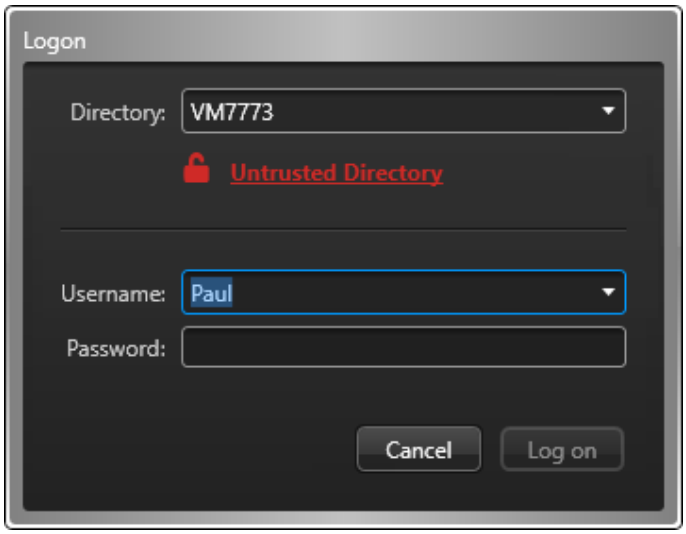
Une fois que vous êtes connecté, vous pouvez vous déconnecter du Répertoire sans fermer Security Desk. Se déconnecter sans quitter est utile si vous souhaitez vous reconnecter avec d'autres identifiants.

Procédure

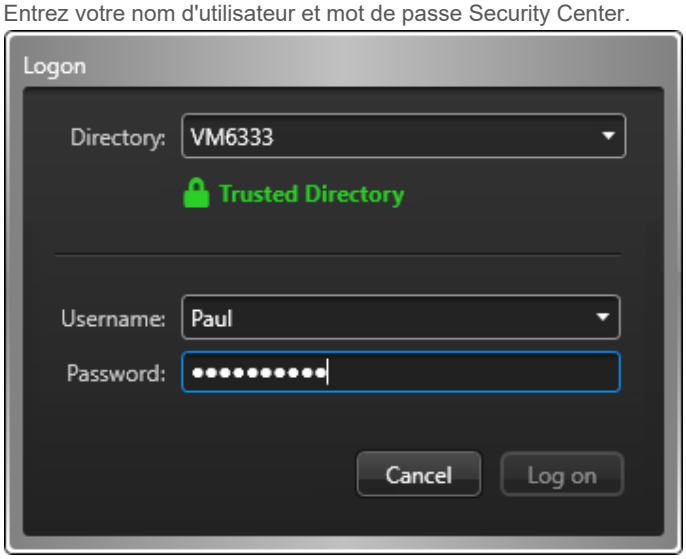
1. Ouvrez Security Desk.
    a. Jusqu'à Windows 8, cliquez sur Démarrer > Tous les programmes > GenetecSecurity Center 5.9 > Security Desk
    b. Sous Windows 10, cliquez sur Démarrer > GenetecSecurity Center 5.9 > Security Desk
2. Dans la boîte de dialogue Connexion, entrez le nom du Répertoire.
   Si le Répertoire ne répond pas, vérifiez l'orthographe ou contactez votre administrateur.



Si le Répertoire n’est pas fiable, cela peut indiquer une attaque de type man-in-the-middle. Ne faites rien sans le feu vert de votre administrateur.

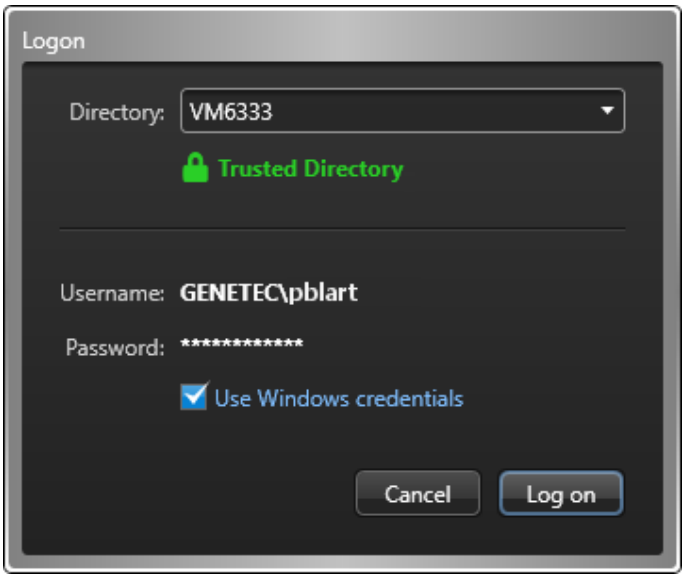


3. Entrez votre nom d'utilisateur et mot de passe Security Center.

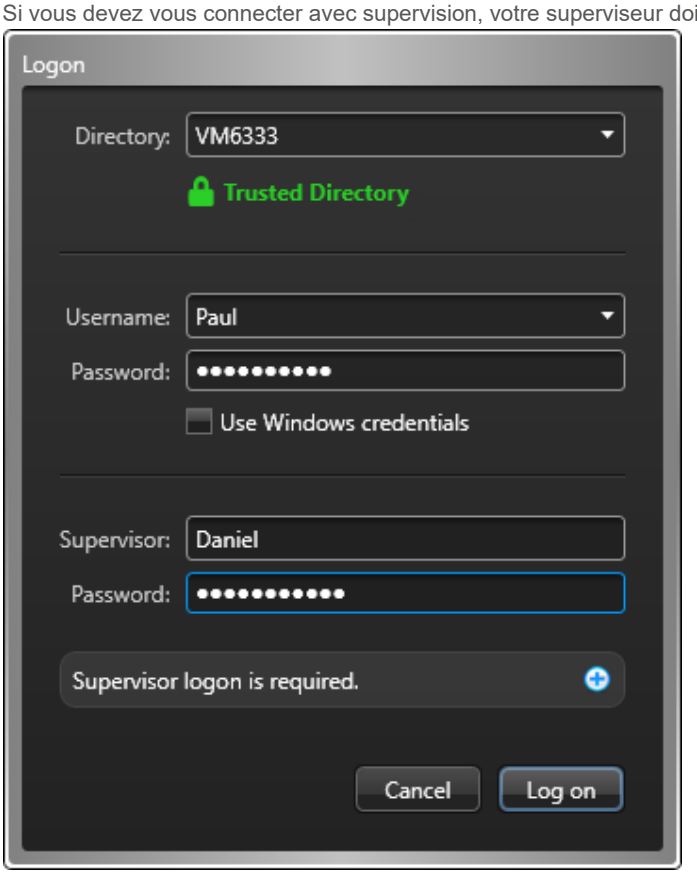


Si l’authentification unique est déployée, vous devez cliquer sur Connexion pour votre *fournisseur d'identité* ou ajouter le nom de domaine à la fin de votre nom d’utilisateur, sous la forme `nom_utilisateur@nom_domaine`. Vous serez ensuite redirigé vers votre fournisseur d'identité pour l'authentification. Passez à Connexion à l'aide de l'authentification Web.

4. Pour vous connecter avec votre compte utilisateur Windows, sélectionnez Utiliser la sécurité Windows.
   Cette option n’est disponible que si Active Directory est configuré sur votre système.



5. Cliquez sur Connexion.
6. Si vous devez vous connecter avec supervision, votre superviseur doit fournir un nom d'utilisateur et mot de passe.



7. Cliquez sur Connexion.
   Security Desk est lancé.
   REMARQUE : Après une période d'inactivité, votre session Security Desk peut être verrouillée. Vous devez alors saisir à nouveau vos identifiants pour utiliser l'application.
8. Pour vous déconnecter, cliquez sur l'onglet accueil ( ), puis cliquez sur Déconnexion.
   Par défaut, vous êtes invité à enregistrer votre espace de travail lorsque vous vous déconnectez de Security Desk. Vous pouvez modifier ce comportement dans la section Interaction utilisateur de la boîte de dialogue Options.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

1.1.3.1 | Connexion à l'aide de l'authentification Web

Si vous cliquez sur le bouton Connexion ou si Security Center détecte que l'authentification Web est activée pour votre domaine, vous serez redirigé vers un formulaire Web pour saisir vos identifiants.

Avant de commencer

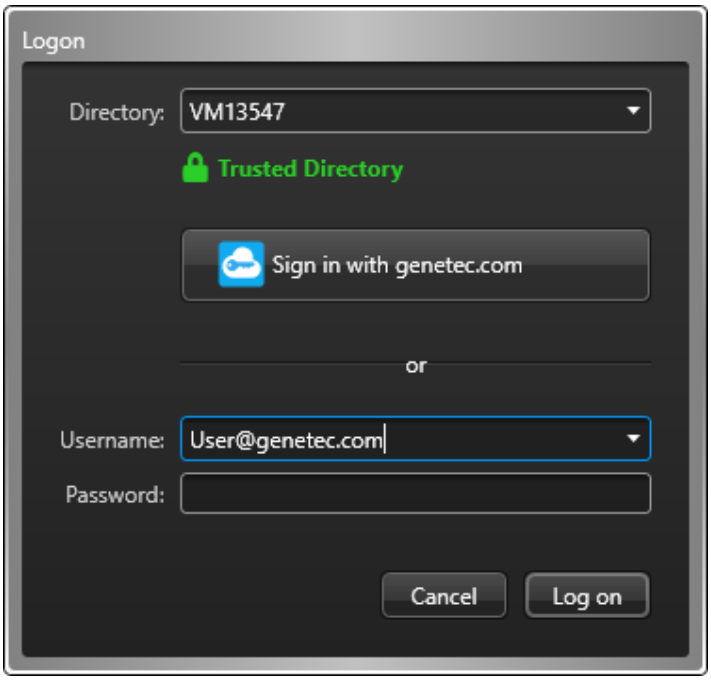
Ouvrez Security Desk et entrez le nom du Répertoire dans la boîte de dialogue Connexion.

À savoir

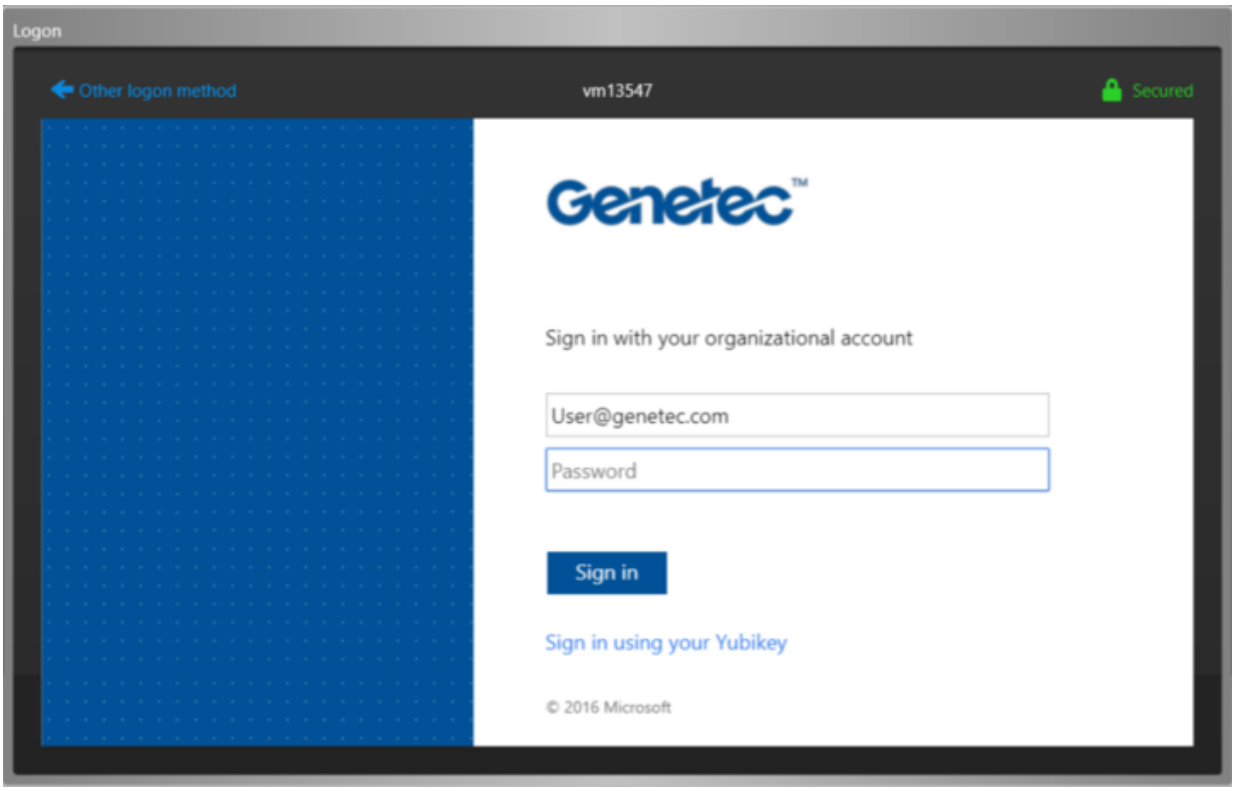
On parle d'authentification basée sur le Web (ou authentification passive) lorsque l'application client redirige l'utilisateur vers un formulaire web géré par un fournisseur d'identité de confiance. Le fournisseur d'identité peut demander différents types d'identifiants (mots de passe, jetons de sécurité, vérifications biométriques, et ainsi de suite) pour créer une protection multi-couches contre les accès illicites. Également appelé authentification à plusieurs facteurs.
REMARQUE : Security Desk mémorise tous les paramètres de connexion valides et rappelle automatiquement ceux utilisés pour la dernière tentative de connexion.

Procédure

1. Dans le champ Nom d'utilisateur, saisissez votre nom d'utilisateur, suivi du nom de domaine au format *NomUtilisateur@NomDomaine* ou cliquez sur le bouton Connexion de votre fournisseur d'identité.



2. Si vous avez saisi votre nom d'utilisateur et votre domaine, cliquez sur le champ Mot de passe ou appuyez sur la touche Tab.
   Si Security Center détecte que l'*authentification Web* est activée pour votre domaine, vous êtes redirigé vers un formulaire Web. La capture d'écran suivante fournit un exemple. L'aspect de votre page de connexion peut être différent.



3. Dans le formulaire Web, saisissez les informations nécessaires et cliquez sur Connexion.

Sujet parent : Se connecter à Security Center via Security Desk

1.1.4 | Fermer Security Desk

Vous pouvez fermer Security Desk et enregistrer votre espace de travail, qui sera rétabli à la connexion suivante.

À savoir

Par défaut, vous êtes invité à enregistrer votre espace de travail lorsque vous fermez Security Desk. Vous pouvez modifier ce comportement dans la section Interaction utilisateur de la boîte de dialogue Options.

Procédure

1. Cliquez sur le bouton Quitter () dans le coin supérieur droit de la fenêtre de Security Desk.
   Vous êtes alors invité à enregistrer les tâches en cours dans votre espace de travail.
2. Cliquez sur Enregistrer pour charger automatiquement la liste de tâches actuelle lors de l'ouverture suivante de Security Desk.

1.1.4.1 | Enregistrer automatiquement votre espace de travail à la fermeture du client

Lorsque vous fermez l'application client, vous êtes invité à enregistrer les modifications apportées à votre espace de travail. Vous pouvez configurer l'application client pour enregistrer ou abandonner automatiquement les modifications.

À savoir

Ce réglage est conservé dans votre profil utilisateur et s'applique à Security Desk et Config Tool.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Interaction utilisateur.
2. Dans la section Avant de fermer l'application, cliquez sur Enregistrer la liste des tâches et sélectionnez l'une des options suivantes :
   - Demander à l'utilisateur : Toujours demander avant d'enregistrer l'espace de travail.
   - Oui : Toujours enregistrer l'espace de travail sans confirmation.
   - Non : Ne jamais enregistrer l'espace de travail.
3. Cliquez sur Enregistrer.

Sujet parent : Fermer Security Desk

1.1.5 | Présentation de la page d'accueil

La page d'accueil est la page principale dans Security Center. Ouvrez la page d'accueil en cliquant sur l'onglet Accueil ().

A	Champ de recherche	Tapez le nom de la tâche recherchée. Les tâches correspondantes (texte trouvé dans la catégorie, le nom ou la description) sont affichées.
B	Tâches privées	Affiche les tâches enregistrées que vous avez créées et qui ne sont visibles que par votre utilisateur.
C	Tâches publiques	Affiche les tâches partagées par plusieurs utilisateurs Security Center.
D	Outils	Affiche les outils Security Center standard, les outils externes et les applications que vous pouvez lancer depuis votre page d'accueil.
E	Options	Configurez les options pour votre application.
F	Favoris et Éléments récents	Affiche les tâches et les outils utilisés récemment ou que vous avez ajoutés à vos Favoris.
G	**Zone de notification**	Affiche des informations importantes à propos de votre installation. Survolez une icône pour afficher des informations système, ou cliquez deux fois pour effectuer une action.
H	**Onglets des tâches**	Affiche les tâches ouvertes dans des onglets individuels. Cliquez pour basculer entre les tâches.
I	**Page Tâches**	Affiche toutes les tâches disponibles. Sélectionnez une tâche à ouvrir. Si vous avez plusieurs instances de la tâche, vous êtes invité à taper un nom.

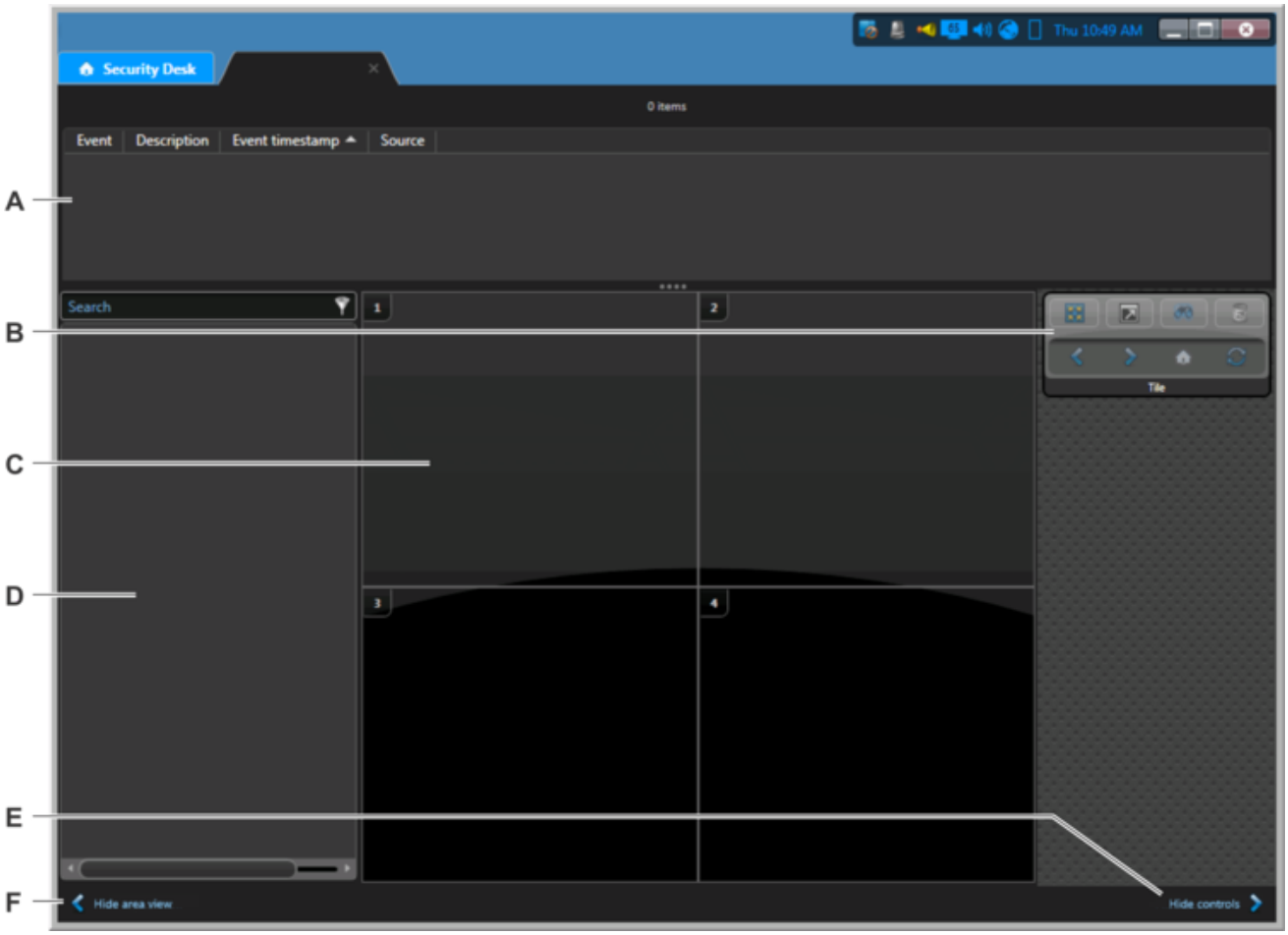
Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Configurer la zone de notification
- Enregistrer une tâche dans Security Center
- Ouvrir les tâches
- Raccourcis vers des outils externes

1.1.6 | Présentation des éléments d'interface

Security Desk offre une interface utilisateur standard dans la tâche Surveillance et la plupart des tâches de rapport qui est divisée en quatre parties principales : la Vue secteur, le Volet de rapport, le Canevas et les Commandes.



A	Volet de rapport	Affiche des événements, alarmes actives ou résultats de recherche sous forme de tableau, selon la tâche utilisée. Les informations sont affichées sous forme de texte ou de graphiques (photo du détenteur de carte, frise chronologique, et ainsi de suite).
B	Commandes	Contient des widgets qui correspondent au type d'entité affiché dans la taille sélectionnée sur le canevas.
C	Canevas	Permet d'afficher et de contrôler les entités dans *mode Tuile* ou *mode Carte*.
D	Vue secteur	Affiche la liste des entités qui composent votre système, et que vous pouvez faire glisser sur le canevas.
E	Masquer les commandes	Cliquez pour afficher ou masquer les commandes.
F	Masquer la vue secteur	Cliquez pour afficher ou masquer la vue secteur.

Regardez cette vidéo pour en savoir plus.

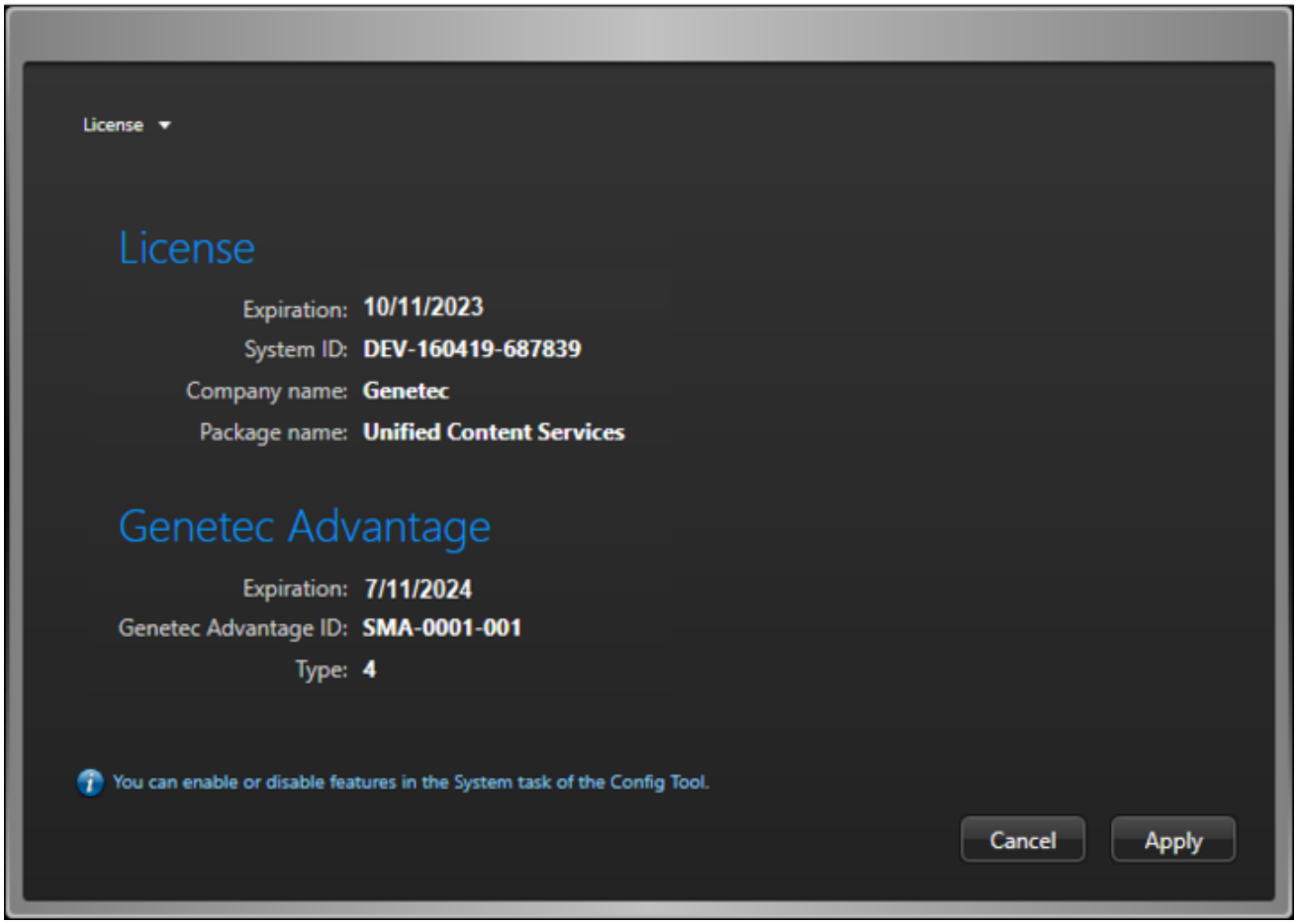
Explorer

- Surveiller les événements de RAPI dans mode Carte

1.1.7 | Présentation de la page À propos

La page À propos contient des informations sur votre logiciel Security Center, comme la licence achetée, le numéro de CMA, la date d'expiration de la licence, la version du logiciel, etc.

Les options de licence sont soit prises en charge, non prises en charge ou soumises à un seuil d'utilisation. Pour les options limitées par un seuil d'utilisation, Config Tool affiche l'utilisation actuelle rapportée au plafond autorisé.



Selon les options de votre licence, les onglets suivants sont disponibles :

Licence
Indique la date d'expiration de la licence et les informations dont vous aurez besoin si vous contactez le centre d'assistance technique de Genetec™ : ID système, Nom de la société, Nom du forfait et numéro de Contrat de maintenance applicative (CMA). IMPORTANT : Trente jours avant l'expiration de votre licence ou de votre CMA, vous recevrez un message dans Config Tool vous alertant de l'expiration imminente. Config Tool se connecte à GTAP pour valider le SMA.

Security Center
Cet onglet affiche toutes les options Security Center génériques.

Synergis
Cet onglet affiche toutes les options de contrôle d'accès. Il n'est affiché que si le *contrôle d'accès Synergis*™ est pris en charge.

Omnicast
Cet onglet affiche toutes les options vidéo. Il n'est affiché que si la *vidéosurveillance Omnicast* est prise en charge.

AutoVu
Cet onglet affiche toutes les options de RAPI. Il n'est affiché que si la *RAPI AutoVu* est prise en charge.

Plan Manager
Cet onglet contient les options de Plan Manager.

Mobile
Cet onglet affiche toutes les options de contrôle d'accès Web et mobile Security Center.

Certificats
Cet onglet dresse la liste des *certificats de SDK* inclus dans la clé de licence.

Bon de commande
Cet onglet reproduit votre commande.

Les boutons suivants sont également disponibles sur la page À propos :

Aide
Cliquez pour ouvrir l'aide en ligne. Vous pouvez aussi cliquer sur F1.

Changer de mot de passe
Cliquez pour modifier votre mot de passe.

Nous contacter
Cliquez pour visiter GTAP ou le forum GTAP. Vous devez disposer d'une connexion Internet pour visiter ces sites web.

Composants installés
Cliquez pour afficher le nom et la version de tous les composants logiciels installés (fichiers DLL).

Copyright
Afficher les informations de copyright concernant le logiciel.

Envoyer un commentaire
Cliquez pour nous envoyer vos commentaires.
Explorer

- Changer de mot de passe
- Envoi de commentaire

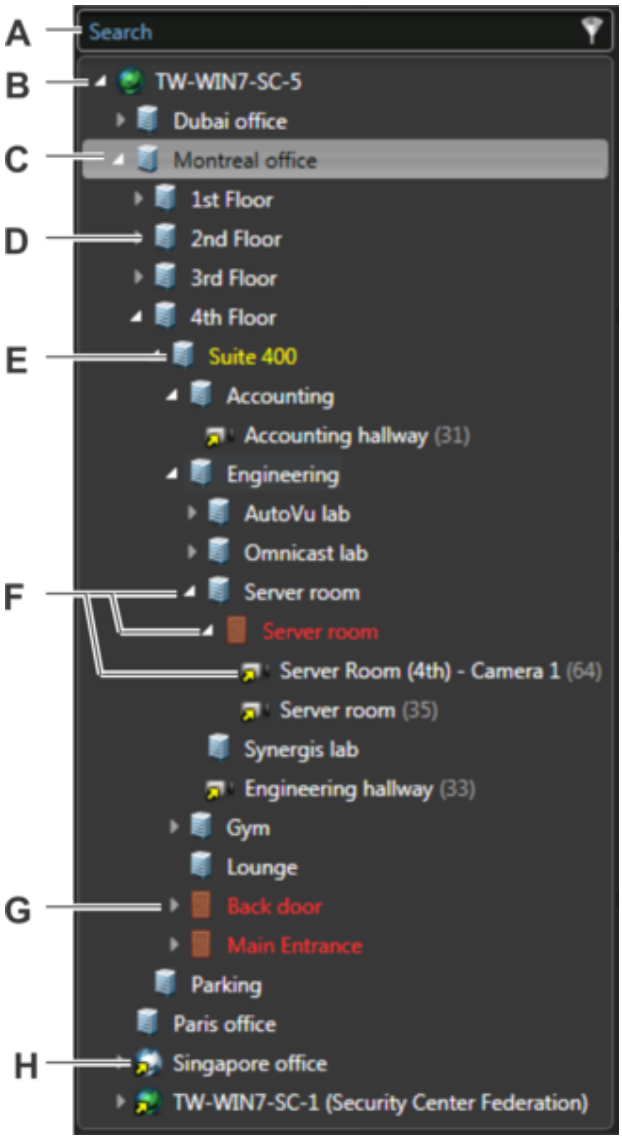
1.1.8 | À propos de la vue secteur dans Security Desk

La vue secteur permet de rechercher et d'afficher de manière simple et rapide toutes les entités du système.

Les *entités* de la vue secteur sont classées hiérarchiquement sous forme d'une *arborescence d'entités*, en fonction de leurs relations logiques avec les *secteurs*. Par exemple, les portes menant à un secteur, ainsi que d'autres périphériques situés dans ce secteur comme des caméras, sont affichées en tant qu'*entités enfant* du secteur, directement sous le secteur dans l'arborescence.

Dans la vue secteur, vous pouvez effectuer les tâches suivantes :

- Rechercher des entités à afficher sur le canevas.
- Faire glisser une entité de la vue secteur vers le canevas.
- Renommer les entités locales.
- Basculer vers la page de configuration des entités, si vous disposez des privilèges adéquats.



A	Champ de recherche	Tapez dans le champ Rechercher pour rechercher les entités qui contiennent le texte correspondant dans leur catégorie, nom ou description.
B	Entité Système	L'entité système ( ) ne peut pas être affichée sur le canevas.
C	Configurer les entités	Faites un clic droit sur une entité dans la vue secteur, puis cliquez sur Configurer une entité ( ) pour basculer vers la page de configuration de l'entité dans Config Tool. Vous devez disposer du privilège d'utilisateur de modification d'entités pour utiliser cette commande.
D	Entité secteur	Les entités Secteur ( ) peuvent représenter une notion ou un lieu physique. Il s'agit d'un regroupement logique.
E	Entité jaune	Lorsqu'un nom d'entité est affiché en jaune, cela indique un problème avec les paramètres associés.
F	Flèches	Cliquez sur les flèches de l'arborescence pour afficher ou masquer des entités enfant.
G	Entité rouge	Indique que l'entité est hors ligne et que le serveur ne parvient pas à s'y connecter, ou que le serveur est hors ligne.
H	Entité fédérée	Les entités importées depuis les *systèmes fédérés* sont indiquées par une petite flèche jaune sur leur icône ( ). Ces entités sont appelées *entités fédérées*.

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Afficher une entité sur le canevas
- Rechercher des entités
- États des entités

1.1.9 | Changer de mot de passe

Une fois que vous êtes connecté à Security Center, vous pouvez modifier votre mot de passe.

À savoir

Il est recommandé de changer régulièrement de mot de passe.

Procédure

1. Sur la page d'accueil, cliquez sur À propos.
2. Sur la page À propos, cliquez sur Modifier le mot de passe.
3. Dans la boîte de dialogue Changer de mot de passe, entrez l'ancien mot de passe, puis entrez et confirmez le nouveau mot de passe.
4. Cliquez sur OK.

1.1.10 | Envoi de commentaire

Vous pouvez envoyer un commentaire à Genetec Inc. si vous souhaitez attirer notre attention sur quelque chose, comme un problème d'interface ou de compréhension d'un réglage.

Procédure

1. Sur la page d'accueil, cliquez sur À propos > Envoyer un commentaire.
2. Tapez votre message dans la boîte de dialogue Envoyer un commentaire.

3. Pour ajouter une pièce jointe, cliquez sur Pièces jointes et faites un choix parmi les options suivantes :
   - Pour joindre des informations sur le système, sélectionnez Informations système.
   - Pour joindre un fichier, tel qu'un fichier journal, sélectionnez Fichiers, cliquez sur , sélectionnez un fichier, puis cliquez sur Ouvrir.
   - Pour joindre une capture de l'écran actuel, sélectionnez Captures d'écran, puis cliquez sur .
     CONSEIL : Vous pouvez déplacer la boîte de dialogue pour naviguer jusqu'à l'écran pertinent et capturer l'écran sans fermer la boîte de dialogue.
4. Cliquez sur Envoyer.

1.2 | Canevas Security Center dans Security Desk

1.2.1 | À propos des tuiles

Une tuile est une fenêtre individuelle dans le canevas, utilisée pour afficher une seule entité. L'entité affichée est généralement la vidéo d'une caméra, une carte ou tout autre élément de nature graphique. Son aspect dépend de l'entité affichée.

Les tuiles peuvent afficher les éléments suivants :

- Entités
- Informations sur l'événement
- Vidéo en temps réel et enregistrée
- Images vidéo
- Photos et informations de titulaires de cartes et visiteurs
- Lectures de RAPI
- Pages web
- Modules externes de tuile
- cartes

Le contenu est automatiquement affiché dans les tuiles lorsque des événements associés aux entités que vous surveillez surviennent. Vous pouvez également afficher des entités en les faisant glisser sur une tuile. Security Desk Les tuiles sont dotées d'une *mémoire de tuile* qui permet à Security Desk de mémoriser les 8 dernières entités affichées dans chaque tuile. Les commandes du widget de tuile permettent d'afficher le contenu précédent, suivant et initial de la tuile.

Faites un clic droit sur une tuile pour afficher les commandes du menu de la tuile.

La figure suivante montre une tuile affichant une caméra.

A	ID de tuile	L'ID de tuile est le numéro affiché dans le coin supérieur gauche de la tuile. Ce numéro identifie de manière unique la tuile sur le canevas. Si l'ID de la tuile est affiché en bleu, cela signifie que la surveillance d'événements est activée pour la tuile. Il est affiché en noir lorsque la surveillance est désactivée. Si elle est rouge avec une fine bordure bleue, la surveillance d'événements et d'alarmes est activée pour la tuile.
B	Barre d'outils de tuile	Affiche l'entité par nom. En cas d'événement, les informations correspondantes sont également affichées dans la barre d'outils de la tuile.
C	Cadre jaune	Indique que la tuile est sélectionnée.
D	Flux vidéo	La vidéo diffusée est affichée dans la tuile. Cliquez deux fois pour remplir le canevas avec le contenu de la tuile.
E	Commandes vidéo intégrées à la tuile	Utilisez les commandes vidéo intégrées à la tuile lorsque vous visionnez de la vidéo dans une tuile.
F	État de l'enregistrement	État d'enregistrement actuel d'une caméra donnée. Il existe quatre états d'enregistrement : *activé*, *désactivé*, *enregistrement en cours (déverrouillé)* et *enregistrement en cours (verrouillé)*. Vert indique qu'elle n'enregistre pas. Rouge indique qu'elle enregistre.
G	Frise chronologique	Représentation graphique d'une séquence vidéo, avec des repères temporels représentant du mouvement et des signets. Des vignettes peuvent être ajoutées à la frise pour aider à identifier les sections dignes d'intérêt. Utilisez la frise chronologique pour contrôler la vidéo enregistrée.

Explorer

- Personnaliser l'affichage des tuiles dans Security Center

1.2.2 | Commandes du menu de tuile

Vous pouvez contrôler les tuiles et les entités qu'elles contiennent avec les commandes disponibles dans le menu de la tuile.

Certaines commandes sont toujours disponibles, tandis que d'autres commandes sont contextuelles et varient en fonction du type d'entité affiché dans la tuile. Le tableau suivant présente les commandes du menu de la tuile.

Commande		Description
Caméra		Commandes relatives à la vidéosurveillance. Les autres commandes de caméra sont disponibles dans le widget Caméra.
	Enregistrement auxiliaire	Si la caméra est contrôlée par un Archiveur auxiliaire, démarrez l'enregistrement manuellement sur l'Archiveur auxiliaire en cliquant sur le bouton enregistrer () en regard du nom du rôle Archiveur auxiliaire.
	 Protéger la vidéo contre l'effacement	Protège l'enregistrement vidéo actuel contre la suppression en fonction des contraintes d'espace disque du rôle Archiveur. Cette commande n'est disponible que lorsque du contenu vidéo est affiché dans la tuile.
	 Supprimer la protection de confidentialité	Affiche le flux vidéo confidentiel (privé) qui contient la vidéo d'origine provenant de l'unité vidéo, sans floutage ou censure.

Commande		Description
	Rétablir la protection de confidentialité	Affiche le flux vidéo public qui contient le contenu flouté par la protection de la confidentialité avec application de l'anonymisation vidéo. Tous les accès normaux à la vidéo accéderont alors toujours à la vidéo floutée.
	Bloquer	Empêcher les utilisateurs d'afficher le flux vidéo sélectionné. Cette commande n'est disponible que lorsque du contenu vidéo est affiché dans la tuile.
	Débloquer	Empêcher les utilisateurs d'afficher le flux vidéo sélectionné. Cette commande n'est disponible que lorsque du contenu vidéo est affiché dans la tuile.
	Sélectionner le flux en direct	Sélectionnez le flux vidéo provenant de la caméra et que vous souhaitez afficher dans la tuile. Le flux Temps réel est affiché par défaut. Cette commande n'est disponible que lorsque de la vidéo en direct est affichée dans la tuile, et que l'unité vidéo prend en charge plusieurs flux.
	Sélectionner la source de lecture vidéo	Sélectionnez la source d'archivage pour la lecture vidéo (Archiveur ou Archiveurs auxiliaires). Par exemple, si vous souhaitez exporter une séquence vidéo avec une résolution, une vitesse ou un flux vidéo particulier, sélectionnez l'Archiveur configuré avec les réglages correspondants. Par défaut, l'option Toutes les sources est affichée. Cette commande n'est disponible que lorsque de la vidéo enregistrée est affichée dans la tuile.
	Commandes	Commandes supplémentaires relatives aux caméras (lire un clip audio, activer la lumière blanche, autofocus, et ainsi de suite). Ces commandes de caméra contextuelles sont actuellement prises en charge pour certaines caméras Axis, Panasonic et Bosch.
Surveillance	Surveiller les alarmes	Activer ou désactiver la surveillance d'alarmes dans la tuile. Une coche bleue indique que la surveillance d'alarmes est activée.
	Surveiller les événements	Activer ou désactiver la surveillance d'événements dans la tuile. Une coche bleue indique que la surveillance d'événements est activée.
Analyser		Permet d'ouvrir une tâche d'*Investigation* basée sur l'entité sélectionnée. Cette entité sera déjà sélectionnée dans les filtres de recherche.
Signaler un incident		Créez un rapport d'incident pour signaler quelque chose que vous observez dans la tuile.
Démarrer l'enregistrement d'incident		Lancez l'enregistrement vidéo pour toutes les entités placées dans la tuile (caméras, secteurs, portes, titulaires de cartes, et ainsi de suite) pour créer un rapport d'incident.
Agrandir la tuile		Agrandissez la tuile actuelle pour remplir le canevas. Masque toutes les autres tuiles.
Passer la tuile en plein écran		Masquez la vue secteur et les commandes, et remplissez le canevas avec la tuile actuelle. Force l'affichage de la tuile en mode plein écran.
Naviguer	Précédent	Afficher le contenu précédent de la tuile.
	Avance rapide	Afficher le contenu suivant de la tuile.
	Accueil	Afficher le contenu initial de la tuile.

Commande	Description
Actualiser	Actualiser le contenu de la tuile.
Ajouter au tableau de bord	Seulement pour les entités Security Center. Ajoute l'entité au tableau de bord en tant que Widget Tuile.
Effacer tout	Effacer le contenu des tuiles.

1.2.3 | Afficher une entité sur le canevas

Vous pouvez afficher une entité sur le canevas depuis la vue secteur ou le volet de rapport.

À savoir

Toutes les entités affichées dans la vue secteur et certains événements et entités dans le volet de rapport peuvent être affichés dans une tuile du canevas, à l'exception de l'entité Système ( ). Les entités peuvent également apparaître automatiquement dans une tuile lorsqu'un événement survient.

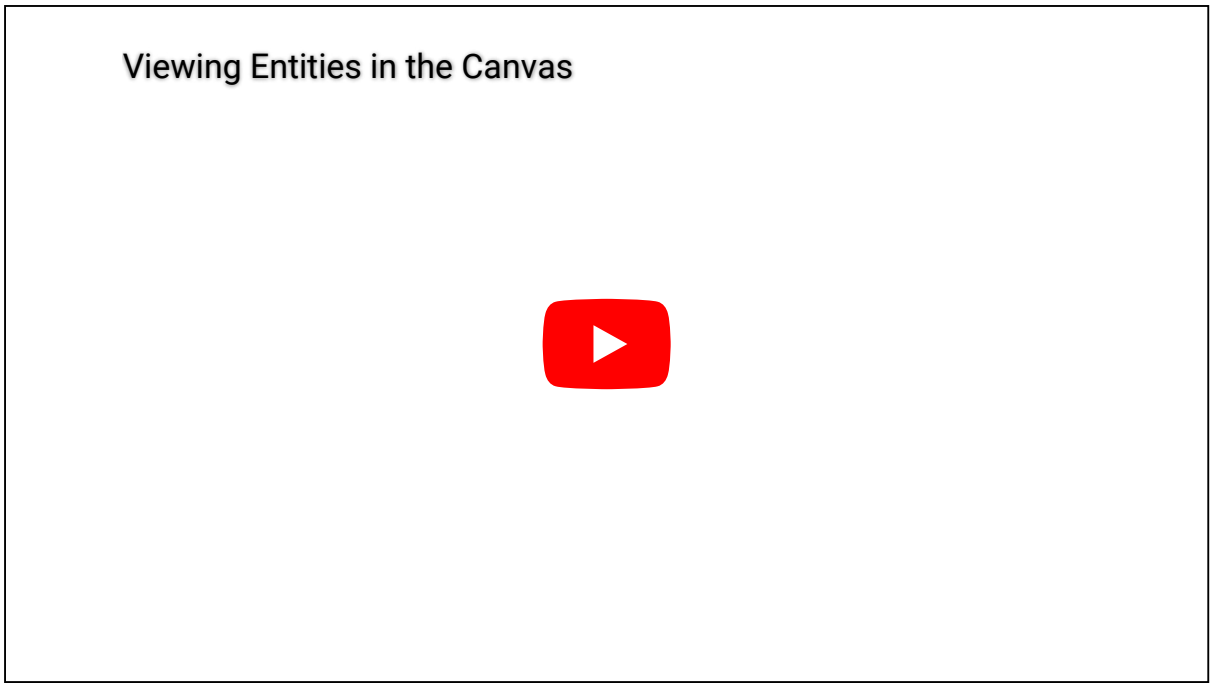
Le cas échéant, vous pouvez afficher des informations complémentaires en regard des entités dans la vue secteur en personnalisant l'affichage des entités.

Procédure

1. Dans la vue secteur ou le volet de rapport, procédez de l'une des manières suivantes :
   - Pour afficher une seule entité, cliquez deux fois sur l'entité ou faites-la glisser sur une tuile.
   - Pour afficher plusieurs entités, appuyez sur les touches Ctrl ou Maj pendant que vous sélectionnez les entités, puis faites glisser les entités sur une tuile. Cette méthode ne fonctionne que si vous disposez de suffisamment de tuiles vides.
2. Pour contrôler les entités, faites un clic droit dans la tuile et utilisez les commandes du menu, ou utilisez les widgets du volet Commandes.
3. Pour effacer les entités du canevas, procédez de l'une des manières suivantes :
   - Faites un clic droit sur une tuile et sélectionnez Effacer ( ).
   - Sélectionnez une tuile et appuyez sur la touche Retour arrière.
   - (Vide toutes les tuiles) En bas du canevas, cliquez sur Effacer tout ( ).
   - (Vide toutes les tuiles) Appuyez sur Ctrl+Retour arrière.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



Explorer

- États des entités

1.2.3.1 | Personnaliser l'affichage des entités sur le canevas

Vous pouvez afficher l'ID logique (un numéro d'identification unique) des entités dans la vue secteur pour vous aider à les identifier. Vous pouvez également savoir depuis quel *Active Directory (AD)* l'entité a été importée.

À savoir

Ces réglages sont conservés dans votre profil utilisateur et s'appliquent à Security Desk et Config Tool.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Interaction utilisateur.
2. Pour afficher l'ID logique entre parenthèses après le nom de l'entité, sélectionnez l'option Afficher l'ID logique.
3. Pour afficher le nom d'utilisateur et le nom de domaine Active Directory, sélectionnez l'option Montrer le nom de domaine Active Directory si pertinent.
4. Cliquez sur Enregistrer.

Sujet parent : Afficher une entité sur le canevas

1.2.4 | Développer le contenu d'une tuile

Lorsqu'une entité est affichée dans une tuile associée à d'autres entités, vous pouvez développer l'entité et afficher toutes les entités associées dans des tuiles distinctes.

À savoir

Les entités associées à plusieurs entités sont appelées des *entités composites* (par exemple, une porte associée à plusieurs caméras). Si vous surveillez la porte et qu'un événement survient, seule la première caméra est affichée, car les autres caméras sont *réduites*. Si vous développez la porte, vous pouvez afficher toutes les caméras dans des tuiles distinctes.
Limitation : Limité à 16 éléments non développés.

Procédure

1. Sélectionnez une tuile qui affiche une entité composite.
2. Cliquez sur en regard du nom de l'entité dans la barre d'outils de la tuile.
3. Dans le menu déroulant, sélectionnez un des éléments suivants :

   - Une caméra associée (par exemple *Main Entrance* ou *Front Hallway*).

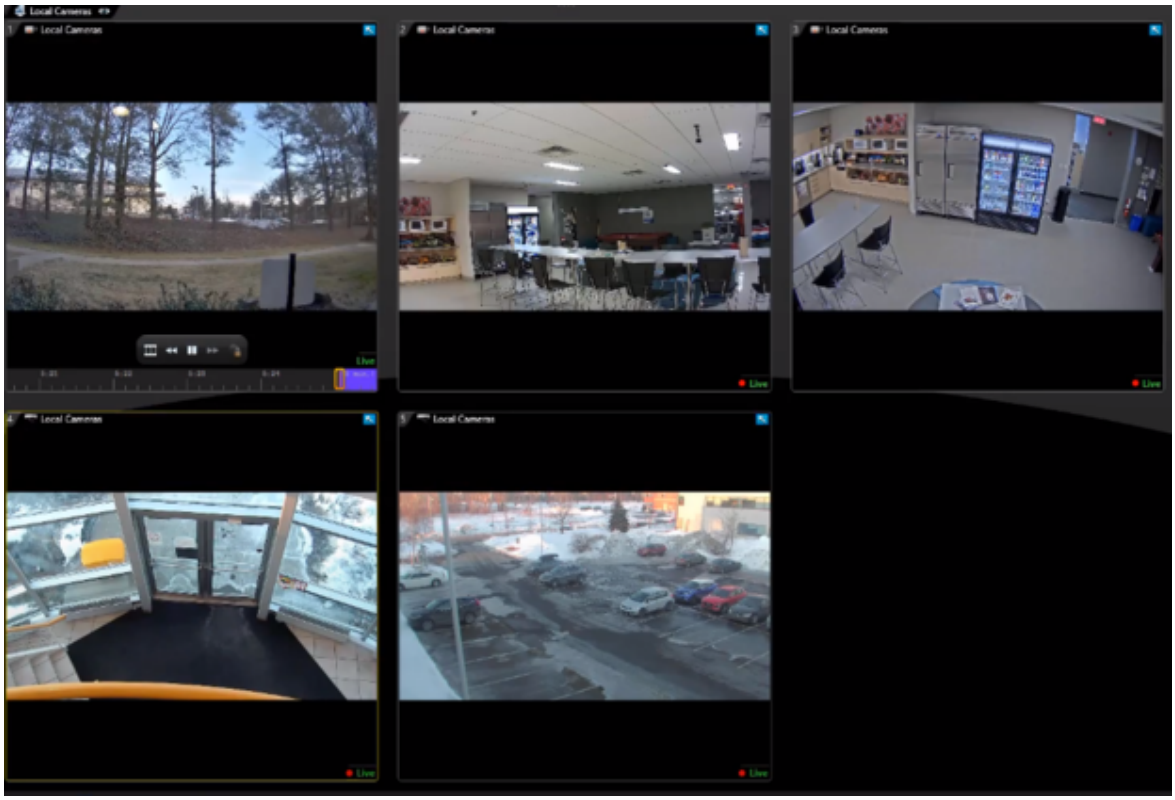
   Développer
   Afficher toutes les entités associées à l'entité sélectionnée dans des tuiles distinctes.

   Démarrer le cycle
   Faites défiler les entités associées à l'entité composite dans la tuile. La durée d'affichage de chaque entité est configurée dans la boîte de dialogue Options.
   REMARQUE : Lorsqu'une caméra PTZ est associée à l'entité composite et que vous commencez à activer le PTZ, le cycle s'interrompt. Vous pouvez cliquer sur Démarrer le cycle une fois que vous avez fini d'utiliser le PTZ.

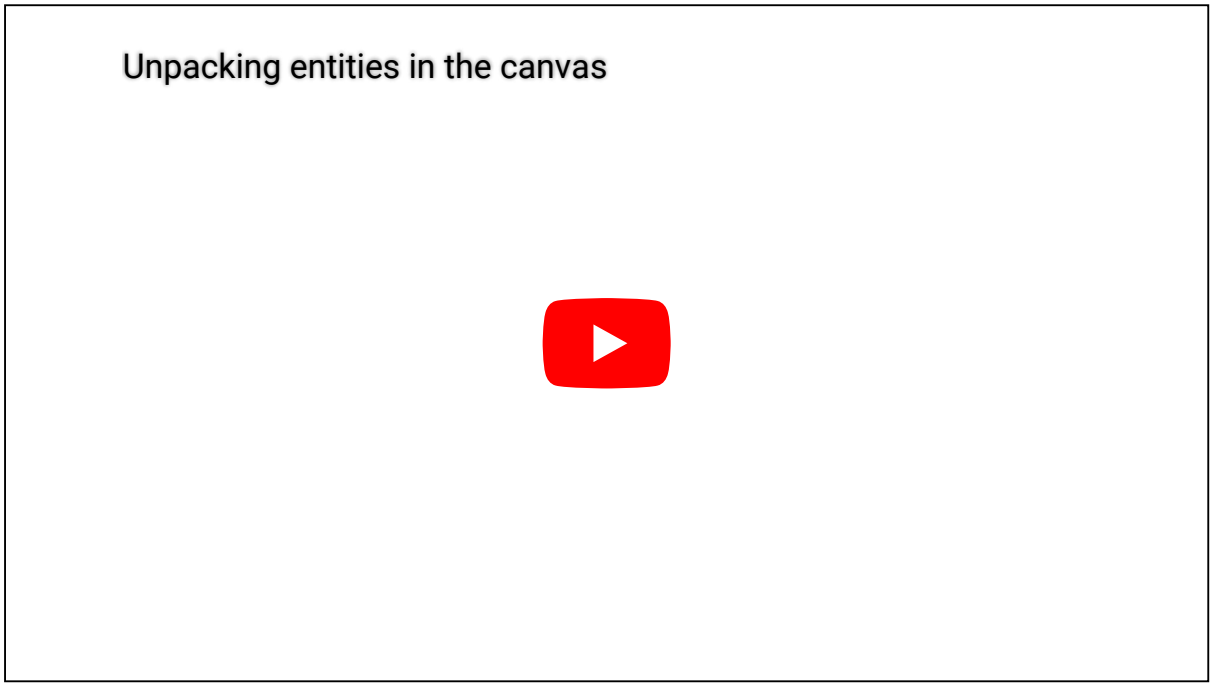
4. Pour réduire les tuiles une fois que vous avez vu ce que vous vouliez voir, cliquez sur Réduire ( ) dans l'angle supérieur gauche de la tuile.

Exemple

La porte *Main Entrance* est associée à deux caméras :la caméra *Main Entrance* et la caméra *Front Hallway*. Un événement *Accès refusé* est survenu à la porte principale, et l'événement est affiché dans une tuile. Puisque le contenu de la tuile est réduit, seule la première caméra est affichée (Main Entrance) tant que vous ne développez pas le contenu de la tuile.



Regardez cette vidéo pour en savoir plus. Cliquez sur l’icône Sous-titres (CC) pour activer les sous-titres dans l’une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s’affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



1.2.4.1 | Personnaliser les options de cycle d'entités

Vous pouvez choisir le nombre de secondes d'affichage de chaque entité d'une entité composite (alarme, secteur, séquence de caméras, et ainsi de suite) dans une tuile Security Desk.

À savoir

Ce réglage est conservé dans votre profil utilisateur.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Général.
2. Dans la section Durée d'affichage, définissez la valeur Cycle d'entités.
3. Cliquez sur Enregistrer.

Sujet parent : Développer le contenu d'une tuile

1.2.5 | Basculer le canevas en mode plein écran

Le mode plein écran de Security Desk permet de masquer la vue secteur, la barre des tâches et le volet Commandes afin de n'afficher que le canevas et les flux vidéo que vous surveillez. Vous pouvez également agrandir une tuile particulière.

À savoir

Le mode vidéo en plein écran ressemble à l'affichage sur un moniteur analogique. Lorsque Security Desk est connecté à plusieurs moniteurs et que vous basculez le canevas en mode plein écran, chaque moniteur affiche un canevas distinct. Vous pouvez sélectionner les moniteurs qui basculent en mode plein écran dans la boîte de dialogue Options.

Procédure

1. Procédez de l'une des manières suivantes :
   - Pour agrandir le canevas, appuyez sur F11 > F10.

     Tout est masqué à l'exception des tuiles du canevas.
   - Pour agrandir une seule tuile, appuyez sur ALT+ENTRÉE.
2. Utilisez les raccourcis clavier pour contrôler les flux vidéo.
3. Pour afficher la barre des tâches, survolez le haut de la fenêtre Security Desk avec la souris.
4. Pour quitter le mode plein écran, procédez de l'une des manières suivantes :
   - Si le canevas est agrandi, appuyez sur F11 > F10.
   - Si une tuile est agrandie, appuyez sur ALT+ENTRÉE.

Explorer

- Raccourcis clavier par défaut dans Security Desk

1.2.5.1 | Sélectionner les moniteurs à basculer en mode plein écran

Lorsque Security Desk est connecté à plusieurs moniteurs, vous pouvez sélectionner les moniteurs à basculer en mode plein écran dans la boîte de dialogue Options.

À savoir

Ces réglages s'appliquent au poste Security Desk local et affectent Security Desk et Config Tool pour tous les utilisateurs.

Procédure

1. Sur votre moniteur par défaut, sélectionnez la page d'accueil et cliquez sur Options > Général.
2. Dans la section Moniteurs plein écran, sélectionnez les moniteurs qui peuvent basculer en plein écran.
   Cette section n'apparaît que lorsque Security Desk est connecté à plusieurs moniteurs.
3. Cliquez sur Enregistrer.

Sujet parent : Basculer le canevas en mode plein écran

1.2.6 | Modifier la mosaïque des tuiles

Vous pouvez modifier la disposition des tuiles sur le canevas.

À savoir

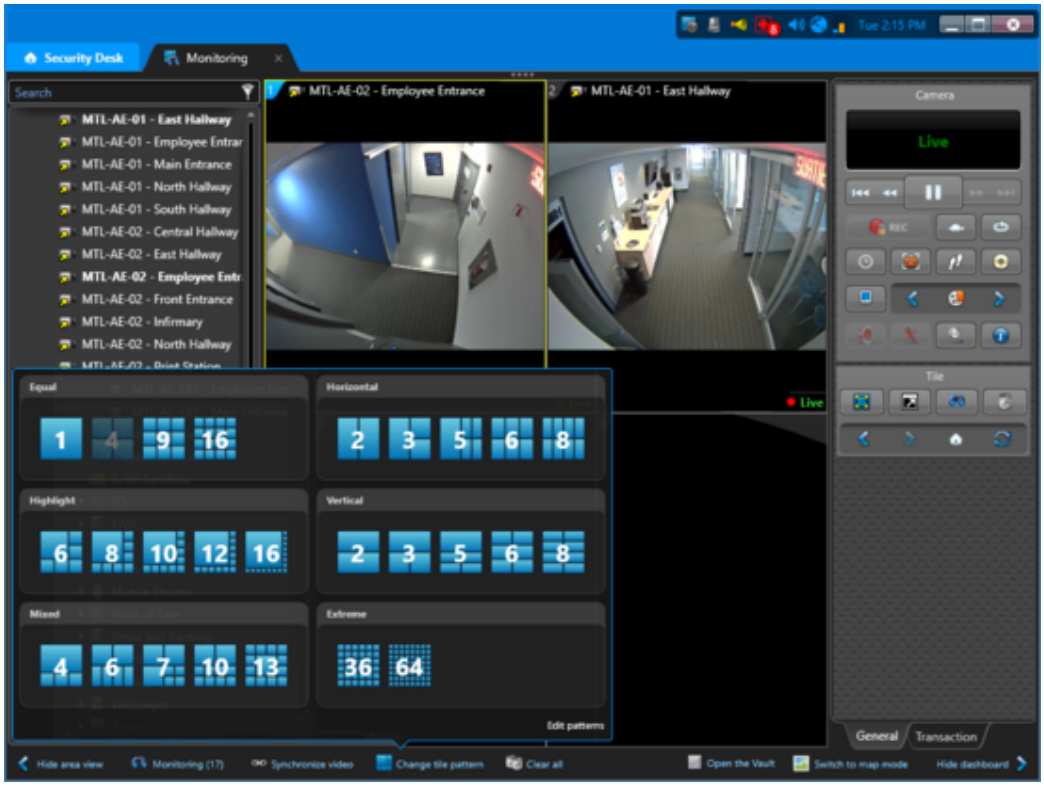
Par défaut, une mosaïque de 2 x 2 tuiles est affichée sur le canevas.

Procédure

1. En bas du canevas, cliquez sur Modifier la mosaïque ( ).
2. Procédez de l'une des manières suivantes :
   - Sélectionnez l'une des mosaïques affichées.

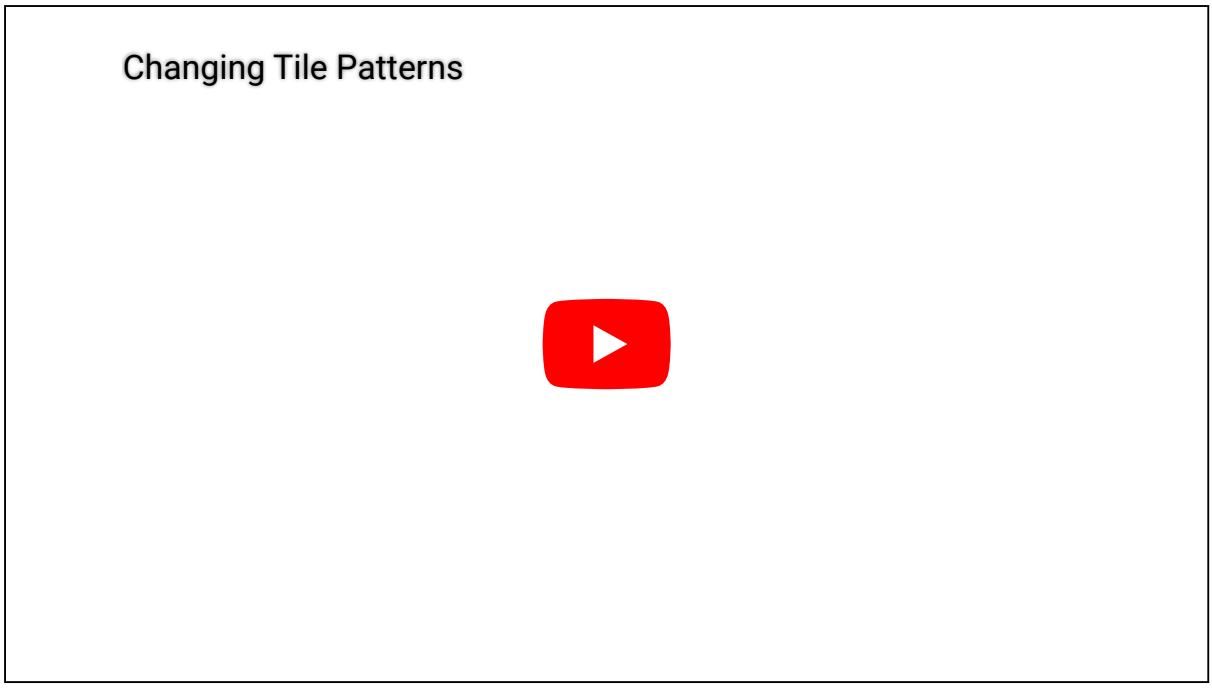
     Il peut s'agir des mosaïques par défaut, ou de celles que vous avez ajoutées à vos favoris.
   - Cliquez sur Plus, et sélectionnez l'une des autres mosaïques.

     Affichez une grande tuile et jusqu'à 64 petites tuiles.



Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l’icône Sous-titres (CC) pour activer les sous-titres dans l’une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s’affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



Explorer

- Modifier et créer des mosaïques

1.2.7 | Modifier et créer des mosaïques

Pour personnaliser votre espace de travail, vous pouvez modifier les 26 mosaïques de tuiles disponibles sur le canevas, supprimer les mosaïques par défaut, et créer des mosaïques.

À savoir

L'éditeur de mosaïques de Security Desk ne vous permet que de créer des mosaïques de 8x8 tuiles maximum.

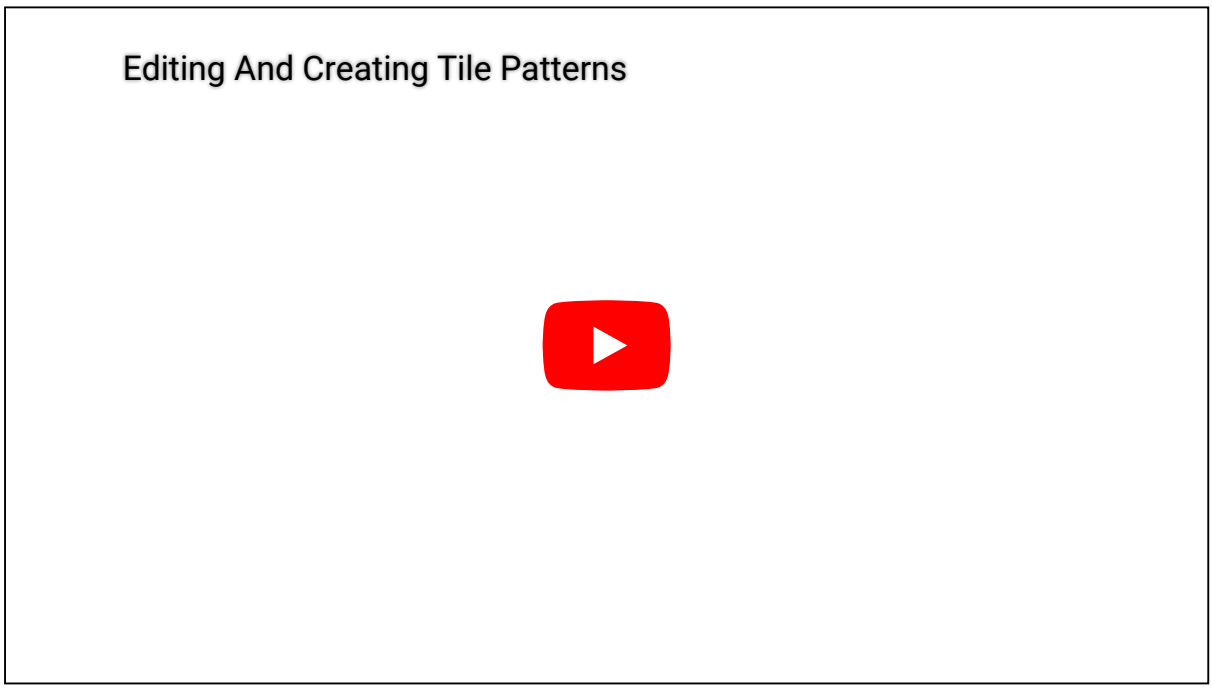
Les réglages de mosaïques de tuiles sont enregistrés au niveau du poste. Vous devez disposer du privilège *Modifier les mosaïques* pour modifier et créer des mosaïques.

Procédure

1. En bas du canevas, cliquez sur Modifier la mosaïque ( ).
2. Cliquez sur Plus > Modifier les mosaïques.
3. Procédez de l'une des manières suivantes :
   - Sélectionnez une mosaïque existante.
   - Pour créer une mosaïque, cliquez sur .
4. Dans le champ Nom, saisissez un nom pour la mosaïque.
5. Dans le champ Catégorie, sélectionnez le groupe auquel la mosaïque doit appartenir.
6. Pour afficher la mosaïque dans la boîte de dialogue principale lorsque vous cliquez sur Modifier la mosaïque ( ), sélectionnez Afficher en tant que favori ( ).
7. Pour modifier le nombre de lignes et de colonnes, utilisez le sélecteur de Lignes et de Colonnes, ou cliquez sur les lignes dans le graphique.
8. Pour supprimer une mosaïque, sélectionnez la mosaïque, puis cliquez sur .
9. Pour rétablir la configuration par défaut de l'ensemble des mosaïques, cliquez sur Valeurs par défaut.
   IMPORTANT : Toutes les mosaïques qui ne sont pas des mosaïques par défaut sont supprimées.
10. Cliquez sur Enregistrer et fermer.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



1.2.8 | Personnaliser l'affichage des tuiles dans Security Center

Vous pouvez personnaliser ce qui est affiché dans les tuiles du canevas depuis la boîte de dialogue Options.

À savoir

Vous pouvez masquer la frise chronologique, les commandes vidéo intégrées à la tuile, la barre d'outils de la tuile et l'*ID de tuile*. Les réglages de tuile sont conservés dans votre profil utilisateur.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Visuel.
2. Dans la liste déroulante Afficher la frise chronologique, sélectionnez les conditions d'affichage de la frise chronologique dans les tuiles, pour la vidéo en direct et enregistrée :

   Masquage automatique
   N'afficher la frise chronologique que lorsque la souris survole la tuile.

   Toujours
   Toujours afficher la frise chronologique.

   Jamais
   Ne jamais afficher la frise chronologique.

3. Pour afficher les commandes vidéo (lecture, pause, et ainsi de suite) lorsque vous survolez une tuile avec la souris, sélectionnez l'option Afficher les commandes vidéo en incrustation.
4. Pour afficher le chemin complet de l'entité avec son nom dans la barre d'outils de la tuile, sélectionnez l'option Afficher les noms d´entité avec le chemin d'accès complet.
   Le chemin d'une entité correspond à la hiérarchie de *secteurs* qui englobent l'entité dans l'arborescence de la vue secteur. Lorsque le chemin est trop long, un astérisque (*) est affiché à la place.

Bureau de Paris/Entrée principale », ou « */*/Porte arrière ».
REMARQUE : Cette option s'applique également aux alarmes. Lorsque cette option est sélectionnée, le chemin complet de l'entité ayant déclenché l'alarme est affiché dans la colonne Source des tâches Surveillance et Surveillance d'alarmes.

5. Pour n'afficher la barre d'outils de la tuile que lorsque vous survolez la tuile, sélectionnez l'option Masquer automatiquement la barre d'outils de tuile.
   Désactivez cette option pour afficher la barre d'outils de tuile en permanence.
6. Pour n'afficher l'ID de la tuile que lorsque vous survolez la tuile, sélectionnez l'option Masquer automatiquement le numéro de tuile.
   Désactivez cette option pour afficher L'ID de tuile en permanence.
7. Cliquez sur Enregistrer.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Commandes vidéo intégrées à la tuile
- À propos des tuiles

1.3 | Widgets Security Center dans Security Desk

1.3.1 | Widget Alarme

Le widget *Alarme* apparaît lorsqu'une entité alarme est affichée dans la tuile active. Il offre plusieurs manières de répondre à une alarme.

Si une alarme déclenchée exige une condition d'acquittement (comme *Porte fermée*), le bouton *Analyser* apparaît dans le widget Alarme lorsque l'alarme concernée est affichée dans la tuile actuelle avant acquittement.

Les commandes dans le widget Alarme sont disponibles dans les tâches *Surveillance*, *Surveillance d'alarmes* et *Rapport d'alarmes*.

Les commandes du widget Alarme sont décrites ci-dessous :

Bouton	Commande	Description
	Acquitter (par défaut)[1]	Acquitter l'alarme. L'alarme n'est plus active, et elle supprimée du canevas et de la liste d'alarmes.
	Acquitter (secondaire)[1]	Placer l'alarme en état acquittée *secondaire*. La fonction de l'acquittement secondaire est définie par votre société. Par exemple, en cas de fausse alerte, vous pouvez acquitter l'alarme de cette façon. Cet état peut également servir à filtrer les recherches d'alarme.
	Acquitter de force[1]	Forcez l'acquittement de l'alarme. Cette option est utile pour effacer les alarmes en cours d'analyse et dont la condition d'acquittement n'est pas encore effacée.
	Analyser	Analysez l'alarme. Cette action permet aux autres utilisateurs du système de savoir que vous avez vu l'alarme sans l'acquitter, ce qui fait que l'alarme n'est pas supprimée de la liste des alarmes actives.
	Mettre l'alarme en rappel[1]	Placer l'alarme en veille pendant 30 secondes. Lorsqu'elle est en veille, l'alarme est temporairement retirée du canevas. Vous pouvez modifier le délai de veille par défaut dans la boîte de dialogue Options.
	Transférer l'alarme[1]	Transférez l'alarme à un autre utilisateur. Avant de transférer une alarme, vous devez sélectionner un utilisateur, et vous pouvez ajouter un message.
	Afficher la procédure d'alarme	Affichez la procédure particulière de l'alarme (lorsqu'une procédure est définie par l'administrateur). Les procédures d'alarme sont faciles à créer et peuvent prendre la forme de pages HTML ou d'applications Web développées par les utilisateurs.

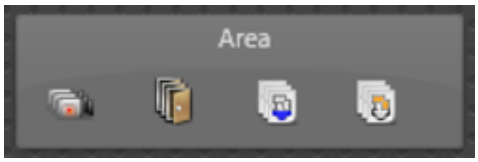
[1] Lorsque vous appuyez sur Ctrl+Maj tout en cliquant sur la commande, celle-ci s'applique à toutes les alarmes affichées sur le canevas.

Explorer

- Transférer une alarme automatiquement
- Personnalisation du comportement des alarmes dans Security Center
- Présentation de la tâche Rapport d'alarmes dans Security Center

1.3.2 | Widget Secteur

Le widget *Secteur* est ouvert lorsque la tuile actuelle affiche un secteur.



Les commandes incluses dans le widget Secteur sont *récursives*, ce qui signifie qu'elles sont appliquées à toutes les entités imbriquées dans le secteur concerné. Cliquez sur l'une des commandes pour afficher un menu de commandes disponibles.

Les commandes du widget Secteur sont décrites ci-dessous :

Bouton	Commande	Description
	Caméras	Appliquer les commandes à toutes les caméras du secteur : **Démarrer l'enregistrement** Activer l'enregistrement sur les caméras. **Arrêter l'enregistrement** Arrêter l'enregistrement sur les caméras. **Ajouter un signet** Ajouter un signet aux caméras. **Bloquer** Empêcher les utilisateurs d'afficher les flux vidéo. **Débloquer (récursif)** Autoriser les utilisateurs à afficher les flux vidéo.
	Portes	Appliquer les commandes à toutes les portes du secteur : **Ignorer les horaires de déverrouillage** Verrouiller les portes qui obéissent potentiellement à un horaire de déverrouillage. **Réactiver la synchronisation** Réactiver les horaires de déverrouillage des portes. **Déverrouiller les portes du périmètre du secteur** Déverrouiller les portes du périmètre d'un secteur pour une durée égale au *Délai d'accès normal* configuré pour les portes.
	Zones	Appliquer les commandes à toutes les zones du secteur : **Armer** Armer les zones. **Désarmer** Désarmer les zones.
	Secteurs de détection d'intrusion	Appliquer les commandes à tous les secteurs de détection d'intrusion du secteur : REMARQUE : Certaines commandes seront indisponibles si vous n'avez pas les privilèges nécessaires ou si elles ne sont pas prises en charge par votre tableau d'intrusion.

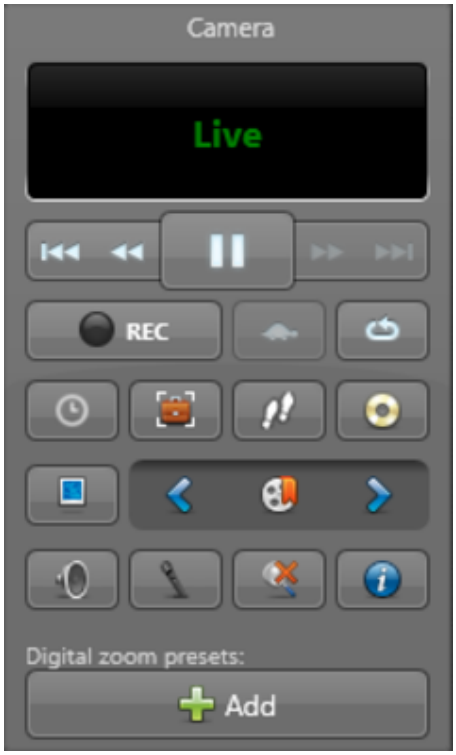
Bouton	Commande	Description
		Armer Arme les secteurs de détection d'intrusion sélectionnés. Les options suivantes sont disponibles : **Global** Arme tous les capteurs dans les secteurs de détection d'intrusion. Tout capteur peut déclencher l'alarme en cas d'activation. **Périmètre** Arme uniquement les capteurs définis comme étant dans le périmètre. L'activité sur les capteurs à l'intérieur des secteurs, comme les capteurs de mouvement, est ignorée. **Instantané** Arme les secteurs immédiatement. **Délai** Arme les secteurs après un délai. Si vous ne spécifiez pas la durée, la valeur par défaut du tableau est utilisée. **Mode d'armement** **Normal** Arme les secteurs de détection d'intrusion normalement. Les secteurs avec des capteurs actifs ou en mode problème restent désarmés. **Forcer** Si un ou plusieurs secteurs de détection d'intrusion ne sont pas prêts pour l'armement normal, cette option force l'armement des secteurs. Cette option ignore à titre temporaire les capteurs actifs ou en mode problème pendant la séquence d'armement. Si un capteur ignoré retrouve un état normal pendant l'armement, l'activité peut déclencher l'alarme. **Contourner** Si un ou plusieurs secteurs de détection d'intrusion ne sont pas prêts pour l'armement normal, cette option contourne automatiquement les capteurs actifs ou en mode problème avant l'armement des secteurs. Les capteurs restent contournés pendant que les secteurs sont armés. Le désarmement d'un secteur supprime le contournement de ses capteurs. **Désarmer** Désarme les secteurs de détection d'intrusion. L'activité des capteurs au sein des secteurs est ignorée par le tableau d'intrusion. **Déclencher une alarme d'intrusion** Déclenche une alarme d'intrusion dans les secteurs de détection d'intrusion sélectionnés. **Couper le son de l'alarme** S'il existe une alarme active dans un secteur de détection d'intrusion sélectionné, coupe la sirène du tableau d'intrusion. Selon votre tableau d'intrusion et le type d'alarme, cliquer sur Couper le son de l'alarme peut également acquitter l'alarme. **Acquitter l'alarme** Acquitte l'alarme active dans un secteur de détection d'intrusion sélectionné.

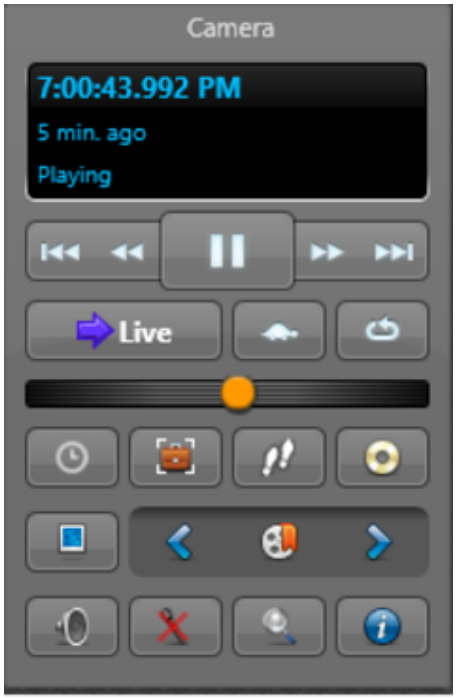
1.3.3 | Widget Caméra

Le widget *Caméra* apparaît dans le volet Commandes lorsque la tuile sélectionnée affiche une caméra.

Les boutons affichés dans le widget Caméra varient en fonction de la tâche que vous effectuez et du type de caméra. Par exemple, si la caméra affichée dans la tuile diffuse de la vidéo en temps réel, vous disposez d'un ensemble de boutons correspondants. Lorsque l'image affichée dans la tuile provient d'un enregistrement, les boutons affichés ne sont pas tous les mêmes. Si la caméra prend en charge l'audio, les boutons audio sont disponibles. Dans le cas contraire, ils sont grisés.

Les deux images suivantes montrent le widget Caméra avec de la vidéo en direct sans audio dans une tuile, et de la vidéo enregistrée avec audio dans une tuile.





Les commandes du widget caméra sont décrites ci-dessous :

Bouton	Commande	Description
	Saut arrière[1]	Saut arrière. Chaque clic sur ce bouton entraîne un saut arrière de 15 secondes dans l'enregistrement. Vous pouvez configurer cette valeur dans la boîte de dialogue Options.
	Rembobiner[1]	Inverse le sens de lecture. Chaque clic sur ce bouton ajuste la vitesse de lecture arrière, de -1x à -2x, -4x, -6x, -8x, -10x, -20x, -40x, -100x. Cliquez sur le bouton de Lecture pour revenir à la lecture avant en vitesse 1x (vitesse normale).
	Image précédente[1]	Affiche l'image précédente de la vidéo. Ou utilisez la molette pour obtenir le même résultat. Cette commande n'est disponible que lorsque la vidéo est mise en pause.
	Pause[1]	Suspend la lecture sur l'image en cours.
	Lecture[1]	Lance la lecture de l'enregistrement à vitesse normale (1x).
	Image suivante[1]	Affiche l'image suivante de la vidéo. Ou utilisez la molette pour obtenir le même résultat. Cette commande n'est disponible que lorsque la vidéo est mise en pause.

Bouton	Commande	Description
	Avance rapide[1]	Accélère la lecture. Chaque clic successif sur ce bouton augmente la vitesse de lecture de 1x à 2x, 4x, 6x, 8x, 10x, 20x, 40x, 100x. Cliquez sur le bouton Lecture pour rétablir la vitesse de lecture normale (1x).
	Saut avant[1]	Saut avant. Chaque clic sur ce bouton entraîne un saut avant de 15 secondes dans l'enregistrement. Vous pouvez configurer cette valeur dans la boîte de dialogue Options.
	Basculer vers le direct[1]	Bascule l'image affichée de la vidéo enregistrée vers la vidéo en direct.
	Enregistrement démarré	(Rouge) - La caméra enregistre. Cliquez pour arrêter l'enregistrement.
	Enregistrement démarré	(Rouge clignotant) La caméra enregistre mais arrive au bout de sa durée d'enregistrement manuelle (30 secondes restantes). Cliquez pour prolonger l'enregistrement de cinq minutes.
	Enregistrement démarré (par le système)	La caméra enregistre, et elle est contrôlée par une configuration système. Vous ne pouvez pas cliquer pour arrêter l'enregistrement.
	Enregistrement arrêté	La caméra n'enregistre pas. Cliquer pour démarrer l'enregistrement. L'enregistrement s'arrête automatiquement après cinq minutes. Vous pouvez également arrêter l'enregistrement manuellement. Si la caméra est également contrôlée par un Archiveur auxiliaire, vous pouvez démarrer l'enregistrement manuellement sur l'Archiveur auxiliaire en faisant un clic droit sur le bouton d'état d'enregistrement, en sélectionnant Enregistrement auxiliaire, puis en cliquant sur le bouton enregistrer () en regard du nom du rôle Archiveur auxiliaire.
	Enregistrement arrêté (par le système)	La caméra n'enregistre pas, et elle est contrôlée par une configuration système. Vous ne pouvez pas cliquer pour lancer l'enregistrement.
	Problème d'enregistrement	Problème d'enregistrement de la caméra. Il peut s'agir d'une erreur d'écriture sur disque, d'écriture dans la base de données de l'Archiveur, ou d'un problème de diffusion vidéo en continu. Si vous rencontrez cette erreur, contactez votre administrateur système pour résoudre le problème.
	Ralenti[1]	Bascule entre la vitesse de lecture normale (1x) et ralentie (1/8x). En mode ralenti, cliquez sur les boutons Avancer ou Rembobiner pour régler la vitesse de lecture de 1/8x à 1/4x, 1/3x, 1/2x, vers l'avant ou l'arrière.
	Lecture en boucle	Créez une section en boucle. Lorsque vous cliquez sur ce bouton, un marqueur () apparaît à chaque extrémité de la frise chronologique. Faites glisser les marqueurs dans la frise pour indiquer le début et la fin de la séquence à lire en boucle.
	Curseur de vitesse	Faites glisser le curseur vers la droite pour régler la vitesse de lecture sur 2x, 4x, 6x, 8x, 10x, 20x, 40x, 100x. Faites glisser le curseur vers la gauche pour lancer la lecture arrière de -1x à -2x, -4x, -6x, -8x, -10x, -20x, -40x, -100x.
	Curseur de vitesse (limité)	Identique au curseur de vitesse précédent, sauf que la vitesse de lecture arrière est limitée à : -10x, -20x, -40x, -100x. Le curseur de vitesse limité est utilisé avec les caméras Omnicast™ 4.x fédérées qui ne prennent pas en charge toutes les vitesses de rembobinage.

Bouton	Commande	Description
	Molette	Remplace le curseur de vitesse lorsque la lecture est en pause. Utilisez-la pour naviguer image par image, vers l'avant ou vers l'arrière.
	Aller à l'heure spécifique[1]	Ouvrez une fenêtre de navigateur pour aller à un endroit précis de l'enregistrement (date et heure).
	Recherche rapide	Ouvre la boîte de dialogue Recherche rapide.
	Activer la filature visuelle[1]	Suit un individu ou un objet qui traverse le champ de plusieurs caméras dans une même tuile.
	Exporter la vidéo[1]	Créez des fichiers vidéo autonomes qui peuvent être lus sans connexion au Répertoire Security Center.
	Enregistrer un instantané[1]	Enregistre l'image vidéo actuelle dans un fichier.
	Signet précédent[1]	Basculer vers le signet précédent.
	Ajouter un signet[1]	Ajouter un signet à la vidéo.
	Signet suivant[1]	Basculer vers le signet suivant.
	Écouter[1]	Activez le haut-parleur. Cette commande n'est disponible que si la caméra prend en charge l'audio.
	Arrêter l'écoute[1]	Désactivez le haut-parleur. Cette commande n'est disponible que si la caméra prend en charge l'audio.
	Parler[1]	Activez le microphone. Cette commande n'est disponible que si la caméra prend en charge l'audio.
	Arrêter la conversation	Désactivez le microphone. Cette commande n'est disponible que si la caméra prend en charge l'audio.
	Activer/désactiver le zoom numérique	Appliquer un zoom numérique x2 à l'image. Le zoom numérique peut ensuite être réglé dans la tuile.
	Afficher les propriétés du flux	Affiche les propriétés du flux vidéo sélectionné.
	Préréglages de zoom numérique	Lorsque vous appliquez un zoom numérique à la tuile sélectionnée, cliquez sur ce bouton pour ajouter un préréglage de zoom numérique pour la position actuelle de la caméra.

[1] Lorsque vous appuyez sur Ctrl+Maj tout en cliquant sur la commande, celle-ci s'applique à toutes les caméras affichées sur le canevas.

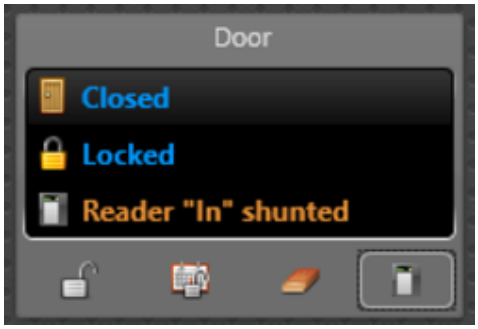
Regardez cette vidéo pour en savoir plus. Cliquez sur l’icône Sous-titres (CC) pour activer les sous-titres dans l’une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s’affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Options vidéo dans Security Desk
- Basculer entre les modes vidéo
- Effectuer des recherches vidéo ciblées
- Faire un zoom avant et arrière
- Ajouter des signets à une séquence vidéo
- Capturer des instantanés vidéo
- Surveiller les zones de stationnement

1.3.4 | Widget Porte

Le widget Porte apparaît lorsqu'une entité porte est affichée dans la tuile active. Il permet de contrôler l'accès par la porte concernée. Le widget Porte affiche également l'état actuel de la porte (ouverte ou fermée), du verrouillage (verrouillée ou déverrouillée, déverrouillée en mode maintenance ou non sécurisée) et du lecteur (en cas de désactivation).



Les commandes du widget Porte sont décrites ci-dessous :

Bouton	Commande	Description
	Déverrouiller[1]	Déverrouille temporairement la porte pendant 5 secondes (ou toute autre *période d'accès par défaut* définie par l'administrateur système).
	Ignorer les horaires de déverrouillage	Déverrouillez la porte indéfiniment à des fins de maintenance, ou afin de verrouiller ou déverrouiller la porte pour une durée déterminée.

Bouton	Commande	Description
	Annuler	Rétablir les horaires de déverrouillage.
	Pardonner une violation antiretour	Pardonnez une violation antiretour. Ce bouton n'est disponible qu'en cas de violation antiretour.
	Lecteur (désactiver ou activer)	Sélectionnez le lecteur à désactiver (contourner) ou activer. Ce bouton n'est disponible que si votre équipement de contrôle d'accès prend en charge le contournement du lecteur.

[1] Lorsque vous appuyez sur Ctrl+Maj tout en cliquant sur la commande, celle-ci s'applique à toutes les portes affichées sur le canevas.

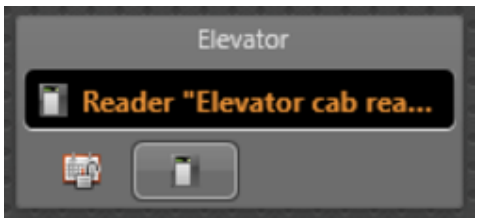
Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Autoriser le franchissement d'une porte
- Affichage des portes sur le canevas de Security Desk

1.3.5 | Widget Ascenseur

Le widget *Ascenseur* apparaît lorsqu'une entité ascenseur est affichée dans la tuile active. Vous pouvez utiliser le widget pour ignorer l'horaire de l'ascenseur et contourner son lecteur.



Les commandes du widget Ascenseur sont décrites ci-dessous :

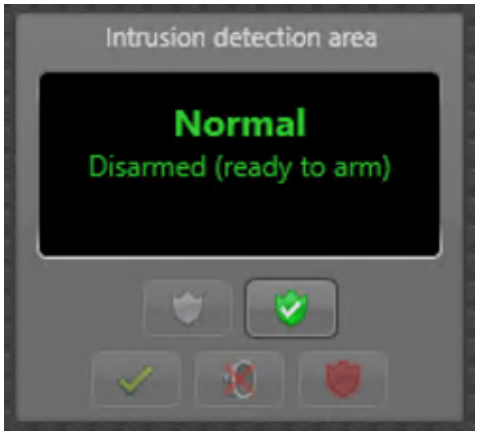
Bouton	Commande	Description
	Ignorer les horaires d'ascenseur	Déverrouillez l'ascenseur indéfiniment à des fins de maintenance, ou afin de verrouiller ou déverrouiller l'ascenseur pour une durée déterminée. REMARQUE : Ce bouton n'est activé que si l'ascenseur est contrôlé par une unité de contrôle d'accès exécutant Synergis™ Softwire 10.6 ou ultérieur.
	Lecteur (désactiver ou activer)	Sélectionnez le lecteur à désactiver (contourner) ou activer. Ce bouton n'est disponible que si votre équipement de contrôle d'accès prend en charge le contournement du lecteur.

Explorer

- Contrôler l'accès aux étages d'ascenseur

1.3.6 | Widget Secteur de détection d'intrusion

Lorsqu'un secteur de détection d'intrusion est affiché dans une tuile Security Desk, vous pouvez armer ou désarmer le secteur, et interagir avec les alarmes d'intrusion dans le widget *Secteur de détection d'intrusion*.



Le widget Secteur de détection d'intrusion est décrit dans le tableau suivant :
REMARQUE : Certaines commandes seront indisponibles si vous n'avez pas les privilèges nécessaires ou si elles ne sont pas prises en charge par le tableau d'intrusion que vous utilisez.

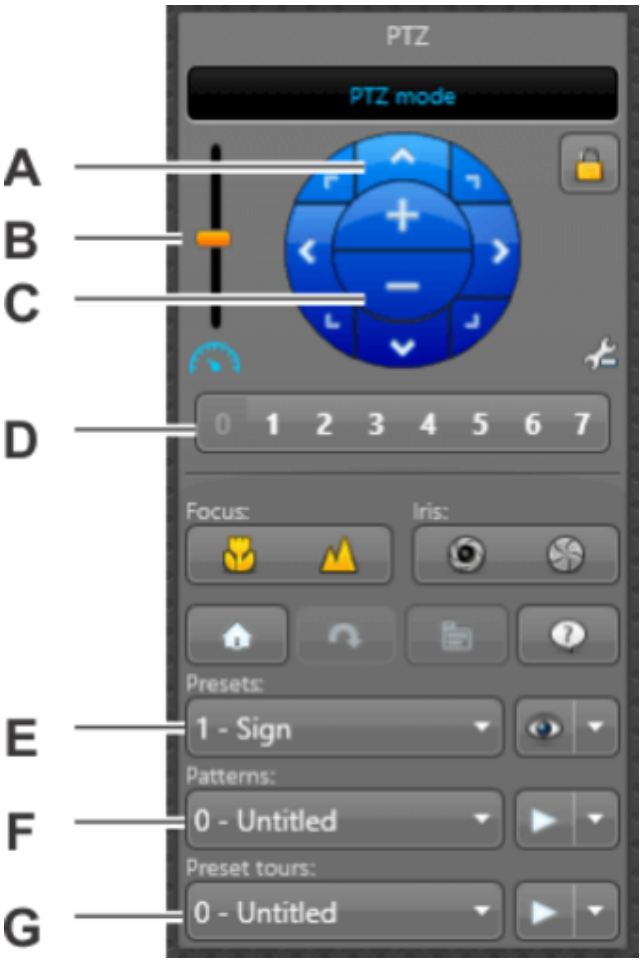
Bouton	Commande	Description
	Désarmer	Désarmez le secteur, en faisant en sorte que tous les capteurs attribués au secteur de détection d'intrusion sélectionné soient ignorés par le tableau d'intrusion.

Bouton	Commande	Description
	Armer	Arme le secteur de détection d'intrusion. Les options suivantes sont disponibles : **Global** Arme tous les capteurs au sein du secteur de détection d'intrusion. Tout capteur peut déclencher l'alarme en cas d'activation. **Périmètre** Arme uniquement les capteurs désignés en tant que capteurs de périmètre. L'activité sur les capteurs à l'intérieur du secteur, comme les capteurs de mouvement, est ignorée. **Instantané** Arme le secteur immédiatement. **Délai** Arme le secteur au bout d'un délai. Si vous ne spécifiez pas la durée, la valeur par défaut du tableau est utilisée. **Forcer** Si le secteur n'est pas prêt pour l'armement normal, cette option force l'armement du secteur. Cette option ignore à titre temporaire les capteurs actifs ou en mode problème pendant la séquence d'armement. Si un capteur ignoré retrouve un état normal pendant l'armement, l'activité peut déclencher l'alarme. **Contourner** Si le secteur n'est pas prêt pour l'armement normal, cette option contourne automatiquement les capteurs actifs ou en mode problème avant l'armement du secteur. Les capteurs restent contournés pendant que le secteur est armé. Désarmer le secteur supprime le contournement.
	Déclencher une alarme d'intrusion	Déclencher une alarme d'intrusion pour le secteur de détection d'intrusion sélectionné.
	Couper le son de l'alarme	S'il existe une alarme active pour le secteur de détection d'intrusion sélectionné, coupez la sirène du tableau d'intrusion. Selon votre tableau d'intrusion et le type d'alarme, Couper le son de l'alarme peut également acquitter l'alarme. Par exemple, avec les tableaux de détection d'intrusion Bosch en Mode 2, les alarmes *Burglary* (Cambriolage) sont acquittées depuis Security Desk, tandis que les alarmes *Fire* (Incendie) sont acquittées sur le pavé numérique du tableau.
	Acquitter l'alarme	Acquitter l'alarme d'intrusion pour le secteur de détection d'intrusion sélectionné.

1.3.7 | Widget PTZ

Le widget *PTZ* permet de réaliser des opérations de type panoramique, inclinaison et zoom sur la caméra affichée. Il apparaît dans le volet Commandes lorsque la tuile sélectionnée affiche une caméra compatible PTZ ().

IMPORTANT : Toutes les caméras PTZ ne prennent pas en charge toutes les commandes de PTZ. Si certains boutons de PTZ sont grisés, cela signifie que la caméra PTZ que vous utilisez ne prend pas en charge les commandes correspondantes.

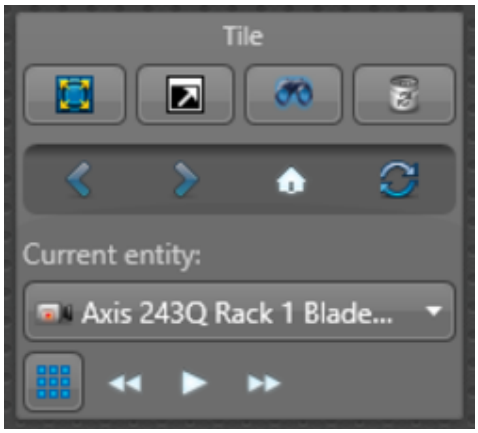


Bouton/lettre	Commande	Description
A	Flèches directionnelles	Réglez le panoramique du moteur PTZ avec les huit flèches directionnelles.
B	Curseur de vitesse	Réglez la vitesse du Moteur de PTZ.
C	Zoom avant/arrière	Agrandissez et réduisez l'affichage avec les commandes plus (+) et moins (-).
D	Bouton d'accès rapide	Déplacez le moteur de PTZ vers l'un des huit préréglages PTZ.
E	Préréglages	Sélectionnez un préréglage dans la liste déroulante pour régler le moteur de PTZ sur le réglage correspondant, enregistrer un nouveau préréglage ou renommer le préréglage.
F	Parcours	Sélectionnez un parcours de PTZ dans la liste déroulante pour lancer un parcours de PTZ (série de préréglages ou de mouvements PTZ enregistrés), enregistrer un nouveau parcours ou renommer le parcours.
G	Rondes prédéfinies	Sélectionnez une commande auxiliaire dans la liste déroulante pour la lancer, l'arrêter ou la renommer.
	Verrouiller le PTZ	Verrouillez le moteur de PTZ pour avoir le contrôle exclusif du PTZ.
	Basculer en mode avancé	Affichez le menu Mode PTZ avancé.
	Mise au point proche	Faites la mise au point du PTZ de près.

Bouton/lettre	Commande	Description
	Mise au point lointaine	Faites la mise au point du PTZ de loin.
	Ouvrir l'iris	Contrôlez manuellement l'Iris (ouverture).
	Fermer l'iris	Contrôlez manuellement l'Iris (fermeture).
	Origine PTZ	Aller à la position d'origine (par défaut) du PTZ.
	Basculer	Basculez le moteur de PTZ de 180 degrés.
	Menu activé/désactivé	Ouvrir le menu de PTZ. Cette option est réservée aux caméras PTZ analogiques.
	Commandes spécifiques	Utilisez des commandes propres au modèle de la caméra.
	Aller au préréglage	Basculez vers la position prédéfinie sélectionnée dans la liste déroulante. **Enregistrer** Remplacer le préréglage sélectionné dans la liste déroulante par la position actuelle du PTZ. **Effacer le préréglage** Effacer la position PTZ du préréglage.
	Lancer le parcours	Lancez le parcours de PTZ sélectionné dans la liste déroulante. Vous pouvez cliquer sur un préréglage ou bouton de PTZ pour arrêter le parcours. **Renommer** Renommez le préréglage, parcours ou auxiliaire sélectionné. **Enregistrer un parcours** Enregistrez un nouveau parcours de PTZ. **Effacer le parcours** Effacer le parcours.
	Démarrer une commande auxiliaire.	Démarrez une commande de PTZ auxiliaire (comme un essuie-glace).
	Arrêter la commande auxiliaire	Arrêtez la commande de PTZ auxiliaire.
	Renommer	Renommez le préréglage, parcours ou auxiliaire sélectionné.

1.3.8 | Widget Tuile

Le widget *Tuile* contrôle les propriétés de la tuile active. Il est toujours affiché dans le volet Commandes.



Les commandes du widget Tuile sont décrites ci-dessous. Les mêmes commandes sont disponibles dans le menu de tuile.

Bouton	Commande	Description
	Agrandir la tuile	Agrandissez la tuile actuelle pour remplir le canevas. Masque toutes les autres tuiles.
	Passer la tuile en plein écran	Masquez la vue secteur et les commandes, et remplissez le canevas avec la tuile actuelle. Force l'affichage de la tuile en mode plein écran.
	Surveillance[1]	Démarre la surveillance d'alarme ou d'événement dans une tuile.
	Effacer tout[1]	Effacer le contenu des tuiles.
	Précédent	Afficher le contenu précédent de la tuile.
	Avance rapide	Afficher le contenu suivant de la tuile.
	Accueil	Afficher le contenu initial de la tuile.
	Actualiser	Actualiser le contenu de la tuile.
n/a	Entité actuelle	Sélectionnez l'entité de l'entité composite à afficher. Sélectionnez par exemple une caméra associée au secteur actuel.
	Développer	Afficher toutes les entités associées à l'entité sélectionnée dans des tuiles distinctes.
	Réduire	Réduire toutes les entités associées.
	Aller au contenu précédent du cycle[1]	Basculer vers l'entité précédente de l'entité composite.
	Démarrer le cycle[1]	Faites défiler les entités associées à l'entité composite dans la tuile. La durée d'affichage de chaque entité est configurée dans la boîte de dialogue Options.
	Arrêter le cycle[1]	Arrêter l'affichage cyclique des entités.
	Aller au contenu suivant du cycle[1]	Basculer vers l'entité suivante de l'entité composite.

[1] Lorsque vous appuyez sur Ctrl+Maj tout en cliquant sur la commande, celle-ci s'applique à toutes les tuiles affichées sur le canevas.

Explorer

- Sélectionner des entités à surveiller
- Développer le contenu d'une tuile
- Surveiller les zones de stationnement

1.3.9 | Widget Zone

Le widget *Zone* n'apparaît que lorsque la tuile active affiche une zone.

Les commandes du widget Zone sont décrites ci-dessous :

Bouton	Commande	Description
	Désarmer[1]	Désarmer la zone sélectionnée (entrées désactivées).
	Armer[1]	Armer la zone sélectionnée (entrées activées).

[1] Lorsque vous appuyez sur Ctrl+Maj tout en cliquant sur la commande, celle-ci s'applique à toutes les zones affichées sur le canevas.

1.4 | Tâches Security Center dans Security Desk

1.4.1 | Ouvrir les tâches

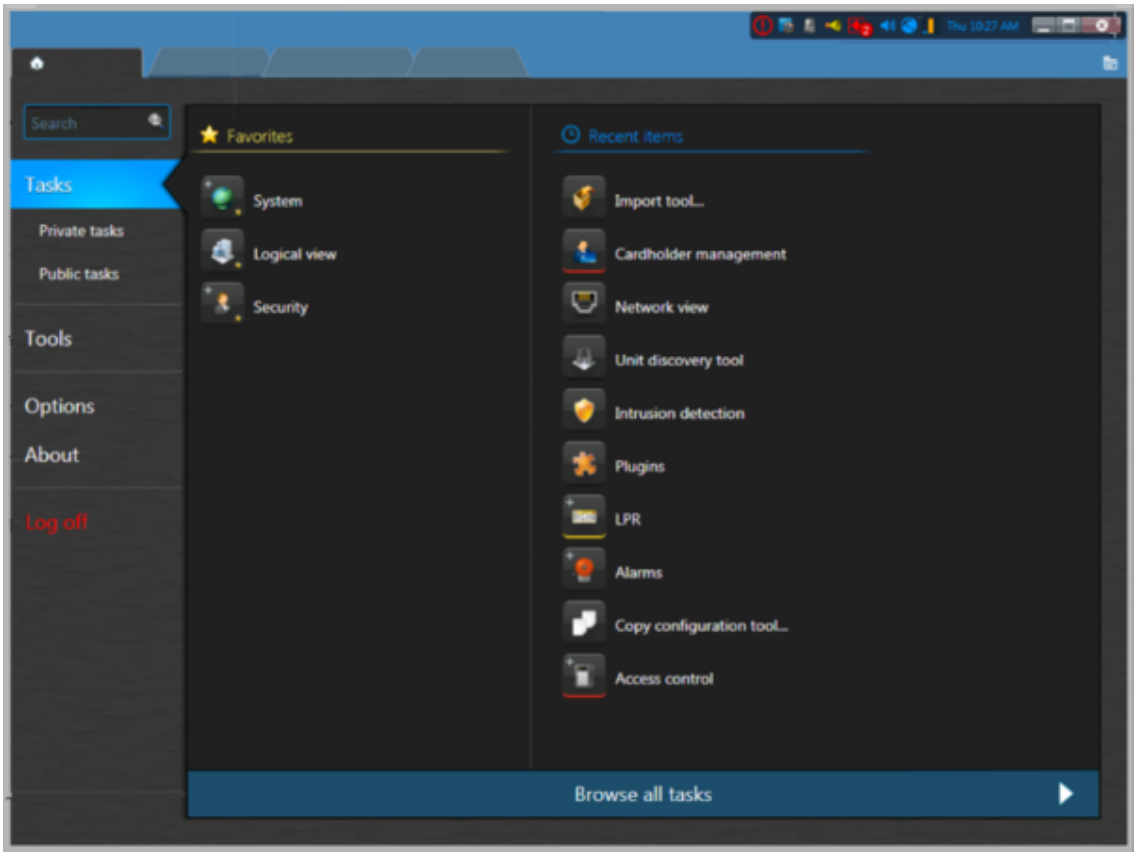
Avant de faire quoi que ce soit dans Security Center, vous devez généralement ouvrir une ou plusieurs tâches.

À savoir

Il n'est possible d'exécuter qu'une seule instance de certaines tâches Security Center, tandis que vous pouvez exécuter plusieurs instances d'autres tâches en les dupliquant. Les tâches à instance unique ne peuvent pas être renommées.

Procédure

1. Sur la page d'accueil, procédez de l'une des manières suivantes :
   - Tapez le nom de la tâche dans le champ Rechercher.
   - Cliquez sur l'onglet Tâches, puis cliquez sur Parcourir toutes les tâches.
   - Pour ouvrir une tâche enregistrée, cliquez sur l'onglet Tâches privées ou Tâches publiques.
2. Cliquez sur la tâche.
   REMARQUE : Pour ouvrir la tâche en arrière-plan, appuyez sur Ctrl et cliquez sur la tâche.
   Si une seule instance est autorisée pour le type de tâche sélectionné, la tâche est créée immédiatement.
3. Si plusieurs instances de la tâche sont autorisées, entrez le nom de la tâche, puis cliquez sur Créer.
   La nouvelle tâche est ouverte et ajoutée à votre liste de tâches.



Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

1.4.2 | Enregistrer une tâche dans Security Center

Vous pouvez enregistrer vos tâches sous forme de tâches privées accessibles par vous seul ou de tâches publiques accessibles par tous.

À savoir

Lorsque vous enregistrez une tâche, les réglages de filtres de recherche, la disposition (ordre des colonnes dans le volet de rapport, disposition sur le canevas, et ainsi de suite), et les entités affichées dans chaque tuile sont également enregistrés.
REMARQUE : Le résultat des requêtes n'est pas enregistré. Il est recalculé à chaque fois que vous lancez la requête.
Avantages de l'enregistrement des tâches :

- Vous pouvez fermer votre tâche, puis la recharger avec la même disposition en cas de besoin.
- Vous pouvez partager les tâches publiques avec d'autres utilisateurs.
- Vous pouvez utiliser les tâches publiques en tant que modèles de rapport dans le cadre de l'action *Envoyer un rapport par e-mail*.

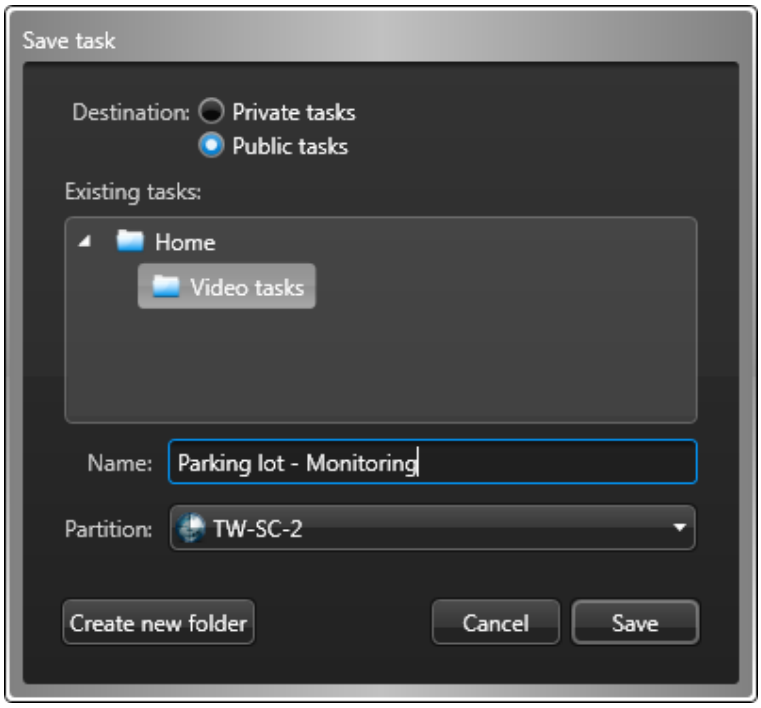
Procédure

1. Faites un clic droit sur l'onglet de la tâche et cliquez sur Enregistrer sous.
   REMARQUE : Le bouton Enregistrer sous n'est disponible que si les filtres de recherche sont valables. Votre requête est valable si le bouton Créer un rapport est activé.
2. Dans la boîte de dialogue Enregistrer la tâche, sélectionnez la manière d'enregistrer la tâche :

   Tâches privées
   Tâche enregistrée qui n'est visible que par l'utilisateur qui l'a créée.

   Tâches publiques
   Tâche enregistrée pouvant être partagée par plusieurs utilisateurs de Security Center.

3. (Facultatif) Pour enregistrer la tâche dans un dossier sur la page Tâches privées ou Tâches publiques, cliquez sur Créer un dossier, donnez un nom au dossier, puis cliquez sur Créer.
   Si vous sélectionnez le dossier Accueil ou si vous ne sélectionnez pas de dossier, la tâche est enregistrée sur la page principale de la page Tâches privées ou Tâches publiques.
4. Nommez la tâche à enregistrer, ou sélectionnez une tâche existante pour la remplacer.
   Vous pouvez enregistrer une tâche Surveillance qui affiche les caméras de votre parc de stationnement sous le nom *Parc de stationnement - Surveillance*, ou enregistrer une tâche d'investigation qui recherche les signets vidéo ajoutés lors des dernières 24 heures sous le nom *Signets du jour*.



5. (Tâches publiques seulement) Sélectionnez la *partition* à laquelle la tâche doit appartenir.
   Seuls les utilisateurs qui appartiennent à la partition peuvent afficher ou modifier la tâche publique.
6. Cliquez sur Enregistrer.

Lorsque vous avez terminé

- Pour enregistrer les modifications apportées à la tâche, faites un clic droit sur l'onglet de la tâche, puis cliquez sur Enregistrer.
- Si vous modifiez la disposition de la tâche (par exemple si vous redimensionnez ou masquez des colonnes du rapport), vous pouvez revenir à la version enregistrée de la tâche en faisant un clic droit sur l'onglet de la tâche, puis en cliquant sur Recharger.

1.4.3 | Enregistrer les dispositions dans Security Center

Vous pouvez enregistrer la disposition de votre tâche Surveillance dans une vue secteur accessible par tous.

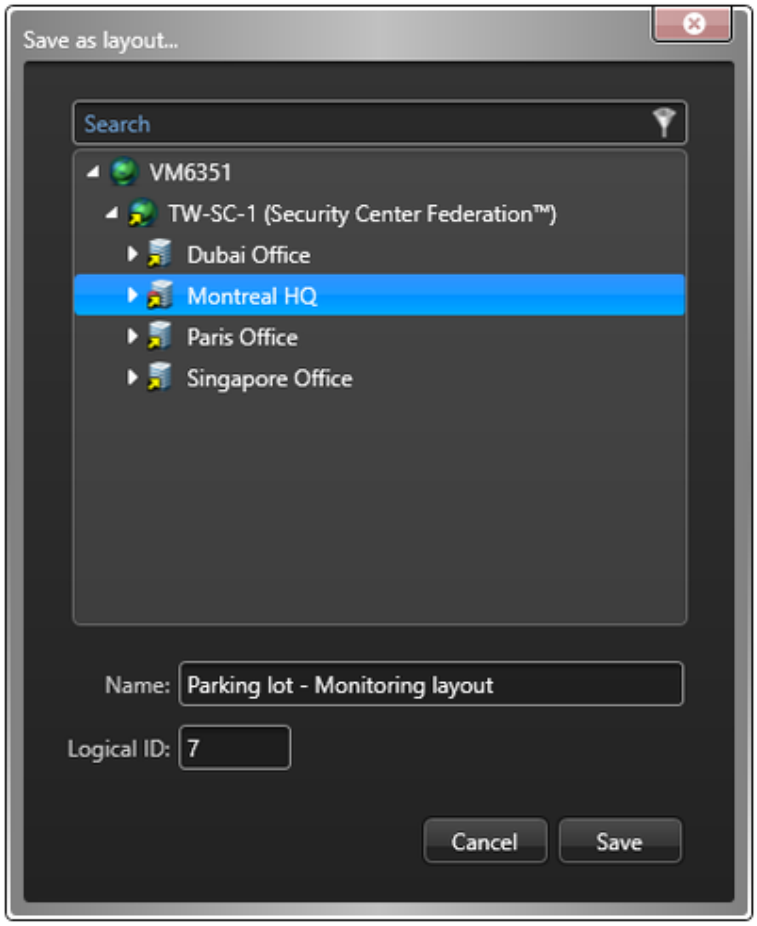
À savoir

Lorsque vous enregistrez une tâche *Surveillance* en tant que disposition, la mosaïque et les entités dans chaque tuile (le contenu des tuiles) sont enregistrées. L'état de la surveillance (surveillance d'événements et d'alarmes) des tuiles, et le mode vidéo des caméras (en direct ou enregistré) ne sont pas enregistrés avec la disposition.
REMARQUE : L'élément de menu Enregistrer en tant que disposition n'est disponible que dans la tâche Surveillance.
Voici les avantages de l'enregistrement de la disposition d'une tâche Surveillance :

- Vous pouvez modifier rapidement les entités surveillées (caméras, portes, et ainsi de suite) sans quitter la tâche Surveillance.
- Vous pouvez partager des dispositions avec d'autres utilisateurs qui ont accès à la vue secteur qui contient la disposition enregistrée.

Procédure

1. Dans la tâche Surveillance, faites un clic droit sur l'onglet de la tâche et cliquez sur Enregistrer en tant que disposition.



REMARQUE : Seuls les utilisateurs avec les droits d'accès à la vue secteur peuvent afficher ou modifier la disposition.
2. Dans la boîte de dialogue Enregistrer en tant que disposition, utilisez le menu déroulant pour sélectionner le secteur dans lequel vous souhaitez enregistrer la disposition.
3. Donnez un Nom à la disposition.
   Si vous surveillez les caméras de votre parc de stationnement, vous pouvez enregistrer votre tâche Surveillance en tant que disposition intitulée *Parc de stationnement - Surveillance*.
4. (Facultatif) Entrez un ID logique.
5. Cliquez sur Enregistrer.

Lorsque vous avez terminé

- Cliquez deux fois sur la disposition enregistrée ou faites-la glisser de la vue secteur sur la tâche Surveillance pour changer rapidement de flux vidéo sans quitter la tâche Surveillance.
  IMPORTANT : Si vous surveillez une alarme, celle-ci n'est pas remplacée par la disposition. L'entité chargée par la disposition ne sera visible qu'après acquittement de l'alarme.
- Pour modifier la disposition, faites un clic droit sur l'onglet de la tâche, puis cliquez sur Enregistrer en tant que disposition, utilisez le menu déroulant pour sélectionner à nouveau la disposition, puis modifiez le Nom ou l'ID logique et cliquez sur Enregistrer.
- Pour modifier le nom, la description et l'ID logique, faites un clic droit sur l'entité dans la vue secteur, et cliquez sur Configurer une entité () pour ouvrir la page de configuration de la disposition dans Config Tool.
- Pour modifier la mosaïque et les entités associées à chaque tuile, faites un clic droit sur l'entité dans la vue secteur, puis cliquez sur Remplacer par la disposition actuelle.

1.4.4 | Organiser vos tâches enregistrées dans Security Center

Si vous avez de nombreuses tâches privées ou publiques enregistrées dans Security Desk ou Config Tool, vous pouvez les classer dans des dossiers pour mieux les retrouver.

À savoir

Tâche enregistrée qui n'est visible que par l'utilisateur qui l'a créée. Tâche enregistrée pouvant être partagée par plusieurs utilisateurs de Security Center.

Procédure

1. Sur la page d'accueil de Security Desk ou Config Tool, cliquez sur Tâches privées ou Tâches publiques.
2. Pour déplacer une tâche vers un dossier :
   a. Faites un clic droit sur une tâche, et sélectionnez Déplacer.
   b. Dans la boîte de dialogue Déplacer vers, cliquez sur Créer un dossier.
   c. Nommez le dossier, puis cliquez sur Créer.
   d. Dans la boîte de dialogue Déplacer vers, sélectionnez le nouveau dossier, puis cliquez sur Déplacer.
   Pour renommer un dossier, faites un clic droit sur le dossier et cliquez sur Renommer.
   REMARQUE : Les dossiers ne sont créés que lorsque vous y déplacez une tâche d'un autre dossier. Vous ne pouvez pas créer de dossiers vides.
3. Pour déplacer un dossier :
   a. Faites un clic droit sur un dossier, et sélectionnez Déplacer.
   b. Dans la boîte de dialogue Déplacer vers, sélectionnez un dossier existant ou créez un dossier, puis cliquez sur Déplacer.
4. Pour trier les tâches, faites un clic droit sur un dossier, cliquez sur Trier, puis sélectionnez une des options suivantes :

   Trier par type
   Triez les tâches enregistrées qui ne sont pas dans des dossiers par type de tâche.

   Trier par nom
   Trier les dossiers et tâches enregistrées par ordre alphabétique.

5. Pour supprimer un dossier, faites un clic droit sur le dossier et cliquez sur Supprimer.

1.4.5 | Ajouter des tâches à votre liste de Favoris

Vous pouvez ajouter des tâches et des outils à vos *Favoris* pour qu'ils soient affichés en regard des *Éléments récents* sur la page d'accueil au lieu de la liste de toutes les tâches.

À savoir

Les tâches que vous ajoutez à la liste *Favoris* sont propres à votre compte utilisateur. Les tâches qui figurent dans la liste *Favoris* n'apparaissent pas dans la liste des *Éléments récents*.

Procédure

1. Procédez de l'une des manières suivantes :
   - Sur la page d'accueil, survolez une tâche avec la souris, puis cliquez sur Ajouter aux favoris ().
   - Sur la page d'accueil, faites glisser une tâche de la liste Éléments récents vers la liste Favoris.
   - Faites un clic droit sur l'onglet de la tâche et cliquez sur Ajouter aux favoris.
2. Pour supprimer une tâche de la liste Favoris, procédez de l'une des manières suivantes :
   - Sur la page d'accueil, survolez une tâche avec la souris, puis cliquez sur Supprimer des favoris ().
   - Faites un clic droit sur l'onglet de la tâche et cliquez sur Supprimer des favoris.

1.4.5.1 | Masquer les listes Favoris et Éléments récents sur votre page d'accueil

Vous pouvez masquer l'affichage des listes Favoris et *Eléments récents* sur votre page d'accueil pour que la liste complète des tâches s'y affiche à la place.

À savoir

Lorsque vous désactivez l'affichage des listes *Favoris* et *Éléments récents* sur votre page d'accueil, le système n'oublie pas les éléments enregistrés dans ces listes. Et le système continue à suivre les éléments récemment utilisés.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Visuel.
2. Désélectionnez l'option Afficher les éléments récents et les favoris sur la page d'accueil.
3. Cliquez sur Enregistrer.

Résultats

À partir de maintenant, seule la liste complète des tâches est affichée lorsque vous cliquez sur Tâches sur la page d'accueil.
Sujet parent : Ajouter des tâches à votre liste de Favoris

1.4.6 | Envoyer une tâche dans Security Center

Si vous avez sélectionné des entités particulières à surveiller ou que vous avez configuré des filtres de recherche particuliers pour une tâche d'investigation, vous pouvez partager la disposition de la tâche avec un autre utilisateur Security Desk en lui envoyant la tâche.

Avant de commencer

Par défaut, lorsqu'une tâche est reçue, une fenêtre de confirmation apparaît sur le poste, et l'utilisateur doit accepter la tâche avant qu'elle se charge dans Security Desk. Si vous envoyez des tâches à un moniteur Security Desk et que vous ne voulez pas que la fenêtre de confirmation apparaisse, désactivez l'option Demander confirmation avant d'ouvrir les tâches envoyées par d'autres utilisateurs dans la boîte de dialogue Options sur le poste de destination.

Pour envoyer une tâche, les destinataires doivent être en ligne. Si vous envoyez une tâche à un moniteur Security Desk, l'utilisateur doit être connecté sur le poste concerné.

À savoir

L'envoie de tâches vers un moniteur Security Desk est généralement utilisé pour les postes dotés de plusieurs moniteurs, comme les murs vidéo. Cette fonctionnalité vous permet d'envoyer une tâche directement à un moniteur particulier d'un mur, sans intervention d'un opérateur.

Procédure

1. Ouvrez la tâche que vous souhaitez envoyer.
2. Configurez la tâche.
   Modifiez la disposition des tuiles, affichez certaines caméras, configurez des filtres de recherche, ajoutez des entités à surveiller, etc.
3. Faites un clic droit sur l'onglet de la tâche et cliquez sur Envoyer.
4. Dans la boîte de dialogue Envoyer une tâche.
5. Spécifiez si vous souhaitez envoyer la tâche à un Utilisateur ou à un Moniteur Security Desk.
6. Dans la liste Sélectionner une destination, sélectionnez les utilisateurs ou moniteurs à qui vous souhaitez envoyer la tâche.
7. (Facultatif) Si vous envoyez la tâche à un utilisateur, rédigez un commentaire dans le champ Message.
8. Cliquez sur Envoyer.

Résultats

Si l'option Demander confirmation avant d'ouvrir les tâches envoyées par d'autres utilisateurs est activée sur le poste destinataire, la demande de confirmation apparaît et le destinataire doit accepter la tâche pour qu'elle soit chargée.

1.4.6.1 | Envoyer une tâche avec une action manuelle dans Security Center

Pour partager immédiatement une disposition de tâche avec quelqu'un d'autre ou afficher une tâche sur un mur vidéo, vous pouvez envoyer la tâche à un autre utilisateur ou à un moniteur Security Desk à l'aide d'une action éclair à usage unique.

Avant de commencer

Par défaut, lorsqu'une tâche est reçue, une fenêtre de confirmation apparaît sur le poste, et l'utilisateur doit accepter la tâche avant qu'elle se charge dans Security Desk. Si vous envoyez des tâches à un moniteur Security Desk et que vous ne voulez pas que la fenêtre de confirmation apparaisse, désactivez l'option Demander confirmation avant d'ouvrir les tâches envoyées par d'autres utilisateurs dans la boîte de dialogue Options sur le poste de destination.

Pour envoyer une tâche, les destinataires doivent être en ligne. Si vous envoyez une tâche à un moniteur Security Desk, l'utilisateur doit être connecté sur le poste concerné.

À savoir

L'envoie de tâches vers un moniteur Security Desk est généralement utilisé pour les postes dotés de plusieurs moniteurs, comme les murs vidéo. Cette fonctionnalité vous permet d'envoyer une tâche directement à un moniteur particulier d'un mur, sans intervention d'un opérateur.

Seules les *tâches publiques* enregistrées peuvent être envoyées avec une action éclair.

Procédure

1. Dans la zone de notification, cliquez sur Actions éclair ().
2. Dans la boîte de dialogue Actions éclair, cliquez sur Action manuelle.
3. Dans la boîte de dialogue Configurer une action, sélectionnez Envoyer une tâche dans la liste des actions.
4. Dans la liste déroulante Tâche, sélectionnez la tâche publique enregistrée que vous souhaitez envoyer.
5. Spécifiez si vous souhaitez envoyer la tâche à un Utilisateur ou à un Moniteur Security Desk.
6. Dans la liste Sélectionner une destination, sélectionnez l'utilisateur ou le moniteur auquel vous souhaitez envoyer la tâche.

CONSEIL : Lorsque vous sélectionnez un moniteur en tant que destination, vous verrez parfois des entités affichées en rouge et en blanc dans la liste des moniteurs. Les moniteurs affichés en rouge sont actuellement déconnectés. Les moniteurs affichés en blanc sont actuellement connectés.

7. (Facultatif) Si vous envoyez la tâche à un utilisateur, rédigez un commentaire dans le champ Message.
8. Cliquez sur OK.

Résultats

Si l'option Demander confirmation avant d'ouvrir les tâches envoyées par d'autres utilisateurs est activée sur le poste destinataire, la demande de confirmation apparaît et le destinataire doit accepter la tâche pour qu'elle soit chargée.

Sujet parent : Envoyer une tâche dans Security Center

1.4.7 | Fermer une tâche avec une action système dans Security Center

Vous pouvez supprimer des tâches depuis un autre poste avec une action manuelle.

À savoir

Vous ne pouvez pas supprimer une tâche individuelle depuis un poste distant. La commande **Effacer les tâches** supprime toutes les tâches ouvertes.

Vous ne pouvez fermer des tâches que pour des utilisateurs qui sont actuellement en ligne.

Procédure

1. Dans la zone de notification, cliquez sur Actions éclair ().
2. Dans la boîte de dialogue Actions éclair, cliquez sur Action manuelle.
3. Dans la liste des actions, cliquez sur Effacer les tâches.
4. Dans la liste déroulante, sélectionnez la tâche publique enregistrée que vous souhaitez supprimer.
5. Spécifiez si vous souhaitez supprimer la tâche pour un utilisateur (Utilisateur) ou à un poste (Moniteur).
6. Dans la liste Sélectionner une destination, sélectionnez l'utilisateur ou le poste pour lequel vous souhaitez supprimer les tâches.
7. Cliquez sur OK.

Résultats

Toutes les tâches ouvertes sont immédiatement supprimées du moniteur distant. Un message de confirmation est affiché sur le poste de l'envoyeur.

1.4.8 | Personnaliser le comportement des tâches dans Security Desk

Une fois que vous maîtrisez l'utilisation des tâches dans Security Center, vous pouvez personnaliser la manière dont le système les gère avec la boîte de dialogue Options.

À savoir

Les réglages de tâches sont conservés dans votre profil utilisateur Security Center et s'appliquent à Security Desk et Config Tool. Toutefois, les options Cycle de tâches et Demander confirmation avant d'ouvrir les tâches envoyées par d'autres utilisateurs sont enregistrées en tant que réglages en local de votre profil utilisateur Windows.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Général.

2. Réglez la valeur de Cycle de tâches pour spécifier durée d'affichage dans Security Desk de chaque tâche lors du cycle des tâches ouvertes.
   REMARQUE : Le *Cycle de tâches* peut être activé en faisant un clic droit sur la barre des tâches.
3. Cliquez sur l'onglet Interaction utilisateur.
4. Dans la section Messages système, configurez les options suivantes :

   Demander le nom de tâche à la création
   Sélectionnez cette option si vous souhaitez que Security Desk vous invite à saisir un nom lorsque vous créez une tâche qui accepte les instances multiples.

   Confirmer avant de fermer une tâche
   Sélectionnez cette option si vous souhaitez que Security Desk vous demande de confirmer la suppression des tâches de l'interface.

   Demander confirmation avant d'ouvrir les tâches envoyées par d'autres utilisateurs
   Sélectionnez cette option si vous souhaitez que Security Desk vous demande de confirmer l'ouverture des tâches envoyées par d'autres utilisateurs.

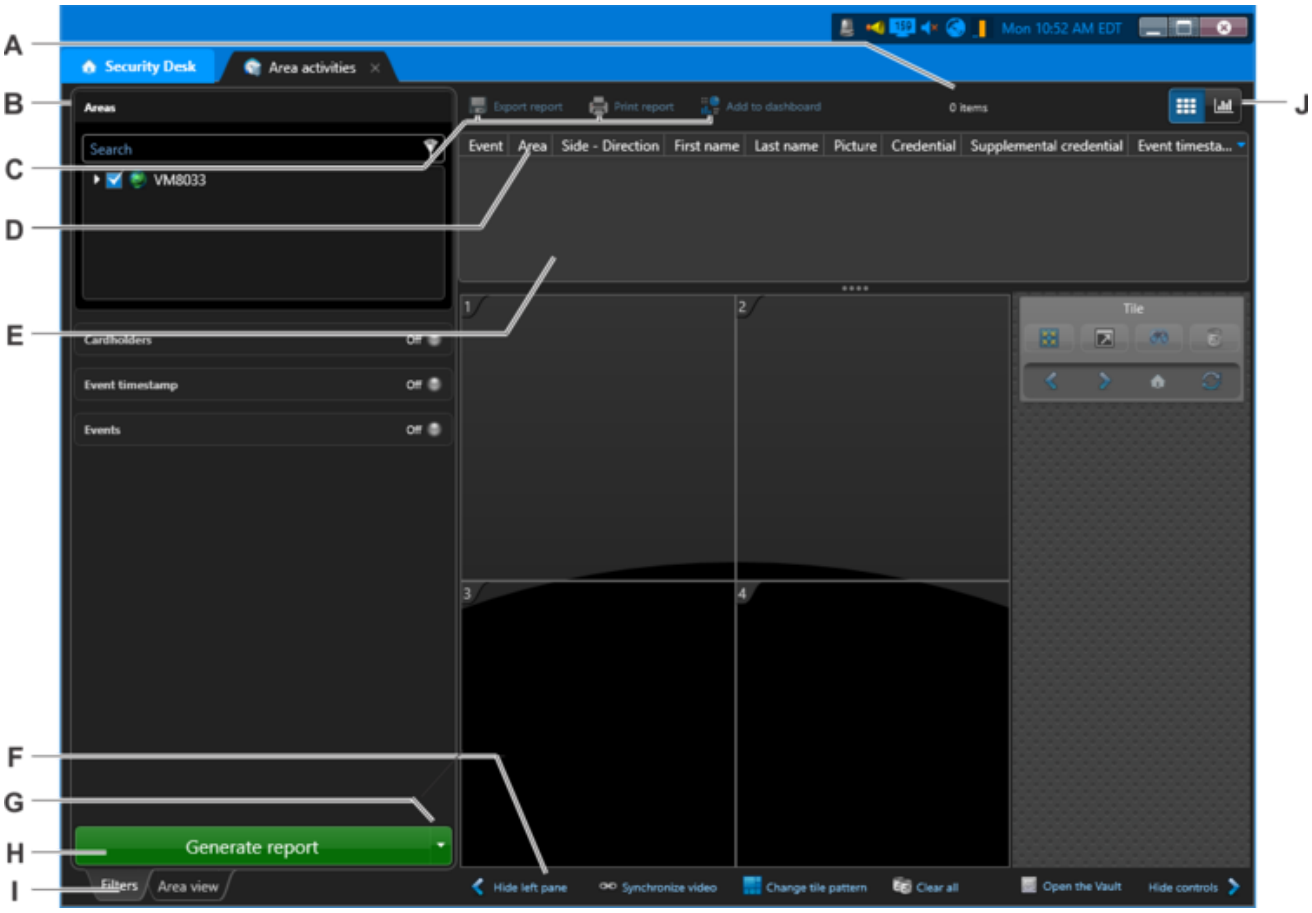
5. Dans la section Recharger la tâche, spécifiez la manière dont vous souhaitez que Security Desk se comporte lorsque quelqu'un met à jour une *tâche publique* que vous avez ouverte :
   - *Demander à l'utilisateur*. Vous demander avant de charger la définition de tâche mise à jour.
   - *Oui*. Recharger la tâche sans demander.
   - *Non*. Ne jamais recharger la tâche.
6. Cliquez sur Enregistrer.

1.5 | Rapports Security Center dans Security Desk

1.5.1 | Présentation de l'espace de travail des tâches de rapport

Les tâches de rapport permettent d'effectuer des recherches personnalisées sur les entités, activités et événements au sein de votre système Security Center à des fins d'investigation ou de maintenance. La plupart des tâches d'investigation et de maintenance sont des tâches de rapport.

Cette section présente la mise en page des tâches de rapport et décrit les éléments communs à la majorité des tâches de rapport. La tâche *Activités de secteurs* est utilisée en tant qu'exemple. Vous pouvez ouvrir la tâche Activités de secteurs en tapant son nom dans le champ Rechercher de la page d'accueil.



A	Nombre de résultats	Affiche le nombre de résultats obtenus. Un avertissement est émis si votre recherche renvoie trop de résultats. Dans ce cas, modifiez les filtres de recherche pour réduire le nombre de résultats.
B	Filtres de recherche	Utilisez les filtres de l'onglet Filtres pour définir votre recherche. Cliquez sur un en-tête de filtre pour l'activer ou le désactiver ( ). Les filtres non valables affichent *Attention* ou *Erreur*. Survolez le filtre avec la souris pour afficher le motif de l'erreur.
C	Exportez, imprimez ou ajoutez au tableau de bord	Cliquez pour exporter le rapport, l'imprimer ou l'ajouter à un tableau de bord
D	Sélectionner les colonnes	Faites un clic droit sur un en-tête de colonne pour sélectionner les colonnes à afficher dans le volet de rapport.
E	Volet de rapport	Consultez le résultat du rapport. Faites glisser un élément de la liste vers une tuile du canevas, ou faites un clic droit sur l'élément pour afficher les options supplémentaires, si disponibles (pour lancer un rapport associé par exemple).
F	Commandes de tuile	Commandes associées aux tuiles du canevas : **Synchroniser la vidéo** Synchronisez la vidéo affichée sur le canevas. **Effacer tout** Effacer le contenu des tuiles. **Modifier la mosaïque** Changer la mosaïque sur le canevas.

G	Créer et enregistrer le rapport	Cliquez pour exécuter et enregistrer directement le rapport dans un fichier (au format PDF, CSV ou Excel). Ce bouton est désactivé si vous n'avez pas sélectionné de filtres ou en cas de filtres non valables.
H	Créer un rapport	Exécuter la recherche. Ce bouton est désactivé si vous n'avez pas sélectionné de filtres ou en cas de filtres non valables. Pendant l'exécution de la requête, l'intitulé du bouton devient *Annuler*. Cliquez sur *Annuler* pour interrompre la recherche.
I	onglet Filtres	Utilisez l'onglet Filtres pour personnaliser et filtrer vos recherches. L'onglet Filtres n'apparaît que dans les tâches de rapport. REMARQUE : Cliquez sur l'onglet Vue secteur pour sélectionner des entités à afficher sur le canevas.
J	Tuiles ou graphiques	Si le rapport prend en charge les tuiles, ouvrez la vue tuiles avec le commutateur () en haut à droite de la tâche. Dans le cas contraire, ouvrez la vue graphique à l'aide du bouton Graphiques (). • Si le rapport prend en charge les tuiles : Cliquez sur le bouton Tuiles () pour afficher la vue Tuiles sous le volet de rapport. • Si le rapport prend en charge les graphiques : Cliquez sur le bouton Graphiques () pour afficher la vue Graphiques sous le volet de rapport.

1.5.2 | À propos des rapports visuels

Les graphiques dynamiques de Security Desk fournissent des données visuelles qui peuvent servir à effectuer des recherches, analyser des situations et identifier des activités répétitives.

Les rapports visuels peuvent afficher les données sous forme de graphique sur un axe donné en utilisant des courbes ou des barres pour représenter les données du rapport. L'axe des X représente toutes les étiquettes (grouper par), tandis que l'axe des Y représente le nombre d'instances relatif à l'axe des X.

Sur l'axe des X, deux types de regroupement sont possibles :

- **Valeurs nominales :** Les données peuvent être réparties sur plusieurs colonnes sur l'axe des X. Par exemple, les valeurs de l'axe des X peuvent être triées par le nombre d'instances, et l'utilisateur peut choisir le regroupement (Top 3, Top 5 ou Top 10).
- **Dates :** Les données peuvent être réparties chronologiquement sur l'axe des X. Par exemple, l'utilisateur peut modifier le regroupement par intervalle de temps (Heure, Jour, Semaine, Mois ou Année).

Types de graphiques

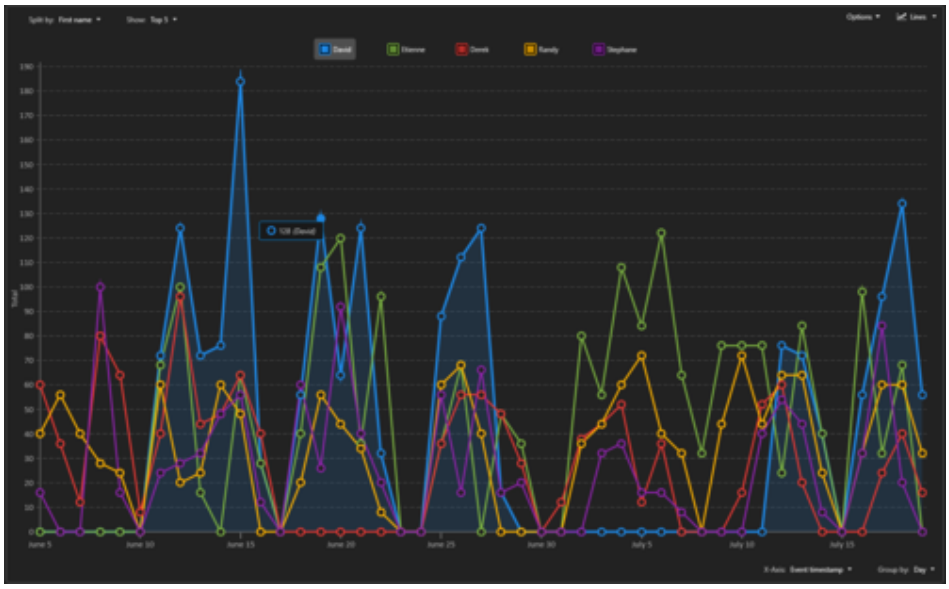
Les types de graphiques suivants sont pris en charge dans Security Center lorsque vous utilisez les fonctions Créer un rapport dans Security Desk : Lignes, Colonnes, Colonnes empilées, Barres, Barres empilées, Anneau et Secteurs.

Graphique Lignes

Utilisez un graphique Lignes pour suivre une tendance dans le temps. Par exemple, le nombre total d'instances du rapport sélectionné rapporté à une frise chronologique.

- Les graphiques de type Lignes sont mieux adaptées que les graphiques de type Barres ou Colonnes lorsque les évolutions sont modestes.
- Ils peuvent également servir à comparer l'évolution de plusieurs groupes sur une même période.

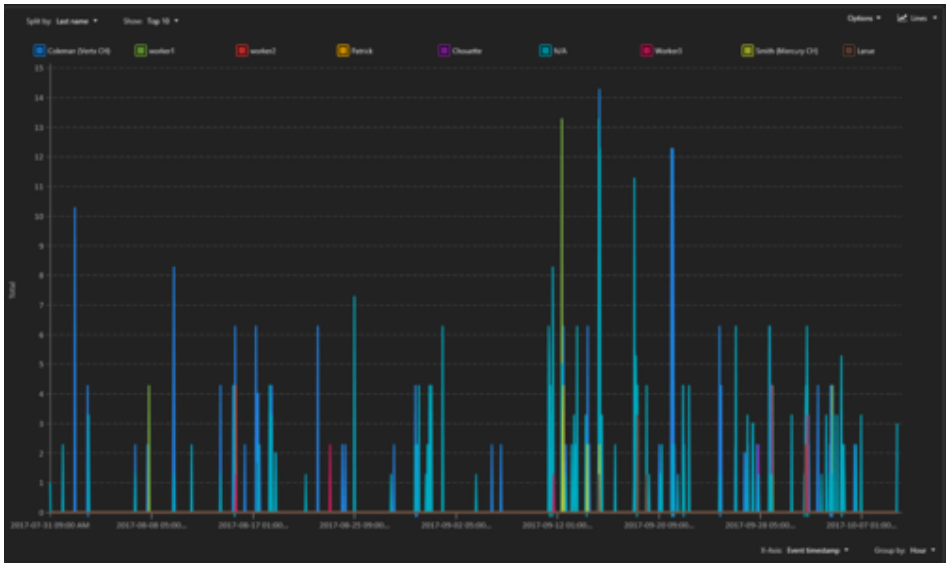
L'exemple suivant montre un rapport Événements de titulaires de cartes, réparti par : Prénom, Afficher : Top 5 et Axe des X : Heure de l'événement, Regrouper par : Jour en tant que graphique Lignes.



Graphique Lignes (simplifié)

Lorsque la plage temporelle est trop grande ou trop précise, de nombreuses données doivent être calculées et affichées à l'écran. Dans ce cas, une version simplifiée du graphique Lignes est affiché.

L’exemple suivant montre une version simplifiée du graphique Lignes.

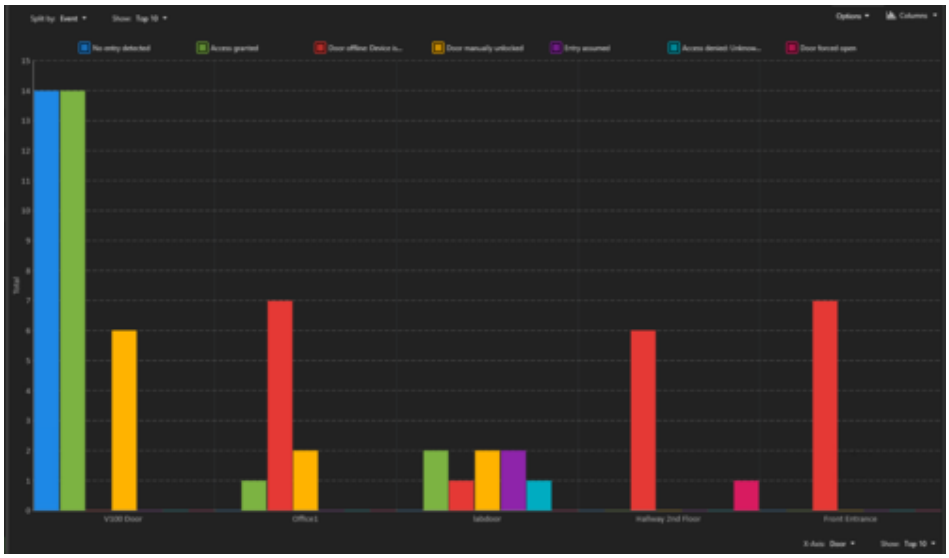


REMARQUE : La version simplifiée d'un graphique Lignes ne prend pas en charge l’interaction à la souris ni l’indication de la valeur Y d'un point donné.

Graphique en colonnes

Utilisez un graphique Colonnes si vous souhaitez regrouper les données par catégorie et afficher le résultat sous forme de barres verticales.

L’exemple suivant montre un rapport d'accès aux portes, réparti par : Événement, Afficher : Top 10 et Axe des X : Porte, Afficher : Top 10 sous forme de graphique Colonnes.



Barres empilées

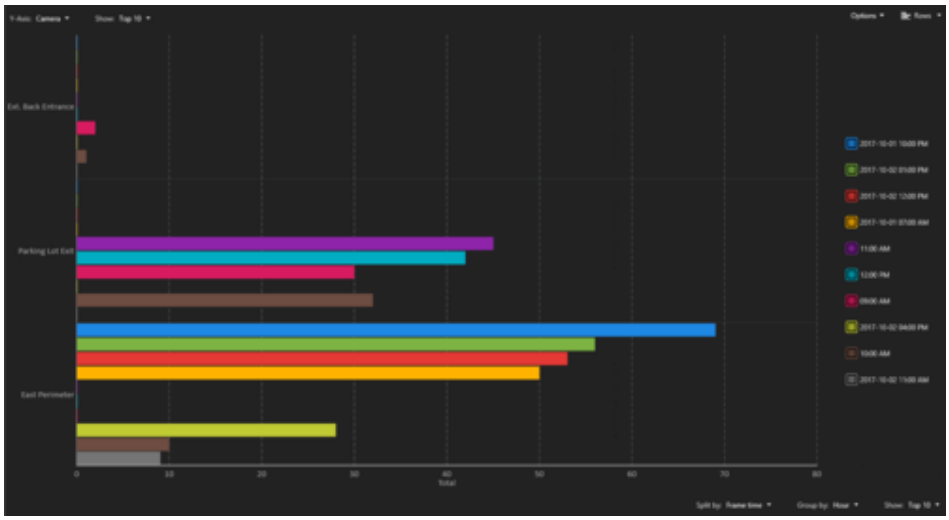
Utilisez un graphique Colonnes empilées si vous souhaitez regrouper les données par catégorie et afficher le résultat sous forme de barres verticales. L'axe des Y peut servir à répartir les données et obtenir des informations plus précises sur la valeur des X.

L’exemple suivant montre un rapport d'activité de portes, réparti par : Événement, Afficher : Top 10 et Axe des X : Porte, Afficher : Top 10 sous forme de graphique Colonnes empilées.

Lignes

Utilisez un graphique Barres si vous souhaitez regrouper les données par catégorie et afficher le résultat sous forme de barres horizontales.

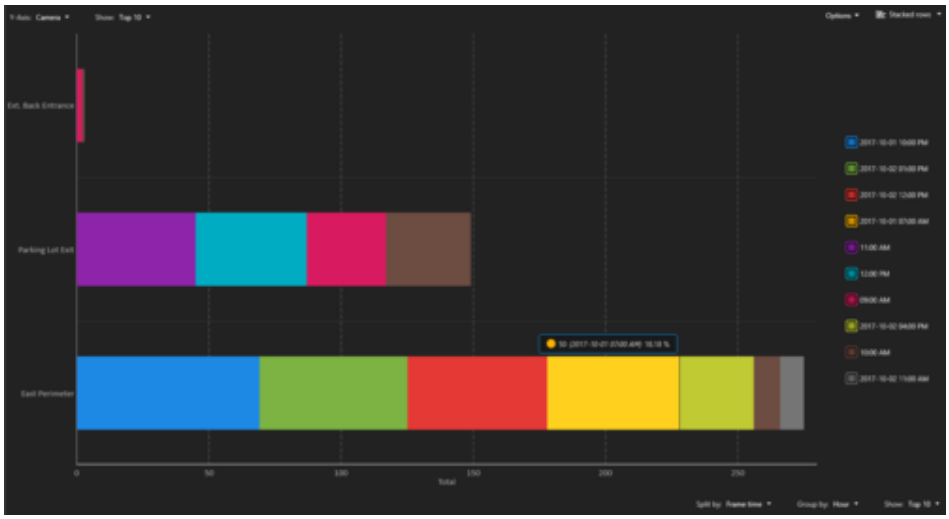
L’exemple suivant montre un rapport de détection d’intrusion, axe des Y : Caméra, Afficher : Top 10 et Répartir par : Heure d'image, Regrouper par : Heure, Afficher : Top 10 sous forme de graphique Barres.



Courbes empilées

Utilisez un graphique Barres empilées si vous souhaitez regrouper les données par catégorie et afficher le résultat sous forme de barres horizontales. L'axe des X peut servir à répartir les données et obtenir des informations plus précises sur la valeur des Y.

L’exemple suivant montre un rapport de détection d’intrusion, axe des Y : Caméra, Afficher : Top 10 et Répartir par : Heure d'image, Regrouper par : Heure, Afficher : Top 10 sous forme de graphique Barres empilées.

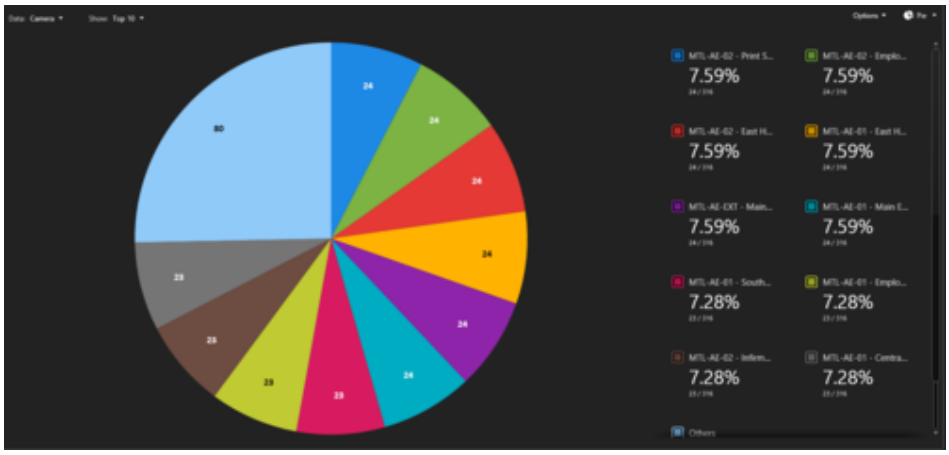


Graphiques Secteurs et Anneau

Utilisez un graphique de type Secteurs ou Anneau lorsque vous souhaitez comparer toutes les données d'un rapport.
REMARQUE : Les graphiques de type Secteurs ou Anneau ne représentent pas les évolutions dans le temps.

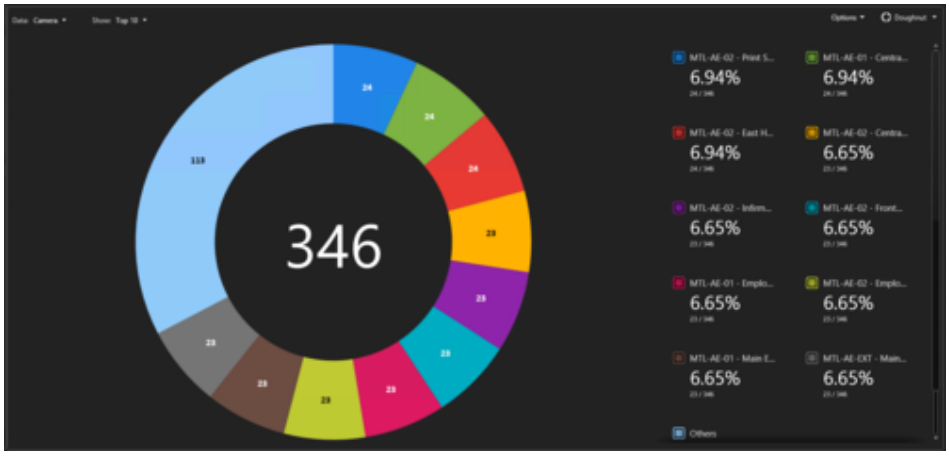
Graphique Secteurs

L’exemple suivant montre un rapport d’événements de mouvement d'une caméra, Données : Caméra, Afficher : Top 10 sous forme de graphique Secteurs.



Graphique Anneau

L’exemple suivant montre un rapport d’événements de caméra, Données : Caméra, Afficher : Top 10 sous forme de graphique Anneau.



Regardez cette vidéo pour en savoir plus. Cliquez sur l’icône Sous-titres (CC) pour activer les sous-titres dans l’une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s’affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Générer des rapports visuels

1.5.3 | Générer un rapport

Pour générer un rapport dans n'importe quelle tâche de rapport, vous devez définir les filtres de recherche, puis exécuter la requête. Vous pouvez ensuite interagir avec le résultat du rapport.

À savoir

Les tâches de rapport permettent d'effectuer des recherches personnalisées sur les entités, activités et événements au sein de votre système Security Center à des fins d'investigation ou de maintenance. La plupart des tâches d'investigation et de maintenance sont des tâches de rapport.

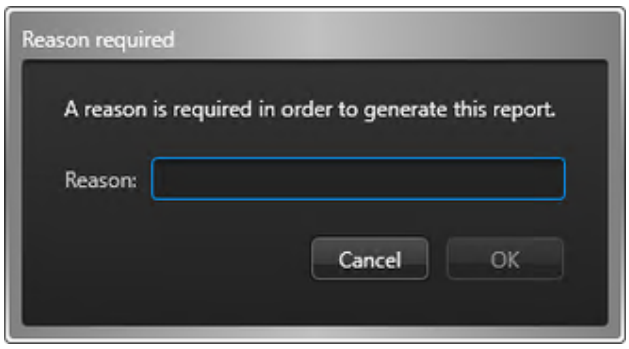
Le nombre maximum de résultats de rapports dans Security Center est 10 000. Par défaut, le nombre maximum de résultats est réglé sur 2000. Vous pouvez modifier cette valeur dans la section Performances de la boîte de dialogue Options dans Security Center.

Si vous souhaitez générer un rapport de plus de 10 000 résultats, utilisez la commande Créer et enregistrer le rapport.

REMARQUE : Ces instructions ne décrivent que la procédure générale de création d'un rapport.

Procédure

1. Ouvrez une tâche de création de rapports.
2. Dans l'onglet Filtres, utilisez les filtres pour personnaliser la recherche.
   REMARQUE : Certains filtres sont dotés d'un bouton Sélectionner tout. Ce bouton n'apparaît pas lorsqu'il y a un choix de plus de 100 entités (par exemple, si vous avez une liste de 1500 titulaires de cartes), car la création du rapport serait trop longue.
3. Sélectionnez la plage horaire du rapport.
4. Cliquez sur Générer le rapport.
   En cas de filtre non valable, le bouton Générer le rapport reste désactivé.
   IMPORTANT : La boîte de dialogue Exiger la raison est affichée lors de la création d'un rapport qui contient des données de RAPI.

   Le motif de la recherche RAPI est alors consigné et inclus dans les journaux d'audit de l'historique d'activité (rapport généré) pour respecter la réglementation des États.

   Le résultat de la requête est affiché dans le volet de rapport.
   CONSEIL : Vous pouvez trier le résultat par colonnes. Vous pouvez également faire un clic droit sur la ligne des titres pour sélectionner des colonnes, puis ajouter ou supprimer des colonnes.
5. Analysez le résultat de la requête.
   La nature des résultats obtenus dépend du type de tâche de rapport. Lorsque des séquences vidéo ou des données de RAPI sont associées aux résultats de la recherche, vous pouvez les visionner sur le canevas en faisant glisser un élément du rapport vers une tuile.
6. Exploitez le résultat de la recherche.
   Selon le contenu du résultat de la recherche, vous pouvez imprimer le rapport, enregistrer le rapport au format Excel ou PDF, exporter les séquences vidéo, etc.
7. (Facultatif) Enregistrez le rapport comme modèle.

Lorsque vous enregistrez la disposition du rapport (filtres de requête et colonnes) en tant que modèle, vous pouvez ensuite l'envoyer à un autre poste ou utilisateur avec l'action *Envoyer un rapport par e-mail*.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Générer des rapports visuels

1.5.3.1 | Sélectionner la plage horaire d'un rapport

Vous pouvez spécifier une plage horaire pour filtrer vos requêtes.

À savoir

Si la plage horaire est non valable, une icône d'erreur ( ) apparaît, et vous ne pouvez pas générer le rapport. Lorsque la plage horaire recouvre plusieurs jours, une icône d'avertissement ( ) apparaît dans le filtre indiquant que la création du rapport risque d'être plus longue.
IMPORTANT : Si votre système comprend des appareils situés dans plusieurs fuseaux horaires, vos filtres de plage horaire sont affectés.

Procédure

1. Sélectionnez une tâche de création de rapport existante ou créez-en une.
2. Dans la section Plage horaire, sélectionnez un des modes de plage horaire suivants :
   REMARQUE : Selon la tâche de rapport que vous utilisez, ce filtre est parfois appelé Déclenchée le ou Heure de l'événement.

   Au cours du dernier
   Un intervalle de temps relatif de secondes, minutes, heures, jours, semaines, mois ou années dans le passé. Le résultat du rapport peut changer à chaque exécution, car l'intervalle de temps commence lorsque le rapport est généré.

   Durant le(s) prochain(es)
   Une plage horaire relative de secondes, minutes, heures, jours, semaines, mois ou années dans le futur. Le résultat du rapport peut changer à chaque exécution, car l'intervalle de temps commence lorsque le rapport est généré.

Plage spécifique
Pour une plage de dates et heures absolue en utilisant les champs *De* et *À*. Le rapport produira le même résultat à chaque fois.

3. Si vous sélectionnez le mode de plage horaire Plage spécifique, modifiez les champs De et À de la manière suivante :
   a. En regard du champ De ou À, cliquez sur Début ou Maintenant.
   b. Pour modifier la date, cliquez sur la flèche, puis sélectionnez une date dans le calendrier.
      Vous pouvez faire un zoom arrière pour voir plusieurs années en cliquant sur l'en-tête du calendrier, ou en cliquant sur l'année ou le mois.
   c. Pour choisir une heure, cliquez sur le lien Spécifier l'heure, puis entrez l'heure directement dans les champs.

Sujet parent : Générer un rapport
Explorer

- Personnaliser les réglages de fuseau horaire
- Ouvrir les tâches

1.5.3.2 | Exporter un rapport

Toutes les tâches de rapport vous permettent d'exporter les rapports que vous avez générés. Pour exporter les données de rapport sous forme de liste (au format CSV, Excel ou PDF), utilisez l'option *Données*. Pour exporter les données de rapport sous forme de graphique (JPEG ou PNG), utilisez l'option *Graphique*. Vous pouvez également sélectionner les deux options pour créer un rapport sous forme de liste et de graphique.

À savoir

Vous ne pouvez pas exporter plus de 10 000 résultats.

Procédure

1. Au sommet du volet de rapport, cliquez sur Exporter un rapport ( ).
2. Dans la boîte de dialogue, sélectionnez Données, Graphique ou les deux, et configurez les options suivantes :

   Format de fichier
   (Données seulement) Sélectionnez le format de fichier (CSV, Excel ou PDF).

   (Graphiques seulement) Sélectionnez le format de fichier (JPEG ou PNG).

   Fichier de destination
   Spécifiez le nom du fichier de destination.

   Orientation
   (PDF seulement) Sélectionnez l'orientation en mode portrait ou paysage du fichier PDF.

   Dossiers des fichiers joints
   (CSV seulement) Spécifiez l'emplacement où les fichiers joints, comme les photos de titulaires de cartes ou les images de plaques, doivent être enregistrés.

   REMARQUE : Les options affichées dans la boîte de dialogue peuvent varier selon que le rapport prenne en charge ou non les graphiques. La fonction Graphiques n'est pas prise en charge pour les rapports suivants : Diagnostic de porte, Explorateur de fichiers vidéo et recherche de mouvement.
3. Cliquez sur Exporter.

Sujet parent : Générer un rapport
Explorer

- Présentation de la tâche Rapport d'alarmes dans Security Center

1.5.3.3 | Imprimer les rapports générés

Toutes les tâches de rapport vous permettent d'imprimer les rapports que vous avez générés. Pour imprimer les données du rapport sous forme de liste, utilisez l'option *Imprimer les données*. Pour imprimer un rapport visuel ou un graphique, utilisez l'option *Imprimer le graphique*.

À savoir

NitroPdf n'est pas actuellement pris en charge.

Procédure

Pour imprimer un rapport (données) :

1. Au sommet du volet de rapport, cliquez sur Imprimer un rapport (), puis sur Imprimer les données.
2. Dans la fenêtre Aperçu du rapport, cliquez sur Imprimer et sélectionnez une imprimante.

   CONSEIL : Vous pouvez également exporter () l'aperçu du rapport sous forme de document Microsoft Excel, Word ou Adobe PDF.

Pour imprimer un rapport (graphique) :

1. Au sommet du volet de rapport, cliquez sur Imprimer un rapport (), puis sur Imprimer le graphique.
2. Dans la fenêtre Imprimer, sélectionnez une imprimante et cliquez sur Imprimer.

Sujet parent : Générer un rapport
Explorer

- Présentation de la tâche Rapport d'alarmes dans Security Center

1.5.3.4 | Personnaliser les réglages de fuseau horaire

Si votre système Security Center comprend des appareils situés dans plusieurs fuseaux horaires, vous devez décider si les requêtes seront effectuées en fonction d'un fuseau particulier ou du fuseau de chaque appareil.

À savoir

Les réglages de fuseau horaire affectent le fonctionnement des filtres de plage horaire dans les rapports. Si vous sélectionnez un fuseau horaire fixe, les horaires provenant d'un appareil (comme une *unité de contrôle d'accès* ou une *unité vidéo*) dans un autre fuseau horaire sont ajustés pour prendre en compte la différence.

Les réglages de fuseau horaire sont conservés dans votre profil utilisateur et s'appliquent à Security Desk et Config Tool.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Date et heure.
2. Pour ajouter les abréviations de fuseau horaire à tous les horodatages dans Security Center, sélectionnez l'option Afficher les abréviations de fuseau horaire.
3. Sélectionnez la manière dont les champs horaires sont affichés et interprétés dans Security Center :
   - Pour afficher et interpréter l'heure en fonction du fuseau horaire de chaque appareil, sélectionnez l'option fuseau horaire de chaque périphérique.

     Cette option permet à chaque appareil de suivre un fuseau horaire différent. Sélectionnez cette option pour toujours afficher l'heure locale de chaque périphérique.

   - Pour afficher et interpréter l'heure en fonction d'un fuseau horaire particulier, sélectionnez l'option fuseau horaire suivant, et choisissez le fuseau horaire dans la liste déroulante.
4. Cliquez sur Enregistrer.

Exemple

Si vous créez un rapport avec une plage horaire de 9:00 à 10:00 GMT-5, et que des appareils situés à Vancouver (GMT-8) sont inclus dans la recherche, le résultat dépend de vos réglages de fuseau horaire :

- Fuseau horaire de chaque appareil : Le rapport affiche les événements survenus entre 9:00 et 10:00 GMT-8.
- Fuseau horaire fixe (réglé sur GMT-5) : Le résultat du rapport contient des événements survenus entre 6:00 et 7:00 sur la côte Ouest (GMT-8) en raison des trois heures de différence entre la côte Est et Vancouver.

Sujet parent : Générer un rapport

1.5.4 | Générer des rapports visuels

Vous pouvez afficher les rapports sous forme de graphiques dynamiques ou de graphiques. Ces données de rapport visuelles peuvent être analysées pour identifier des activités récurrentes et enrichir votre compréhension.

Avant de commencer

- Vous devez avoir la licence *Graphiques* pour générer des rapports visuels.
- Seuls les utilisateurs disposant du privilège *Afficher les graphiques* peuvent accéder aux graphiques des rapports.

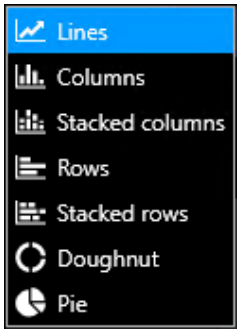
À savoir

Voici des exemples de cas d'utilisation des *rapports visuels* :

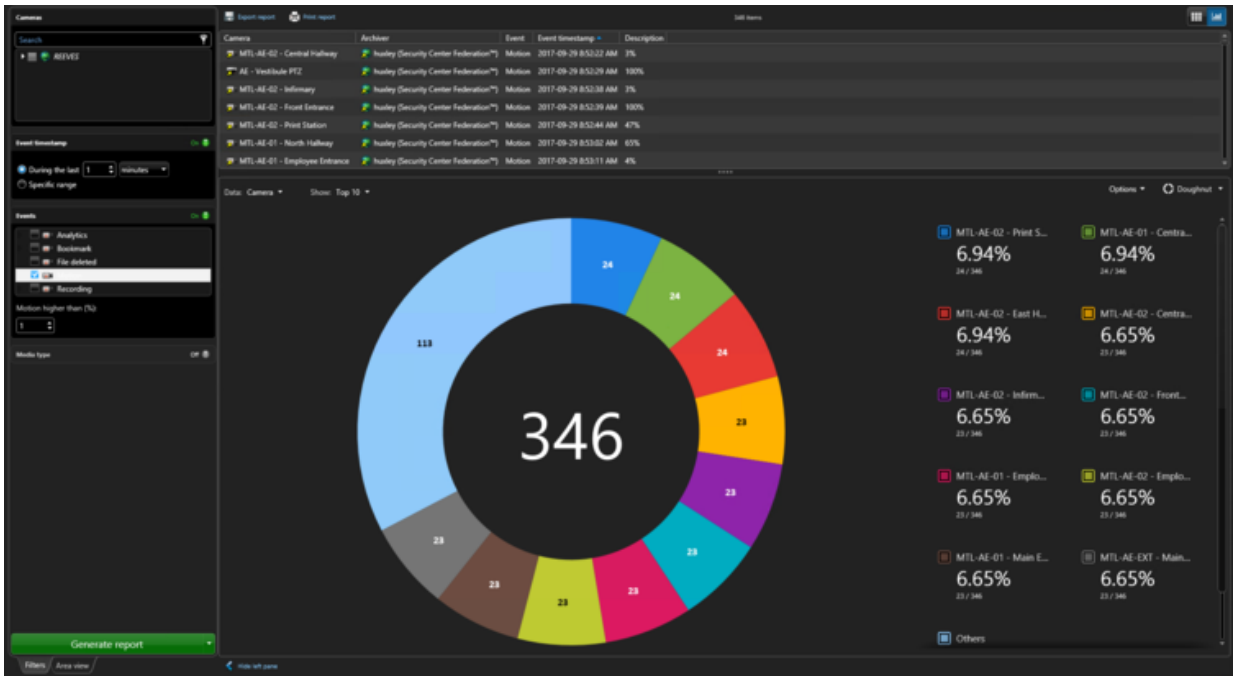
- Omnicast™ Tâche Événements de caméra : Affichez les rapports de caméras sous forme de graphiques pour comprendre l'activité de plusieurs caméras sur une période donnée.
- KiwiVision™ Analyse vidéo de sécurité : Exécutez des rapports visuels pour obtenir une vue d'ensemble de votre environnement sécurisé.
- Synergis™ Activités de portes : Affichez les événements sous forme de graphiques pour tirer des enseignements à propos de votre système de contrôle d'accès.
- AutoVu™ Tâche Lectures : Utilisez les rapports visuels pour mieux comprendre les rapports de RAPI concernant la circulation de véhicules dans votre environnement.

REMARQUE : La fonction Graphiques n'est pas prise en charge pour les rapports suivants : Diagnostic de porte, Explorateur de fichiers vidéo et recherche de mouvement.

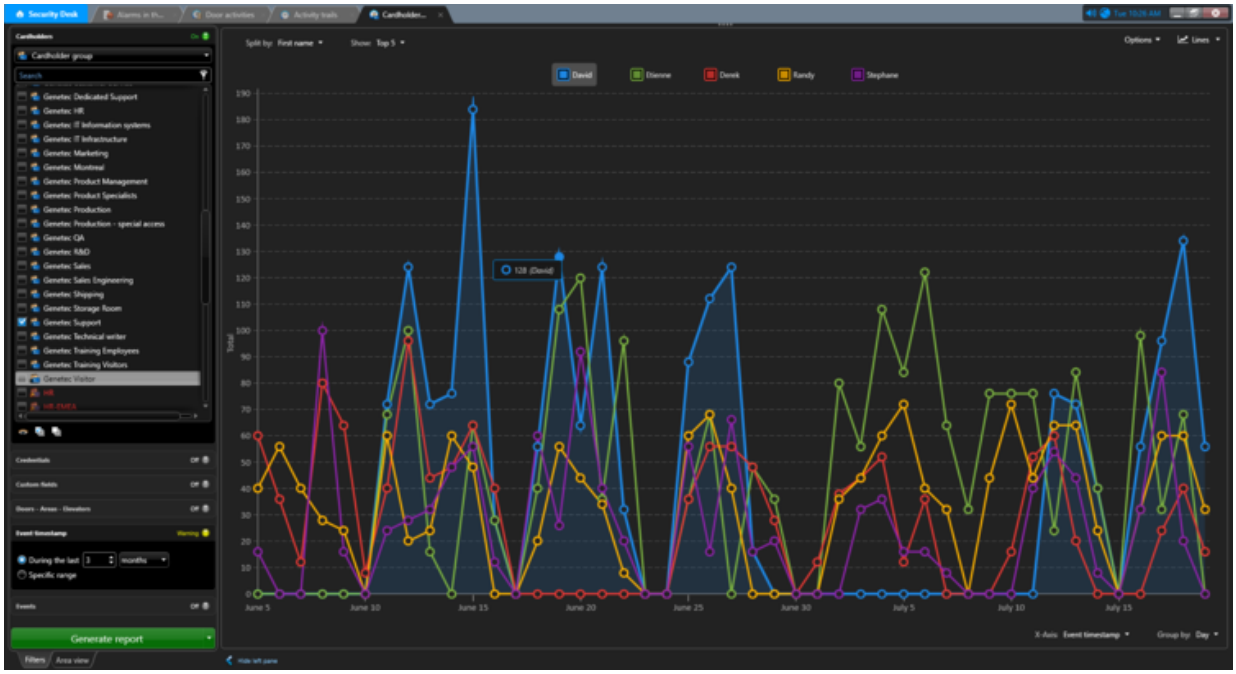
Procédure

1. Générez un rapport qui prend en charge la fonction de graphiques.
2. Cliquez sur Graphiques ().
3. Dans le volet Graphiques, sélectionnez un type de graphique dans le menu déroulant.


4. Sélectionnez les données que vous souhaitez afficher dans le rapport visuel à l'aide des menus déroulants du volet Graphiques : Répartir par, Afficher (Top 10, Top 5, or Top 3), Axe X, Axe Y ou Données.
REMARQUE : Les choix disponibles dans les menus déroulants varient en fonction du type de graphique et des données affichées dans le volet de rapport.
Le graphique Anneau suivant montre le Top 10 des événements de caméra.



Le graphique Lignes suivant montre le Top 5 des événements de titulaires de cartes répartis par Prénom et Heure d'événement regroupés par Jour sur une période donnée.



5. Affichez ou masquez des informations dans le rapport visuel :
   - Sélectionnez ( ) ou désélectionnez ( ) un élément de la légende du graphique.
   - Dans le menu déroulant Options, sélectionnez ou désélectionnez les options Afficher la grille et Afficher les valeurs pour afficher ou masquer la grille, et le nombre de résultats représenté par chaque point de données dans le rapport visuel.
   - Placez le curseur de la souris sur les éléments du graphique ou du diagramme pour afficher des informations supplémentaires. L'élément correspondant dans la légende est également mis en évidence.
6. Imprimez ou exportez le rapport sous forme de données (Excel, CSV ou PDF) ou sous forme de graphique (PNG ou JPEG).
   Les formats disponibles dépendent des résultats de la requête.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Générer un rapport
- À propos des rapports visuels
- Exporter un rapport
- Imprimer les rapports générés

1.5.5 | Créer et enregistrer un rapport

Au lieu d'attendre la création d'un rapport puis d'exporter le résultat, vous pouvez directement créer et enregistrer un rapport dans un emplacement donné.

À savoir

La création et l'enregistrement d'un rapport est utile, car vous n'êtes pas obligé de patienter devant votre poste pendant la création du rapport. En outre, cette option est utile si votre requête renvoie beaucoup de résultats, car vous n'êtes pas limité à 10 000 résultats comme lorsque vous générez un rapport normalement.
REMARQUE : Les tâches qui prennent en charge cette commande sont celles dont les résultats sont récupérés dans une base de données de rôle, pas dans le Répertoire.

Procédure

1. Sélectionnez une tâche de création de rapport existante ou créez-en une.
2. Dans l'onglet Filtres, utilisez les filtres pour personnaliser la recherche.
   REMARQUE : Certains filtres sont dotés d'un bouton Sélectionner tout. Ce bouton n'apparaît pas lorsqu'il y a un choix de plus de 100 entités (par exemple, si vous avez une liste de 1500 titulaires de cartes), car la création du rapport serait trop longue.
3. Faites un clic droit sur un en-tête de colonne dans le volet de rapport, et cliquez sur Sélectionner les colonnes ( ).
4. Sélectionnez les colonnes à inclure dans le rapport enregistré, puis cliquez sur Enregistrer.
5. Cliquez sur la liste déroulante en regard de Créer un rapport, et cliquez sur Créer et enregistrer le rapport.
   REMARQUE : Pour exporter les rapports Historique de configuration ou Historique d'activité, vous devez les créer et les enregistrer à l'aide d'une action manuelle.
6. Dans la boîte de dialogue, configurez les options suivantes :

   Format de fichier
   Sélectionnez le format de fichier. Seul le format CSV est pris en charge.

Fichier de destination
Spécifiez le nom du fichier de destination.

Orientation
(PDF seulement) Sélectionnez l'orientation en mode portrait ou paysage du fichier PDF.

Dossiers des fichiers joints
Spécifiez l'emplacement où les fichiers joints, comme les photos de titulaires de cartes ou les images de plaques, doivent être enregistrés.

7. Cliquez sur Exporter.

Résultats

Le rapport est enregistré à l'emplacement spécifié.

1.5.5.1 | Créer et enregistrer un rapport à l'aide d'une action système

Vous pouvez créer et enregistrer un rapport à l'aide d'une action manuelle.

Avant de commencer

- Enregistrez la tâche que vous souhaitez créer et exporter en tant que *tâche publique*, en spécifiant les filtres et les colonnes de votre choix. Pour en savoir plus, voir Enregistrer une tâche dans Security Center.
- Réglez le nombre maximum de résultats pouvant être enregistrés au format PDF ou Excel, et spécifiez le dossier de destination dans l'onglet *Propriétés* du Gestionnaire de rapports.

Procédure

1. Dans la zone de notification, cliquez sur Actions éclair ( ).
2. Dans la boîte de dialogue Actions éclair, cliquez sur Action manuelle.
3. Dans la liste des actions, cliquez sur Exporter un rapport.
4. Dans la liste déroulante Rapport, sélectionnez la tâche publique enregistrée que vous souhaitez exporter.
5. Dans la liste déroulante Format de fichier, sélectionnez PDF, Excel ou CSV.
6. (PDF seulement) Dans la liste déroulante Orientation, sélectionnez le format portrait ou paysage pour le fichier PDF.
7. Pour remplacer un précédent rapport exporté dans le dossier de destination, sélectionnez l'option Remplacement du fichier existant.
8. Cliquez sur OK.

Résultats

Le rapport est enregistré à l'emplacement spécifié.
Sujet parent : Créer et enregistrer un rapport

1.5.6 | Personnaliser le volet de rapport

Une fois que vous avez généré un rapport, vous pouvez personnaliser l'affichage des résultats dans le volet de rapport.

Procédure

1. Créez votre rapport.
2. Sélectionnez les colonnes à afficher :
   a. Faites un clic droit sur un en-tête de colonne dans le volet de rapport, puis cliquez sur Sélectionner les colonnes ( ).
   b. Sélectionnez les colonnes que vous souhaitez afficher et désélectionnez celles que vous souhaitez masquer.
   c. Pour modifier l'ordre d'affichage des colonnes, utilisez les flèches et .
   d. Cliquez sur OK.

3. Pour modifier la largeur d'une colonne, cliquez sur un séparateur entre deux colonnes et faites-le glisser vers la droite ou vers la gauche.
4. Pour modifier l'ordre des colonnes, cliquez sans relâcher sur un en-tête de colonne et faites-la glisser à l'endroit voulu.
5. Pour trier le rapport en fonction d'une colonne particulière, cliquez sur l'en-tête de la colonne concernée. Cliquez une deuxième fois sur l'en-tête pour inverser l'ordre de tri.
   REMARQUE : Toutes les colonnes contenant des valeurs d'horodatage sont triées en fonction de leur valeur UTC (GMT). Si vous choisissez d'afficher les heures dans Security Center en fonction des fuseaux horaires de chaque périphérique (plutôt qu'en fonction d'un fuseau horaire fixe), les heures peuvent s'afficher dans le désordre lorsque le rapport porte sur des périphériques situés dans différents fuseaux horaires.
6. Pour agrandir le volet de rapport, faites glisser le séparateur entre le volet de rapport et le canevas jusqu'au bas de la fenêtre de l'application.
7. Enregistrez la disposition de la tâche et les modifications apportées au volet de rapport de la manière suivante :
   - Pour enregistrer la tâche en tant que tâche *publique* ou *privée*, faites un clic droit sur l'onglet de la tâche, puis cliquez sur Enregistrer sous.
   - Pour enregistrer l'espace de travail afin de le retrouver lors de la prochaine utilisation de Security Desk, faites un clic droit dans la barre des tâches, puis cliquez sur Enregistrer l'espace de travail.

Explorer

- Personnaliser les réglages de fuseau horaire
- Enregistrer une tâche dans Security Center

1.5.7 | Personnaliser le comportement des rapports

Utilisez la boîte de dialogue Options pour spécifier le nombre de résultats à afficher ainsi que les réglages de messages d'avertissements.

À savoir

Lorsqu'une recherche atteint la limite spécifiée, elle s'arrête automatiquement et produit un message d'avertissement. La valeur maximale autorisée est 10 000. Les réglages de tâches sont conservés dans votre profil utilisateur et s'appliquent à Security Desk et Config Tool.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Performances.
2. Dans la section Rapports, spécifiez le Nombre maximum de résultats.
   Cette option définit le nombre maximum de résultats renvoyés par une requête d'une tâche de rapport. Cette limite permet d'assurer des performances stables en cas de résultats trop volumineux lorsque la requête est trop générale.
3. Cliquez sur l'onglet Interaction utilisateur.
4. Si vous souhaitez que Security Center affiche un message d'alerte à chaque fois que vous vous apprêtez à exécuter une requête qui risque de prendre du temps, sélectionnez l'option Afficher un avertissement si la requête risque de prendre un certain temps.
5. Cliquez sur Enregistrer.

1.6 | Tâches de base dans Security Desk

1.6.1 | Surveiller les événements

Avec la tâche Surveillance, vous pouvez surveiller les événements, comme les événements de contrôle d'accès associés aux portes et titulaires de cartes, les lectures et alertes de plaques d'immatriculation provenant d'unités de RAPI fixes et mobiles, et les événements associés aux caméras, le tout en temps réel.

À savoir

Pour surveiller des événements, vous devez surveiller les entités qui les déclenchent. Ces entités sont sélectionnées dans la tâche *Surveillance*. Vous pouvez personnaliser la manière dont la tâche Surveillance affiche les informations en fonction de vos objectifs. Par exemple, si vous surveillez des caméras, vous pouvez masquer tout à l'exception des tuiles de caméras, pour afficher des images de plus grande taille. Vous pouvez créer plusieurs tâches Surveillance pour surveiller différents ensembles d'entités, comme les caméras ou les portes.

Procédure

1. Sélectionnez les événements à surveiller.
2. Sélectionnez les entités associées aux événements que vous souhaitez surveiller.
   Une fois les entités sélectionnées, les événements qui surviennent au sein du système sont affichés en temps réel dans la liste d'événements, en ordre chronologique. Vous ne pouvez pas modifier l'ordre d'affichage des événements.
3. Pour afficher la liste d'événements, faites glisser le séparateur depuis le sommet de fenêtre de la tâche Surveillance.
4. Pour choisir les informations à afficher dans la liste d'événements, faites un clic droit sur un en-tête de colonne, puis cliquez sur Sélectionner les colonnes pour choisir les éléments à afficher dans la liste.
   Dans un système de contrôle d'accès, vous ne souhaiterez peut-être n'afficher que les champs des titulaires de cartes et des identifiants. Dans un système RAPI, vous pouvez n'afficher que les numéros de plaques et images contextuelles.
5. Pour effacer la liste d'événements, cliquez sur Effacer la liste d'événements () dans le coin supérieur droit de la tâche Surveillance.
6. Pour surveiller les événements sur le canevas, sélectionnez l'un des deux modes suivants :

   mode Tuile
   Le mode Tuile est le mode de fonctionnement principal du canevas Security Desk, et qui présente les informations dans des tuiles distinctes. Vous pouvez activer ou désactiver la surveillance pour chaque tuile.

   mode Carte
   Mode de fonctionnement du canevas Security Desk qui remplace les tuiles et les commandes par une carte géographique qui présente tous les événements géoréférencés actifs de votre système. Le basculement vers le mode Carte est une fonctionnalité de AutoVu™ et de Genetec Mission Control™ et nécessite une licence pour un de ces produits.
   REMARQUE : Pour basculer entre le mode tuile et le mode carte, votre compte doit avoir le privilège *Basculer en mode carte*.

7. Dans la vue secteur, faites glisser les entités que vous souhaitez observer sur le canevas.
8. (Facultatif) Pour empêcher que le contenu d'une tuile soit remplacé par de nouveaux événements, désactivez la surveillance dans la tuile concernée.
   CONSEIL : Cela peut s'avérer utile si vous affichez un module externe de tuile sur le canevas, et que vous ne souhaitez pas qu'un événement le remplace.
   a. Sélectionnez une tuile sur le canevas.
   b. Dans le widget Tuile, cliquez sur Surveillance (), puis sur Surveiller les événements.
   La coche en regard de Surveiller les événements disparaît et l'arrière-plan des ID de tuile devient noir.

Explorer

- Surveiller les événements de RAPI dans mode Tuile
- Surveiller les événements de RAPI dans mode Carte

1.6.1.1 | Sélectionner des événements à surveiller

Avant d'utiliser la tâche Surveillance, vous devez sélectionner les types d'événements que vous souhaitez surveiller.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Événements.
2. Sur la page Options d'événements, sélectionnez les événements à surveiller.
3. Dans la colonne Afficher dans la tuile, cochez les événements que vous souhaitez afficher sur le canevas de la tâche Surveillance. Lorsqu'une case est décochée, l'événement n'apparaît que dans la liste d'événements.
4. Cliquez sur Enregistrer.

Lorsque vous avez terminé

Sélectionnez les entités à surveiller qui déclenchent les types d'événements que vous avez sélectionnés.
Sujet parent : Surveiller les événements
Explorer

- Types d'événements

1.6.1.2 | Sélectionner des entités à surveiller

Avant de surveiller des événements dans la tâche Surveillance, vous devez sélectionner les entités qui déclenchent ces événements.

Avant de commencer

Sélectionnez les événements à surveiller.

À savoir

Pour surveiller des événements, il est important de sélectionner les entités que vous souhaitez surveiller, car certains événements peuvent être générés par différentes entités. Par exemple, un événement *Accès autorisé* peut être généré par un titulaire de cartes, un visiteur ou un identifiant. Si vous ne surveillez que les titulaires de cartes, vous ne recevrez pas tous les événements Accès autorisé.

Procédure

1. Sur la page d'accueil, cliquez sur Tâches > Surveillance.
2. (Facultatif) Pour donner un nom unique à l'onglet, faites un clic droit sur l'onglet, cliquez sur Renommer la tâche ; dans la zone Nom de la tâche, tapez un nom, puis cliquez sur Renommer.
   Vous pouvez renommer l'onglet pour indiquer ce qui est surveillé, par exemple *Surveillance d'événements de caméra*.
   C'est particulièrement utile lorsque vous avez plusieurs onglets de surveillance ouverts en même temps.
3. Dans la vue secteur, sélectionnez les entités particulières que vous souhaitez surveiller (caméras, portes, titulaires de cartes, véhicules de patrouille, caméras fixes AutoVu™ Sharp, listes de véhicules recherchés, et ainsi de suite).
   Pour sélectionner plusieurs entités, appuyez sur les touches Ctrl ou Maj pendant que vous cliquez sur les entités.
4. Faites glisser les entités sélectionnées sur l'icône Surveillance ( ) au bas de la tâche Surveillance.
   Les entités sélectionnées sont ajoutées à la liste Surveillance des événements.
   REMARQUE : Par défaut, toutes les tuiles sont armées pour surveiller les événements. Vous pouvez armer et désarmer toutes les tuiles à tout moment en cliquant sur . Lorsqu'une tuile est armée pour surveiller les événements, l'arrière-plan de l'ID de la tuile est bleu.
5. (Facultatif) Pour ajouter des entités supplémentaires depuis la boîte de dialogue Surveillance des événements, procédez de la manière suivante :
   a. Cliquez sur Surveillance ( ), puis sous Surveillance des événements, cliquez sur Ajouter ( ).
   b. Sélectionnez le type d'entité à surveiller (vue secteur, titulaire de cartes, groupe de titulaires de carte, visiteur, liste de véhicules recherchés, permis, utilisateur, actif, et ainsi de suite).
      CONSEIL : Certains types d'entités (secteurs, caméras, portes, ascenseurs, zones, et ainsi de suite) n'apparaissent que dans la *vue secteur*.
   c. Sélectionnez les entités particulières que vous souhaitez surveiller (caméras, portes, titulaires de cartes, véhicules de patrouille, caméras fixes AutoVu™ Sharp, listes de véhicules recherchés, et ainsi de suite).
   d. Pour ajouter un filtre conditionnel, sélectionnez une entité dans la liste déroulante Pour.
      Vous pouvez surveiller des événements pour un groupe de titulaires de carte à une porte spécifique.
      REMARQUE : Seuls les événements associés au groupe de titulaires de cartes *et* la porte sont surveillés. Vous ne recevrez pas d'autres événements pour la porte à moins de surveiller également cette porte.
   e. Cliquez sur Ajouter.
6. (Facultatif) Dans la colonne *Tuile* de la liste Surveillance des événements, sélectionnez la tuile censée afficher l'entité.
   Vous pouvez associer plusieurs entités à une même tuile. Par défaut, les événements sont affichés dans n'importe quelle tuile (Tous).

Vous pouvez configurer la Tuile 1 pour qu'elle affiche les événements qui surviennent à la porte *Entrée principale*.

Résultats

La surveillance est activée dans les tuiles du canevas. En cas de nouvel événement, Security Desk affiche celui-ci dans une tuile vide. Lorsqu'il n'y a plus de tuiles vides, l'entité affichée depuis le plus longtemps est automatiquement remplacée par le nouvel événement.

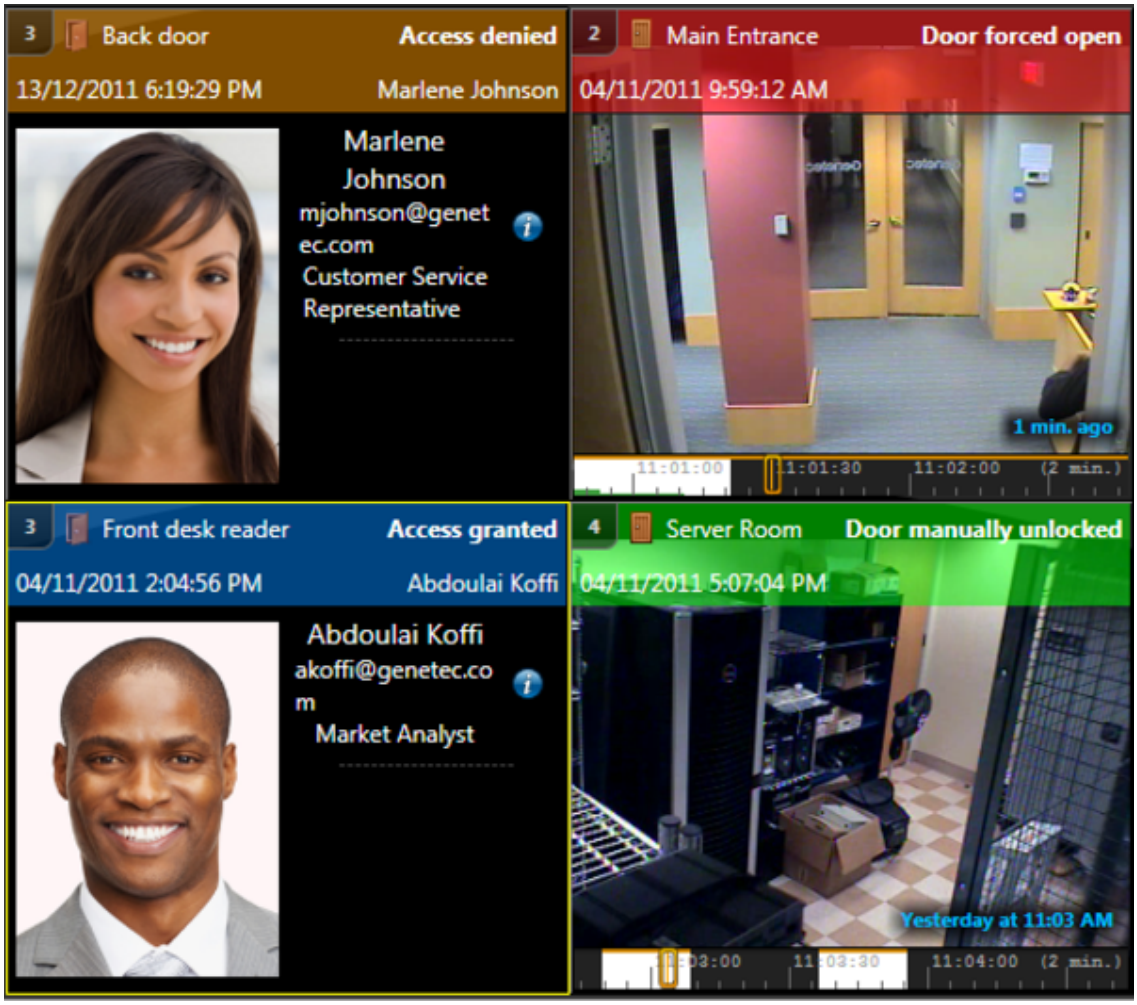
Sujet parent : Surveiller les événements

1.6.1.3 | Couleurs d'événements

Lorsque vous surveillez des entités, les événements générés sont affichés sur le canevas dans différentes couleurs correspondant aux types d'événements. Pour les systèmes complexes, cela permet de se concentrer sur les événements les plus importants.

Les couleurs d'événement sont configurées dans Config Tool.

La figure suivante montre quatre événements de contrôle d'accès différents associés à différentes couleurs.



Sujet parent : Surveiller les événements

1.6.1.4 | Personnaliser les options de la tâche Surveillance

Vous pouvez personnaliser le nombre d'événements récupérés depuis la base de données et affichés lorsque vous chargez une tâche Surveillance enregistrée.

À savoir

Ce réglage est conservé dans votre profil utilisateur.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Performance.
2. Dans l'option Nombre maximal d'événements à afficher, sélectionnez le nombre maximum d'événements à charger.
3. Cliquez sur Enregistrer.

Sujet parent : Surveiller les événements

1.6.2 | Périodes d'occurrence des événements

Certaines unités de détection d'intrusion et unités de contrôle d'accès peuvent stocker des événements qui se produisent lorsque les unités sont déconnectées de Security Center, mais continuent de fonctionner physiquement. Les périodes d'occurrence indiquent le moment où ces événements hors ligne se sont produits et déterminent ce qui se passe avec les événements après que les unités se sont reconnectées à Security Center.

La période d'occurrence d'un événement est indiquée dans la colonne Période d'occurrence dans les rapports et dans la tâche Surveillance. Les événements sont traités différemment dans Security Center, selon que son entité source est une unité de détection d'intrusion ou une unité de contrôle d'accès.

Le tableau suivant répertorie les différentes périodes d'occurrence et leur incidence sur les événements :

Période d'occurrence	Comment l'événement est traité dans Security Center
En ligne	• L'événement est survenu lorsque l'entité était en ligne. • L'événement est enregistré dans la base de données et accessible dans les rapports. • L'événement est affiché dans la tâche Surveillance. • L'événement peut déclencher des actions via les événements-actions.
Délai de grâce	• L'événement est enregistré dans la base de données et accessible dans les rapports. • L'événement est affiché dans la tâche Surveillance. • L'événement peut déclencher des actions via les événements-actions.
	• Pour les unités de détection d'intrusion : l'événement s'est produit pendant le Délai de grâce configuré pour l'extension d'unité dans Config Tool. • Pour les unités de contrôle d'accès : l'événement s'est produit dans les 15 minutes précédant la réactivation de l'unité.

Alarme hors ligne	• L'événement est enregistré dans la base de données et accessible dans les rapports.
	• L'événement n'apparaît pas dans la tâche Surveillance, sauf pour des événements d'intrusion spécifiques.
	• L'événement peut déclencher les actions suivantes par le biais d'événements-actions :
	  ◦ *Déclencher l'alarme*
	  ◦ *Ajouter un signet*

Période d'occurrence	Comment l'événement est traité dans Security Center

	• Pour les unités de détection d'intrusion : l'événement s'est produit entre le Délai de grâce et le Délai de grâce de l'alarme configuré pour l'extension d'unité dans Config Tool. Les événements suivants apparaissent dans la tâche Surveillance et peuvent déclencher des actions via des événements-actions :
	  ◦ *Alarme d'entrée activée*
	  ◦ *Alarme de secteur de détection d'intrusion activée*
	  ◦ *Contrainte de secteur de détection d'intrusion*
	  ◦ *Altération d'unité de détection d'intrusion*
	• Pour les unités de contrôle d'accès : l'événement s'est produit dans les 72 heures précédant la réactivation de l'unité.

Hors ligne	• L'événement est enregistré dans la base de données et accessible dans les rapports. • L'événement n'est pas affiché dans la tâche Surveillance. • L'événement ne peut pas déclencher d'actions par le biais d'événements-actions.
	• Pour les unités de détection d'intrusion : l'événement s'est produit entre le Délai de grâce de l'alarme et le Délai de grâce de persistance configuré pour l'extension d'unité dans Config Tool. • Pour les unités de contrôle d'accès : l'événement s'est produit plus de 72 heures avant la réactivation de l'unité.

Motifs de passage hors ligne des unités

Une unité de contrôle d'accès ou de détection d'intrusion peut être hors ligne dans Security Center pour les raisons suivantes :

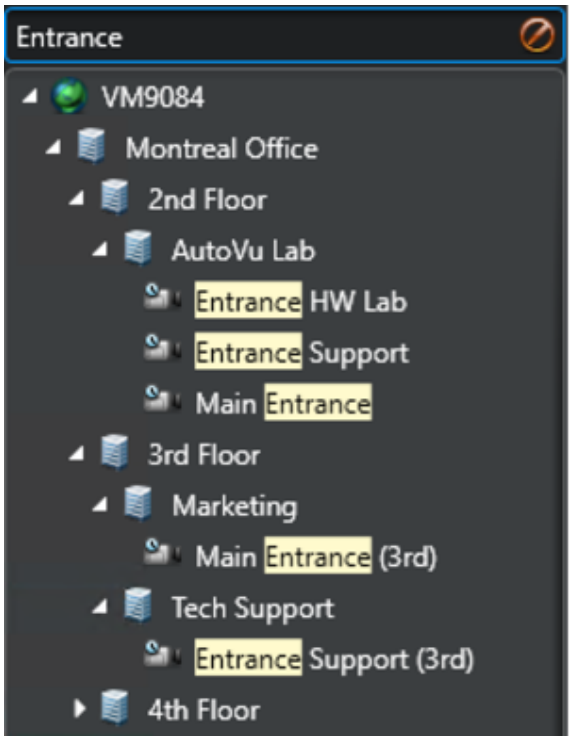
- L'unité est en cours de redémarrage.
- Le micrologiciel de l'unité est en cours de mise à jour.
- La connexion de l'unité avec le *Gestionnaire d'accès* ou le *Gestionnaire d'intrusions* a été perdue.
- La connexion du Gestionnaire d'accès ou du Gestionnaire d'intrusions avec le *Directory* a été perdue. Dans ce cas, le rôle se déconnecte des unités tant que la connexion au Répertoire n'est pas rétablie.

1.6.3 | Rechercher des entités

Si vous ne trouvez pas l'entité qui vous intéresse dans une tâche, vous pouvez rechercher l'entité par nom.

Procédure

1. Dans le champ Rechercher du sélecteur, entrez le nom de l'entité recherchée.
2. Cliquez sur Rechercher ( ).



Seules les entités dont le nom contient le texte saisi sont affichées.

3. Cliquez sur Effacer le filtre ( ) pour annuler l'utilisation du filtre.

Explorer

- États des entités

1.6.3.1 | Rechercher des entités avec l'outil de recherche

Vous pouvez appliquer des filtres pour isoler les entités qui vous intéressent à l'aide de l'*Outil de recherche*.

À savoir

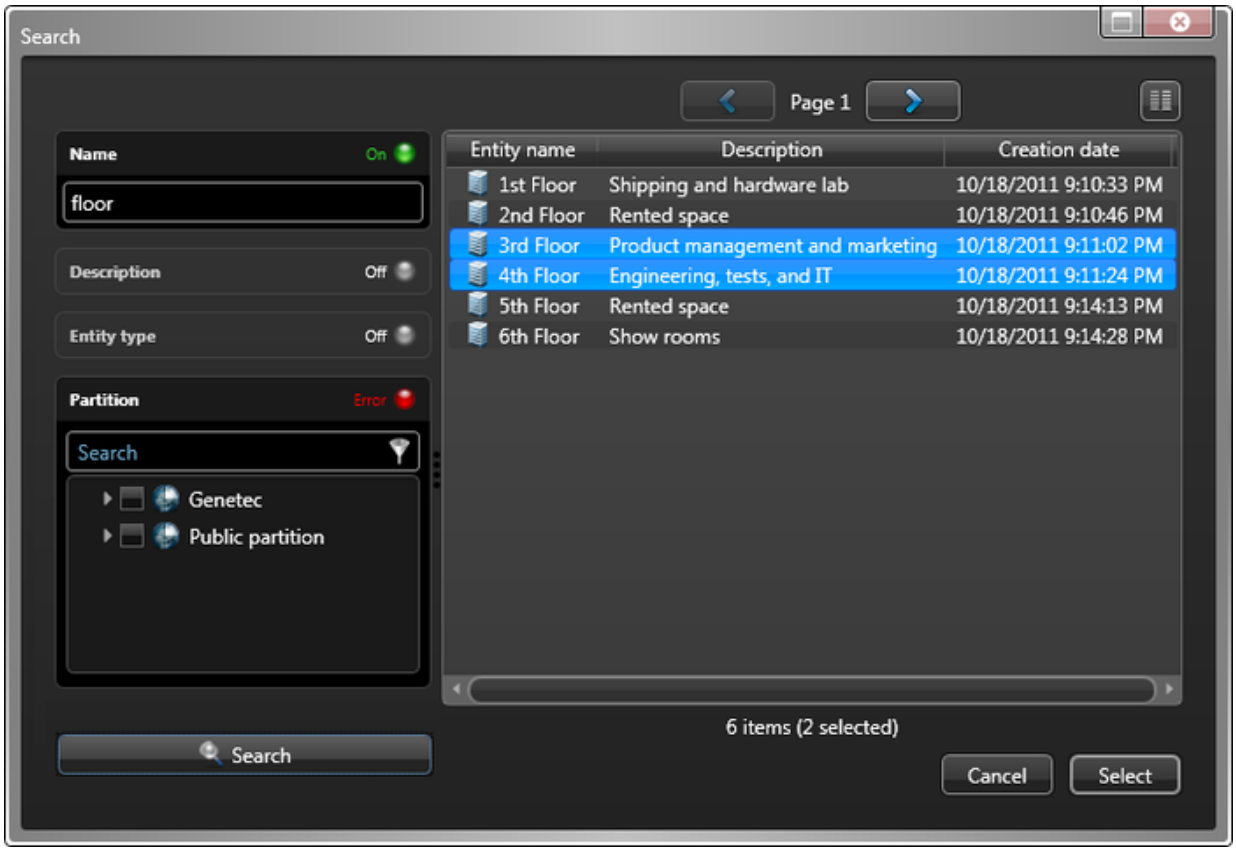
L'*Outil de recherche* est disponible dans de nombreuses tâches. Les filtres disponibles dépendent de la tâche que vous utilisez. Par exemple, vous pouvez filtrer les entités par nom, description, type, partitions, etc.

Procédure

1. Dans le champ Rechercher du sélecteur, cliquez sur Appliquer un filtre personnalisé ( ).
2. Dans la fenêtre Rechercher, utilisez les filtres pour définir vos critères de recherche.
   - Pour activer un filtre, cliquez sur son en-tête. Les filtres actifs sont affichés avec un voyant vert ( ).
   - Pour désactiver un filtre ( ), cliquez sur son en-tête.

   REMARQUE : Les filtres non valables sont affichés en rouge. Survolez l'en-tête avec la souris pour afficher la nature du problème.
3. Cliquez sur Rechercher ( ).
   Le résultat de la recherche est affiché sur la droite. Le nombre de résultats est indiqué au bas de la liste.
4. Cliquez sur Sélectionner les colonnes ( ) pour choisir les colonnes à afficher dans la liste des résultats.
5. Sélectionnez les entités de votre choix.

   CONSEIL : Maintenez la touche CTRL enfoncée pour sélectionner plusieurs éléments. Cliquez sur et pour parcourir les pages de résultats.



6. Cliquez sur Sélectionner.
   Seules les entités sélectionnées sont affichées dans le sélecteur.
7. Cliquez sur Effacer le filtre ( ) pour annuler l'utilisation du filtre.

Sujet parent : Rechercher des entités

1.6.4 | Déclenchement d'actions éclair dans Security Center

Vous pouvez créer une action éclair à déclencher avec les touches de fonction de votre clavier ou depuis la zone de notification.

À savoir

Une action éclair est une *action* associée à une touche de fonction de l'ordinateur. Vous pouvez déclencher une action éclair dans Security Desk en appuyant sur Ctrl+*touche de fonction* (par exemple, `Ctrl+F1` déclenche la première action éclair de la liste), ou depuis la zone de notification.
REMARQUE : L'affectation des actions éclair aux touches de fonction est propre à votre compte utilisateur.

Procédure

1. Dans la zone de notification, cliquez sur Actions éclair ( ).
2. Dans la boîte de dialogue Actions éclair, cliquez sur Modifier.
3. Cliquez sur Ajouter ( ).
4. Nommez l'action éclair dans le champ Nom.
5. Dans la fenêtre Configurer une action, sélectionnez un type d'action, puis spécifiez les réglages requis par l'action.
6. Cliquez sur OK.
   L'action éclair est créée et la boîte de dialogue Action éclair se ferme.
7. Pour ouvrir à nouveau la boîte de dialogue Action éclair, cliquez sur Actions éclair ( ) dans la zone de notification.
8. (Facultatif) Cliquez sur Modifier et procédez de l'une des manières suivantes :

- Pour créer une autre action éclair, cliquez sur Ajouter ( ).
- Pour supprimer l'action éclair sélectionnée, cliquez sur Supprimer ( ).
- Pour modifier l'action éclair sélectionnée, cliquez sur Modifier ( ).
- Si vous avez créé plusieurs actions éclair, cliquez sur pour déplacer l'action éclair sélectionnée vers le haut de la liste. Vous modifiez ainsi la touche de fonction affectée à l'action.
- Si vous avez créé plusieurs actions éclair, cliquez sur pour déplacer l'action éclair sélectionnée vers le bas de la liste. Vous modifiez ainsi la touche de fonction affectée à l'action.

9. Cliquez sur Terminé.
   Les actions éclair que vous avez créées sont présentées avec les touches de fonctions associées (F1, F2, et ainsi de suite).
10. Déclenchez l'action éclair de l'une des manières suivantes :
    - Sélectionnez une action éclair, puis cliquez sur Exécuter.
    - Appuyez sur Ctrl+*Fn*.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Types d'actions

1.6.5 | Déclenchement d'actions ponctuelles dans Security Center

Dans Security Center, vous pouvez déclencher une action ponctuelle depuis la zone de notification.

À savoir

Bien que les actions soient généralement déclenchées par le biais du mécanisme événement-action, vous pouvez les déclencher manuellement depuis la zone de notification en cas de besoin.
Pour les actions suivantes, seuls les utilisateurs actuellement en ligne peuvent être le destinataire :

- Effacer les tâches
- Afficher une entité dans Security Desk
- Jouer un son
- Envoyer un message
- Envoyer une tâche

Procédure

1. Dans la zone de notification, cliquez sur Actions éclair ( ).
2. Dans la boîte de dialogue Actions éclair, cliquez sur Action manuelle.
3. Dans la fenêtre Configurer une action, sélectionnez un type d'action, puis spécifiez les réglages requis par l'action.
4. Cliquez sur OK.

Résultats

L'action manuelle est déclenchée.
Explorer

- Types d'actions

1.6.6 | Configurer la zone de notification

Vous pouvez sélectionner les icônes à afficher dans la zone de notification.

À savoir

Par défaut, la zone de notification apparaît dans le coin supérieur droit de la fenêtre de l'application.

Les réglages de zone de notification sont conservés dans votre profil utilisateur et s'appliquent à Security Desk et Config Tool.

BONNE PRATIQUE : Il est recommandé d'afficher les icônes que vous utilisez régulièrement, afin de pouvoir basculer facilement vers les tâches associées.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Visuel.
2. Dans la liste déroulante en regard des icônes de la section Barre d'outils, sélectionnez le mode d'affichage de chaque élément :

   Afficher
   Toujours afficher l'icône.

   Masquer
   Toujours masquer l'icône.

   N'afficher que les notifications
   N'afficher l'icône qu'en cas de notification.

3. Cliquez sur Enregistrer.

1.6.6.1 | Icônes de la zone de notification dans Security Desk

La zone de notification contient des icônes qui offrent un accès rapide à certaines fonctionnalités du système, et des indicateurs d'événements système et d'informations d'état. Les réglages de zone de notification sont conservés dans votre profil utilisateur et s'appliquent à Security Desk et Config Tool.

Le tableau suivant présente les icônes de la zone de notification et leur utilisation :

Icône	Nom	Description
	Horloge	Affiche l'heure locale. Survolez l'horloge pour afficher la date actuelle dans une infobulle. Vous pouvez personnaliser les réglages de fuseaux horaires.
	Jauge des ressources	Affiche l'utilisation des ressources sur votre ordinateur (processeur, mémoire, processeur graphique et réseau). Survolez l'icône pour afficher le pourcentage d'utilisation des ressources. Cliquez pour ouvrir la boîte de dialogue Informations matérielles afin de consulter des informations et des conseils de dépannage supplémentaires.
	Infos sur la session	Indique le nom de l'utilisateur et le Répertoire Security Center actuels. Cliquez deux fois pour basculer entre l'affichage bref et détaillé.
	Volume	Affiche le niveau du volume (de 0 à 100) de Security Desk. Cliquez pour régler le volume avec un curseur, ou pour couper le son.
	ID de moniteur	Affiche le numéro d'ID logique affecté à votre moniteur Security Desk. Un ID unique est attribué à chaque moniteur, pour le contrôle par clavier CCTV, les macros et la surveillance à distance.
	Surveillance à distance	Affiche le nombre d'utilisateurs qui contrôlent votre poste Security Desk à distance. Cliquez pour afficher des informations sur les utilisateurs qui contrôlent votre poste Security Desk, ou pour les déconnecter si vous avez les privilèges nécessaires.
	Messages système	Affiche le nombre de messages système (dysfonctionnements, avertissements, messages). Cliquez pour ouvrir la boîte de dialogue Messages système et consulter ces messages. En cas de dysfonctionnement, l'icône devient rouge (). En cas d'avertissement, l'icône devient jaune. S'il n'y a que des messages, l'icône devient bleue. Pour en savoir plus, voir Afficher les messages système.
	Mises à jour	Apparaît si une mise à niveau critique du micrologiciel est nécessaire. Cliquez sur l'icône pour afficher les détails.
	Détection d'intrusion	Indique le nombre d'entités de détection d'intrusion qui nécessitent votre attention (). Cliquez pour afficher les détails dans la boîte de dialogue Présentation de la détection d'intrusion.
	Actions éclair	Cliquez pour ouvrir la boîte de dialogue *Actions éclair* et déclencher une action ponctuelle ou une action éclair. Les actions éclair sont des actions associées aux touches de fonction de votre clavier. Pour en savoir plus, voir Déclenchement d'actions éclair dans Security Center.
	Manette de jeu	Indique qu'un contrôleur USB, comme une manette, est actuellement connecté à votre poste Security Desk.
	Clavier CCTV	Indique qu'un clavier de sécurité est connecté à votre poste Security Desk.
	Niveaux de risque	Indique si un niveau de risque est activé au sein du système. L'icône devient rouge () lorsqu'un niveau de risque est activé. Cliquez pour ouvrir la boîte de dialogue *Niveaux de risque* et activer ou désactiver un niveau de risque. Pour en savoir plus, voir Réagir aux événements critiques avec les niveaux de risque.
	Alarmes	Indique si un niveau de risque est activé au sein du système. L'icône devient rouge () lorsqu'un niveau de risque est activé. Cliquez pour ouvrir la boîte de dialogue *Niveaux de risque* et activer ou désactiver un niveau de risque. Pour en savoir plus, voir Acquittement des alarmes.

Icône	Nom	Description
	Inventaire	Indique le nombre de fichiers de déchargement MLPI en attente de rapprochement. Cliquez pour ouvrir la tâche Gestion d'inventaire et rapprocher les lectures. Pour en savoir plus, voir Créer un inventaire de parc de stationnement.
	Cycle de tâches	Cliquez pour activer ou désactiver le cycle de tâches. Pour en savoir plus sur le réglage de la durée d'affichage de chaque tâche, voir Personnaliser le comportement des tâches dans Security Desk.
	Tâche de fond	Indique qu'un processus est exécuté en arrière-plan, comme une exportation de fichier vidéo. Cliquez sur l'icône pour en savoir plus sur le processus en cours d'exécution.
	Demandes de cartes	Indique le nombre de demandes d'impression de cartes d'identification en attente (). Cliquez pour ouvrir la boîte de dialogue *Demandes de cartes* et répondre aux requêtes. Pour en savoir plus, voir Répondre aux demandes de cartes d'identification.
	Conversion de fichiers vidéo	Indique le nombre de demandes d'impression de cartes d'identification en attente (). Cliquez pour ouvrir la boîte de dialogue *Demandes de cartes* et répondre aux requêtes. Pour en savoir plus, voir Convertir des fichiers vidéo au format ASF ou MP4.

Sujet parent : Configurer la zone de notification

1.6.7 | Déplacer la barre des tâches

Vous pouvez configurer la barre des tâches afin de l'afficher sur n'importe quel bord de la fenêtre de l'application, ou pour ne l'afficher que lorsque vous survolez son emplacement attitré.

À savoir

Lorsque vous masquez automatiquement la barre des tâches, la zone de notification est également masquée. Ces réglages sont conservés dans votre profil utilisateur et s'appliquent à Security Desk et Config Tool.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Visuel.
2. Dans la liste déroulante Position de la barre des tâches, sélectionnez le bord de votre choix.
3. Le cas échéant, sélectionnez l'option Masquer automatiquement la barre des tâches.
4. Pour afficher le nom de la tâche actuelle lorsque le *cycle de tâches* est activé et que la barre des tâches est masquée, sélectionnez l'option Afficher le nom de tâche en incrustation.
5. Cliquez sur Enregistrer.

1.6.8 | Surveillance à distance

La tâche Distant permet de surveiller et contrôler à distance d'autres instances de Security Desk de votre système, en utilisant les tâches *Surveillance* et *Surveillance d'alarmes*.

La tâche Distant propose les deux modes suivants :

Mode simple
Permet de contrôler un poste de travail Security Desk individuel.

Mode Mur d'images
Permet de contrôler un groupe de moniteurs Security Desk qui composent un mur d'images. Si votre site est équipé d'un mur vidéo physique, vous pouvez contrôler ses moniteurs depuis votre Security Desk local. Chaque moniteur du mur d'images physique est ajouté sous forme de Security Desk distant distinct dans la tâche Distant.

Les actions que vous effectuez sur le poste Security Desk distant sont affichées en local dans la tâche Distant, ainsi que sur le poste Security Desk que vous contrôlez. Vous pouvez exploiter toutes les autres tâches locales pendant que vous surveillez un autre Security Desk à distance.

IMPORTANT : Vous ne pouvez pas surveiller des Security Desk distants lorsqu'une version plus ancienne de Security Center est installée. La rétrocompatibilité n'est pas prise en charge pour la surveillance à distance.

1.6.9 | Se connecter aux applications Security Desk distantes

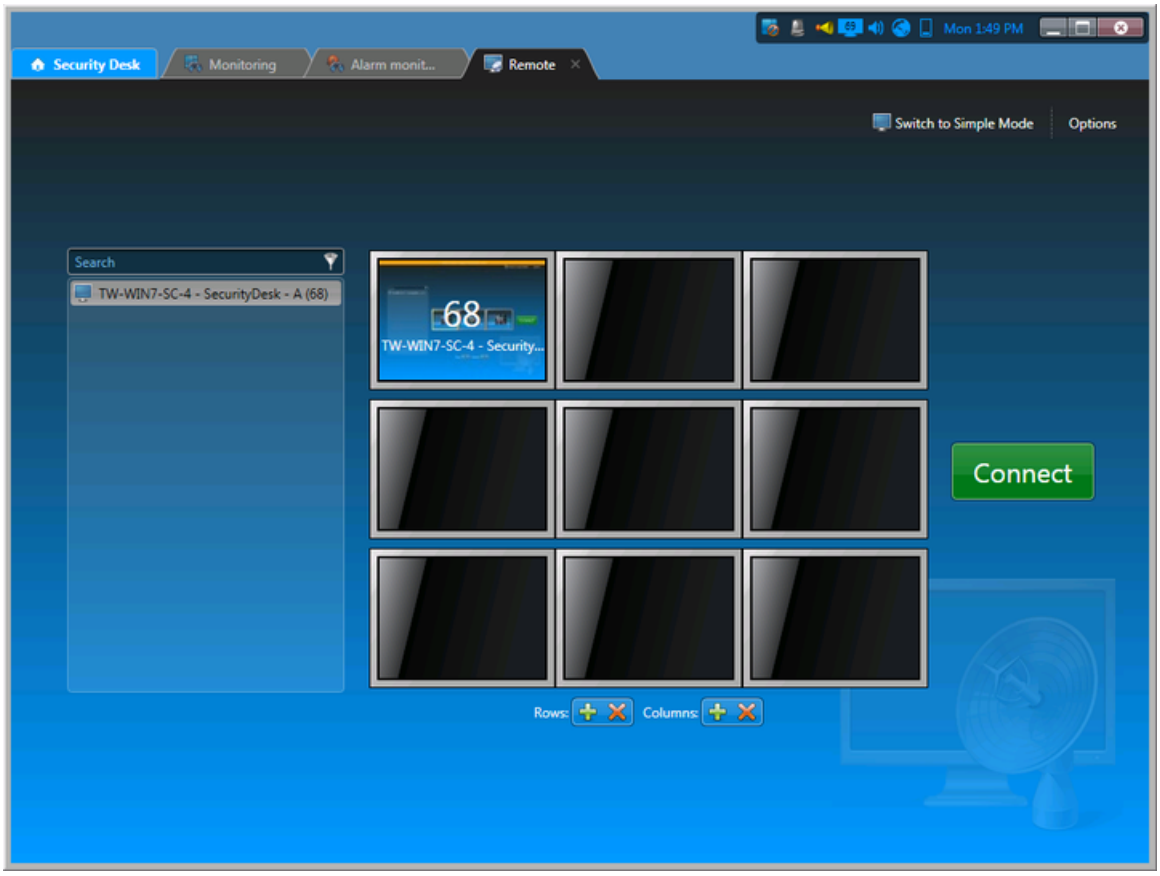
Pour surveiller et contrôler un Security Desk à distance, vous devez vous connecter à un poste Security Desk distant (*Mode simple*) ou a plusieurs moniteurs Security Desk distants (*Mode Mur d'images*).

Avant de commencer

- L'instance de Security Desk distante doit être lancée et connectée au même Répertoire Security Center.
- Vous devez avoir les droits *Contrôle à distance utilisateur* sur les instances de Security Desk auxquelles vous souhaitez vous connecter. Dans Config Tool, votre administrateur système doit sélectionner les postes que vous pouvez contrôler à distance.
  REMARQUE : Cette étape n'est nécessaire que si l'utilisateur n'appartient pas au groupe Administrateurs.
- Vous devez avoir au moins le ou les mêmes privilèges utilisateur que l'utilisateur connecté au poste Security Desk distant. S'il vous manque des privilèges utilisateur par rapport à l'utilisateur distant, votre demande de connexion au poste Security Desk distant est refusée.
- Vous devez être membre des mêmes partitions que l'utilisateur connecté au poste Security Desk distant. Si vous n'avez pas accès à des partitions auxquelles l'utilisateur distant a accès, la connexion à distance est également refusée.
- Vous devez disposer du privilège *Mode espion* pour vous connecter à des Security Desk en mode espion.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Distant.
2. Pour vous connecter à un poste Security Desk distant, sélectionnez un poste Security Desk distant dans la liste déroulante. Pour vous connecter à plusieurs moniteurs Security Desk distants, procédez de la manière suivante :
   a. Cliquez sur Basculer en mode Mur d'images.
   b. Pour configurer la disposition du mur d'images, utilisez les boutons  et  dans les sections Lignes et Colonnes.
   c. Dans la liste déroulante, cliquez deux fois sur les moniteurs Security Desk distants auxquels vous souhaitez vous connecter.
   Les moniteurs sélectionnés sont ajoutés aux tuiles vides. Pour supprimer un moniteur d'une tuile, cliquez sur  dans la tuile concernée.



3. (Facultatif) Cliquez sur Options et sélectionnez l'une des options suivantes ou les deux :

   Mode espion
   Permet de se connecter à un Security Desk distant sans être détecté. Ce mode ne permet pas d'entreprendre des actions. Vous ne pouvez que surveiller.

   Faible bande passante
   Permet de limiter la consommation de bande passante durant la surveillance d'une instance de Security Desk à distance.

   Cette option est utile, car d'ordinaire, chaque commande exécutée sur le Security Desk distant est également exécutée sur votre poste Security Desk local, ce qui peut augmenter la bande passante utilisée.

4. Cliquez sur Connexion.

Résultats

Vous êtes connecté au poste Security Desk distant. Si vous utilisez le mode Mur d'images, le moniteur placé dans la première tuile est affiché.

Lorsque vous avez terminé

Une fois connecté, vous pouvez afficher les tâches déjà ouvertes sur le poste Security Desk distant. Toutefois, vous ne pouvez utiliser que les tâches *Surveillance* et *Surveillance d'alarmes*. Le message suivant est affiché pour toutes les autres tâches : *Cette tâche ne peut pas être contrôlée à distance*.
REMARQUE : Sur le poste Security Desk distant, le nombre d'utilisateurs connectés à distance est indiqué sur l'icône Surveillance à distance de la zone de notification ( ), sauf si ces utilisateurs sont en mode espion. Cliquez sur l'icône Surveillance à distance pour afficher les utilisateurs contrôlant votre Security Desk à distance et les systèmes connectés. Si vous avez les privilèges d'utilisateur requis, vous pouvez déconnecter ces utilisateurs de votre Security Desk.
Explorer

- Présentation de la tâche Distant

1.6.10 | Surveiller les événements sur les applications Security Desk distantes

Dans la tâche *Surveillance* du poste Security Desk distant, vous pouvez utiliser un sous-ensemble des actions disponibles dans une tâche *Surveillance* locale. Par exemple, vous ne pouvez que surveiller la vidéo et les entités vidéo et de contrôle d'accès (caméras, secteurs, portes, ascenseurs, secteurs de détection d'intrusion, et ainsi de suite).

Avant de commencer

Connectez-vous à une ou plusieurs applications Security Desk distantes.

Procédure

1. Ouvrez la tâche Surveillance.
   Si le poste distant n'a pas de tâche Surveillance ouverte, procédez de la manière suivante :
   a. Effectuez un clic droit sur l'onglet Accueil, puis cliquez sur Nouvelle tâche ( ).
   b. Cliquez sur Surveillance, et nommez la tâche.
   c. Cliquez sur Créer.
2. Sélectionnez des entités à surveiller.
   La procédure est la même que pour une tâche *Surveillance* en local.
3. Pour afficher une entité dans une tuile du canevas, cliquez deux fois sur l'entité ou faites-la glisser depuis la vue secteur.
   L'entité est affichée dans votre tâche Distant, en local, ainsi que sur le poste distant.

Explorer

- Sélectionner des entités à surveiller

1.6.11 | Surveiller les alarmes sur les applications Security Desk distantes

Dans la tâche *Surveillance d'alarmes* du poste Security Desk distant, vous pouvez acquitter toutes les alarmes actives.

Avant de commencer

Connectez-vous à une ou plusieurs applications Security Desk distantes.

Procédure

1. Ouvrez la tâche Surveillance d'alarmes.
   Si le poste distant n'a pas de tâche Surveillance d'alarmes ouverte, procédez de la manière suivante :
   a. Effectuez un clic droit sur l'onglet Accueil, puis cliquez sur Nouvelle tâche ( ).
   b. Cliquez sur Surveillance d'alarmes, puis sur Créer.
2. Sélectionnez une alarme active sur le canevas, puis acquittez l'alarme.

Explorer

- Acquittement des alarmes

1.6.12 | Actions que vous pouvez effectuer sur les applications Security Desk distantes

Le tableau suivant présente ce que vous pouvez faire lorsque vous surveillez un poste Security Desk distant avec la tâche *Distant*.

Pour en savoir plus sur ces commandes, suivez les liens dans la colonne *Voir*.

Commande	Description	Raccourci clavier par défaut	Voir
Contrôle des caméras			

Commande	Description	Raccourci clavier par défaut	Voir
Visionner la vidéo en direct	Afficher de la vidéo dans la tâche *Surveillance*. REMARQUE : Vous ne pouvez pas entendre le son du moniteur distant sur votre poste Security Desk en local.		Modes vidéo en temps réel et enregistrée
Changer de flux	Changer de flux vidéo provenant de la caméra sélectionnée.		Changer de flux vidéo
Basculer vers la lecture	Basculer vers la vidéo enregistrée lorsque vous affichez la vidéo en temps réel.	P	Modes vidéo en temps réel et enregistrée
Pause/lecture	Suspendre ou lancer la lecture de l'enregistrement vidéo.	G	Modes vidéo en temps réel et enregistrée
Image précédente	Lorsque la lecture vidéo est mise en pause, aller à l'image vidéo précédente.	N	Widget Caméra
Image suivante	Lorsque la lecture vidéo est mise en pause, aller à l'image vidéo suivante.	M	Widget Caméra
Saut arrière	Effectuer un saut arrière dans la vidéo enregistrée en fonction du temps de recul spécifié dans l'onglet Options vidéo.	Ctrl+Maj+N	Widget Caméra
Saut avant	Effectuer un saut avant dans la vidéo enregistrée en fonction du temps de recul spécifié dans l'onglet Options vidéo.	Ctrl+Maj+M	Widget Caméra
Aller à une date/heure particulière	Basculer vers un instant précis de l'enregistrement vidéo.		Basculer entre les modes vidéo
Basculer vers le temps réel	Basculer vers la vidéo en direct.	L	Basculer entre les modes vidéo
Contrôle des caméras PTZ			
Panoramique vers la gauche du PTZ	Effectuer un panoramique vers la gauche avec la caméra PTZ.	Flèche gauche	Widget PTZ
Panoramique vers la droite du PTZ	Effectuer un panoramique vers la droite avec la caméra PTZ.	Flèche droite	

Commande	Description	Raccourci clavier par défaut	Voir
Inclinaison vers le bas du PTZ	Incliner la caméra PTZ vers le bas.	FLÈCHE BAS	
Inclinaison vers le haut du PTZ	Incliner la caméra PTZ vers le haut.	FLÈCHE HAUT	
Zoom avant du PTZ	Effectuer un zoom avant sur l'image de la caméra PTZ.	Maintenir la touche PLUS (+) enfoncée	
Zoom arrière du PTZ	Effectuer un zoom arrière sur l'image de la caméra PTZ.	Maintenir la touche MOINS (-) enfoncée	
Aller au préréglage	Basculer vers un préréglage.		
Renommer un préréglage/parcours/auxiliaire	Renommer un préréglage, parcours ou auxiliaire.		
Enregistrer un préréglage	Enregistrer un préréglage.		
Aller à la position d'origine	Aller à la position d'origine (par défaut) du PTZ.		
Régler la vitesse du moteur de PTZ	Réglez la vitesse du Moteur de PTZ.		
Verrouiller/déverrouiller le moteur de PTZ	Verrouiller les commandes de PTZ pour bloquer les autres utilisateurs.		
Mise au point proche/lointaine	Faire la mise au point manuelle sur l'image, de près ou de loin.		
Miroir horizontal/vertical	Basculez le moteur de PTZ de 180 degrés.		
Lancer un parcours PTZ	Lancez un parcours de PTZ. Cliquer sur un préréglage ou bouton de PTZ pour arrêter le parcours.		
Enregistrer un parcours de PTZ	Enregistrez un nouveau parcours de PTZ.		
Activer/désactiver l'auxiliaire	Démarrer ou arrêter la commande de PTZ auxiliaire.		
Contrôler la disposition du poste Security Desk distant			
Fermer toutes les tâches ouvertes	Fermer toutes les tâches ouvertes sur le poste Security Desk distant.		Ouvrir les tâches

Commande	Description	Raccourci clavier par défaut	Voir
Enregistrer l'espace de travail	Enregistrer la liste de tâches, qui sera automatiquement rétablie lors de la connexion suivante de l'utilisateur au poste Security Desk distant.		Enregistrer une tâche dans Security Center
Lancer le cycle de tâches	Basculer automatiquement entre toutes les tâches chargées dans Security Desk. Par défaut, la durée d'affichage est de 4 secondes par tâche.		Ouvrir les tâches
Arrêter le cycle de tâches	Arrêter l'affichage cyclique des tâches.		Ouvrir les tâches
Plein écran	Basculer entre l'affichage de Security Desk en plein écran et dans une fenêtre.		Ouvrir les tâches
Renommer la tâche	Renommer la tâche sélectionnée.		Ouvrir les tâches
Modifier la mosaïque	Changer la mosaïque sur le canevas.	Ctrl+P	• Modifier la mosaïque des tuiles • Personnaliser l'affichage des tuiles dans Security Center

1.7 | Tâches avancées dans Security Desk

1.7.1 | Exécuter une macro

Vous pouvez démarrer et arrêter une macro avec la tâche *État du système*.

Avant de commencer

Vous devez disposer du privilège *Exécuter des macros* pour lancer ou arrêter les macros.

À savoir

Type d'entité qui encapsule un programme C# qui ajoute des fonctionnalités à Security Center.

Procédure

1. Sur la page d'accueil, ouvrez la tâche État du système.
2. Dans la liste déroulante Surveiller, sélectionnez Macros.
   Les macros de votre système sont affichées dans le volet de rapport.

3. Lancez une macro :
   - Sélectionnez une macro dans le volet de rapport, puis cliquez sur Démarrer ( ).
   - Cliquez sur Démarrer ( ), sélectionnez une macro, puis cliquez sur Démarrer.
4. Pour arrêter une macro en cours d'exécution, sélectionnez-la dans le volet de rapport, puis cliquez sur Arrêter ( ).

1.7.2 | Rechercher les modifications apportées à la configuration du système

Vous pouvez découvrir quelles modifications de la configuration du système ont été apportées, par qui, quand et les réglages d'entités concernés (valeurs avant et après) avec le rapport Historiques de configuration.

À savoir

Le rapport Historique de configuration est utile si vous remarquez que les propriétés d'une entité ont été modifiées et que vous devez savoir qui a effectué ces modifications et quand (par exemple, si le mode d'enregistrement d'une caméra a été modifié). Ou si vous avez demandé la mise à jour d'une entité (par exemple, les privilèges d'un utilisateur), vous pouvez vérifier si les modifications ont été faites depuis Config Tool.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Historiques de configuration.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Application
   Application client utilisée pour l'activité.

   Entités
   Sélectionnez les entités que vous souhaitez examiner. Vous pouvez filtrer les entités par nom et par type.

   Heure de modification
   Les entités modifiées durant la plage horaire spécifiée.

   Modifié par
   Utilisateur ou rôle responsable de la modification de l'entité.

3. Cliquez sur Générer le rapport.
   La description et l'horaire des modifications apportées aux entités sélectionnées (valeurs avant et après), ainsi que les personnes responsables, sont affichés dans le volet de rapport.

1.7.2.1 | Colonnes du volet de rapport pour la tâche Historiques de configuration

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Entité
Nom de l'entité affectée par la modification.

Type d'entité
Type d'entité affecté par la modification.

Description
La description de la modification d'entité.

Initiateur
Personne ou rôle ayant effectué la modification de l'entité.

Type d'initiateur
Le type d'entité ayant initié les modifications d'entités.

Machine initiatrice
L'ordinateur utilisé pour effectuer la modification.

Application initiatrice
Application utilisée pour effectuer la modification.

Version d'application d'initiateur
Numéro de version de l'application. Ce champ est vide si l'activité est initiée par une entité rôle.

Heure de modification
Heure de la dernière modification de l'entité.
Sujet parent : Rechercher les modifications apportées à la configuration du système

1.7.3 | Analyser l'activité des utilisateurs dans votre système Security Center

Utilisez le rapport Historiques d'activité pour afficher toutes les activités vidéo, de contrôle d'accès ou de RAPI associées aux utilisateurs.

Avant de commencer

Pour obtenir des résultats dans le rapport Historique d'activité, vous devez déjà être en train de surveiller l'activité des utilisateurs. Vous pouvez sélectionner les activités à surveiller et enregistrer dans la base de données depuis la tâche Système dans Config Tool. Pour en savoir plus, voir le *Guide de l'administrateur Security Center*.

À savoir

Par exemple, vous pouvez utiliser la tâche Historiques d'activité pour savoir qui a lu certains enregistrements vidéo, bloqué une caméra, activé un niveau de risque, demandé l'impression d'un badge, utilisé la tâche Éditeur de permis et de liste de véhicules recherchés ou activé le filtrage de listes de véhicules recherchés.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Historiques d'activité.
2. Dans le filtre Activités, sélectionnez l'activité utilisateur que vous souhaitez examiner.
3. Définissez les autres filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Application
   Application client utilisée pour l'activité.

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

   Événements
   Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

   Impacté
   Les entités impactées par cette activité.

   Initiateur
   Utilisateur ou rôle responsable de l'activité.

4. Cliquez sur Générer le rapport.
   L'activité est affichée dans le volet de rapport.

1.7.3.1 | Activité utilisateur que vous pouvez examiner dans Security Center

Pour examiner l'activité utilisateur dans Security Center à l'aide du rapport Historiques d'activité, familiarisez-vous avec les définitions d'activité.

Activités utilisateur générales

Vous pouvez examiner les activités utilisateur générales suivantes :

Alarme acquittée
Personnes ayant acquitté une alarme active.

Contexte d'alarme modifié
Personnes ayant modifié le contexte d'une alarme.

Alarme acquittée de force
Personnes ayant acquitté de force toutes les alarmes actives.

Alarme transférée
Personnes ayant transféré une alarme active.

Alarme mise en rappel
Personnes ayant mis en rappel une alarme active.

Alarme déclenchée (manuellement)
Personnes ayant manuellement déclenché une alarme.

Toutes les alarmes acquittées de force
Personnes ayant acquitté de force toutes les alarmes actives.

Connexion à distance à Security Desk
Personnes qui se sont connectées à un poste Security Desk distant.

Déconnexion à distance de Security Desk
Personnes qui se sont déconnectées d'un poste Security Desk distant.

Dysfonctionnement ignoré
Personnes ayant ignoré un dysfonctionnement.

Alarme d'intrusion acquittée
Personnes ayant acquitté une alarme d'intrusion.

Alarme d'intrusion coupée
Personnes ayant coupé une alarme d'intrusion.

Alarme d'intrusion déclenchée
Personnes ayant manuellement déclenché une alarme d'intrusion.

Secteur de détection d'intrusion désarmé
Personnes ayant désarmé un secteur de détection d'intrusion.

Contournement des entrées de secteur de détection d'intrusion activé/désactivé
Personnes ayant activé ou désactivé un contournement de capteur dans un secteur de détection d'intrusion.

Armement global du secteur de détection d'intrusion
Personnes ayant effectué l'armement global d'un secteur de détection d'intrusion.

Périmètre de secteur de détection d'intrusion armé
Personnes ayant armé le périmètre d'un secteur de détection d'intrusion.

Macro démarrée/abandonnée
Personnes ayant démarré ou arrêté une macro.

Sortie déclenchée (manuellement)
Personnes ayant déclenché une sortie numérique (à l'aide d'une action éclair par exemple).

Rapport exporté/généré/imprimé
Personnes ayant exporté, créé ou imprimé un rapport.
IMPORTANT : Pour respecter la réglementation des États, si l'option Rapport généré est utilisée pour un rapport Historiques d'activité qui contient des données de RAPI, le motif de la recherche RAPI est inclus dans le champ Description.

Niveau de risque activé/désactivé
Personnes ayant activé ou désactivé un niveau de risque, ainsi que le secteur ou système associé.

Mot de passe d'unité modifié
Personnes ayant modifié le mot de passe de l'unité, et indication d'un changement manuel ou généré par le système.

Mots de passe d'unités exportés
Personnes ayant exporté le rapport Inventaire matériel avec les mots de passe d'unités.

Connexion/déconnexion d'un utilisateur
Personnes qui se sont connectées ou déconnectées d'une application client Security Center particulière.

Échec de la connexion de l'utilisateur
Qui n'a pas réussi à se connecter à une application cliente Security Center et pourquoi.

Zone armée/désarmée
Personnes ayant armé ou désarmé une zone.

Activités utilisateur liées au contrôle d'accès

Vous pouvez examiner les activités utilisateur suivantes concernant le contrôle d'accès :

Redémarrage d'une unité de contrôle d'accès (manuel)
Personnes ayant manuellement redémarré une unité de contrôle d'accès.

Journaux d'assistance d'unité de contrôle d'accès activés/désactivés
Personnes ayant activé ou désactivé les journaux d'assistance des unités de contrôle d'accès.

Synchronisation d'unité de contrôle d'accès démarrée (manuelle)
Personnes ayant manuellement démarré la synchronisation d'une unité de contrôle d'accès.

Violation antiretour pardonnée
Personnes ayant pardonné une violation antiretour.

Badge imprimé
Personnes ayant imprimé un badge d'identification.

Demande d'identifiant annulée/terminée
Personnes ayant terminé ou annulé une demande d'impression de badge d'identification.

Identifiant demandé
Personnes ayant demandé l'impression d'un badge, et pour quelle raison.

Appareil désactivé
Personnes ayant contourné (ou désactivé) un appareil de contrôle d'accès.

Mode de maintenance de porte désactivé
Personnes ayant annulé le mode maintenance pour une porte.

Porte placée en mode maintenance
Personnes ayant déverrouillé une porte en la plaçant en mode maintenance.

Horaire de déverrouillage de porte ignoré (verrouillage/déverrouillage)
Personnes ayant annulé l'horaire de verrouillage ou déverrouillage d'une porte.

Annulation du contournement de l'horaire de déverrouillage de porte
Personnes ayant annulé le contournement des horaires de déverrouillage d'une porte.

Porte déverrouillée (expressément)
Personnes ayant déverrouillé une porte dans Security Desk à l'aide d'une action éclair ou d'une association événement-action.

Porte déverrouillée (manuellement)
Personnes ayant manuellement déverrouillé une porte depuis le widget Security Desk *Porte*.

Contournement de l'horaire d'accès aux étages d'ascenseur annulé
Personnes ayant annulé un changement d'horaire d'ascenseur.

Horaire d'accès aux étages d'ascenseur contourné (accès libre)
Personnes ayant outrepassé un horaire d'ascenseur à accès libre.

Horaire d'accès aux étages d'ascenseur contourné (accès restreint)
Qui a outrepassé un horaire d'ascenseur à accès contrôlé.

Mise à niveau du micrologiciel de l'unité de contrôle d'accès planifiée avec mise à jour de modules d'interface
Personnes ayant planifié une mise à niveau du micrologiciel pour une unité de contrôle d'accès et ses modules d'interface associés.

Mise à niveau du micrologiciel de l'unité de contrôle d'accès planifiée sans mise à jour de modules d'interface
Personnes ayant planifié une mise à niveau du micrologiciel pour l'unité de contrôle d'accès.

Mise à niveau du micrologiciel du module d'interface planifiée
Utilisateur ayant planifié une mise à niveau du micrologiciel d'un module d'interface.

Nombre d'individus remis à zéro
Personnes ayant réinitialisé le nombre de personnes d'un secteur.

Personne ajoutée au secteur
Personnes ayant ajouté un titulaire de carte à un secteur à l'aide du SDK.

Personne supprimée du secteur
Personnes ayant supprimé un titulaire de carte d'un secteur dans la tâche Comptage d'individus.

Annulation de la mise à niveau du micrologiciel planifiée pour l'unité de contrôle d'accès
La mise à niveau planifiée de l'unité a été annulée.

Réinitialisation du certificat de confiance
Personnes ayant réinitialisé le certificat de confiance d'une unité Synergis™ Cloud Link.

Déverrouiller les portes du périmètre du secteur
Personnes ayant déverrouillé une porte de périmètre de zone.

Activité des utilisateurs associée à la RAPI

Vous pouvez examiner les activités associées à la RAPI suivantes :

Application mise à jour
Personnes ayant mis à jour une unité Genetec Patroller™ ou Sharp.

Verbalisation d’une infraction au sein des zones de stationnement déclenché
Personnes ayant verbalisé une infraction dans une zone de stationnement.

Alerte supprimée
Personnes ayant supprimé une alerte.

Liste de véhicules recherchés ou de permis modifiée
Personnes ayant chargé une liste de véhicules recherchés, ou ayant ajouté, supprimé ou modifié des plaques de la liste.

Recherche d'anciennes lectures déclenchée
Personnes ayant effectué une recherche d'anciennes lectures dans Genetec Patroller™.

Rapport de preuves photo imprimé (alertes/lectures)
Personnes ayant imprimé un rapport de preuves d'alertes/lectures.

Filtrage de plaques activé
Rôle Gestionnaire RAPI pour lequel le filtrage de plaques est activé.

Lecture modifiée/déclenchée
Personnes ayant modifié/déclenché une lecture de plaque d'immatriculation.

Lecture/alerte protégée
Personnes ayant protégé une lecture ou alerte de plaque d'immatriculation.

Lecture/alerte déprotégée
Personnes ayant déprotégé une lecture ou alerte de plaque d'immatriculation.

Réinitialiser l'inventaire de zone de stationnement
Personnes ayant réinitialisé l’inventaire d'une zone de stationnement.

Définir la capacité de la zone de stationnement.
Personnes ayant modifié l’occupation d'une zone de stationnement.

Activités utilisateur liées à la vidéo

Vous pouvez examiner les activités utilisateur suivantes concernant la vidéo :

Sauvegarde d'archive démarrée/arrêtée (manuellement)
Personnes ayant manuellement démarré ou arrêté la sauvegarde vidéo depuis un Archiveur.

Consolidation de l'Archiveur démarrée/arrêtée (manuellement)
Personnes ayant démarré ou arrêté la consolidation de la vidéo d'un Archiveur secondaire vers l'Archiveur principal.

Duplication d'archive démarrée/arrêtée (manuellement)
Personnes ayant démarré ou arrêté la duplication d'archives vidéo d'un Archiveur vers un autre.

Restauration d'archive démarrée/arrêtée (manuellement)
Personnes ayant démarré ou arrêté la restauration d'archives vidéo sur un Archiveur.

Récupération des archives depuis les unités démarrée/arrêtée (manuellement)
Personnes ayant démarré ou arrêté le transfert vidéo d'unités vidéo vers un Archiveur.

Limite de largeur de bande dépassée
Personnes ayant demandé un flux vidéo et n'ayant pas pu se connecter parce que la limite de bande passante pour les vidéo redirigées était atteinte. Ou personnes ayant perdu une connexion de flux vidéo parce que la limite de bande passante était atteinte et qu'un utilisateur avec un niveau utilisateur plus élevé a demandé un flux.

Signet supprimé/modifié
Personnes ayant supprimé ou modifié un signet.

Caméra bloquée/débloquée
Personnes ayant bloqué ou débloqué une caméra.

Vidéo confidentielle demandée
Personne ayant demandé à visionner un flux vidéo confidentiel.

Connecté au moniteur analogique
Personnes s'étant connectées à un moniteur analogique.

Déconnecté du moniteur analogique
Personnes s'étant déconnectées d'un moniteur analogique.

Flux de clé supprimé
Personnes ayant supprimé un flux de clé.

Flux en temps réel démarré/arrêté
La caméra affichée ou supprimée.

Flux de lecture
Enregistrements ayant été lus.

PTZ activé
Personnes ayant déplacé un PTZ inactif.

Commande PTZ envoyée
Quelle commande PTZ l'utilisateur a envoyé.

PTZ verrouillé
Personnes ayant verrouillé un PTZ et sur quelle caméra.

Zoom PTZ démarré/arrêté
Personnes ayant démarré ou arrêté le zoom PTZ et sur quelle caméra.

Enregistrement démarré/arrêté (manuellement)
Personnes ayant démarré ou arrêté un enregistrement vidéo manuellement.

Séquence suspendue/reprise
Personnes ayant mis en pause ou repris une séquence vidéo.

Imprimer/enregistrer un instantané
Personnes ayant imprimé ou enregistré un instantané.

Vidéo exportée
Vidéos exportées par l'utilisateur et l'emplacement de l'enregistrement.

Fichier vidéo supprimé (manuellement)
Personnes ayant supprimé un fichier vidéo du système.

Fichier vidéo protégé/déprotégé
Personnes ayant démarré ou arrêté la protection d'un fichier vidéo.

Flux vidéo non acheminé
Personnes dont la requête vidéo a pris fin sans le rendu de la moindre image.

Unité vidéo identifiée/redémarrée/reconnectée
Personnes ayant identifié/redémarré/reconnecté une unité vidéo.

Filature visuelle activée/désactivée
Personnes ayant activé ou désactivé la *filature visuelle* dans une tuile.
Sujet parent : Analyser l'activité des utilisateurs dans votre système Security Center

1.7.3.2 | Colonnes du volet de rapport pour la tâche Historiques d'activité

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Initiateur
Personne ou rôle ayant effectué l'activité.

Type d'initiateur
Le type d'entité ayant initié l'activité.

Nom d'activité
Type de l'activité.

Description
Description de l'événement, activité, entité ou incident.
IMPORTANT : Pour respecter la réglementation des États, si l'option Rapport généré est utilisée pour un rapport Historiques d'activité qui contient des données de RAPI, le motif de la recherche RAPI est inclus dans le champ Description.

Entité concernée
Entités impactées par cette activité.

Type d'entité concernée
Le type d'entité impactée par cette activité.

Machine initiatrice
L'ordinateur sur lequel l'activité a été effectuée.

Application initiatrice
L'application utilisée pour l'activité.

Heure de l'événement
Date et heure de l'événement.

Version d'entité concernée
Le numéro de version de l'entité impactée par cette activité. Ce champ est vide si l'entité concernée n'est pas un rôle.

Version d'application d'initiateur
Numéro de version de l'application. Ce champ est vide si l'activité est initiée par une entité rôle.

Version d'initiateur
Numéro de version de l'initiateur. Ce champ est vide si l'activité est initiée par un utilisateur.

Initiateur d'origine
(Utilisé pour la journalisation à distance sur les systèmes fédérés) La personne ou le rôle ayant effectué l'action sur l'hôte de Federation™. Dans ce cas, l'*Initiateur* correspond à l'utilisateur Federation™.

Sujet parent : Analyser l'activité des utilisateurs dans votre système Security Center

1.7.4 | Afficher les propriétés des unités

Utilisez le rapport Inventaire matériel pour consulter rapidement la liste de toutes les unités locales et fédérées du système, ainsi que des informations comme leur type, fabricant, modèle, adresse IP, etc.

À savoir

Par exemple, vous pouvez utiliser le rapport *Inventaire matériel* pour consulter la version du micrologiciel d'une unité, pour savoir si vous devez la mettre à niveau.
REMARQUE : Le rapport Inventaire matériel affiche des informations sur les unités tant locales que fédérées. Toutefois, certaines fonctions, comme les commandes d'action au bas de l'écran, et certaines propriétés comme *Mot de passe*, *Version du micrologiciel proposée* et *Description du micrologiciel proposée* ne sont pas disponibles pour les unités fédérées.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Inventaire matériel.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Unités
   Sélectionnez les unités ou rôles individuels que vous souhaitez examiner. Sélectionner un rôle équivaut à sélectionner toutes les unités gérées par celui-ci.

   Groupe source
   Sélectionnez la catégorie d'unités (Contrôle d'accès, Détection d'intrusion, RAPI ou Vidéo).

   Recherche avancée
   Vous pouvez choisir d'afficher les contrôleurs, les extensions, les ensembles de verrous, les lecteurs ou une combinaison de ceux-ci.

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

3. Cliquez sur Générer le rapport.
   Les propriétés d'unité sont affichées dans le volet de rapport.

1.7.4.1 | Colonnes du volet de rapport pour la tâche d'inventaire matériel dans Security Center

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Unité
Nom de l'unité.

Type d'unité
Type d'unité (Contrôle d'accès, Détection d'intrusion, RAPI ou Vidéo).

Fabricant
Fabricant de l'unité.

Type de produit
Modèle de l'unité.

Rôle
Rôle qui gère l'unité.

Version du micrologiciel
Version du micrologiciel installé sur l'unité.

Adresse IP
L'adresse IP de l'unité ou de l’ordinateur.

Adresse physique
Adresse MAC de l'interface réseau de l'appareil.

Utilisateur
Nom d'utilisateur utilisé pour la connexion à l'unité.

Fiabilité du mot de passe
Sécurité du mot de passe sur l'unité. Lorsque vous survolez la valeur de fiabilité du mot de passe, une infobulle vous fournit des informations complémentaires. « Inconnu » est affiché pour les unités fédérées.

État
État de l’unité (en ligne, hors ligne, avertissement).

Mot de passe
Le mot de passé est indiqué par une série de '*'.

Si vous avez le privilège *Afficher/exporter les mots de passe d’unités*, cliquez sur pour afficher le mot de passe.

Faites un clic droit sur la colonne Mot de passe pour copier le mot de passe dans le presse-papiers.

Dernière mise à jour du mot de passe
Date de la dernière mise à jour du mot de passe.

Version du micrologiciel proposée
La version recommandée pour la mise à niveau. Cette colonne est vide pour les unités fédérées.

État de la mise à niveau
État de la mise à niveau du micrologiciel (Aucun, Planifié, Démarré, Terminé ou Échec).

Mécanisme d'authentification
Indique le type d'authentification utilisé par la caméra, comme de base, digest, anonyme ou tiers. Si l'unité essaie soudain de se connecter avec un mécanisme d'authentification moins sûr, l'Archiveur refuse la communication et la caméra bascule hors ligne. Par exemple, lorsque l'Archiveur s'attend à ce que la caméra utilise l'authentification digest, mais qu'elle demande à se connecter avec l'authentification de base. La connexion est refusée et la caméra bascule hors ligne.

Mise à niveau suivante
La date de la prochaine mise à niveau basée sur le réglage Reporter la mise à niveau jusqu'au.

Parent
Le parent direct du module d'interface ou des panneaux en aval. Si le parent direct est l'unité de contrôle d'accès, seule la colonne Unité parent est renseignée.

Unité parent
L'unité de contrôle d'accès parent.

Version de la plate-forme
Version actuelle de la plate-forme (correctif de sécurité cumulé) installée sur l’unité.

Description du micrologiciel proposée
La description de la mise à niveau nécessaire. Cette colonne est vide pour les unités fédérées.

À jour
Aucune mise à jour du micrologiciel n’est nécessaire.

Facultatif
La mise à niveau du micrologiciel n'est pas urgente.

Recommandé
La mise à jour du micrologiciel est conseillée.

Faille de sécurité
La mise à jour du micrologiciel corrige une faille de sécurité et est vivement recommandée.

REMARQUE : Cette information n’est disponible que si Genetec™ Update Service est en cours d’exécution.

Description de la plate-forme proposée
La description de la mise à niveau nécessaire. Cette colonne est vide pour les unités fédérées.

À jour
Aucune mise à niveau de la plate-forme n’est nécessaire.

Facultatif
La mise à niveau de la plate-forme n’est pas urgente.

Recommandé
La mise à jour de la plate-forme est conseillée.

Faille de sécurité
La mise à jour de la plate-forme corrige une faille de sécurité et est vivement recommandée.

REMARQUE : Cette information n’est disponible que si Genetec™ Update Service est en cours d’exécution.

Version de la plate-forme proposée
La version recommandée pour la mise à niveau. Cette colonne est vide pour les unités fédérées.

Motif de l'échec de la mise à niveau
Motif de l'échec de la mise à niveau du micrologiciel (par exemple, Unité hors ligne ou Chemin de mise à niveau du micrologiciel non respecté).

Mode sécurisé
(Unités HID seulement) Indique si le mode sécurisé est activé ou désactivé.

Protocole de sécurité
Le protocole de sécurité utilisé par le Gestionnaire d'accès (TLS, Wiegand).

Fuseau horaire
Le fuseau horaire de l'unité.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.
Sujet parent : Afficher les propriétés des unités

1.7.5 | Surveiller les ressources de votre ordinateur

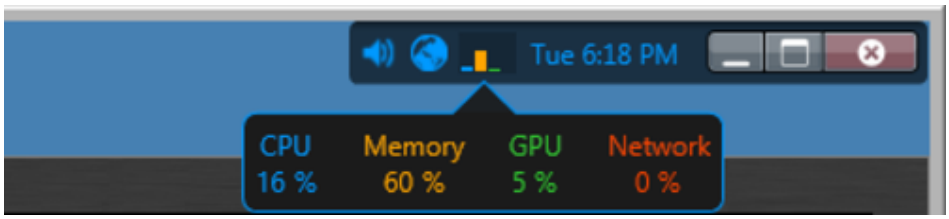
Vous pouvez surveiller le taux d'utilisation des ressources de votre ordinateur en survolant l'icône Jauge des ressources de la zone de notification avec votre souris. Cliquez sur l'icône pour afficher une boîte de dialogue qui résume les ressources matérielles de votre ordinateur et leur utilisation actuelle.

À savoir

Si vous ne voyez pas l'icône Jauge des ressources ( ) dans la zone de notification, réglez sa propriété d'affichage sur Afficher.

Procédure

1. Survolez l'icône Jauge des ressources dans la zone de notification avec la souris pour afficher le taux d'utilisation actuel des ressources de votre ordinateur.



   L'utilisation des ressources de votre ordinateur est présentée quatre catégories :
   - Processeur (bleu)
   - Mémoire (orange)
   - Processeur graphique (vert)
   - Réseau (rouge)

   REMARQUE : Le processeur graphique n'est affiché que si votre carte vidéo prend en charge l'accélération matérielle, et que cette fonctionnalité est activée dans les options vidéo de Security Desk.
2. Cliquez sur l'icône Jauge des ressources de la zone de notification pour obtenir des informations détaillées sur les ressources de votre ordinateur dans la boîte de dialogue Informations matérielles.

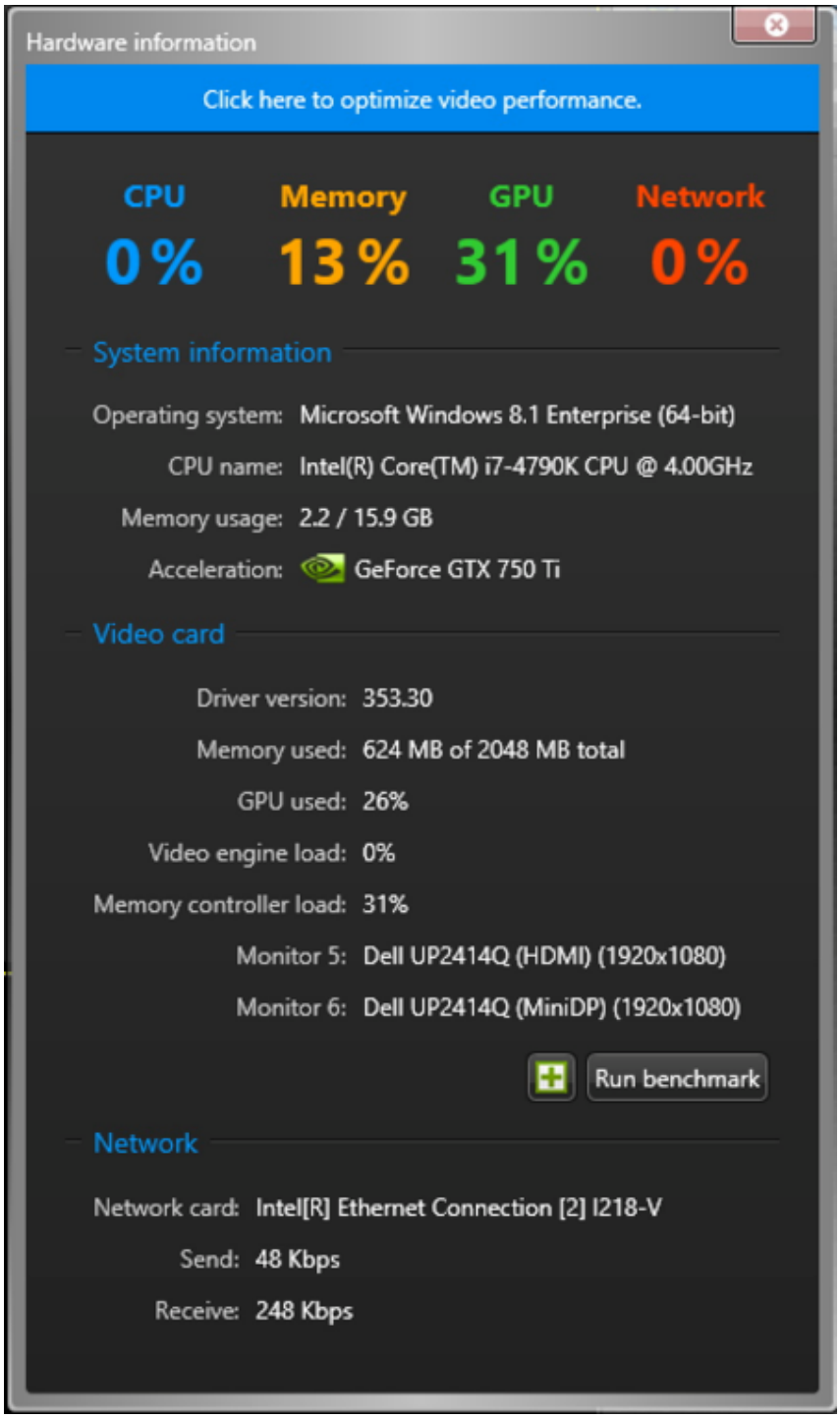
Explorer

- Options vidéo dans Security Desk

1.7.5.1 | Boîte de dialogue Informations matérielles

La boîte de dialogue Informations matérielles fournit un résumé des composants matériels détectés sur votre ordinateur, ainsi que leur taux d'utilisation actuel. Vous pouvez également lancer l'outil d'évaluation matérielle depuis la boîte de dialogue Informations matérielles.

Si les performances laissent à désirer, vous pouvez utiliser ces informations pour identifier le goulot d'étranglement sur votre ordinateur. Si votre carte vidéo a atteint ses limites, affichez moins de flux vidéo.



Les informations de carte vidéo ne sont pas disponibles si vous êtes connecté à votre ordinateur via le bureau à distance.

Le taux d'utilisation du processeur graphique n'est affiché que si votre carte vidéo prend en charge l'accélération matérielle, et que cette fonctionnalité est activée dans les options vidéo de Security Desk. Si votre ordinateur est équipé de plusieurs cartes vidéo, cliquez sur la liste déroulante Accélération pour sélectionner celle que vous souhaitez tester.

Pour en savoir plus sur l'exécution de l'outil d'évaluation matérielle, voir Utilisation de l'outil d'évaluation matérielle.
Sujet parent : Surveiller les ressources de votre ordinateur
Explorer

- Options vidéo dans Security Desk
- Optimiser les performances de décodage vidéo sur votre ordinateur

1.7.5.2 | Utilisation de l'outil d'évaluation matérielle

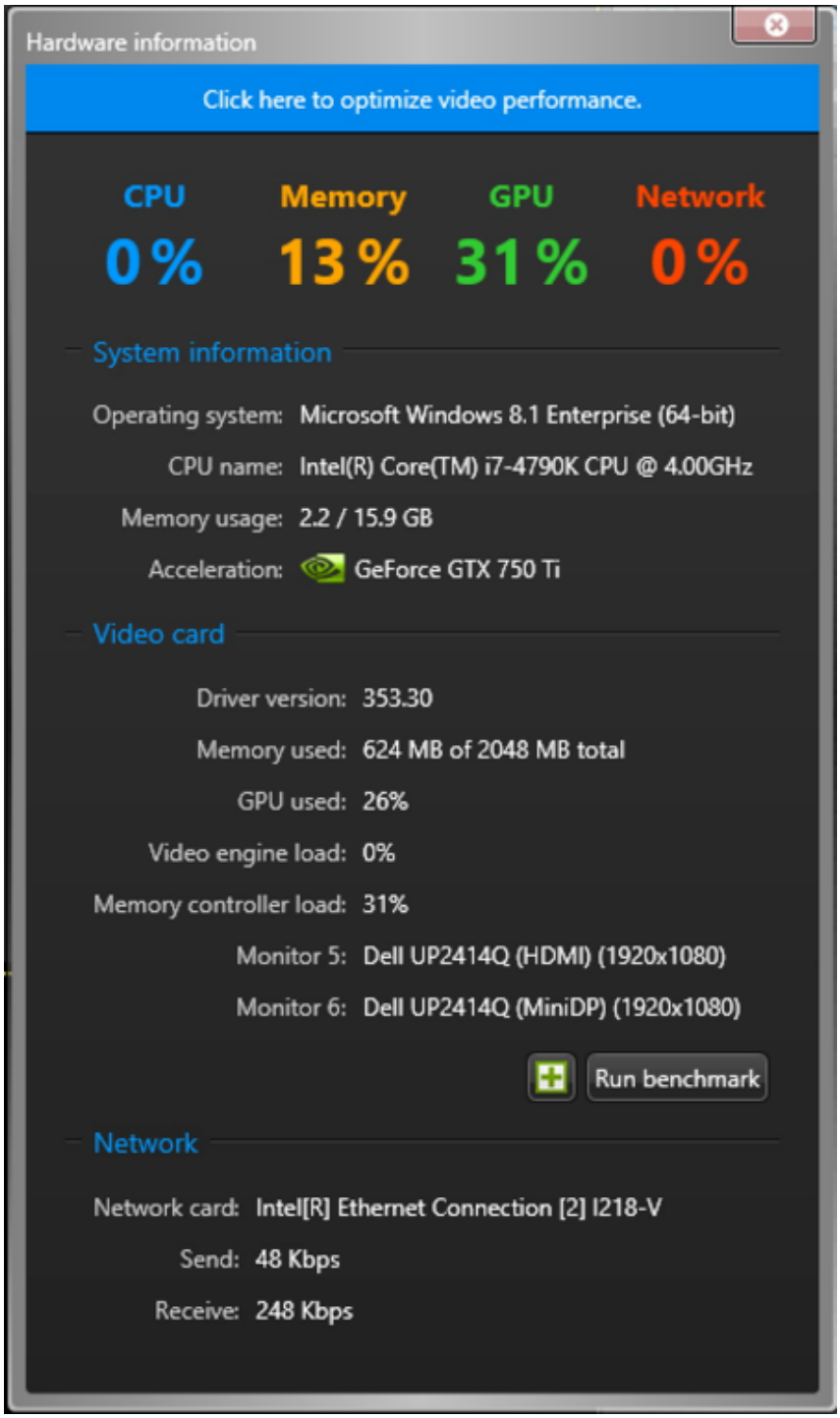
L'outil d'évaluation matérielle vous permet de peaufiner vos réglages pour optimiser les performances des cartes vidéo installées. Vous pouvez exécuter l'outil d'évaluation matérielle dans Config Tool ou Security Desk.

À savoir

- Vous êtes invité à exécuter l'outil d'évaluation matérielle au premier lancement de Security Desk. En outre, une icône d'avertissement jaune apparaît dans la zone de notification lorsque vous modifiez la configuration de la carte vidéo. Il n'y a pas d'avertissement dans Config Tool.
- L'exécution de l'outil d'évaluation matérielle taxe le processeur graphique. Fermez toutes les autres tâches et applications avant de lancer un test pour vérifier que vous obtenez le résultat voulu.
- Pour un résultat optimal, vérifiez que les pilotes de votre processeur graphique sont à jour avant de lancer l'outil d'évaluation matérielle.

Procédure

1. Dans la zone de notification, cliquez deux fois sur l'icône Jauge des ressources ().
   La boîte de dialogue Informations matérielles apparaît.



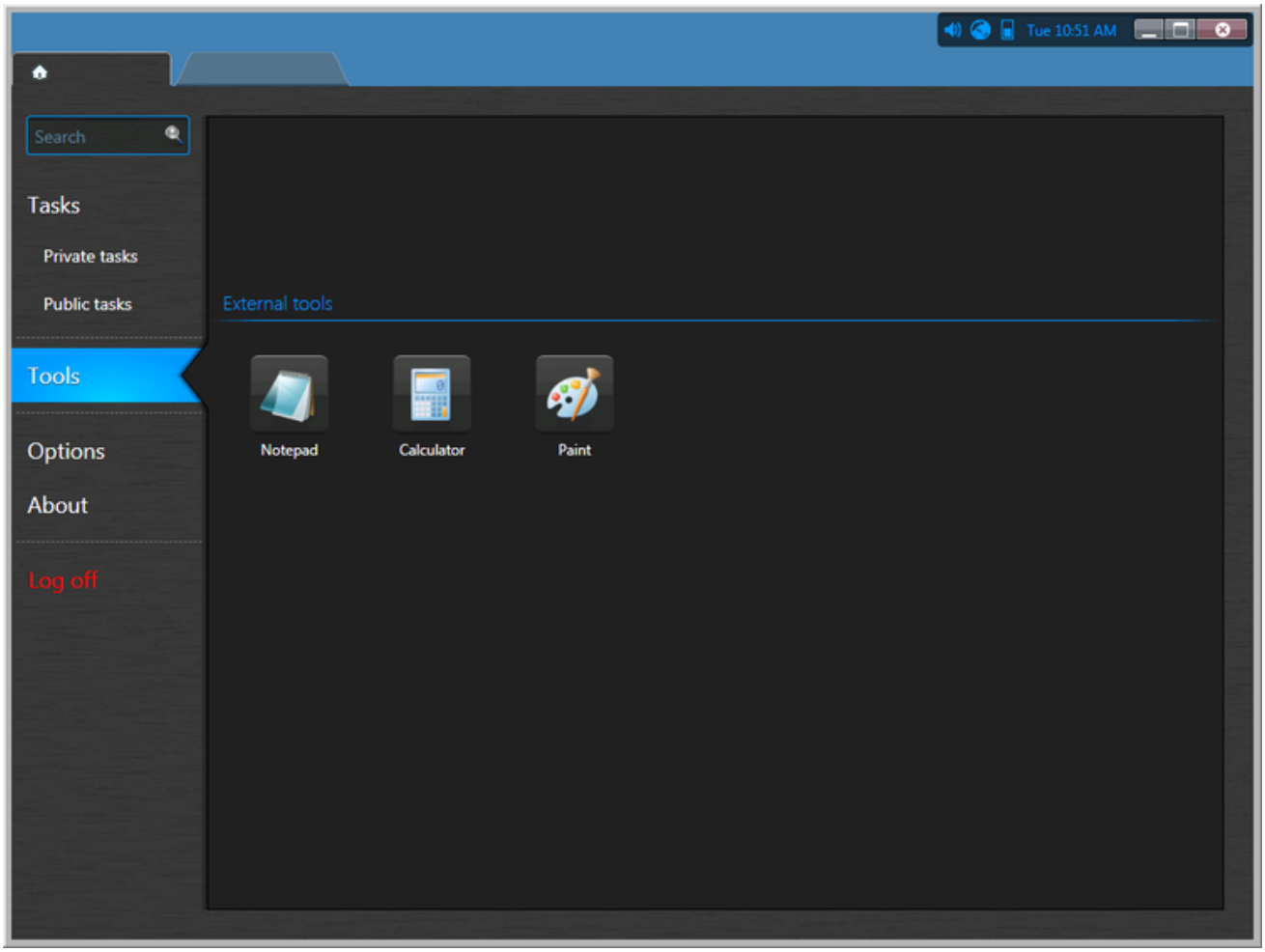
2. Dans la liste déroulante Accélération, sélectionnez la carte vidéo que vous souhaitez tester.
3. Cliquez sur Lancer l'évaluation.
   Une fois le test effectué, la capacité en Images par seconde de la carte sélectionnée est affichée.
4. Cliquez sur Fermer.

Sujet parent : Surveiller les ressources de votre ordinateur

1.7.6 | Raccourcis vers des outils externes

Vous pouvez ajouter des raccourcis vers des outils et applications externes fréquemment utilisés sur la page Outils de Security Center en modifiant le fichier ToolsMenuExtensions.xml.

Ce fichier est situé dans C:\Program files (x86)\Genetec Security Center 5.9 sur un ordinateur 64 bits et dans C:\Program files\Genetec Security Center 5.9 sur un ordinateur 32 bits.



Le contenu d'origine de ce fichier ressemble à ceci :

```
<?xml version="1.0" encoding="utf-8"?>
<ArrayOfToolsMenuExtension xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance xmlns:xsd=http://www.w3.org/2001/XMLSchema>
    <ToolsMenuExtension>
    </ToolsMenuExtension>
</ArrayOfToolsMenuExtension>
```

Chaque raccourci est défini par une balise XML appelée `<ToolsMenuExtension>`. Chaque balise `<ToolsMenuExtension>` peut contenir quatre éléments XML :

- `<Name>` – Nom de commande affiché sur la page Outils.
- `<FileName>` – Commande à exécuter (fichier exécutable).
- `<Icon>` – (Facultatif) Fichier d'icône (.ico). Utilisez cet élément pour remplacer l'icône par défaut extraite du fichier exécutable.
- `<Arguments>` – (Facultatif) Arguments de ligne de commande.

Les noms de balise XML sont sensibles à la casse. Vous pouvez modifier ce fichier XML avec n'importe quel éditeur de texte. Les modifications apportées au fichier sont appliquées au lancement suivant de Security Desk.

REMARQUE : Si le chemin complet n'est pas indiqué dans la balise `<FileName>`, l'application ne peut pas extraire l'icône associée à l'exécutable. Dans ce cas, vous devez spécifier une icône à utiliser avec la balise `<Icon>`.
Le fichier exemple suivant ajoute trois raccourcis (*Bloc-notes*, *Calculatrice* et *Paint*) à la page Outils. En outre, le raccourci *Bloc-notes* est configuré pour ouvrir le fichier C:\SafetyProcedures.txt.

```
<?xml version="1.0" encoding="utf-8"?>
<ArrayOfToolsMenuExtension xmlns:xsi="http://www.w3.org/2001/XMLSchema-...>
    <ToolsMenuExtension>
        <Name>Notepad</Name>
        <FileName>c:\windows\notepad.exe</FileName>
        <Arguments>c:\SafetyProcedures.txt</Arguments>
    </ToolsMenuExtension>
    <ToolsMenuExtension>
```

```
        <Name>Calculator</Name>
        <FileName>c:\windows\system32\calc.exe</FileName>
    </ToolsMenuExtension>
    <ToolsMenuExtension>
        <Name>Paint</Name>
        <FileName>c:\windows\system32\mspaint.exe</FileName>
    </ToolsMenuExtension>
</ArrayOfToolsMenuExtension>
```

1.7.7 | Personnaliser les options de connexion dans Security Desk

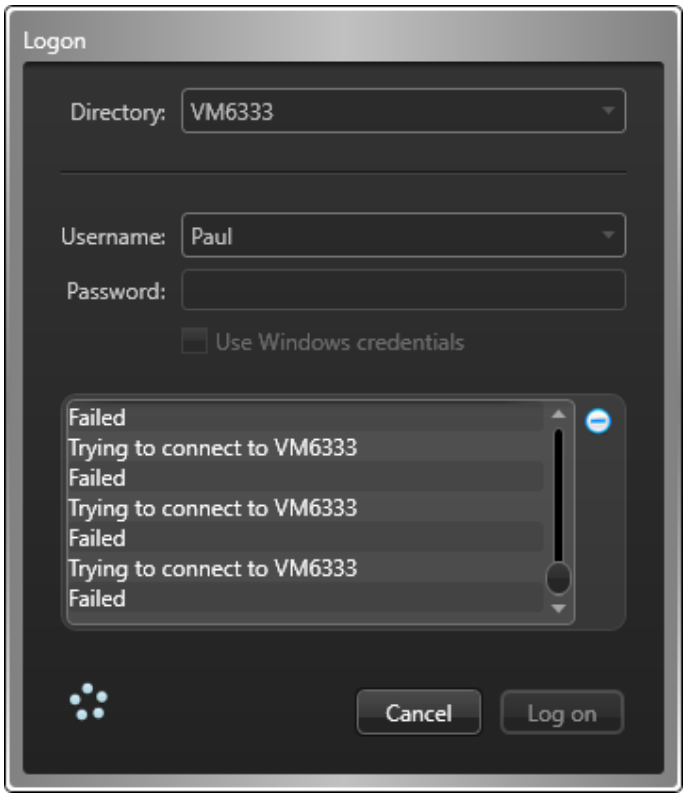
Vous pouvez sélectionner quand et comment les utilisateurs sont autorisés à se connecter à Security Center.

À savoir

Vous devez être un administrateur pour configurer les options de connexion. Ces réglages s'appliquent au poste local et affectent Security Desk et Config Tool pour tous les utilisateurs. Les modifications apportées ne prennent effet qu'au lancement suivant de Security Desk ou Config Tool.

Procédure

1. Sur la page d'accueil de Config Tool, cliquez sur Options > Général.
2. Pour forcer les utilisateurs à se connecter avec leurs identifiants Windows, réglez l'option Utiliser la sécurité Windows sur Toujours.
   Pour utiliser cette option, les utilisateurs qui se connecteront depuis cet ordinateur doivent être importés d'un *Active Directory*.Pour en savoir plus sur l'importation d'utilisateurs depuis un annuaire d'entreprise Active Directory, voir Importer un groupe de sécurité depuis un annuaire Active Directory.
3. Pour forcer tous les utilisateurs à utiliser un Répertoire particulier, sélectionnez l'option Forcer le Répertoire en, et entrez le nom du Répertoire.
   Les utilisateurs ne peuvent alors pas choisir le Répertoire auquel ils se connectent ; le champ Répertoire n'est pas affiché dans la fenêtre Connexion. Toutefois, ils peuvent être automatiquement redirigés vers un autre Répertoire si l'équilibrage de charge est utilisé.
   REMARQUE : En cas d'erreur dans le nom du Répertoire (comme une faute de frappe), les utilisateurs ne pourront pas se connecter la fois suivante.



4. Pour contourner l'équilibrage de charge du Répertoire, sélectionnez l'option Empêcher la redirection de la connexion vers d'autres serveurs Répertoire.
   Les utilisateurs se connecteront au Répertoire par défaut ou au Répertoire qu'ils spécifient à la connexion, et ne seront pas automatiquement redirigés vers un autre serveur. Cette option n'est pertinente que si l'*équilibrage de charge* est configuré pour le Répertoire.
5. Cliquez sur Enregistrer.
6. Pour déverrouiller la session de l'utilisateur après une période d'inactivité, réglez l'option Verrouillage auto sur ACTIVÉ, puis sélectionnez la période d'inactivité avant verrouillage.
   Cette option ne concerne que Security Desk. Avant le verrouillage, le message `Verrouillage imminent de la session` est affiché. Une fois que l'application est verrouillée, l'utilisateur doit se reconnecter pour reprendre la session en cours.
   REMARQUE : Si l'utilisateur est authentifié via Active Directory Federation Services avec authentification passive, l'utilisateur est déconnecté et sa session est fermée au lieu d'être verrouillée.

1.7.8 | Personnaliser les options réseau

Vous pouvez personnaliser la carte réseau, le mode de sélection du réseau et la plage de ports pour assurer une communication optimale entre votre poste et le réseau.

À savoir

Les réglages réseau s'appliquent au poste local et affectent Security Desk et Config Tool pour tous les utilisateurs.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Général.
2. Si votre ordinateur est équipé de plusieurs cartes réseau, sélectionnez la carte à utiliser pour communiquer avec les applications Security Center dans la liste déroulante Carte réseau.
3. Sélectionnez le mode de choix du Réseau :

   Détection automatique
   Security Center détecte automatiquement le réseau auquel votre poste est connecté.

   Spécifique
   Sélectionnez manuellement votre réseau dans la liste déroulante. Cette option est utile si vous avez du mal à recevoir les flux vidéo.

4. Dans l'option Plage de ports UDP entrants, sélectionnez la plage de ports utilisée pour diffuser de la vidéo vers votre poste par *multidiffusion* ou monodiffusion *UDP*.
5. Cliquez sur Enregistrer.

Exemple

Prenons le cas de figure suivant. Vous avez un réseau 10.1.x.x acheminé vers 10.2.x.x. Mais pour une raison quelconque, un poste particulier à l'adresse 10.1.2.3 ne parvient pas à accéder à 10.2.x.x. En spécifiant le réseau manuellement sur ce poste, vous indiquez au rôle Routeur multimédia qu'il doit rediriger les données multimédias depuis 10.2.x.x pour ce poste, au lieu de le forcer à se connecter directement à 10.2.x.x, en vain.

1.8 | Tableaux de bord dans Security Desk

1.8.1 | À propos des tableaux de bord

Tableaux de bord est une tâche d'exploitation qui fournit un canevas vierge sur lequel vous pouvez fixer des widgets, dont des graphiques, rapports et tuiles Security Center. Ces widgets suivent des indicateurs clés et fournissent un aperçu de l'activité et des événements enregistrés par le système.

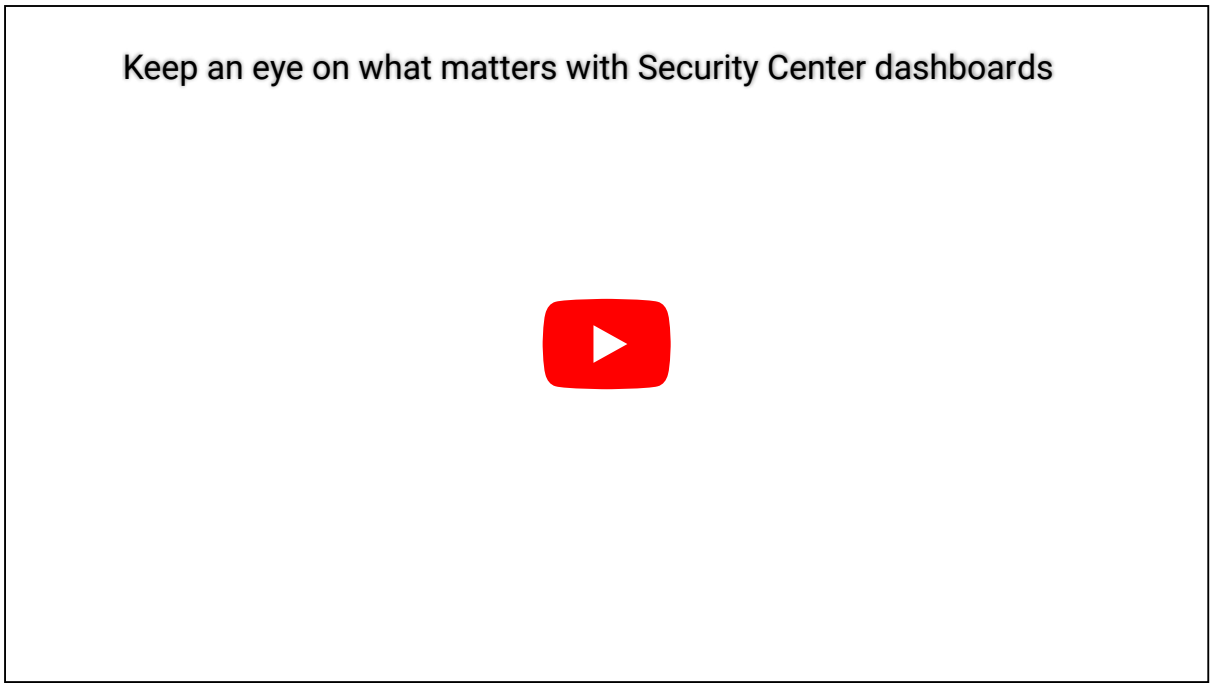
Les tableaux de bord Security Center ont de nombreuses utilisations. Vous pouvez les exploiter pour :

- Créer un tableau de bord de commandement pour surveiller les événements et dépêcher des gardes de sécurité.
- Suivre les indicateurs de performance clés, comme le nombre et les types d'incidents ou les temps d'attente dans les files d'attente.
- Surveiller le bon fonctionnement du système, qu'il s'agisse d'événements importants ou de statistiques de disponibilité des composants matériels et logiciels du système.
  REMARQUE : Un tableau de bord d'état par défaut est disponible comme tâche opérationnelle pour surveiller les informations sur l'état de votre système.

En personnalisant un tableau de bord en fonction de vos besoins, vous pouvez facilement suivre les informations importantes à vos yeux.

Les configurations de tableaux de bord peuvent être enregistrées en tant que tâches publiques ou privées dans Security Desk. Votre tableau de bord peut être personnel ou partagé à l'échelle de l'organisation.

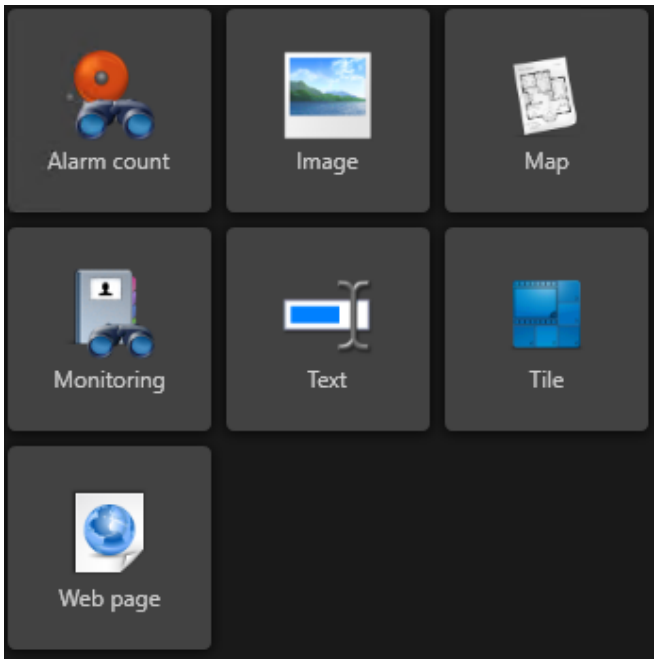
Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



Widgets du tableau de bord

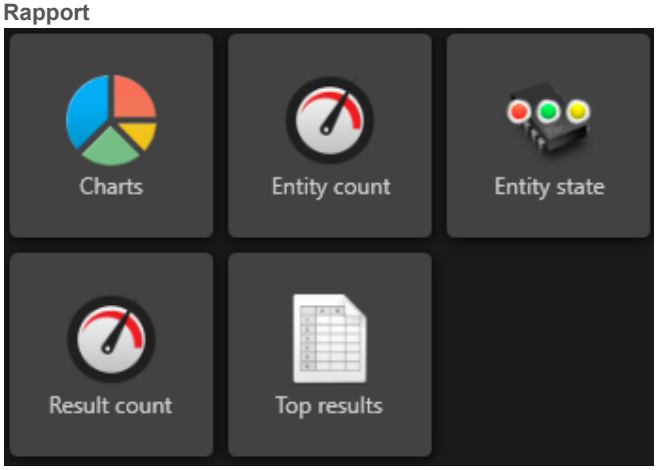
Les widgets sont les composants de base des tableaux de bord. Security Center est livré avec plusieurs widgets qui appartiennent aux catégories suivantes.

Général



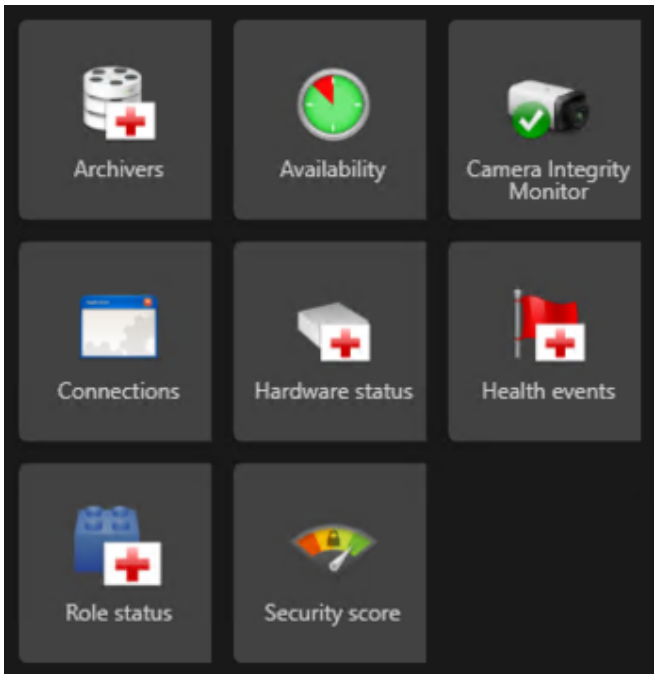
Intégrez des images, du texte et des pages web à votre tableau de bord, ou affichez-y des tuiles Security Center.

Rapport



Fournissez un aperçu des informations clés concernant votre système Security Center. Les rapports peuvent être configurés pour être actualisés à intervalles réguliers.

État



Surveillez l'état du système et les indicateurs de performance qui peuvent être configurés pour être actualisés automatiquement à intervalles réguliers.

Security Center fournit une structure logicielle permettant de créer des widgets personnalisés à l'aide du *SDK* Security Center. Si vous avez besoin d'une assistance pour développer des widgets personnalisés, contactez les Services professionnels Genetec™ par le biais de votre chargé de compte pour faire une demande de devis, ou appelez le bureau de votre région. Pour nous contacter, visitez notre site web.

Privilèges requis

La tâche Tableau de bord est contrôlée via des privilèges. Pour accéder aux tableaux de bord, les utilisateurs doivent disposer des privilèges suivants :

Tâche	Privilèges minimaux requis
Afficher les tableaux de bord	• *Afficher les tableaux de bord* • *Afficher les tâches publiques*

Tâche	Privilèges minimaux requis
Modifier les tableaux de bord	• *Modifier les tableaux de bord* • *Gérer les tâches privées* ou *Modifier les tâches publiques*
Créer des tableaux de bord	• *Modifier les tableaux de bord* • *Gérer les tâches privées* ou *Ajouter des tâches publiques*
Supprimer les tableaux de bord[1]	*Gérer les tâches privées* ou *Supprimer les tâches publiques*

[1] Les tableaux de bord sont supprimés en supprimant la tâche associée.

Certains widgets peuvent exiger des privilèges particuliers.

Explorer

- Widgets de tableau de bord standard
- Créer un tableau de bord

1.8.2 | Widgets de tableau de bord standard

Security Center est livré avec une collection de widgets standard.

Les widgets suivants sont disponibles :

Nom	Icône du widget	Description	Privilèges requis
Nombre d'alarmes		Compte le nombre d'alarmes actives, en cours d'investigation ou nécessitant un acquittement. Vous pouvez configurer le widget pour changer de couleur en fonction du nombre d'alarmes.	Aucun
Image		Affiche des images statiques aux formats suivants : • .jpg • .jpeg • .gif • .png • .bmp	Aucun
Surveillance		Affiche le rapport en direct des événements ou alarmes sélectionnés pour la surveillance. Vous pouvez basculer entre les événements de surveillance et les alarmes si l'option Autoriser le basculement du mode d'affichage est sélectionnée. Les mêmes commandes disponibles dans la tâche Surveillance lorsque la surveillance des alarmes est activée dans le widget.	Aucun

Nom	Icône du widget	Description	Privilèges requis
Texte		Affiche du texte.	Aucun
Tuile		Affiche toute entité pouvant être affichée dans une tuile Security Center[1]	Aucun[2]
Page web		Affiche des pages Web.	*Afficher des pages Web*
Graphiques		Affiche le rapport sélectionné sous forme visuelle.[3]	*Afficher les graphiques*[4]
Nombre d'entités		Affiche le nombre d'entités du type sélectionné.	Aucun
Nombre de résultats		Affiche le nombre de résultats du rapport sélectionné.[2]	Aucun[4]
Principaux résultats		Affiche les principaux résultats du rapport sélectionné.[3]	Aucun[4]
Archiveurs		Affiche les statistiques du rôle Archiveur.	*Statistiques de l'Archiveur*
Disponibilité		Affiche les statistiques de disponibilité du système.	*Rapport d'état*
Surveillance de l'intégrité des caméras		Affiche l'état de sabotage des caméras configurées pour la surveillance d'état des caméras et peut déclencher une mise à jour pour les miniatures et modèles de données associés.	*Réinitialiser la Surveillance de l'intégrité des caméras*
Connexions		Affiche le nombre et les types d'utilisateurs connectés au système.	Aucun

Nom	Icône du widget	Description	Privilèges requis
État du matériel		Affiche l'état matériel des appareils sélectionnés.	Aucun
Dysfonctionnements		Affiche les dysfonctionnements du système.	*Rapport d'état*
État des rôles		Affiche l'état des rôles sélectionnés.	*Afficher les propriétés de rôle*
Score de sécurité		Affiche le score de sécurité de votre système.[5]	*Voir le widget de sécurité*

[1] Vous pouvez également ajouter une entité à votre tableau de bord depuis la tâche Surveillance en faisant un clic droit sur la tuile associée, puis en sélectionnant Ajouter au tableau de bord.

[2] Certaines entités peuvent nécessiter des privilèges particuliers.

[3] Seuls les rapports enregistrés en tant que tâches publiques sont pris en charge. Vous pouvez également ajouter un rapport à votre tableau de bord en sélectionnant Ajouter au tableau de bord dans la tâche de rapport associée dans Security Desk.

[2] Certains rapports peuvent nécessiter des privilèges particuliers.

[5] Pour en savoir plus, voir Fonctionnement du widget Score de sécurité.

Browse

- À propos des tableaux de bord
- Créer un tableau de bord

1.8.3 | Créer un tableau de bord

Vous pouvez créer des tableaux de bord personnalisés et les enregistrer en tant que tâches publiques ou privées dans Security Desk.

Before you begin

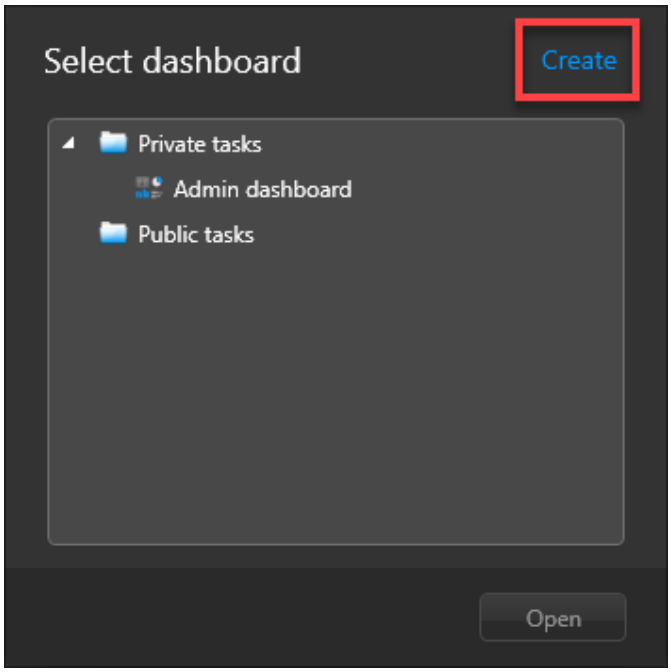
Pour créer un tableau de bord, les utilisateurs doivent disposer des privilèges suivants :

- *Modifier les tableaux de bord*
- *Gérer les tâches privées* ou *Ajouter des tâches publiques*

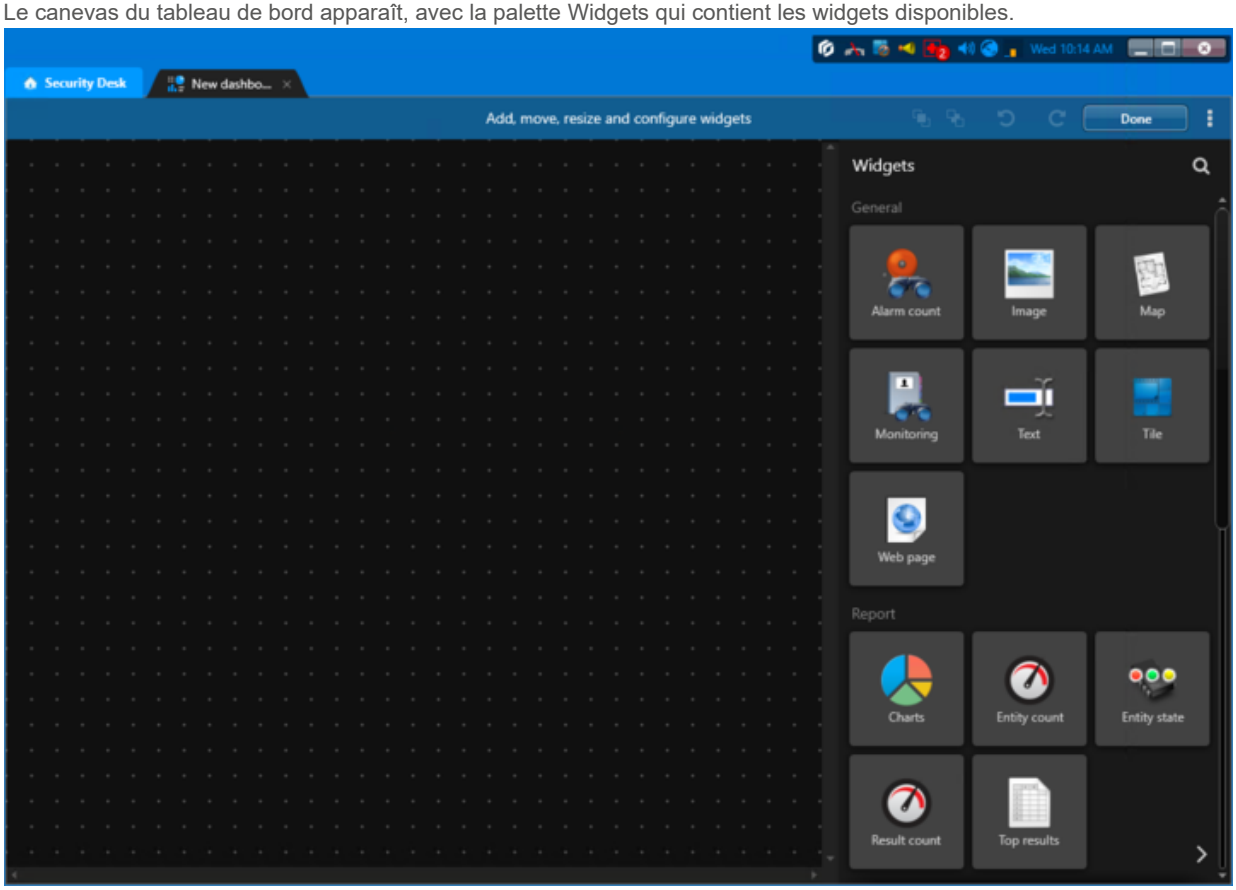
Certains widgets peuvent exiger des privilèges particuliers. Pour en savoir plus, voir Widgets de tableau de bord standard.

Procedure

1. Dans Security Desk, ouvrez la tâche Tableaux de bord.
2. Sur l'écran Sélectionner un tableau de bord, cliquez sur Créer.



3. Donnez un nom au nouveau tableau de bord et enregistrez-le en tant que tâche publique ou privée.
   Un tableau de bord vide est créé.
4. Cliquez sur Ajouter des widgets.
   Le canevas du tableau de bord apparaît, avec la palette Widgets qui contient les widgets disponibles.

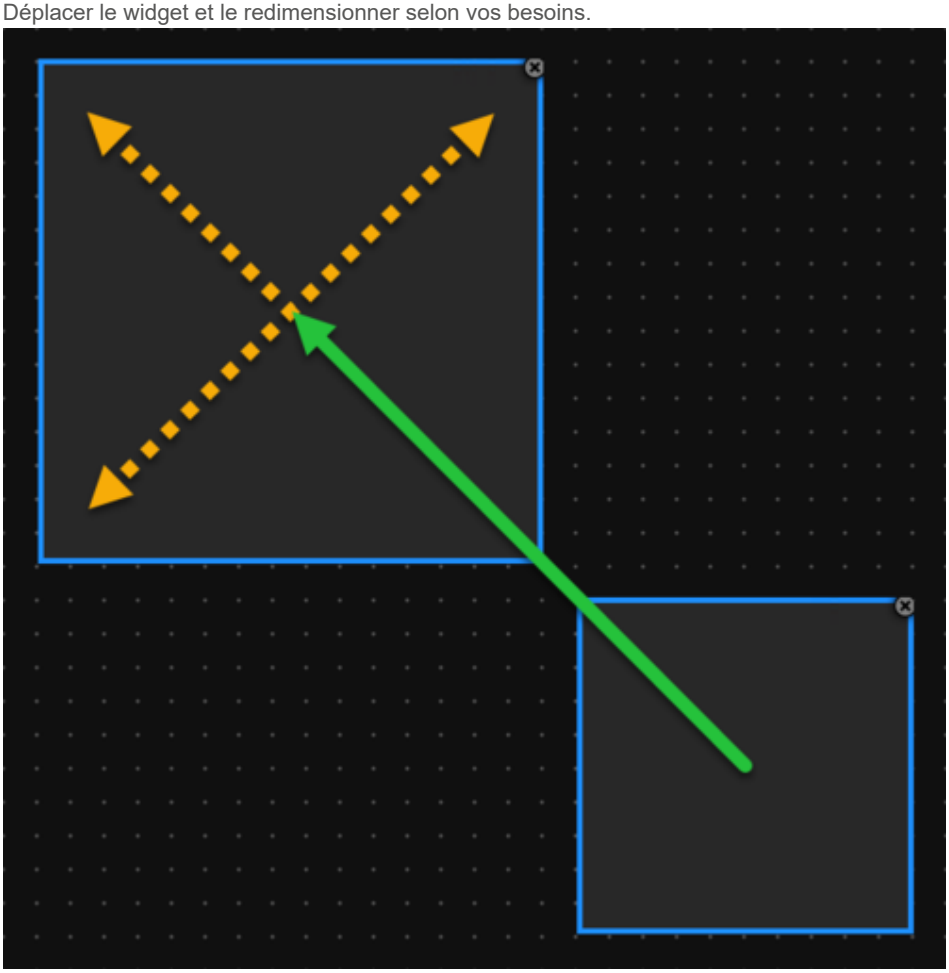


5. Ajoutez des widgets au tableau de bord en les faisant glisser de la palette vers le canevas.
   Tip: Vous pouvez faire une recherche pour trouver le widget qui vous intéresse.

   Par défaut, toutes les modifications apportées à la disposition du tableau de bord et à la configuration des widgets sont enregistrées automatiquement. Pour désactiver ce comportement, désélectionnez enregistrement automatique dans le menu du tableau de bord.

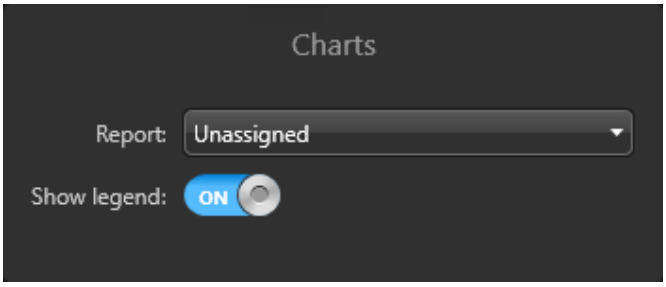
   Pour chaque widget, vous pouvez effectuer les tâches suivantes :

- Déplacer le widget et le redimensionner selon vos besoins.



Le cadre du widget s'aligne sur la grille du canevas. Les widgets peuvent se chevaucher. Vous pouvez placer un widget devant ( ) ou derrière( ) les autres.

- Dans les options de chaque widget, configurez l'affichage du widget.



- Dans les options générales, configurez l'aspect et le comportement du widget. Vous pouvez notamment spécifier le titre du widget, la couleur d'arrière-plan et activer l'actualisation automatique des données.

Les compteurs, graphiques, rapports et pages web doivent être actualisés pour afficher les dernières informations. Les widgets du tableau de bord peuvent être actualisés manuellement ou à intervalles réguliers. La fréquence d'actualisation

automatique peut être spécifiée pour chaque widget ou pour l'ensemble du tableau de bord dans les Options du tableau de bord.

6. Une fois que vous avez ajouté les widgets au tableau de bord, cliquez sur Terminé.

Results

Vous pouvez utiliser cette disposition de tableau de bord. Les tableaux de bord publics sont accessibles par tous les utilisateurs dotés des privilèges *Afficher les tableaux de bord* et *Afficher les tâches publiques*. Les tableaux de bord privés ne sont accessibles que par l'utilisateur actuel.

After you finish

Pour accéder à votre tableau de bord, vous pouvez le sélectionner dans la tâche Tableaux de bord, ou l'ouvrir directement avec la tâche publique ou privée associée.

Browse

- À propos des tableaux de bord
- Widgets de tableau de bord standard

1.9 | Cartes Security Center dans Security Desk

1.9.1 | Utilisation des cartes dans Security Center

Pour enrichir votre connaissance de la situation et renforcer la sécurité du système, vous pouvez utiliser des cartes dans Security Center pour visualiser et parcourir vos installations en temps réel. Les cartes facilitent également la gestion des caméras, des portes et d'autres entités.

Pour utiliser les cartes avec Security Center, *Plan Manager* doit être activé dans votre licence. Pour utiliser les cartes dans Security Desk, vous pouvez utiliser la tâche *Cartes* dédiée aux cartes ou la tâche *Surveillance* générique.
Les cartes permettent d'effectuer les tâches suivantes :

- Utiliser les panoramique et le zoom.
- Parcourir les différentes cartes.
- Étendre une même carte à plusieurs moniteurs.
- Gérer vos entités Security Center, comme les caméras, portes, zones, etc.
- Surveiller et répondre aux alarmes et événements en temps réel.
- Ajouter des entités locales et fédérées.
- Afficher et masquer les informations concernant les *objets cartographiques*.
- Afficher des informations sur les objets cartographiques dans des bulles de texte.
- Rechercher les entités sur les cartes et voir les entités à proximité.
- Repérer les points d'intérêt, comme les sorties de secours, trousses de premiers secours, etc.
- Surveiller et contrôler des caméras, portes, secteurs de détection d'intrusion et zones.
- Surveiller les objets en mouvement, comme les véhicules de patrouille.
- Afficher les lectures et alertes de plaques d'immatriculation provenant de caméras de RAPI fixes.
- Surveiller l'état des entrées numériques (actif, inactif).
- Contrôler le comportement des relais de sortie.
- Exécuter les macros.

Explorer

- Présentation de la tâche Surveillance
- Présentation de la tâche Cartes

1.9.2 | Commandes de base pour les cartes

Dans Security Desk, vous pouvez interagir avec les cartes et les appareils de sécurité qui y figurent à l'aide de commandes standard, par exemple en déplaçant la carte avec la souris ou en cliquant sur des objets cartographiques. La forme du curseur de

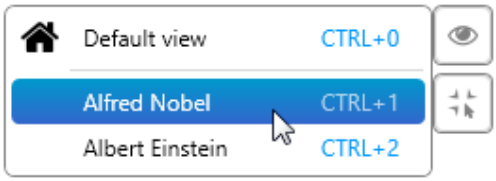
la souris indique les actions que vous pouvez effectuer.

Objets cartographiques

Un objet cartographique est une représentation graphique d'une entité Security Center ou d'un élément géographique (ville, autoroute, rivière, et ainsi de suite) sur vos cartes. Les objets cartographiques vous permettent d'interagir avec votre système sans quitter la carte.

Boutons de commande incrustés

Vous pouvez exécuter les commandes les plus courantes à l'aide des boutons incrustés dans l'angle supérieur droit de la carte.

Bouton	Nom	Entrées alternatives
	Zoom avant	Vous pouvez également effectuer les tâches suivantes : • Actionner la molette de la souris • Double clic • Appuyer sur la touche '+'
	Zoom arrière	Vous pouvez également effectuer les tâches suivantes : • Actionner la molette de la souris • Double clic droit • Appuyer sur la touche '-'
	Sélectionner un préréglage	Cliquez sur le bouton, puis sélectionnez un *préréglage de carte* pour repositionner la carte. Vous pouvez également utiliser Ctrl+numéro de préréglage. 
	Sélectionner la carte	(Canevas Security Desk seulement) Cliquez sur le bouton, puis sélectionnez une zone avec carte ( ) pour afficher la carte associée. Maintenez la touche Ctrl enfoncée lorsque vous sélectionnez la carte pour conserver le *affichage de carte* actuel. REMARQUE : L'icône du bouton correspond à l'icône du secteur sélectionné.
	Clic intelligent	Activer le mode *Clic intelligent*. Le bouton devient bleu et le curseur se transforme en croix. Lorsque le *Clic intelligent* est activé, cliquez n'importe où sur la carte pour orienter toutes les caméras PTZ qui prennent en charge *l'indication de position* sur ce point, dès lors que leur champ de vision n'est pas bloqué par un mur. Pour activer le zoom des caméras PTZ, tracez un rectangle autour de la zone à agrandir. Vous pouvez également maintenir la touche Maj. enfoncée en cliquant pour obtenir le même résultat qu'avec le *clic intelligent*. Si vous êtes dans la tâche Surveillance, toutes les caméras dont le champ de vision englobe l'emplacement cliqué sont affichées dans les tuiles restantes du canevas.
	Envoyer la sélection vers des tuiles	Cliquez sur , puis sur Envoyer la sélection vers des tuiles ( ) pour activer la fonctionnalité de sélection multiple. Vous pouvez également utiliser Alt + clic. Le

Bouton	Nom	Entrées alternatives
		curseur prend la forme d'une croix. Effectuez un cliquer-glisser pour sélectionner plusieurs objets cartographiques avec un rectangle. Lorsque vous relâchez la souris, chaque objet cartographique situé dans le rectangle est affiché dans une tuile de la tâche Surveillance.
	Zoom du secteur	Cliquez sur …, puis sur Zoom du secteur ( ) pour activer la fonctionnalité Zoom du secteur. Vous pouvez également utiliser Ctrl + clic. Le curseur prend la forme d'une croix. Effectuez un cliquer-glisser pour dessiner un rectangle de zoom dans le secteur sélectionné.

Commandes d'étage

Lorsque les cartes sont configurées en tant qu'étages d'un bâtiment, vous pouvez rapidement parcourir le bâtiment à l'aide des commandes incrustées (en bas à droite).

Tous les étages d'un même bâtiment sont liés. Vous pouvez parcourir les étages d'une carte en appuyant sur le bouton de l'étage que vous souhaitez afficher. Les étages sont nommés d'après le nom du secteur avec une abréviation configurable.

REMARQUE : Si Afficher les alarmes des cartes associées est activé dans les options de la carte, le nombre d'alarmes actives sur les autres étages est affiché dans les commandes d'étage.

Lorsqu'un même secteur est inclus dans plusieurs bâtiments, comme une aire de stationnement partagée, les commandes d'étage peuvent servir à parcourir les bâtiments en suivant la flèche.

La navigation inter-étages utilise la même vue par défaut. Maintenez la touche Ctrl enfoncée en changeant d'étage pour rétablir l'affichage par défaut.

Barre d'outils de carte et raccourcis clavier

D'autres commandes de carte sont disponibles dans la Barre d'outils de carte ou par raccourcis clavier. Les commandes propres à chaque type d'objet cartographique sont décrites dans Objets cartographiques pris en charge..

Résultat	Action
Déplacer la carte	Faire glisser.
Agrandir une section de la carte	Appuyez sur la touche Ctrl et tracez un rectangle sur la section de la carte que vous souhaitez agrandir.
Étendre la carte à tous les moniteurs	(Tâche Cartes seulement) Dans la barre d'outils de carte, cliquez sur Réglages > Étendre la carte à tous les moniteurs.
Basculer vers la carte par défaut	(Tâche Cartes seulement) Dans la barre d'outils de carte, cliquez sur Carte par défaut.
Basculer vers une autre carte	Procédez de l'une des manières suivantes :

Résultat	Action
	• Cliquez sur une vignette de carte. • Cliquez sur un lien cartographique, généralement représenté par un polygone de couleur translucide. • Cliquez sur un étage dans les commandes d'étage. • (Tâche Cartes seulement) Dans la barre d'outils de carte, cliquez sur Sélectionner la carte ou cliquez sur le nom d'une carte. • (Canevas Security Desk seulement) Cliquez sur le bouton Sélectionner la carte incrusté sur la carte actuelle. Pour synchroniser la position des cartes, appuyez sur Ctrl pendant que vous basculez vers une autre carte. La nouvelle carte affiche les mêmes coordonnées GPS ou le même affichage de carte. La position est automatiquement synchronisée entre les étages.
Afficher des informations pour un objet cartographique	Procédez de l'une des manières suivantes : • Pour les objets cartographiques qui représentent des entités Security Center, survolez l'objet cartographique pour afficher le nom de l'entité qu'il représente, ou appuyez sur les touches Ctrl+Alt pour afficher le nom de tous les objets cartographiques en même temps. • Pour les objets KML et ESRI, cliquez sur l'objet cartographique pour afficher toutes les informations disponibles dans une bulle de texte. Si des objets se chevauchent, une liste des couches est affichée pour vous permettre de choisir celle qui contient l'objet qui vous intéresse.
Rechercher une entité sur une carte	Procédez de l'une des manières suivantes : • Dans la tâche Cartes : Dans la barre d'outils de carte, cliquez sur  Rechercher puis tapez le nom d'une entité. • Dans la tâche Surveillance : Faites un clic droit sur une entité affichée dans une tuile, puis cliquez sur Me localiser. Si l'entité est affichée sur plusieurs cartes, les icônes de cartes sont affichées dans une fenêtre contextuelle où vous devez choisir la carte qui doit afficher l'entité.
Afficher ou masquer les informations sur la carte	Procédez de l'une des manières suivantes : • Depuis la tâche Cartes : Dans la barre d'outils de carte, cliquez sur  Couches. • Depuis la tâche Surveillance : Faites un clic droit n'importe où sur la carte et cliquez sur Couches. Dans la boîte de dialogue qui apparaît, sélectionnez les couches que vous souhaitez afficher sur la carte puis cliquez sur OK.
Sélectionner un objet cartographique	Par défaut, cliquez sur l'objet cartographique. Ne s'applique qu'aux entités Security Center. Le cas échéant, cette action : • Affiche l'entité associée dans une bulle. • Affiche les widgets associés dans le volet Commandes.
Afficher le menu contextuel d'un objet cartographique	Faites un clic droit sur l'objet cartographique. Ne s'applique qu'aux entités Security Center.
Configurer une entité	Effectuez un clic droit sur l'objet cartographique, puis cliquez sur Configurer l'entité () pour ouvrir la page de configuration de l'entité représentée.

Résultat	Action
	REMARQUE : Vous devez disposer des privilèges d'exécution de Config Tool et d'affichage des configurations d'entités.
Afficher un objet cartographique dans la tâche Surveillance	Par défaut, cliquez deux fois sur l'objet cartographique. Ne s'applique qu'aux entités Security Center.
Afficher plusieurs objets cartographiques dans la tâche Surveillance	Par défaut, appuyez sur la touche Alt tout en traçant un rectangle autour des objets cartographiques que vous souhaitez afficher dans la tâche Surveillance. Ne s'applique qu'aux entités Security Center.

1.9.3 | Afficher ou masquer les informations sur une carte

Vous pouvez choisir la quantité d'information représentée sur une carte en sélectionnant les couches à afficher.

À savoir

Une carte est constituée d'une image d'arrière-plan statique sur laquelle figurent diverses informations appelées *objets cartographiques* organisées en couches. Vous pouvez contrôler la quantité d'informations visible sur la carte en affichant ou masquant n'importe quelle couche (objets cartographiques).

Procédure

1. Procédez de l'une des manières suivantes :
   - Dans la tâche Cartes, cliquez sur Couches dans la barre d'outils de carte.
   - Dans la tâche Surveillance, faites un clic droit n'importe où sur la carte et sélectionnez Couches.
2. Dans la boîte de dialogue qui apparaît, sélectionnez les couches que vous souhaitez afficher sur la carte.
3. Cliquez sur OK.
   REMARQUE : L'option d'annulation des modifications n'est pas disponible pour cette boîte de dialogue.

1.9.4 | Différences entre les tâches Surveillance et Cartes

Pour utiliser les cartes dans Security Desk, vous pouvez utiliser la tâche Cartes dédiée aux cartes ou la tâche Surveillance générique. Le comportement des cartes dans les deux tâches est globalement le même, mais la disposition de l'espace de travail est différente.

La tâche *Surveillance* est plus adaptée lorsque Security Desk ne contrôle qu'un seul moniteur. La tâche *Cartes* est plus adaptée lorsque Security Desk contrôle plusieurs moniteurs.

Fonctionnalité de carte	surveillance, tâche	Tâche Cartes
Utilisation	Votre poste Security Desk ne contrôle qu'un moniteur, et vous devez afficher la carte et la vidéo côte à côte en permanence.	Votre poste Security Desk contrôle plusieurs moniteurs.
Zone d'affichage de la carte	Les cartes sont affichées dans des tuiles.	Une carte remplit l'espace de travail.
Affichage de plusieurs cartes	Chaque tuile peut afficher une tuile différente.	Affiche une carte à la fois.
Étendre la carte à tous les moniteurs	Non pris en charge.	Dans la barre d'outils de carte, cliquez sur Réglages > Étendre la carte à tous les moniteurs.

Fonctionnalité de carte	surveillance, tâche	Tâche Cartes
Cliquer deux fois sur une entité sur la carte	Affiche l'entité dans une tuile libre du canevas. Lorsque toutes les tuiles sont occupées, remplace l'entité la plus ancienne. Peut remplacer la carte elle-même si c'est l'entité la plus ancienne.	Affiche l'entité dans une tâche Surveillance déjà ouverte. Dans le cas contraire, une tâche est ouverte.
Basculer vers une autre carte	Faire glisser une autre carte (secteur) de la vue secteur vers la tuile qui contient la carte actuelle.	Cliquer sur une autre carte dans la barre d'outils de la tâche.
Rechercher des entités sur une carte	Faites un clic droit sur une entité affichée dans une tuile, puis cliquez sur Me localiser. Si l'entité est affichée sur plusieurs cartes, les icônes de cartes sont affichées dans une fenêtre contextuelle où vous devez choisir la carte qui doit afficher l'entité.	Dans la barre d'outils de carte, cliquez sur Rechercher puis tapez le nom d'une entité..
Basculer vers la carte par défaut	Non pris en charge.	Dans la barre d'outils de carte, cliquez sur Carte par défaut..
Basculer vers une carte favorite	Non pris en charge.	Cliquez sur Sélectionner une carte dans la barre d'outils de la tâche et cliquez sur un favori.
Afficher la liste d'alarmes	Taper F9 et cliquer sur Alarmes.	Cliquer sur Alarmes dans la barre d'outils de la tâche.
Afficher la liste d'événements	Taper F9 et cliquer sur Événements.	Cliquer sur Événement passés dans la barre d'outils de la tâche.
Afficher ou masquer les commandes	Tapez F7 ou cliquez sur Masquer les commandes.	Tapez F7 ou cliquez sur Réglages > Afficher les commandes dans la barre d'outils de la tâche.

1.9.5 | Objets cartographiques pris en charge

Un objet cartographique est une représentation graphique d'une entité Security Center ou d'un élément géographique (ville, autoroute, rivière, et ainsi de suite) sur vos cartes. Les objets cartographiques vous permettent d'interagir avec votre système sans quitter la carte.

Les objets cartographiques sont représentés par des icônes dynamiques ou des formes de couleur que vous pouvez survoler et sur lesquelles vous pouvez cliquer. Vous pouvez configurer l'apparence de la plupart des objets cartographiques.

Les objets cartographiques suivants sont pris en charge :

Objet cartographique	Aspect par défaut sur les cartes	Application et actions particulières
Unité de contrôle d'accès	•  - Unité de contrôle d'accès en état *En ligne* •  - Unité de contrôle d'accès en état *Hors ligne* •  - Unité de contrôle d'accès en état *Avertissement*	• Surveillez l'état de l'unité de contrôle d'accès.
Alarme	•  - Alarme inactive •  - Alarme active • Polygone ou ellipse translucide qui adopte la couleur de l'alarme et clignote si l'alarme est active. • Un objet cartographique associé à une alarme active est repéré par une bulle de notification d'alarme de même couleur que l'alarme. • Si Afficher les alarmes des cartes associées est activé dans les options de la carte, le nombre d'alarmes actives sur une carte associée est affiché dans la barre d'outils Cartes, dans les commandes d'étage, et les liens vers la carte concernée.	• Affiche les alarmes sur les cartes, vous permet d'analyser, d'acquitter, de mettre en veille ou de transférer l'alarme, et vous permet de consulter la procédure d'alarme. • Utile lorsqu'aucune des entités associées à l'alarme n'est représentée sur les cartes. • Survoler la bulle pour afficher plus de détails. • Cliquer sur la bulle de notification pour la remplacer par une bulle de tuile. • (Inactive) Cliquer pour déclencher l'alarme manuellement. • (Active) Cliquer pour afficher l'alarme dans une bulle.
Secteur	• Vignette de carte (toujours liée à la carte représentée) • Polygone ou ellipse de couleur translucide (pouvant être associé à une carte)	• Survoler pour afficher le comptage d'individus ou la présence dans le secteur (si activé). • Supprimer des titulaires de cartes sélectionnés d'un secteur. • Cliquez pour afficher le secteur ou la carte dans une bulle, ou pour basculer vers une carte associée (si définie).
Caméra	•  - La caméra n'enregistre pas •  - La caméra enregistre •  - La caméra a détecté du mouvement (effet de vague verte) •  - Caméra en mode maintenance • Les caméras fixes sont représentées avec un champ de vision bleu. • Les caméras PTZ sont affichées avec un champ de vision vert.	• Surveiller les alarmes et les événements de caméras. • Cliquer pour afficher la vidéo en direct ou enregistrée dans une bulle. • Si la caméra prend en charge l'indication de position, faites un cliquer-glisser sur le champ pour actionner le panoramique et l'inclinaison. • Utiliser le widget PTZ pour faire un zoom avant ou arrière. • Cliquer sur un emplacement de la carte en appuyant sur la touche Ctrl pour orienter toutes les caméras disponibles vers l'emplacement concerné.

Objet cartographique	Aspect par défaut sur les cartes	Application et actions particulières
Séquence de caméras	•  - Séquence de caméras	• Affichez plusieurs caméras en même temps. • Orientez les caméras PTZ vers un même emplacement. • Cliquer deux fois sur la séquence de caméras pour afficher toutes les caméras dans des toiles distinctes dans la tâche Surveillance. Si la carte est affichée dans une tuile, elle n'est pas remplacée si toutes les tuiles sont remplies. REMARQUE : La commande de carte Me localiser repère les caméras individuelles dans la séquence de caméras, pas la séquence elle-même.
Bulle de grappe	•  - Trois objets cartographiques ou plus placés trop proches les uns des autres pour être distingués à un niveau de zoom donné sont représentés par une bulle de grappe bleue. La bulle indique le nombre d'objets qu'elle contient. REMARQUE : Le nombre d'objets en grappe comprend les tailles de groupe suivantes : 3, 4, 5, 10, 20, 50, 100, 200, 500. Les comptes intermédiaires ou supérieurs à ces tailles sont indiqués par un signe plus (+). •  - Si la grappe comprend des alarmes actives, une pastille rouge indique le nombre d'alarmes actives qu'elle contient.	• Cliquez pour faire un zoom avant sur la carte afin de voir les objets cartographiques individuels.
Objet personnalisé	• Les objets personnalisés peuvent être ajoutés aux cartes sous forme d'icônes ou de polygones pour ajouter des comportements personnalisés aux cartes.	Parmi les objets personnalisés, on compte une solution d'interphone personnalisée et un traceur GPS pour les unités mobiles. Contactez-nous pour en savoir plus sur les solutions Genetec™ personnalisées.

Objet cartographique	Aspect par défaut sur les cartes	Application et actions particulières
Porte	•  - Porte ouverte •  - Porte fermée et aucun verrou configuré •  - Porte fermée et verrouillée •  - Porte fermée et déverrouillée •  - Porte forcée •  - Porte déverrouillée et en mode maintenance •  - Porte non sécurisée • Les événements sont affichés dans des bulles de notification. La couleur de la bulle correspond à la couleur affectée à l'événement.	• Surveiller les alarmes, l'état des portes et les événements. • Survoler la bulle pour afficher plus de détails. • Cliquer sur la bulle de notification pour la remplacer par une bulle de tuile. • Déverrouiller la porte, ignorer l'horaire de déverrouillage et contourner le lecteur en utilisant le widget Porte ou en faisant un clic droit sur la porte sur la carte.
Objet ESRI	• Objets cliquables sur les cartes ESRI. Dotés de fonctions similaires aux objets KML.	• Incruste des informations utiles sur les cartes, comme les limites d'une ville, les routes ou les caractéristiques hydrographiques. • Peuvent représenter des objets en mouvement, comme des véhicules de patrouille, en actualisant leur position sur la carte à intervalles réguliers.

Objet cartographique	Aspect par défaut sur les cartes	Application et actions particulières
Entrée numérique	•  - Entrée en état *Normal* •  - Entrée en état *Actif* •  - Entrée en état *Problème (court-circuit)* ou *Problème (circuit ouvert)* •  - Entrée en état *Indisponible* • La couleur des états est personnalisable, et l'icône peut être affichée ou masquée en fonction de l'état. Entrées d'intrusion avec types définis : •  - Entrée d'intrusion de type Cambriolage •  - Entrée d'intrusion de type Porte •  - Entrée d'intrusion de type Clôture •  - Entrée d'intrusion de type Incendie •  - Entrée d'intrusion de type Gaz •  - Entrée d'intrusion de type Mouvement •  - Entrée d'intrusion de type Panique •  - Entrée d'intrusion de type Fenêtre	• Surveiller l'état de l'entrée. • Surveiller les secteurs de détection d'intrusion. Les entrées utilisées pour la détection d'intrusion ont des indicateurs visuels supplémentaires : ◦ L'état *Contourner* est indiqué par un 'X' incrusté sur l'icône de l'entrée. Le privilège *Modifier les propriétés d'unités de détection d'intrusion* vous permet de contourner une entrée ou d'annuler un contournement en faisant un clic droit sur l'icône de l'entrée, puis en faisant un choix dans le menu contextuel. ◦ L'état *alarme active* est indiqué par un halo rouge pulsant autour de l'icône de l'entrée. ◦ Faites un clic gauche sur une entrée numérique d'intrusion pour afficher une fenêtre contextuelle avec le nom de l'entité, l'état codé par couleur, l'état de l'alarme, l'état du contournement et les secteurs parents. ◦ L'état d'une entrée avec un type défini est indiqué par un point incrusté dans le coin inférieur gauche de l'icône de l'entrée. REMARQUE : Vous pouvez modifier les icônes de type d'entrée sur la page Définitions des entrées du rôle Gestionnaire d'intrusions.

Objet cartographique	Aspect par défaut sur les cartes	Application et actions particulières
Secteur de détection d'intrusion	•  - Secteur de détection d'intrusion • Les états possibles sont : *Désarmé (non prêt)*, *Désarmé (prêt à armer)*, *Armement*, *Périmètre armé*, *Armement global* et *Alarme active*. • La couleur des états est personnalisable, et l'icône peut être affichée ou masquée en fonction de l'état.	• Surveiller les alarmes et l'état des secteurs de détection d'intrusion. • Armer ou désarmer le secteur de détection d'intrusion depuis le widget ou en faisant un clic droit sur l'objet cartographique. • Déclencher, mettre en sourdine ou acquitter une alarme d'intrusion depuis le widget Secteur de détection d'intrusion ou en faisant un clic droit sur l'objet cartographique. • Modifier l'état *Contournement* d'une ou de plusieurs entrées en faisant un clic droit sur l'objet cartographique, puis sur les entrées.
Objet KML	• Peut représenter n'importe quel élément sous forme de couche transparente cliquable sur une carte géoréférencée.	• Incruste des caractéristiques statiques sur les cartes, comme les limites d'une ville, les routes ou les caractéristiques hydrographiques. • Peut représenter des informations dynamiques, comme les conditions météo ou l'état de la circulation, en actualisant régulièrement la couche de la carte.
Disposition	•  - Disposition • Un objet cartographique lié à une disposition de tâche Surveillance préalablement enregistrée.	• Cliquez pour afficher les caméras surveillées sous forme de séquence dans une bulle. • Cliquez deux fois pour afficher toutes les caméras dans des tuiles distinctes dans la tâche Surveillance. Si la carte est affichée dans une tuile, elle n'est pas remplacée si toutes les tuiles sont remplies.
Caméra de RAPI	•  - Caméra RAPI fixe •  - Caméra de RAPI en mode maintenance • Les lectures et les alertes sont affichées dans des bulles de notification.	• Surveiller les lectures et alertes des caméras de RAPI. • Cliquer pour afficher la vidéo en direct des caméras contextuelles associées.
Macro	•  - Macro	• Exécuter des macros à partir des cartes. • Ignorer le contexte d'exécution par défaut à partir des cartes. • Cliquer sur une macro pour l'exécuter.

Objet cartographique	Aspect par défaut sur les cartes	Application et actions particulières
Lien cartographique	• Vignettes de cartes, texte, icônes, images ou formes géométriques de couleur.	• Cliquer pour basculer vers la carte associée. • Permet de naviguer au sein des cartes sans passer par la barre d'outils. • Utile si la carte est affichée dans la tâche Surveillance. REMARQUE : Si Afficher les alarmes des cartes associées est activé dans les options de la carte, le nombre d'alarmes actives sur une carte associée est affiché sur le lien vers cette carte.
Utilisateur mobile	•  - Utilisateur mobile sans photo	• Lorsque l'affichage des utilisateurs mobiles sur les cartes est activé, affiche les utilisateurs mobiles et vous permet de leur envoyer des messages et de partager des entités. • Survoler la bulle pour afficher le nom d'utilisateur Security Center. • La bulle affiche la photo de l'utilisateur, si elle est disponible.

Relais de sortie	•  - Relais de sortie en état *Normal*
	•  - Relais de sortie en état *Actif*
		• Déclencher les signaux de sortie des relais à partir des cartes.
		• Cliquer pour afficher la liste des signaux de sortie que vous pouvez déclencher.
		• Pour les sorties d'intrusion :
		  ◦ Avec le privilège *Déclencher un signal de sortie*, faites un clic droit sur l'icône de sortie pour changer l'état dans le menu contextuel. Changements d'état possibles :
		  ▪ *Normal* vers *Actif*
		  ▪ *Actif* vers *Normal*
		  ▪ *Inconnu* vers *Normal* ou *Actif*
		  ◦ Cliquer pour afficher un menu contextuel avec le nom de l'entité, l'état et les signaux de sortie associés.

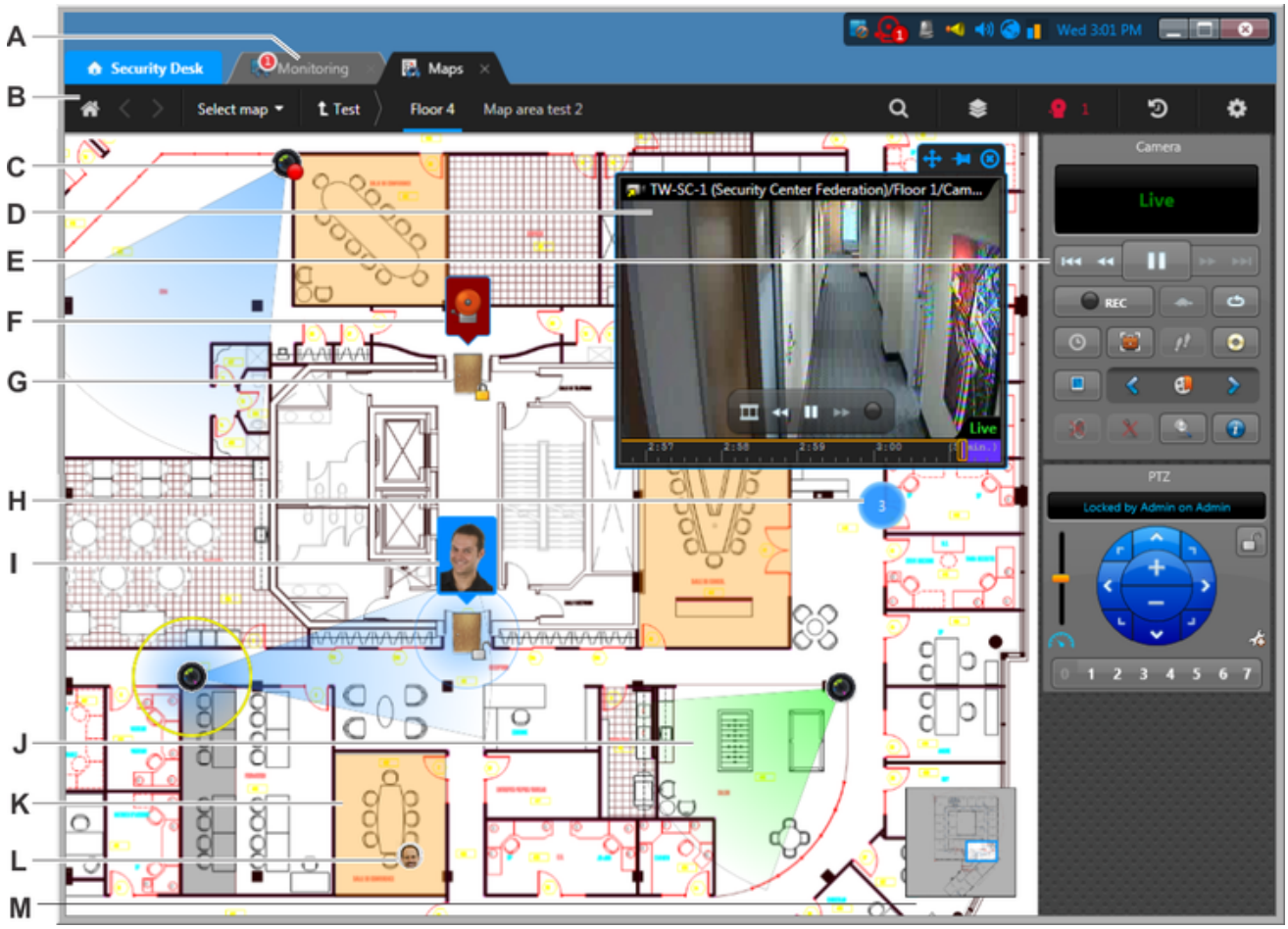
Zone de stationnement	•  - marqueur de zone de stationnement • Polygone de couleur translucide (pouvant être associé à une carte)	• Cliquez sur le marqueur pour afficher le taux d'occupation et le nombre d'infractions de la zone de stationnement dans une fenêtre contextuelle. • Cliquez sur le polygone pour basculer vers la carte associée à la zone de stationnement.

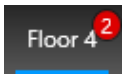
Objet cartographique	Aspect par défaut sur les cartes	Application et actions particulières
Lecteur	•  - Lecteur en état *Activé* (ou *Actif*) •  - Lecteur en état *Désactivé* (ou *Contourné*) •  - Le lecteur est en état *Hors ligne* •  - Le lecteur est en état *Avertissement* • La couleur des états *Activé* et *Désactivé* peut être configurée, et l'indicateur d'état peut être affiché ou masqué.	• Surveiller l'état des lecteurs. • Contourner (désactiver) ou activer les lecteurs.
Texte, images et formes géométriques	• Texte, icônes, images et formes de couleur (polygones et ellipses)	• Vous pouvez les ajouter aux cartes afin de fournir des informations complémentaires, indiquer des points d'intérêt ou créer des liens cartographiques ou des alarmes. Par exemple, une application serait d'indiquer l'emplacement des scanners fixés aux murs sur le plan d'un grand magasin.
Zone	•  - Zone •  - Zone virtuelle •  - Zone d'E/S • Les états possibles sont : *Désarmé*, *Normal*, *Actif* et *Problème*. • La couleur des états est personnalisable, et l'icône peut être affichée ou masquée en fonction de l'état.	• Surveiller les alarmes et l'état de la zone. • Armer et désarmer la zone depuis le widget.

1.9.6 | Présentation de la tâche Cartes

Vous pouvez utiliser la tâche Cartes pour surveiller les *événements* et *alarmes* en temps réel, gérer les entités de votre système de sécurité et parcourir dynamiquement vos installations.

L'image suivante montre une tâche Cartes pour un système de contrôle d'accès et de vidéosurveillance. Security Center Les entités sont représentées sur la carte par des icônes et des zones de couleur cliquables appelées *objets cartographiques*.



A	Par défaut, cliquez deux fois sur tout objet cartographique affichable dans une tuile pour l'ouvrir dans la tâche Surveillance. Le comportement du double clic peut être personnalisé dans les options de la carte.
B	Basculez vers d'autres cartes et configurez les options d'affichage des cartes à l'aide des boutons de la Barre d'outils de carte. Si Afficher les alarmes des cartes associées est activé dans les options de la carte, le nombre d'alarmes actives sur une carte associée est affiché en regard du nom de la carte. 
C	Les objets caméra fixe peuvent inclure un indicateur du champ de vision. L'objet peut également être configuré pour afficher l'état de l'enregistrement ( ) et les événements *Mouvement présent* (avec effet de vague verte) en temps réel.
D	Cliquez sur un objet cartographique (ici une caméra) pour l'afficher dans une bulle. Appuyez sur la touche Ctrl et cliquez pour ouvrir plusieurs bulles. Lorsque vous survolez une bulle avec la souris, l'objet cartographique correspondant est entouré en jaune. En haut de la bulle, vous pouvez cliquer sur Déplacer ( ) pour déplacer la bulle, Fixer à l'écran ( ) pour ancrer la bulle à la carte ou Fermer ( ) pour masquer la bulle.
E	Les widgets correspondant à l'objet cartographique sélectionné (ici une caméra) sont affichés dans le volet Commandes. Pour masquer les commandes, cliquez sur Réglages > Afficher les commandes dans la barre d'outils de la carte.

F	Un objet cartographique associé à une alarme active est repéré par une bulle de notification d'alarme de même couleur que l'alarme. Survoler la bulle pour afficher plus de détails. Cliquer sur la bulle de notification pour la remplacer par une bulle de tuile.
G	Les portes sont représentées sur les cartes par une icône qui indique leur état actuel : *ouverte* ou *fermée*, et *verrouillée* ou *déverrouillée*.
H	Trois objets cartographiques ou plus placés trop proches les uns des autres pour être distingués à un niveau de zoom donné sont représentés par une bulle de grappe bleue. Cliquez pour faire un zoom avant sur la carte afin de voir les objets cartographiques individuels.
I	Les événements sont affichés dans des bulles de notification. La couleur de la bulle correspond à la couleur affectée à l'événement. Survoler la bulle pour afficher plus de détails. Cliquer sur la bulle de notification pour la remplacer par une bulle de tuile.
J	Les objets caméra PTZ peuvent inclure un indicateur du champ de vision. Dans ce cas, faites un cliquer-glisser sur le champ pour actionner le panoramique et l'inclinaison. Faites glisser le pointeur de la souris en le rapprochant de l'icône de la caméra pour incliner la caméra vers le bas, ou en l'éloignant pour incliner la caméra vers le haut. L'objet peut également être configuré pour afficher l'état de l'enregistrement ( ) et les événements *Mouvement présent* (avec effet de vague verte) en temps réel.
K	Les secteurs sont représentés sur la carte par des polygones de couleur. Cliquez sur le polygone pour basculer vers la carte associée au secteur.
L	Si le suivi mobile est activé et si vous avez le privilège *Afficher les utilisateurs mobiles*, les utilisateurs mobiles qui partagent leur position sont automatiquement affichés sur les cartes géoréférencées avec leur photo.

Explorer

- Personnaliser le comportement des cartes dans Security Desk

1.9.6.1 | Barre d'outils de carte

Pour afficher différentes cartes et configurer les options d'affichage de vos cartes, utilisez la barre d'outils de la tâche Cartes.

La barre d'outils de Cartes est divisée en deux parties. Les commandes de navigation de la carte sont situées à gauche. Cliquez sur un nom de carte pour basculer vers la vue par défaut de cette carte. Pour conserver l'*affichage de carte* actuel lorsque du basculement, maintenez la touche Ctrl enfoncée lorsque vous cliquez sur le nom de la carte.

Les commandes d'options d'affichage sont situées à droite.

Carte par défaut
Bascule vers la carte par défaut définie au niveau du système.

Sélectionner la carte
Affiche la liste de favoris et l'arborescence des cartes. La liste des cartes associées à la carte actuelle apparaît en regard de cette commande.

Rechercher
Permet de rechercher les cartes et objets cartographiques par nom.

Couches
Afficher ou masquer les informations sur la carte

Alarmes
Liste des alarmes actives dans une fenêtre flottante. L'icône devient rouge lorsque des alarmes sont actives au sein du système.

- Faites un clic droit sur une alarme pour accéder à son menu contextuel.
- Cliquez deux fois sur une alarme pour basculer vers la carte qui contient l'alarme.
- Cliquez sur pour modifier l'ordre de tri des alarmes ou la position de la fenêtre.
- Cliquez sur Déclencher une alarme pour afficher la liste des alarmes que vous pouvez déclencher manuellement.
- Cliquez sur Tout acq. de force pour forcer l'acquittement de toutes les alarmes du système.

Événements passés
Liste des événements passés dans une fenêtre flottante.

- Faites un clic droit sur un événement pour accéder à son menu contextuel.
- Cliquez deux fois sur un événement pour basculer vers la carte qui contient la source de l'événement.
- Cliquez sur pour modifier l'ordre de tri des événements ou la position de la fenêtre.
- Cliquez sur Effacer pour vider la liste d'événements.

Réglages
Ouvre le menu Réglages.

Afficher les commandes
Affichez ou masquez les commandes. Cette commande est équivalente à l'appui sur la touche F7.

Étendre la carte à tous les moniteurs
Utilisez tous les moniteurs connectés à Security Desk pour afficher la carte.

Gérer
Configurez les favoris et les cartes par défaut.

Ajouter la carte aux favoris
Ajoutez la carte actuelle à la liste de vos favoris.

Modifier la carte
Ouvrez la tâche Map designer dans Config Tool pour modifier la carte actuelle. Vous devez disposer du privilège *Map designer* pour utiliser cette commande.

Définir en tant que carte par défaut
Désignez la carte actuelle en tant que carte par défaut, qui sera chargée à l'ouverture de la tâche Cartes.

Définir en tant que carte par défaut globale
(Administrateurs seulement) Désignez la carte actuelle en tant que carte par défaut globale pour tous les utilisateurs.

Options
Ouvre les Options de la carte.

Aide
Affichez des conseils pour la prise en main des cartes.
Sujet parent : Présentation de la tâche Cartes

1.9.7 | Personnaliser le comportement des cartes dans Security Desk

Vous pouvez personnaliser le comportement des cartes dans la boîte de dialogue Options.

À savoir

Les options des cartes dans Security Desk sont associées à l'utilisateur Windows actuel.

Procédure

1. Ouvrez les Options de la carte.
   - Sur la page d'accueil, cliquez sur Options > Cartes.
   - Dans la tâche Cartes, cliquez sur Réglages > Options > Carte.
2. Le cas échéant, modifiez une ou plusieurs des options suivantes :

- Dans la section Position du volet, sélectionnez la position par défaut des volets de la carte. Les volets peuvent être flottants, ou ancrés à gauche ou à droite de la carte.

  Alarmes
  Position par défaut du volet Alarmes.

  Événements
  Position par défaut du volet Événements.

  Couches de cartes
  Position par défaut du volet Couches.

- Dans la section Éléments de la carte, sélectionnez les actions à entreprendre lors de l'interaction avec les entités de la carte.

  Sur simple clic
  Action à déclencher lors d'un clic sur une entité de la carte.

  Afficher la tuile dans une fenêtre contextuelle
  Valeur par défaut. Affiche l'entité dans une fenêtre contextuelle

  Afficher dans une tâche Surveillance
  Affiche l'entité dans une tâche Surveillance sur un écran local. L'entité est chargée dans une tuile vide si disponible ou remplace le contenu d'une tuile existante.

  Afficher sur un moniteur distant
  Affiche l'entité dans une tâche Surveillance sur tout écran connecté au même Répertoire. Vous devez spécifier l'ID logique du moniteur.

  Ne rien faire
  Désactive l'action sur simple clic.

  Sur double clic
  Action à déclencher lors d'un double clic sur une entité de la carte.

  Afficher dans une tâche Surveillance
  Affiche l'entité dans une tâche Surveillance sur un écran local. L'entité est chargée dans une tuile vide si disponible ou remplace le contenu d'une tuile existante.

  Afficher sur un moniteur distant
  Affiche l'entité dans une tâche Surveillance sur tout écran connecté au même Répertoire. Vous devez spécifier l'ID logique du moniteur.

  Ne rien faire
  Désactive l'action sur double clic.

  Sur lasso
  Action à déclencher lors de la sélection d'entités sur la carte avec le lasso (Alt+cliquer-glisser).

  Afficher dans une tâche Surveillance
  Affiche les entités sélectionnées dans une tâche Surveillance sur un écran local. Les entités sont chargées dans des tuiles vides si disponibles ou remplacent le contenu de tuiles existantes.

  Afficher sur un moniteur distant
  Affiche les entités sélectionnées dans une tâche Surveillance sur tout écran connecté au même Répertoire. Vous devez spécifier l'ID logique du moniteur.

  REMARQUE : Pour afficher l'ID de moniteur dans la zone de notification :
  a. Dans Security Desk, sur la machine connectée au moniteur, cliquez sur Options > Visuel.
  b. Dans la section Dans la zone, réglez ID de moniteur sur Afficher.

- Dans la section Alarmes, sélectionnez Afficher les alarmes des cartes associées pour afficher le nombre d'alarmes actives sur une carte associée dans la barre d'outils de la tâche Cartes, dans les commandes d'étage, et les liens vers la carte concernée.

3. Cliquez sur Enregistrer.

Explorer

- Présentation de la tâche Cartes

1.10 | Raccourcis clavier dans Security Desk

1.10.1 | Raccourcis clavier par défaut dans Security Desk

Ce tableau présente les raccourcis clavier par défaut qui permettent de contrôler les tâches, tuiles et entités sur votre poste. Cette liste est triée par commande, par ordre alphabétique.

REMARQUE : Vous pouvez modifier les raccourcis clavier dans la boîte de dialogue Options.

Commande	Description	Raccourci
Commandes générales		
Verrouillage auto	Verrouiller le poste.	Ctrl+Maj+L
Commandes	Afficher/masquer les commandes.	F7
Afficher le canevas seul, le rapport seul, puis les deux	Basculer entre l'affichage du canevas seul, du volet de rapport seul, ou des deux.	F9
Quitter l'application	Fermez l'application .	Alt+F4
Plein écran	Basculer entre l'affichage de l'application dans une fenêtre et en plein écran.	F11
Aller au contenu suivant du cycle	Lorsque vous affichez une entité composite dans une tuile, basculer vers l'entité associée suivante ou vers la caméra suivante de la séquence.	Ctrl+Flèche droite
Aller au contenu suivant du cycle (toutes les tuiles)	Lorsque vous affichez une entité composite dans une tuile, basculer vers l'entité associée suivante ou vers la caméra suivante de la séquence.	Ctrl+Maj+Flèche droite
Page suivante	Basculer vers l'onglet de tâche suivant.	Ctrl+Tab
Aller au contenu précédent du cycle	Lorsque vous affichez une entité composite dans une tuile, basculer vers l'entité associée précédente ou vers la caméra précédente de la séquence.	Ctrl+Flèche gauche
Aller au contenu précédent du cycle (toutes les tuiles)	Lorsque vous affichez une entité composite dans une tuile, basculer vers l'entité associée précédente ou vers la caméra précédente de la séquence.	Ctrl+Maj+Flèche gauche
Page précédente	Basculer vers l'onglet de tâche précédent.	Ctrl+Maj+Tab
Aide	Ouvrir l'aide en ligne.	F1
Page d'accueil	Aller sur la page d'accueil.	Ctrl+Accent grave (`)

Commande	Description	Raccourci
Action éclair x	Exécuter les actions éclair 1 à 10, une fois qu'elles ont été configurées.	Ctrl+(F1-F10)
Options	Ouvrir la boîte de dialogue Options.	Ctrl+O
Sélectionner les colonnes	Sélectionner les colonnes à afficher/masquer dans le volet de rapport.	Ctrl+Maj+C
Sélecteur	Afficher/masquer le volet sélecteur.	F6
Démarrer le cycle	Basculer automatiquement entre toutes les entités chargées dans Security Desk. Par défaut, la durée d'affichage est de 4 secondes par entité.	Ctrl+Flèche haut
Démarrer le cycle (tous)	Basculer automatiquement entre toutes les entités chargées dans Security Desk. Par défaut, la durée d'affichage est de 4 secondes par entité.	Ctrl+Maj+Flèche haut
Tuiles seulement	Afficher seulement les tuiles d'affichage et la liste des tâches. Le volet sélecteur, le volet événement et les commandes sont masqués. Cette option sert principalement à la tâche *Surveillance*.	F10
Menu contextuel de tuile	Ouvrez le menu contextuel de la tuile sélectionnée sur le canevas. REMARQUE : Ce raccourci clavier ne peut pas être modifié depuis la boîte de dialogue Options.	Maj+F10 ou touche Menu contextuel Appuyez sur `Tab` pour sélectionner successivement les options du menu, puis appuyez sur `Entrée`.
Commandes d'alarmes		
Acquitter (par défaut)	Acquitter l'alarme sélectionnée dans le *Rapport d'alarmes*.	Barre d'espace
Acquitter tout (par défaut)	Acquitter toutes les alarmes dans la tâche *Rapport d'alarmes*.	Ctrl+Maj+Barre d'espace
Afficher la page d'alarme	Ouvrez la tâche *Surveillance d'alarmes*.	Ctrl+A
Mettre l'alarme en rappel (tous)	Placer toutes les alarmes en veille pendant 30 secondes. Lorsqu'une alarme est en veille, elle est temporairement retirée du canevas.	Alt+Ctrl+Maj+S
Mettre l'alarme en rappel	Placer l'alarme en veille pendant 30 secondes. Lorsqu'elle est en veille, l'alarme est temporairement retirée du canevas.	S
Commandes de caméra		
Ajouter un signet	Ajouter un signet à la vidéo dans la tuile sélectionnée (vidéo en direct seulement).	B
Ajouter un signet (tous)	Ajouter des signets à la vidéo dans toutes les tuiles sélectionnées (vidéo en direct seulement).	Ctrl+Maj+B
Copier les statistiques de la tuile vidéo	Copier les statistiques de la tuile sélectionnée.	Ctrl+Maj+X

Commande	Description	Raccourci
sélectionnée		
Exporter de la vidéo	Exporter la vidéo de la tuile sélectionnée.	Ctrl+E
Exporter la vidéo de toutes les tuiles	Exporter la vidéo de toutes les tuiles affichées sur le canevas.	Ctrl+Maj+E
Avance rapide	Lire la vidéo en mode avance rapide.	Point (.)
Avance rapide générale	Lancer l'avance rapide de toutes les caméras affichées sur le canevas.	Ctrl+Maj+Point (.)
Reprise instantanée	Afficher une reprise instantanée dans la tuile sélectionnée.	I
Saut arrière	Effectuer un saut arrière dans la vidéo enregistrée en fonction du temps de recul spécifié dans la boîte de dialogue Options.	Ctrl+Maj+N
Saut arrière général	Effectuer un saut arrière dans la vidéo enregistrée en fonction du temps de recul spécifié dans la boîte de dialogue Options, pour toutes les caméras affichées sur le canevas.	Alt+Ctrl+Maj+N
Saut avant	Effectuer un saut avant dans la vidéo enregistrée en fonction du temps de recul spécifié dans la boîte de dialogue Options.	Ctrl+Maj+M
Saut avant général	Effectuer un saut avant dans la vidéo enregistrée en fonction du temps de recul spécifié dans la boîte de dialogue Options, pour toutes les caméras affichées sur le canevas.	Alt+Ctrl+Maj+M
Image suivante	Lorsque la lecture vidéo est mise en pause, aller à l'image vidéo suivante.	M
Image suivante général	Lorsque la lecture vidéo est mise en pause, aller à l'image vidéo suivante. S'applique à toutes les caméras affichées sur le canevas.	Ctrl+Maj+J
Lecture/Pause	Suspendre ou lancer la lecture de l'enregistrement vidéo.	G
Lecture/Pause générale	Suspendre ou lancer l'enregistrement vidéo pour toutes les caméras affichées sur le canevas.	Ctrl+Maj+G
Image précédente	Lorsque la lecture vidéo est mise en pause, aller à l'image vidéo précédente.	N
Image précédente général	Lorsque la lecture vidéo est mise en pause, aller à l'image vidéo précédente. S'applique à toutes les caméras affichées sur le canevas.	Ctrl+Maj+H
Rembobiner	Rembobiner la vidéo enregistrée.	Virgule (,)
Rembobinage général	Rembobiner toutes les caméras affichées sur le canevas.	Ctrl+Maj+Virgule (,)
Afficher la frise de diagnostic	Afficher la frise chronologique de diagnostic de flux vidéo.	Ctrl+Maj+T
Afficher le diagnostic de flux vidéo	Afficher/masquer le diagnostic du flux vidéo, qui permet de résoudre les problèmes associés.	Ctrl+Maj+D
Afficher les statistiques de flux vidéo dans la tuile	Afficher/masquer le résumé des statistiques de la vidéo dans la tuile sélectionnée.	Ctrl+Maj+A

Commande	Description	Raccourci
Afficher l'état du flux vidéo	Afficher/masquer le résumé de l'état des connexions et redirections du flux vidéo dans la tuile sélectionnée.	Ctrl+Maj+R
Ralenti	Basculer la lecture en mode ralenti.	Maj+Demi-cadratin (-)
Ralenti (tous)	Basculer la lecture en mode ralenti pour toutes les caméras affichées sur le canevas.	Ctrl+Maj+Demi-cadratin (-)
Basculer vers le temps réel	Basculer vers la vidéo en direct.	L
Basculer vers le direct (tout)	Basculer vers la vidéo en direct pour toutes les caméras affichées sur le canevas.	Ctrl+Maj+V
Basculer vers la lecture	Basculer vers la vidéo enregistrée.	P
Basculer l'enregistrement	Démarrer/arrêter l'enregistrement vidéo de la tuile sélectionnée.	R
Basculer l'enregistrement (tous)	Démarrer/arrêter l'enregistrement vidéo pour toutes les caméras affichées sur le canevas.	Alt+Ctrl+Maj+R
Filature visuelle	Activer/désactiver la filature visuelle dans la tuile sélectionnée.	Alt+F
Filature visuelle (tous)	Activer/désactiver la filature visuelle pour toutes les caméras affichées sur le canevas.	Ctrl+Maj+F
Commandes PTZ		
Aller au préréglage	Basculer vers le préréglage de PTZ sélectionné.	<Préréglage PTZ>+Maj+Insert
Panoramique vers la gauche	Effectuer un panoramique vers la gauche avec la caméra PTZ.	Flèche gauche
Panoramique vers la droite	Effectuer un panoramique vers la droite avec la caméra PTZ.	Flèche droite
Inclinaison vers le bas	Incliner la caméra PTZ vers le bas.	Flèche bas
Inclinaison vers le haut	Incliner la caméra PTZ vers le haut.	Flèche haut
Zoom avant	Effectuer un zoom avant sur l'image de la caméra PTZ.	Maintenir la touche Plus (+) enfoncée
Zoom arrière	Effectuer un zoom arrière sur l'image de la caméra PTZ.	Maintenir la touche Demi cadratin (-) enfoncée
Commandes de porte		
Déverrouiller	Déverrouiller la porte sélectionnée.	U
Déverrouiller (tous)	Déverrouiller toutes les portes affichées sur le canevas.	Ctrl+Maj+U
Commandes de tâches		
Renommer la tâche	Renommer la tâche sélectionnée.	F2
Enregistrer sous	Enregistrer une tâche sous un autre nom et un autre mode (privé ou publique).	Ctrl+T

Commande	Description	Raccourci
Enregistrer l'espace de travail	Enregistrer la liste des tâches, qui sera automatiquement rétablie lors de la prochaine connexion au système sous le même nom d'utilisateur.	Ctrl+Maj+S
Tâches enregistrées	Ouvrir la page *Tâches publiques* depuis la page d'accueil.	Ctrl+N
Commandes de tuile		
Précédent	Basculer vers le contenu précédent de la tuile.	Alt+Flèche gauche
Modifier la mosaïque	Changer la mosaïque sur le canevas.	Ctrl+P
Effacer	Sélectionner une tuile particulière sur le canevas.	<ID de tuile>+Retour arrière
Effacer tout	Effacer toutes les tuiles sélectionnées sur le canevas.	Ctrl+Retour arrière
Passer à la mosaïque suivante	Basculer vers la mosaïque suivante.	O
Passer à la mosaïque précédente	Basculer vers la mosaïque précédente.	Q
Afficher la séquence de caméras	Afficher une séquence de caméras dans une tuile particulière.	<ID de séquence de caméra>+Ctrl+ENTRÉE
Afficher l'entité	Afficher une entité dans une tuile particulière.	<ID d'entité>+ENTRÉE
Avance rapide	Basculer vers le contenu suivant de la tuile.	Alt+Flèche droite
Accueil	**mode Carte** Basculer vers la page d'accueil web associée à la carte. **Mode Tuile :** Revenir au contenu que vous avez initialement fait glisser sur la tuile.	Alt+HOME
Agrandir la tuile	Agrandir la tuile sélectionnée pour qu'elle occupe l'intégralité du canevas. Appuyez à nouveau sur E pour réduire la tuile.	E
Passer la tuile en plein écran	Basculer l'affichage de la tuile sélectionnée en mode plein écran. Appuyer à nouveau sur Alt-ENTRÉE pour réduire la tuile.	Alt+ENTRÉE
Surveiller les alarmes	Activer/désactiver la surveillance d'alarmes dans la tuile sélectionnée. Lorsque la surveillance d'alarmes est activée, les alarmes apparaissent automatiquement dans la tuile.	Alt+A
Surveiller toutes les alarmes	Activer/désactiver la surveillance d'alarmes dans toutes les tuiles du canevas. Lorsque la surveillance d'alarmes est activée, les alarmes apparaissent automatiquement dans les tuiles.	Alt+Ctrl+Maj+A
Surveiller les événements	Activer/désactiver la surveillance d'événements dans la tuile sélectionnée. Lorsque la surveillance d'événements est activée, les événements apparaissent automatiquement dans la tuile.	Alt+T
Réduire / développer	Réduire/développer le secteur ou la séquence de caméras de la	Alt+U

Commande	Description	Raccourci
	tuile sélectionnée.	
Actualiser	Actualiser la page ou recharger la tuile sélectionnée.	F5
Sélectionner la tuile suivante	Sélectionner la tuile suivante sur le canevas.	Y
Sélectionner la tuile précédente	Sélectionner la tuile précédente sur le canevas.	T
Lancer le cycle de tâches	Basculer automatiquement entre toutes les tâches chargées dans Security Desk. Par défaut, la durée d'affichage est de 4 secondes par tâche.	Ctrl+Q
Arrêter le cycle de tâches	Arrêter l'affichage cyclique des tâches.	ÉCHAP
Basculer la surveillance (tous)	Activer/désactiver la surveillance d'événements dans toutes les tuiles du canevas. Lorsque la surveillance d'événements est activée, les événements apparaissent automatiquement dans les tuiles.	Alt+Ctrl+Maj+T

Explorer

- Personnaliser les raccourcis clavier

1.10.2 | Basculer entre les tâches au clavier

Vous pouvez ouvrir une tâche publique enregistrée ou basculer entre les tâches publiques sur votre poste à l'aide de raccourcis clavier.

Avant de commencer

Vous devez connaître l'ID logique de la tâche publique. Pour trouver l'ID logique d'une tâche, consultez la tâche *Système* dans Config Tool.
IMPORTANT : Plusieurs entités peuvent avoir un même ID logique. Dans ce cas, une caméra ou un moniteur analogique avec un même ID est affiché sur le canevas, et le raccourci ne bascule pas vers la tâche.

Procédure

Pour basculer entre les tâches au clavier :

Tapez l'ID de la tâche, puis appuyez sur ENTRÉE.
`<50><ENTRÉE>`.

1.10.2.1 | Basculer entre les tâches sur un moniteur distant au clavier

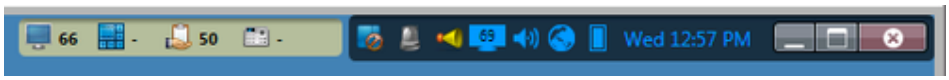
Si vous contrôlez un mur d'images ou un moniteur logique, vous pouvez ouvrir une tâche publique enregistrée ou basculer entre les tâches publiques sur le poste distant à l'aide de raccourcis clavier.

Avant de commencer

Vous devez connaître l'ID logique de la tâche publique. Pour trouver l'ID logique d'une tâche, consultez la tâche *Système* dans Config Tool.
IMPORTANT : Plusieurs entités peuvent avoir un même ID logique. Dans ce cas, une caméra ou un moniteur analogique avec un même ID est affiché sur le canevas, et le raccourci ne bascule pas vers la tâche.

À savoir

Lorsque vous tapez le raccourci, les ID de la tâche et du moniteur sont affichés en haut de la fenêtre Security Desk, à côté de la zone de notification. Vous pouvez ainsi voir les chiffres que vous avez saisis.



Procédure

1. Tapez l'ID du moniteur Security Desk distant, puis appuyez sur la touche POINT (.).

   CONSEIL : L'ID du moniteur Security Desk est affiché dans la zone de notification (

). S'il n'est pas affiché, vous pouvez activer l'affichage de l'icône d'ID de moniteur dans la boîte de dialogue Options.
2. Tapez l'ID logique de la tâche, puis appuyez sur ENTRÉE.
   `<65><POINT><POINT><50><ENTRÉE>`.

Sujet parent : Basculer entre les tâches au clavier

Explorer

- Configurer la zone de notification

1.10.3 | Afficher les caméras au clavier

Vous pouvez afficher une caméra dans une tuile ou basculer entre les caméras sur votre poste à l'aide de raccourcis clavier.

À savoir

Les tuiles sont dotées des ID 1 à 26, en fonction de la mosaïque affichée. Il est plus facile de sélectionner les caméras à afficher lorsque leur ID logique est affiché dans la vue secteur. Vous pouvez activer cette option dans la boîte de dialogue Options.

Procédure

1. Tapez l'ID de la tuile, puis appuyez sur la touche Point (.).
2. Tapez l'ID de la caméra, puis appuyez sur Entrée.
   `<2><Point><15><Entrée>`.

Résultats

La caméra est affichée dans la tuile que vous avez sélectionnée. Si vous ne sélectionnez pas de tuile, la caméra est affichée dans la première tuile libre.

Explorer

- Personnaliser l'affichage des entités sur le canevas

1.10.3.1 | Afficher les caméras sur un moniteur distant au clavier

Si vous contrôlez un mur d'images ou un moniteur logique, vous pouvez afficher une caméra ou une tuile, ou basculer entre les caméras sur le poste distant à l'aide de raccourcis clavier.

Avant de commencer

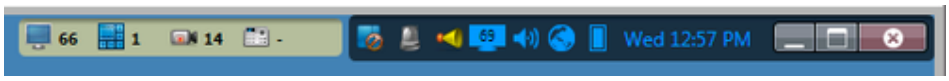
Vous devez connaître l'ID du moniteur distant. Vous pouvez trouver l'ID du moniteur Security Desk dans la zone de notification (

). S'il n'est pas affiché, vous pouvez activer l'affichage de l'icône d'ID de moniteur dans la boîte de dialogue Options.

À savoir

Les tuiles sont dotées des ID 1 à 26, en fonction de la mosaïque affichée. Il est plus facile de sélectionner les caméras à afficher lorsque leur ID logique est affiché dans la vue secteur. Vous pouvez activer cette option dans la boîte de dialogue Options.

Lorsque vous tapez le raccourci, les ID du moniteur, de la tuile et de la caméra sont affichés en haut de la fenêtre de votre poste Security Desk, à côté de la zone de notification. Vous pouvez ainsi voir les chiffres que vous avez saisis.



Procédure

1. Tapez l'ID du moniteur Security Desk distant, puis appuyez sur la touche Point (.).
2. Tapez l'ID de la tuile, puis appuyez sur Point.
3. Tapez l'ID de la caméra, puis appuyez sur Entrée.
   `<65><Point><3><Point><12><Entrée>`.

Résultats

Si vous ne sélectionnez pas de tuile, la caméra est affichée dans la première tuile libre.
Sujet parent : Afficher les caméras au clavier
Explorer

- Configurer la zone de notification

1.10.4 | Personnaliser les raccourcis clavier

Vous pouvez affecter, modifier, importer ou exporter les raccourcis clavier associés aux commandes dans Security Center.

À savoir

Un raccourci clavier ne peut être affecté qu'à une seule commande. Si vous affectez un raccourci clavier existant à une nouvelle commande, il est supprimé de la commande précédente. La configuration de raccourcis clavier est enregistrée avec votre profil utilisateur et s'applique à Security Desk et à Config Tool. Si votre société utilise un ensemble de raccourcis standard, vous pouvez également exporter une configuration de raccourcis clavier dans un fichier XML, puis l'importer sur les autres postes.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Raccourcis clavier .
2. (Facultatif) Importez une configuration de raccourcis clavier de la manière suivante :
   a. Cliquer sur Importer.
   b. Dans la boîte de dialogue qui apparaît, sélectionnez un fichier, puis cliquez sur Ouvrir.
3. Dans la colonne Commande, sélectionnez la commande à laquelle vous souhaitez affecter un raccourci clavier.
4. Cliquez sur Ajouter un élément ( ), puis appuyez sur la combinaison de touches souhaitée.
   Si le raccourci est déjà affecté à une autre commande, un message apparaît.
   - Cliquez sur Annuler pour choisir un autre raccourci.
   - Cliquez sur Affecter pour affecter le raccourci à la commande sélectionnée.
5. Cliquez sur Enregistrer.
6. Pour envoyer vos raccourcis à un autre utilisateur, exportez la configuration de la manière suivante :
   a. Sur la page d'accueil, cliquez sur Options > Raccourcis clavier .
   b. Cliquez sur Exporter.
   c. Dans la boîte de dialogue qui apparaît, sélectionnez un nom de fichier, puis cliquez sur Enregistrer.
7. Pour restaurer les raccourcis clavier par défaut :
   a. Sur la page d'accueil, cliquez sur Options > Raccourcis clavier .
   b. Cliquez sur Rétablir les valeurs par défaut > Enregistrer.

Explorer

- Raccourcis clavier par défaut dans Security Desk

2 | Présentation de la vidéo dans Security Desk

2.1 | Présentation rapide des vidéos dans Security Desk

2.1.1 | À propos de Security Center Omnicast™

Security Center Omnicast™ est le système de gestion vidéo (SGV) sur IP qui confère aux organisations de toutes tailles la capacité de déployer un système de surveillance adapté à leurs besoins. Prenant en charge un large éventail de caméras IP, il répond à la demande croissante en matière de vidéo HD et d'analyse, tout en protégeant la vie privée.

Omnicast™ offre les fonctionnalités principales suivantes :

- Visionnement de vidéo en direct et enregistrée provenant de toutes les *caméras*
- Affichage de 64 flux vidéo simultanés sur un même poste de travail
- Affichage de toutes les caméras sur des frises chronologiques indépendantes ou synchronisées
- Contrôle complet du PTZ à l'aide d'un clavier CCTV ou PC, ou à l'écran à la souris
- Zoom numérique
- Détection de mouvements
- Filature visuelle :permet de suivre un individu ou un objet en mouvement qui traverse le champ de plusieurs caméras
- Recherche vidéo par *signet*, mouvement ou date et heure
- Exporter la vidéo
- Protection de la vidéo contre la suppression involontaire
- Signatures électroniques pour protéger la vidéo contre les altérations
- Protection de la confidentialité des individus dans la vidéo

Omnicast™ assure aussi la prise en charge vidéo des *événements* suivis par d'autres systèmes unifiés par Security Center.

- Amélioration de tous les signalements d'événements par vidéo en direct ou enregistrée
- Amélioration de la surveillance d'alarmes par vidéo en direct ou enregistrée
- Amélioration de la détection d'intrusion par vidéo en direct ou enregistrée
- Amélioration du système de contrôle d'accès Synergis™ par vidéo en direct ou enregistrée
  - Vérification vidéo :comparaison de la photo d'un *titulaire de cartes* à l'image vidéo en direct ou enregistrée
  - Consolidation de tous les événements d'accès par vidéo en direct ou enregistrée
- Amélioration du système de reconnaissance automatique de plaques d'immatriculation AutoVu™ par vidéo en direct ou enregistrée

2.2 | Caméras Security Center dans Security Desk

2.2.1 | À propos des caméras (codeurs vidéo)

Une entité caméra représente une source vidéo unique dans le système. La source vidéo peut être une caméra IP, ou une caméra analogique connectée au codeur vidéo d'une unité vidéo. Plusieurs flux vidéo peuvent être générés à partir d'une même source vidéo.

Un codeur vidéo est un appareil vidéo qui convertit une source vidéo analogique en un format numérique à l'aide d'un algorithme de compression standard, comme le H.264, MPEG-4 ou M-JPEG. Le codeur vidéo est l'un des nombreux équipements dont sont dotées les unités vidéo.

Chaque codeur vidéo peut générer un ou plusieurs flux vidéo utilisant différents types de compression vidéo et différents formats pour différents usages. Sur une caméra IP, la caméra et le codeur vidéo forment une unité indissociable, et les deux termes sont souvent utilisés de manière interchangeable.

Les caméras (ou codeurs vidéo) sont automatiquement créées lors de l'ajout des unités vidéo auxquelles elles appartiennent à Security Center.

2.2.2 | Afficher une caméra dans une tuile

Vous pouvez afficher les caméras sur le canevas depuis toutes les tâches vidéo de Security Desk.

Procédure

1. Procédez de l'une des manières suivantes :
   - Repérez une caméra dans la vue secteur, puis cliquez deux fois sur la caméra ou faites-la glisser sur une tuile.
   - Faites glisser une caméra du volet de rapport sur une tuile.
2. Pour contrôler la caméra, faites un clic droit dans la tuile et utilisez les commandes du menu, ou utilisez les widgets du volet Commandes.
3. Pour effacer les caméras du canevas, procédez de l'une des manières suivantes :
   - Faites un clic droit sur une tuile et sélectionnez Effacer ( ).
   - Sélectionnez une tuile et appuyez sur la touche Retour arrière.
   - (Vide toutes les tuiles) En bas du canevas, cliquez sur Effacer tout ( ).
   - (Vide toutes les tuiles) Appuyez sur Ctrl+Retour arrière.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

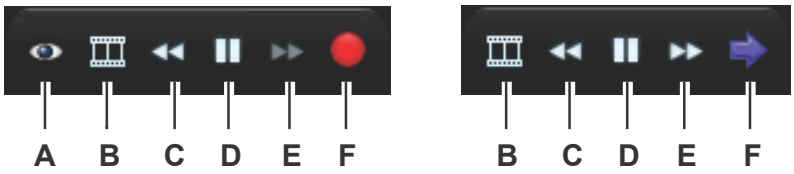
2.2.3 | Commandes vidéo intégrées à la tuile

Lorsque vous affichez une caméra sur le canevas, des commandes vidéo sont incrustées sur l'image vidéo lorsque vous survolez la tuile avec le curseur de la souris.

Vous pouvez également masquer ces commandes dans la boîte de dialogue Options.

Les figures suivantes montrent les commandes vidéo intégrées aux tuiles pour de la vidéo en direct et enregistrée.

Vidéo en direct : Vidéo enregistrée :



A	• Aller au préréglage PTZ Seulement disponible pour les caméras PTZ avec positions prédéfinies. Indique à la caméra PTZ d'aller à une position prédéfinie. • Aller au préréglage du zoom numérique Seulement disponible pour les caméras fixes avec préréglages de zoom numérique. Indique à la caméra PTZ d'aller au préréglage de zoom numérique spécifié.
B	Afficher/masquer les vignettes
C	Rembobiner (lecture arrière)
D	Pause
E	Avance rapide
F	La commande dépend de l'utilisation du mode vidéo en direct ou enregistré : • Vidéo en direct : État de l'enregistrement • Vidéo enregistrée : Basculer vers la vidéo en direct Si la caméra est également contrôlée par un Archiveur auxiliaire, vous pouvez démarrer l'enregistrement manuellement sur l'Archiveur auxiliaire en faisant un clic droit sur le bouton d'état d'enregistrement, en sélectionnant Enregistrement auxiliaire, puis en cliquant sur le bouton enregistrer ( ) en regard du nom du rôle Archiveur auxiliaire. REMARQUE : Divers boutons et couleurs de boutons peuvent être affichés selon la tâche effectuée. Pour en savoir plus, voir Widget Caméra.

Explorer

- Widget Caméra
- Personnaliser l'affichage des tuiles dans Security Center

2.2.4 | Contrôler les séquences de caméras

Vous pouvez contrôler les séquences de caméras affichées sur le canevas depuis toutes les tâches vidéo de Security Desk.

À savoir

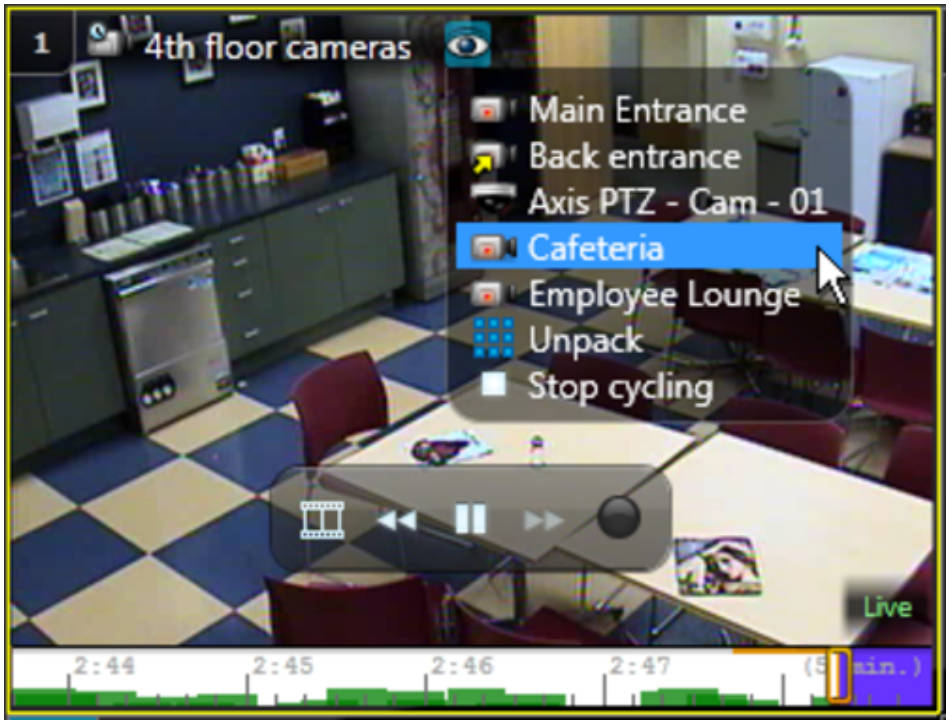
Les séquences de caméras sont des groupes de caméras enregistrés sous forme d'une même entité. Dans la vue secteur, elles sont représentées par une icône de caméra dotée d'une horloge ( ). Lorsqu'une caméra d'une séquence bascule en mode hors ligne, l'état de l'entité ne vire pas au rouge (hors ligne), mais le flux vidéo correspondant est inaccessible.

Lorsqu'une séquence de caméras est affichée dans une tuile, les caméras associées sont affichées tour à tour. Lorsque vous ajoutez des séquences de caméras sur le canevas, la rotation des caméras est synchronisée.

REMARQUE : Si une caméra PTZ est associée à la séquence et que vous activez le PTZ, le cycle s'interrompt. Vous pouvez cliquer sur Démarrer le cycle une fois que vous avez fini d'utiliser le PTZ.

Procédure

1. Affichez la séquence de caméras de l'une des manières suivantes :
   - Repérez la séquence de caméras dans la vue secteur, puis cliquez deux fois sur la séquence ou faites-la glisser sur une tuile.
   - Faites glisser la séquence de caméras du volet de rapport sur une tuile.
2. Dans la barre d'outils de la tuile, cliquez sur .



3. Dans la liste déroulante des entités réduites, procédez de l'une des manières suivantes :
   - Pour suspendre la séquence et rester sur la caméra actuelle, cliquez sur Arrêter le cycle.
   - Pour afficher toutes les caméras en même temps, cliquez sur Développer.
   - Pour forcer la séquence à afficher un flux particulier, cliquez sur la caméra correspondante.

Explorer

- Synchroniser la vidéo dans les tuiles

2.2.5 | Affichage des caméras PTZ sur le canevas

Lorsqu'une caméra PTZ ( ) est affichée dans une tuile, un curseur de zoom apparaît lorsque la souris survole la vidéo, indiquant que des commandes de PTZ sont disponibles.

L'illustration suivante montre les différents composants d'une tuile lorsqu'une caméra PTZ est affichée.

A	Direction du panoramique du moteur de PTZ. Plus la flèche est longue, plus le déplacement du moteur est rapide. Plus la flèche est courte, plus le déplacement du moteur est lent.
B	Curseur utilisé pour faire un zoom avant et arrière.
C	Position et valeur de zoom actuelles du moteur de PTZ.

2.2.6 | Contrôle des caméras PTZ

Vous pouvez contrôler les caméras PTZ affichées sur le canevas depuis toutes les tâches vidéo de Security Desk.

À savoir

Certains modèles de caméras PTZ prennent en charge deux commandes de PTZ complémentaires :

Rectangle de zoom
Agrandir une zone en traçant un cadre sur l'image vidéo. Fonctionne comme le zoom numérique des caméras fixes.

Centrage sur clic
Centrer la caméra sur un point de l'image vidéo en un seul clic.

Pour activer ces commandes, vous devez configurer le PTZ pour le rectangle de zoom et le centrage sur clic dans Config Tool.
CONSEIL : Il est plus commode d'utiliser les commandes de PTZ lorsque les commandes vidéo intégrées à la tuile sont masquées. Vous pouvez masquer ces commandes dans la boîte de dialogue Options.

Le contrôle du PTZ peut être verrouillé s'il est utilisé par quelqu'un dont le niveau utilisateur est supérieur au vôtre. En cas de conflit entre utilisateurs du même niveau, le premier arrivé est le premier servi.

Procédure

1. Pour afficher une caméra PTZ, cliquez deux fois sur la caméra dans la vue secteur, ou faites-la glisser sur une tuile du canevas.
2. Pour développer la tuile, cliquez deux fois sur la barre d'outils de la tuile.
3. Pour faire un zoom avant ou arrière, procédez de l'une des manières suivantes :

- Survolez la tuile avec la souris, puis déplacez la poignée du curseur de zoom vers le haut pour faire un zoom avant et vers le bas pour faire un zoom arrière.
  CONSEIL : Vous pouvez également utiliser la molette de votre souris pour faire un zoom avant ou arrière.
- Si votre caméra PTZ prend en charge la fonction *Rectangle de zoom*, tracez un rectangle sur l'image vidéo pour faire un zoom avant.

4. Pour effectuer un panoramique avec le moteur PTZ, vous pouvez :
   a. Cliquez sur la tuile de la caméra PTZ.
   Une flèche blanche apparaît.
   b. Cliquez sur la flèche blanche une fois pour la changer en flèche bleue
   Une flèche bleue indique la direction du mouvement. Plus la flèche est longue, plus le déplacement du moteur est rapide. Plus la flèche est courte, plus le déplacement du moteur est lent.
   c. Cliquez dans la direction correspondant au déplacement souhaité du moteur PTZ.
   a. Cliquer une fois sur le point bleu au milieu de la tuile PTZ.
   b. Cliquez dans la direction correspondant au déplacement souhaité du moteur PTZ.
   Les flèches bleues suivent vos mouvements.
5. Pour orienter la caméra en fonction d'une position prédéfinie, procédez de l'une des manières suivantes :
   - Dans la tuile vidéo, cliquez sur le bouton (Aller aux préréglages PTZ), puis sélectionnez un préréglage dans la liste.
   - Dans le widget, cliquez sur un des boutons d'accès rapide numérotés.
   - Dans le widget, cliquez sur le bouton (basculer en mode avancé), sélectionnez un préréglage dans la liste Préréglages, puis cliquez sur le bouton (Préréglage).
6. Si votre caméra PTZ prend en charge la fonction *Centrage sur clic*, cliquez sur la vidéo pour centrer l'image sur le point correspondant.

Explorer

- Personnaliser les raccourcis clavier

2.2.7 | Redresser les images d'objectifs de caméras 360°

Pour afficher une image capturée par un objectif de caméra grand-angle ou panoramique 360° sous forme d'image rectangulaire dans une tuile Security Desk, vous pouvez la redresser ou l'aplatir en faisant un zoom sur l'image de la caméra.

Avant de commencer

Configurez l'objectif de la caméra dans Config Tool.

À savoir

Le temps nécessaire pour le redressement dépend de votre ordinateur et de la résolution finale. Par exemple, la durée de redressement sera quatre fois plus longue en 640x480 qu'en 320x240.

Procédure

1. Affichez une caméra grand-angle ou panoramique 360° dans une tuile.
2. Pour faire un zoom sur l'image, utilisez la molette de la souris, ou tracez un cadre autour de la zone qui vous intéresse.
   REMARQUE : Lorsque vous utilisez la molette de la souris, le zoom est centré sur l'image, et pas sur l'emplacement du pointeur de la souris.

3. Pour parcourir l'image agrandie, cliquez sur la vignette dans le coin supérieur gauche de la tuile.

4. Pour faire un zoom arrière, utilisez la molette de la souris ou le curseur de zoom dans la partie droite de la tuile.

2.2.8 | Afficher de la vidéo sur des moniteurs analogiques

Vous pouvez afficher de la vidéo en direct sur un moniteur analogique en affichant une caméra ou séquence de caméras dans une entité moniteur analogique ( ) sur le canevas. Vous pouvez également recevoir des alarmes sur le moniteur analogique si l'entité moniteur analogique est destinataire des alarmes.

Avant de commencer

Votre unité de décodage doit être connectée à un moniteur analogique et doit être ajoutée dans Security Center en tant qu'entité unité de décodage vidéo.

À savoir

Si votre unité de décodage vidéo prend en charge plusieurs moniteurs analogiques (par exemple, si elle est connectée à plusieurs moniteurs d'un mur d'images), chaque moniteur est ajouté en tant qu'entité moniteur analogique distincte dans Security Center. Vous pouvez dès lors reproduire la disposition physique de votre mur d'images en ajoutant les entités moniteur analogique au canevas.

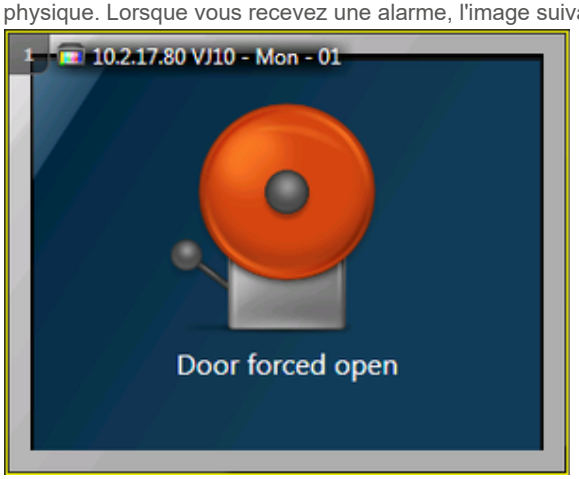
Les caméras fédérées Omnicast™ 4.x ne sont pas prises en charge sur les moniteurs analogiques dans Security Center

Procédure

1. Cliquez deux fois sur l'entité moniteur analogique dans la vue secteur, ou faites-la glisser sur une tuile du canevas.
2. Cliquez deux fois ou faites glisser une caméra ou séquence de caméras prise en charge dans la tuile qui affiche le moniteur analogique.
   REMARQUE : Les caméras prises en charge doivent provenir du même fabricant que l'unité de décodage vidéo et utiliser le même format vidéo.

   La vidéo en temps réel provenant de la caméra est affichée sur le moniteur analogique physique. Dans Security Desk, seuls le nom et l'icône de la caméra sont affichés.

3. Pour contrôler les caméras affichées, utilisez les widgets du volet Commandes (comme le widget Caméra ou PTZ).
4. Pour supprimer la caméra du moniteur analogique, cliquez sur dans la tuile.
   Si votre moniteur analogique est destinataire d'alarmes, vous pouvez recevoir les alarmes sur le moniteur analogique physique. Lorsque vous recevez une alarme, l'image suivante est affichée dans la tuile qui affiche le moniteur analogique.



5. Pour acquitter l'alarme, cliquez sur Acquitter (par défaut) ( ) dans le widget Alarme.

Explorer

- Widget Caméra
- Widget PTZ

2.2.9 | Synchroniser la vidéo dans les tuiles

Vous pouvez forcer la synchronisation de la vidéo en temps réel ou enregistrée affichée dans toutes les tuiles.

À savoir

Vous ne pouvez pas synchroniser la vidéo des entités qui sont affichées dans une tuile dans le cadre d'un événement ou d'une alarme. La vidéo associée à l'événement ou à l'alarme est destinée à montrer ce qui s'est passé pendant cette période.

Procédure

1. Sélectionnez une tuile.
2. En bas du canevas, cliquez sur Synchroniser la vidéo ( ).
   L'activation force toutes les tuiles à afficher de la vidéo en temps réel ou enregistrée. Le point de référence est la tuile sélectionnée. Voici les cas de figure :

- Lorsque la tuile sélectionnée affiche de la vidéo enregistrée, la synchronisation force toutes les tuiles à afficher de la vidéo enregistrée. Toutes les vidéos enregistrées affichent alors la même date et heure, et sont synchronisées à la milliseconde près.
- Lorsque la tuile sélectionnée affiche de la vidéo en temps réel, la synchronisation force toutes les tuiles à afficher de la vidéo en temps réel. Cette option est utile si les champs de plusieurs caméras se chevauchent. La synchronisation permet alors d'afficher un même événement enregistré sous plusieurs angles.

3. Pour désactiver la synchronisation, cliquez sur Arrêter la synchronisation vidéo ( ) en bas du canevas.

2.2.10 | Changer de flux vidéo

Vous pouvez changer le flux vidéo d'une caméra qui affiche de la vidéo dans une tuile.

Avant de commencer

Si votre caméra prend en charge plusieurs flux, ils doivent être activés et configurés dans Config Tool pour pouvoir choisir un flux vidéo par défaut.

À savoir

La majorité des *codeurs vidéo* et *caméras IP* pris en charge par Security Center peuvent générer plusieurs *flux* par caméra individuelle. Cette capacité est utile lorsque vous souhaitez configurer une qualité différente pour le flux vidéo en direct et le flux enregistré. Des flux supplémentaires peuvent être configurés pour d'autres besoins comme l'accès à distance (bas débit) ou pour des flux basse et haute résolution.

Procédure

1. Faites un clic droit sur la vidéo en direct affichée dans une tuile.
2. Cliquez sur Camera > Sélectionner le flux en direct.
3. Sélectionnez l'un des flux vidéo suivants :

En direct
Flux par défaut utilisé pour afficher la vidéo en direct.

Enregistrement
Flux enregistré par l'Archiveur pour une analyse différée.

Distant
Flux utilisé pour la vidéo en direct lorsque la bande passante est limitée.

Basse résolution
Flux utilisé à la place du flux *en direct* lorsque la tuile utilisée pour afficher le flux dans Security Desk est petite.

Haute résolution
Flux utilisé à la place du flux *en direct* lorsque la tuile utilisée pour afficher le flux dans Security Desk est grande.

Automatique
Security Desk utilise le flux *Basse résolution* ou *Haute résolution* en fonction de la taille de la tuile.

Explorer

- Commandes du menu de tuile

2.2.11 | Faire un zoom avant et arrière

Pour mieux voir certains détails de l'image que vous surveillez, vous pouvez agrandir la vidéo en direct ou enregistrée affichée dans une tuile, que vous utilisiez une caméra fixe ou une caméra PTZ.

À savoir

Si le flux vidéo par défaut de la caméra est réglé sur *Automatique*, le flux vidéo bascule en haute résolution lorsque vous activez le zoom numérique.

Procédure

1. Cliquez sur une tuile qui contient de la vidéo en direct ou enregistrée.
2. Procédez de l'une des manières suivantes :
   - Cliquez et faites glisser la souris pour définir la zone de zoom (rectangle bleu), puis relâchez le bouton de la souris. Cette méthode ne fonctionne pas avec les caméras PTZ.
   - Faites défiler la molette de la souris vers l'avant pour agrandir et vers l'arrière pour réduire. Avec les caméras PTZ, cette méthode ne fonctionne qu'après application du zoom numérique.
   - Dans le widget Caméra, cliquez sur Activer/désactiver le zoom numérique ( ).
   - Effectuez un clic droit dans la tuile et cliquez sur Caméra > Activer/désactiver le zoom numérique ( ).

   Une vignette de l'image entière apparaît dans le coin supérieur gauche de la tuile, et le niveau de zoom est indiqué dans la tuile.
3. La vignette de zoom permet d'effectuer les tâches suivantes :
   - Faites glisser le cadre rouge pour déplacer la zone agrandie.
   - Cliquez sur l'image agrandie et faites-la glisser pour déplacer la zone de zoom.
   - Utilisez le curseur pour augmenter ou réduire le facteur de zoom.
4. Pour quitter le zoom, cliquez sur Activer/désactiver le zoom numérique ( ) dans le widget Caméra.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Personnaliser les options de flux vidéo
- Options vidéo dans Security Desk

2.2.12 | Créer un préréglage de zoom numérique

Lorsque vous agrandissez l'image d'une caméra dans une tuile, vous pouvez définir des préréglages de zoom numérique pour les zones pertinentes de l'image.

À savoir

Vous pouvez créer autant de préréglages que vous voulez. Les préréglages de zoom numérique ne sont pas pris en charge par les caméras PTZ.
REMARQUE : Les préréglages PTZ créés dans la version actuelle risquent de ne pas être disponibles dans les versions précédentes de Security Desk.

Procédure

1. Appliquez une méthode de zoom numérique à une image affichée dans une tuile.
2. Dans le widget Caméra, cliquez sur Ajouter ( ).
3. Dans la boîte de dialogue Créer un préréglage, nommez le préréglage puis cliquez sur Créer.
   Un préréglage est créé pour la position actuelle de l'image. Vous pouvez désormais activer un préréglage de zoom en le sélectionnant dans le menu déroulant Préréglages de zoom numérique du widget Caméra.
4. Si vous avez déplacé l'image de la caméra, cliquez sur Préréglage ( ) pour revenir à la position prédéfinie.
5. Dans la section Préréglages de zoom numérique, cliquez sur la flèche du menu déroulant en regard de Préréglage ( ) pour accéder aux options de préréglage supplémentaires suivantes :

   Enregistrer
   Remplacer le préréglage sélectionné dans la liste déroulante par la position actuelle du PTZ.

   Supprimer
   Supprime le préréglage.

   Ajouter un préréglage
   Crée un préréglage de zoom numérique.

Explorer

- Faire un zoom avant et arrière

2.2.13 | À propos de la filature visuelle

La filature visuelle vous permet de suivre un individu en mode vidéo en direct ou enregistrée entre les diverses caméras de votre installation.

Avantages

La filature visuelle vous offre un gain de temps et simplifie les tâches de surveillance et d'enquête. Elle vous permet de suivre une personne rapidement sans perdre de temps à rechercher la caméra pertinente. Vous n'avez pas besoin de vous souvenir des noms des caméras de votre système, car elles sont toutes liées entre elles.

L'association de caméras offre également les avantages suivants :

- Former rapidement de nouveaux opérateurs.
- Réduire le stress de l'opérateur lors de situations à haut niveau d'alerte.

Cas d'utilisation courants

Voici quelques cas d'utilisation courants de la filature visuelle :

Suivi des suspects
Suivre un suspect en mode vidéo en direct ou enregistrée suite à un incident.

Rondes de garde
Réaliser des rondes de garde manuelles à votre convenance.

Itinéraires de sortie
Surveiller les individus lorsqu'ils sortent d'un bâtiment.

Escortes de visiteurs
Suivre les visiteurs et leurs escortes dans votre établissement.

Processus commerciaux
Surveiller les individus lors d'un itinéraire de collecte et de distribution d'argent dans un casino.

Quais de chargement
Suivre les marchandises au fur et à mesure de leur réception et déchargement.

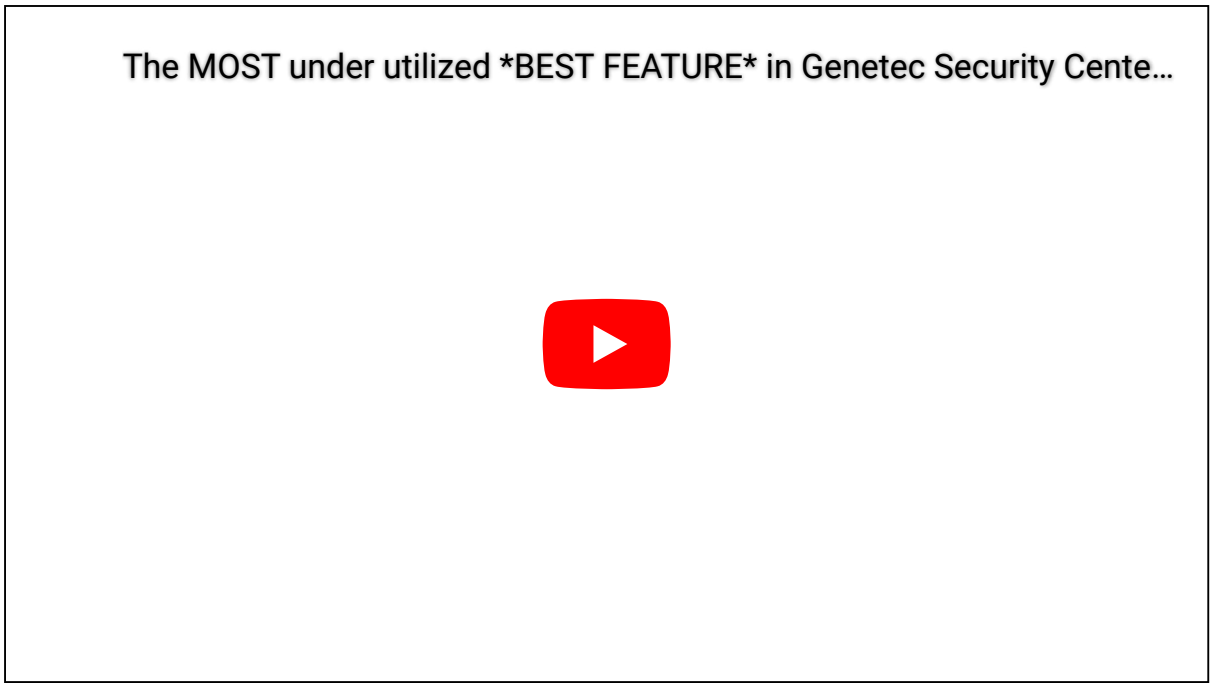
Fonctionnement

Lorsque vous activez la filature visuelle à l'aide de l'icône de pieds () dans Security Desk, des formes colorées sont affichées sur l'image vidéo, selon leur configuration. Chaque forme correspond à un champ de vision de la caméra que vous pouvez visualiser en le sélectionnant. Si plusieurs caméras sont associées à une forme, une liste de noms de caméras s'affiche lorsque vous cliquez sur la forme.

Lorsque vous placez le pointeur de votre souris sur une forme, vous pouvez voir un aperçu de la prochaine image de la caméra.

CONSEIL : Vous pouvez appuyer sur `Ctrl + Maj + F` pour activer la filature visuelle pour toutes les caméras affichées dans le canevas.

Regardez cette vidéo pour en savoir plus.



2.2.13.1 | Suivre des cibles en mouvement

Vous pouvez suivre un individu dans votre installation en temps réel ou en mode lecture après un incident, en utilisant la fonction de suivi visuel dans une tuile sur le canevas.

Avant de commencer

Configurez la filature visuelle.

Procédure

1. Cliquez sur une tuile contenant de la vidéo en direct ou enregistrée.
2. Activez la filature visuelle dans la tuile de l'une des manières suivantes :
   - Dans le widget Caméra, cliquez sur Activer la filature visuelle ( ).
   - Faites un clic droit dans la tuile et cliquez sur Caméra > Activer la filature visuelle ( ).
   - Appuyez sur les touches `Alt+F` du clavier.
3. Lorsque le sujet quitte le champ de la caméra, cliquez sur la forme de couleur représentant un lien vers la caméra suivante.
   Placez le pointeur de votre souris sur une forme pour voir un aperçu de la prochaine image de la caméra.

Exemple

Si quelqu'un vole quelque chose dans votre établissement, vous pouvez enquêter sur le vol en utilisant une combinaison de suivi visuel et de rapport d'incident.

Dans la tâche Surveillance, démarrez l'enregistrement de l'incident ( ) et activez le suivi visuel ( ). Lisez la vidéo et suivez la personne pendant qu'elle se déplace dans votre établissement. Lorsque vous arrêtez l'enregistrement d'un incident, les caméras que vous avez activées pendant l'enregistrement sont incluses dans le rapport d'incident. Plus important encore, les segments vidéo inclus ont l'horodatage correct qui correspond à la date à laquelle la personne s'est rendue dans ces zones. Lorsque vous examinez le rapport exporté ou enregistré, les segments vidéo sont lus en séquence comme dans un film.

Sujet parent : À propos de la filature visuelle

2.2.14 | Ajouter des signets à une séquence vidéo

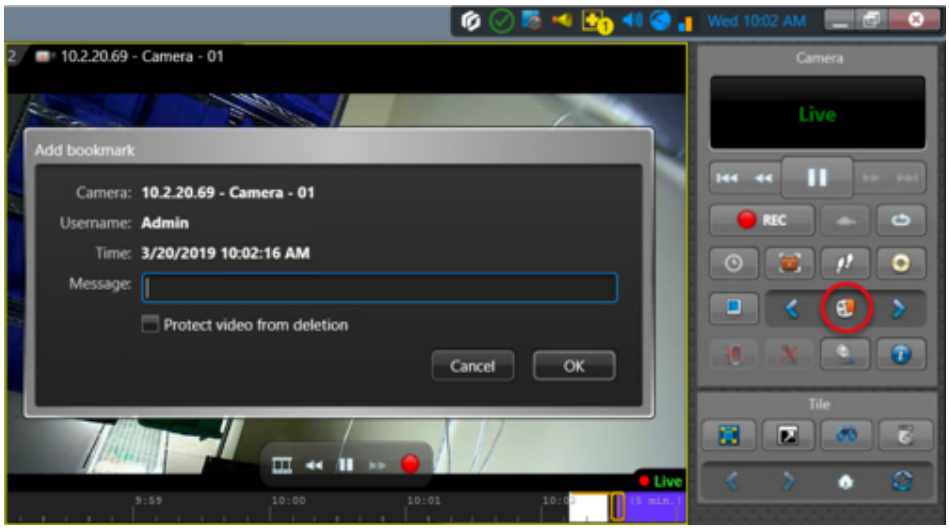
Si vous voyez un élément significatif, vous pouvez ajouter un signet à la vidéo que vous visionnez.

À savoir

- Indicateur d'un événement ou incident servant à repérer un emplacement particulier d'une séquence vidéo enregistrée. Un signet contient également une brève description textuelle qui permet d'effectuer une recherche dans les séquences vidéo.
- Si une caméra n'enregistre pas, l'ajout d'un signet déclenche l'enregistrement.
- Si vous ajoutez un signet à un clip vidéo exporté, le signet n'est stocké que dans le clip vidéo exporté, et pas dans la vidéo archivée d'origine.

Procédure

1. Dans le widget Caméra, cliquez sur Ajouter un signet ( ).
2. (Facultatif) Dans la boîte de dialogue Ajouter un signet, saisissez une brève description dans le champ Message.
   L'horodatage du signet est réglé sur l'heure indiquée dans la boîte de dialogue.
3. (Facultatif) Protégez la séquence vidéo contenant le signet contre le nettoyage d'archives en procédant de la manière suivante :
   REMARQUE : Vous ne pouvez protéger la séquence vidéo que si le signet est ajouté à une caméra locale (non fédérée).
   a. Sélectionnez l'option Protéger la vidéo contre la suppression.
   b. Dans la boîte de dialogue Protéger les archives, définissez l'heure de début et l'heure de fin de la séquence vidéo à protéger, ainsi que la durée de la protection.
      Par défaut, la séquence vidéo protégée démarre une minute avant le signet, et se termine 4 minutes après celui-ci. La durée de protection par défaut est de 5 jours.
   c. Cliquez sur Protéger.
4. Si vous n'avez pas sélectionné l'option Protéger la vidéo contre la suppression, cliquez sur OK pour ajouter le signet ou sur Annuler pour quitter sans ajouter de signet.
   Laisser le champ Message vide n'annule pas l'action.



Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Présentation de la tâche Signets

2.2.14.1 | Afficher de la vidéo associée à un signet

Pour afficher une séquence vidéo qui contient des signets, vous pouvez créer un rapport qui contient tous les signets enregistrés avec la tâche Signets.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Signets.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Caméras
   Sélectionnez la caméra à examiner.

Champs personnalisés
Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

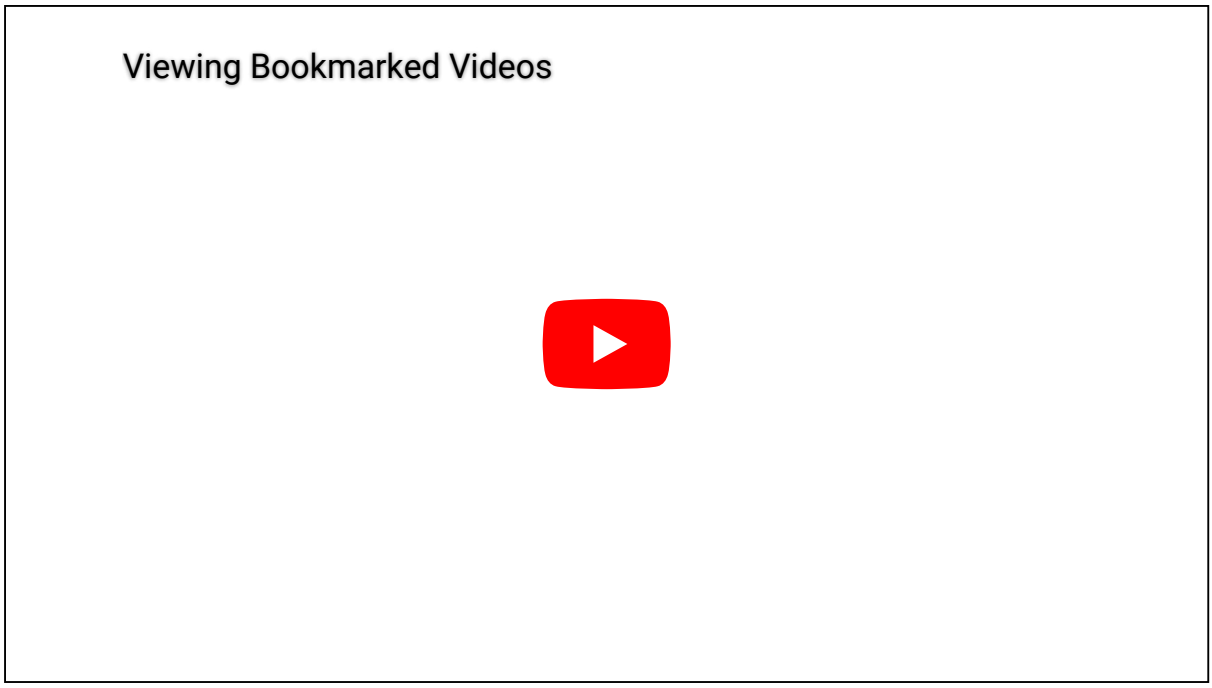
Message
Saisissez le texte que vous souhaitez rechercher dans le signet. Tous les signets sont recherchés si la chaîne est laissée vide.

Plage horaire
La plage horaire pour le rapport.

3. Cliquez sur Générer le rapport.
   Les signets sont affichés dans le volet de rapport. Un message d'avertissement apparaît si votre recherche ne renvoie pas de résultat.
4. Pour afficher la vidéo associée à un signet, faites glisser le signet du volet de rapport vers une tuile du canevas.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



Sujet parent : Ajouter des signets à une séquence vidéo

2.2.15 | Capturer des instantanés vidéo

Que vous consultiez de la vidéo en direct ou enregistrée dans une tuile, vous pouvez capturer l'image vidéo actuelle dans un fichier, puis classer et partager les captures avec l'outil Coffre-fort.

À savoir

- Tous les instantanés sont enregistrés selon la convention suivante : NomCaméra (Date Heure).png. Par défaut, les instantanés sont enregistrés au format PNG à l'emplacement suivant : C:\Users\Username\AppData\Local\Genetec Security Desk version#\Vault.
- Si vous comptez utiliser l'instantané dans le cadre d'une enquête, notez que seuls les fichiers JPEG intègrent les balises EXIF qui fournissent les informations de traçabilité.

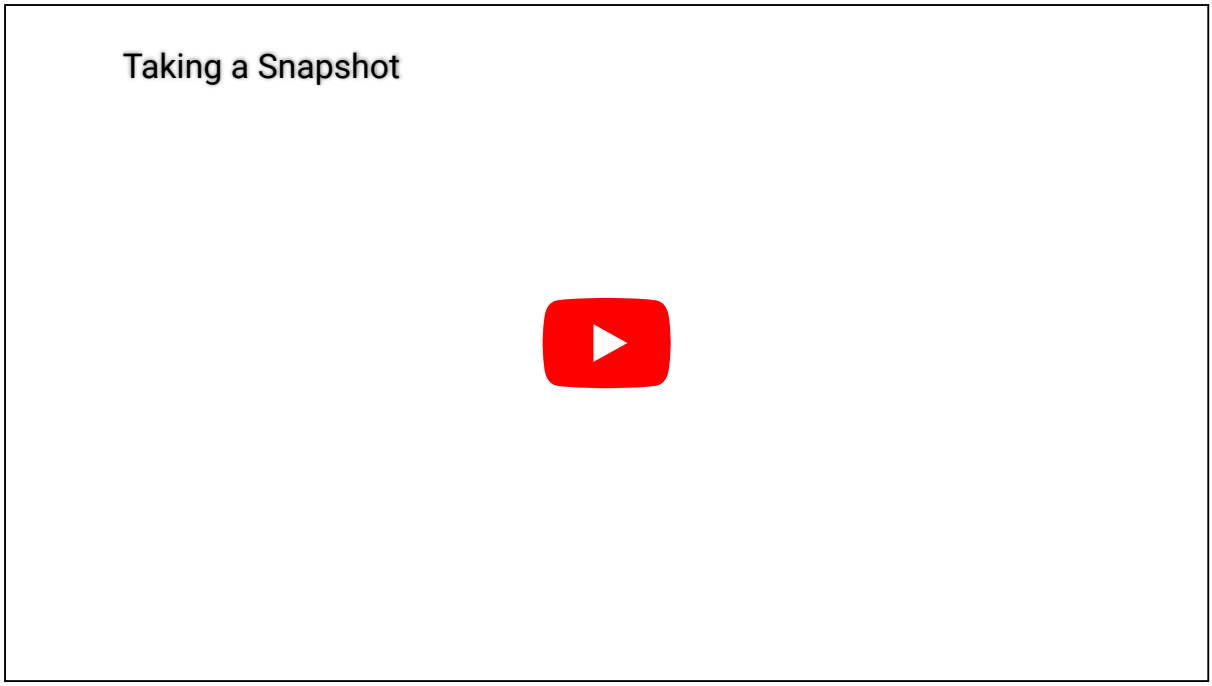
Procédure

1. Sélectionnez la tuile qui affiche la vidéo pour laquelle vous souhaitez capturer un instantané.
2. Procédez de l'une des manières suivantes :
   - Dans le widget Caméra, cliquez sur Enregistrer un instantané ( ).
   - Effectuez un clic droit sur la tuile, puis cliquez sur Caméra > Enregistrer un instantané ( ).

   Une vignette d'aperçu apparaît dans le coin supérieur droit de la fenêtre de Security Desk pendant 2 secondes.
3. Pour ouvrir le Coffre-fort, sur la page d'accueil, cliquez sur Outils > Coffre-fort.
   Le Coffre-fort affiche des vignettes de tous les instantanés.
4. Pour modifier un instantané, procédez de l'une des manières suivantes :
   - Sélectionnez l'instantané et cliquez sur Modifier ( ).
   - Faites un clic droit sur l'instantané et cliquez sur Modifier.
5. Pour imprimer un instantané, procédez de l'une des manières suivantes :
   - Sélectionnez l'instantané, puis cliquez sur Imprimer ( ).
   - Effectuez un clic droit sur l'instantané, puis cliquez sur Imprimer.
6. Pour supprimer un instantané, effectuez un clic droit sur la vignette et cliquez sur Supprimer.
   Les fichiers d'image ne seront alors plus disponibles.
7. Pour renommer un instantané, effectuez un clic droit sur la vignette et cliquez sur Renommer.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



Explorer

- Modifier un instantané vidéo dans Security Center

2.2.15.1 | Personnalisation des options d'instantané dans Security Center

Avant de capturer des instantanés vidéo, vous pouvez choisir le format et l'emplacement des fichiers, et activer l'incrustation du nom de la caméra, de l'horodatage et du nom d'utilisateur sur l'image.

À savoir

- Les options Écrire le nom et l'horodatage de la caméra et Écrire le nom de l'utilisateur sont enregistrées avec votre profil utilisateur Security Center. Les autres réglages d'instantanés sont enregistrés en local avec votre profil d'utilisateur Windows.
  IMPORTANT : Les instantanés sont enregistrés dans le même dossier que les fichiers vidéo exportés. Si vous modifiez l'emplacement du dossier, vous ne pourrez plus afficher les vidéos et instantanés existants avec l'outil Coffre-fort.
- Le système peut ajouter des balises EXIF aux instantanés exportés au format JPEG. Les balises EXIF contiennent des informations comme le nom de la caméra, la date de création de l'instantané et les coordonnées de la caméra, ce qui peut être utile dans le cadre de l'analyse d'un incident. Les données EXIF sont uniquement disponibles si l'option Inclure des propriétés supplémentaires pour exportation/instantané est activée dans l'onglet Avancé pour un utilisateur dans Config Tool.

Procédure

1. Sur la page d'accueil de Security Desk, cliquez sur Options > Vidéo.
2. Dans la section Coffre-fort, configurez les options suivantes :

   Emplacement
   Le chemin Windows vers le dossier de stockage des fichiers vidéo et instantanés. Le chemin par défaut est : C:\Users\Username\AppData\Local\Genetec Security Center version #\Vault.

   Nettoyage automatique
   La période de rétention en jours des vidéos et des instantanés exportés dans le Coffre-fort. Lorsque cette option est désactivée, les vidéos et les instantanés exportés dans le coffre-fort ne sont jamais supprimés automatiquement.

3. Dans la section Instantanés, configurez les options suivantes :

   Format de fichier
   Formats pris en charge : BMP, JPG, PNG et GIF. Le format par défaut est PNG.

   Écrire le nom de la caméra et l'horodatage
   Pour indiquer la date, l'heure et le nom de la caméra sur l'instantané.

   Écrire le nom de l'utilisateur
   Le *Prénom* et le *Nom* de l'utilisateur sont imprimés sur l'instantané. Si l'utilisateur n'a pas de nom et prénom, son Nom d'utilisateur est imprimé sur l'image.

4. Cliquez sur Enregistrer.

Sujet parent : Capturer des instantanés vidéo

2.2.15.2 | Modifier un instantané vidéo dans Security Center

Pour garantir la confidentialité ou masquer des éléments d'un instantané vidéo, vous pouvez utiliser les outils d'édition dans l'éditeur d'image de l'instantané vidéo.

Avant de commencer

Capturez un instantané de l'image vidéo.

À savoir

- Les instantanés sont stockés dans le Coffre-fort.
- Tous les instantanés sont enregistrés selon la convention suivante : NomCaméra (Date Heure).png. Par défaut, les instantanés sont enregistrés au format PNG à l'emplacement suivant : C:\Users\Username\AppData\Local\Genetec Security Desk version#\Vault.

Procédure

1. Sur la page d'accueil, cliquez sur Outils > Coffre-fort.
2. Dans le Coffre-fort, ouvrez l'*Éditeur d'image* de la manière suivante :
   - Sélectionnez l'instantané et cliquez sur Modifier ().
   - Faites un clic droit sur l'instantané et cliquez sur Modifier.
3. Modifiez l'instantané à l'aide des outils suivants :
   - Faire pivoter l'image
   - Inverser l'image
   - Recadrer l'image ()
   - Ajuster la transparence ()
   - Ajuster la luminosité et le contraste ()
   - Masquer ou flouter des parties de l'image à l'aide de l'outil Masque ()
   - Agrandir ou réduire l'image en appuyant sur la touche `Ctrl` tout en utilisant la molette de la souris

     Une fois l'image agrandie, vous pouvez effectuer un panoramique et faire défiler l'image. Pour un panoramique, appuyez sur la touche `Ctrl` tout en faisant un cliquer-glisser avec la souris. Pour faire défiler l'image verticalement, utilisez la molette de la souris. Pour faire défiler l'image horizontalement, utilisez la molette de la souris tout en appuyant sur la touche `Maj`.
4. Cliquez sur Enregistrer sous et enregistrez l'instantané modifié.
   IMPORTANT : Si vous avez besoin de conserver l'instantané original, vous devez enregistrer l'instantané modifié sous un autre nom.

Sujet parent : Capturer des instantanés vidéo
Explorer

- Capturer des instantanés vidéo

2.2.15.3 | Afficher les données EXIF d'un instantané

Le format Exchangeable Image File (EXIF) intègre des informations complémentaires dans un fichier d'image, comme l'heure de la prise de vue. Ces informations complémentaires fournissent de la traçabilité qui peut servir aux autorités internes ou externes lors d'une enquête ou devant les tribunaux, si admissible.

Avant de commencer

Réglez les options d'instantané.

À savoir

- Tous les instantanés sont enregistrés selon la convention suivante : NomCaméra (Date Heure).png. Par défaut, les instantanés sont enregistrés au format PNG à l'emplacement suivant : C:\Users\Username\AppData\Local\Genetec Security Desk version#\Vault.
- Les données EXIF ne sont disponibles que si l'option Inclure des propriétés supplémentaires pour exportation/instantané est activée dans l'onglet Avancé d'un utilisateur dans Config Tool.
- Les données EXIF ne sont disponibles que pour les fichiers JPEG.
- Les données EXIF peuvent être modifiées. Vous savez qu'un fichier a été altéré si la Date de modification ne correspond plus à la Date de création.
- Des lecteurs EXIF tiers gratuits sont disponibles en ligne ou au téléchargement. Exemples de lecteurs EXIF : http://metapicz.com ou http://regex.info/exif.cgi.
- Le nom des balises EXIF varie selon les lecteurs. Par exemple, le nom de l'utilisateur ayant créé l'instantané apparaît sous Auteurs dans les Priorités Windows et sous Artiste sur metapicz.com.

Procédure

Pour afficher des informations supplémentaires sur un fichier dans Security Desk :

1. Ouvrez le Coffre-fort : sur la page d'accueil, cliquez sur Outils > Coffre-fort.
   Le Coffre-fort affiche des vignettes de tous les instantanés.
2. Faites un clic droit sur un fichier dans le Coffre-fort et sélectionnez Afficher les propriétés.

Pour afficher les données EXIF d'un instantané sous Microsoft Windows :

1. Dans l'Explorateur de fichiers, faites un clic droit sur une image, cliquez sur Propriétés, puis cliquez sur l'onglet Détails.
   Les données EXIF suivantes sont disponibles.

   Modèle de la caméra
   Le nom de la caméra d'où provient l'instantané vidéo.

   Date heure
   Date et heure d'exportation de l'instantané.

   Date
   Identique à Date heure.

   Hôte
   Le nom de l'ordinateur sur lequel l'instantané a été créé.

   Artiste
   Le nom de l'opérateur Security Desk ayant exporté l'instantané.

   Latitude/LatitudeRef
   La latitude de la caméra, qui peut servir à indiquer l'emplacement de la caméra sur une carte.

   Longitude/LongitudeRef
   La longitude de la caméra, qui peut servir à indiquer l'emplacement de la caméra sur une carte.

   Commentaires
   Informations complémentaires sur l'instantané, au format XML.

2. Cliquez sur la zone Commentaires pour afficher toutes les informations qui s'y trouvent.
   La liste suivante contient les balises XML et des données fictives.

   <G64xAuditMetadata>
   La balise XML qui indique le début des données de commentaire.

   <Version>1</Version>
   Numéro de version de l'image.

   <OperatorName>Admin</OperatorName>
   Le nom de l'opérateur Security Desk ayant exporté l'instantané. Dans cet exemple, il s'agit de l'utilisateur Admin.

   <WorkstationName>SecurityDesk</WorkstationName>
   Le nom de l'ordinateur sur lequel l'instantané a été créé.

   <ExportTime>18/10/2016 11:23:57 AM EDT</ExportTime>
   Date et heure d'exportation de l'instantané dans Security Desk.

   <Sequences>
   Balise XML qui indique le début des informations sur la caméra.

   <CameraName>Caméra de l'accueil</CameraName>
   Le nom de la caméra d'où provient l'instantané vidéo.

<StartTime>18/10/2016 11:23:56 AM EDT</StartTime>
Date et heure d'exportation de l'instantané.

<EndTime />
Ne s'applique qu'à la vidéo. Balise vide pour un instantané.

<CameraLocation>< Altitude>0</Altitude>< Latitude>85.051128779806589</Latitude>< Longitude>-180</Longitude></CameraLocation>
Les coordonnées géographiques de la caméra, qui peuvent servir à indiquer l'emplacement de la caméra sur une carte.

</Sequences>
Balise XML qui indique la fin des informations sur la caméra.

<Encryption>false</Encryption>
Indique si le chiffrement flux fusion était activé (true) ou désactivé (false) lorsque la caméra a capturé l'image vidéo. Le chiffrement assure la confidentialité de vos archives vidéo.

<MetadataType>Instantané</MetadataType>
Indique s'il s'agit d'un instantané ou d'une vidéo.

</G64xAuditMetadata>
Balise XML qui indique la fin des commentaires EXIF.

Sujet parent : Capturer des instantanés vidéo

2.2.16 | Blocage de caméra

Fonctionnalité Omnicast™ qui permet de restreindre l'affichage de la vidéo (en direct ou enregistrée) provenant de certaines caméras aux utilisateurs dotés d'un niveau utilisateur minimum.

Le blocage de caméras est conçu pour les installations qui offrent un accès grand public à de la vidéo en direct. Dans certains cas, les caméras risquent de diffuser du contenu qui n'est pas adapté à tous les publics. Vous pouvez dès lors empêcher les utilisateurs d'afficher un segment ou une vidéo entière en bloquant la caméra.

Fonctionnement

Le blocage de caméras est basé sur un attribut utilisateur appelé le niveau utilisateur. Le niveau utilisateur le plus élevé est 1 et le plus faible est 254. Lorsque vous bloquez une caméra, les utilisateurs dotés d'un niveau utilisateur inférieur au niveau que vous sélectionnez ne peuvent pas afficher la vidéo (en temps réel, enregistrée ou mise en cache), ni exporter de la vidéo pendant une durée que vous spécifiez.

Le blocage de caméras est soumis aux conditions suivantes :

- Un utilisateur ne peut que bloquer une caméra pour une personne dont le niveau utilisateur est inférieur au sien. Cela signifie que les utilisateurs avec un niveau utilisateur de 254 ne peuvent bloquer personne et que les utilisateurs avec un niveau utilisateur égal à 1 ne peuvent être bloqués par personne.
- Un utilisateur dont le niveau utilisateur est supérieur au niveau de blocage d'une caméra peut visionner la caméra.
- Un utilisateur peut débloquer ou modifier le niveau de blocage d'une caméra si son niveau utilisateur est supérieur ou égal à l'utilisateur ayant bloqué la caméra.
- Si plusieurs réglages de blocage sont appliqués à une caméra, le niveau utilisateur le plus élevé ayant été spécifié correspond au niveau de blocage actif.

Vous bloquez une caméra de 13 h à 16 h et réglez le niveau utilisateur sur 20. Un autre utilisateur bloque la caméra de 15 h à 17 h et règle le niveau utilisateur sur 100. Entre 15 h et 17 h, le niveau de blocage est réglé sur 100.

Explorer

- Bloquer l'affichage vidéo par les utilisateurs

2.2.17 | Bloquer l'affichage vidéo par les utilisateurs

En cas d'événement critique durant la capture vidéo qui ne doit pas être accessible par certains utilisateurs, vous pouvez empêcher les utilisateurs d'afficher un segment ou une vidéo entière en bloquant la caméra.

Avant de commencer

Procédez de la manière suivante :

- Vérifiez que vous disposez du privilège d'utilisateur *Bloquer et débloquer la vidéo*.
- Vérifiez que la caméra que vous souhaitez bloquer ne provient pas d'un système Omnicast™ fédéré.

À savoir

Vous pouvez bloquer une caméra qui affiche de la vidéo en direct ou enregistrée dans une tuile depuis toute tâche Security Desk. Par exemple, vous pouvez bloquer une caméra qui affiche de la vidéo en direct depuis la tâche *Surveillance*, ou bloquer de la vidéo enregistrée dans une archive vidéo depuis la tâche *Archives*. Les utilisateurs dotés d'un niveau utilisateur inférieur au niveau que vous sélectionnez ne peuvent pas afficher la vidéo (en direct, enregistrée ou mise en cache), ni exporter de la vidéo pendant une durée que vous spécifiez. La mention **Bloqué** est affichée dans la tuile s'ils tentent d'afficher une caméra durant la plage horaire de blocage.

REMARQUE : Dans la tâche *État du système*, vous pouvez bloquer et débloquer les caméras, et afficher l'état de blocage des caméras.

Procédure

1. Sélectionnez une caméra affichée dans une tuile.
2. Faites un clic droit dans la tuile et cliquez sur Caméra > Bloquer ().
3. Dans l'option Début, sélectionnez la date et l'heure de démarrage du blocage de la vidéo.
4. Dans l'option Fin, sélectionnez la durée de vidéo à bloquer :

   Jusqu'au
   La vidéo est bloquée jusqu'à la date et l'heure spécifiées.

   Pour
   La vidéo est bloquée pendant la durée spécifiée (jours, heures, minutes ou secondes).

   Indéfiniment
   Toutes les vidéos à compter de la valeur de Début (dont les nouveaux enregistrements) sont bloquées tant que vous ne débloquez pas manuellement la caméra.

5. Sélectionnez un niveau utilisateur minimum avec le curseur Niveau utilisateur.

   L'affichage de la vidéo est bloqué pour tous les utilisateurs dont le niveau est inférieur au niveau sélectionné. Le niveau utilisateur le plus élevé est 1 et le plus faible est 254.

6. Cliquez sur OK.

   La caméra est bloquée pour les utilisateurs dont le niveau utilisateur est inférieur au niveau que vous avez sélectionné. Les utilisateurs dont le niveau utilisateur est supérieur ou égal peuvent voir que la caméra est bloquée, car des traits horizontaux sont affichés dans la frise chronologique de la caméra.

7. Pour débloquer la caméra, effectuez un clic droit dans la tuile, puis cliquez sur Caméra > Débloquer ().

Explorer

- Commandes du menu de tuile
- Blocage de caméra
- Surveiller l'état de votre système Security Center

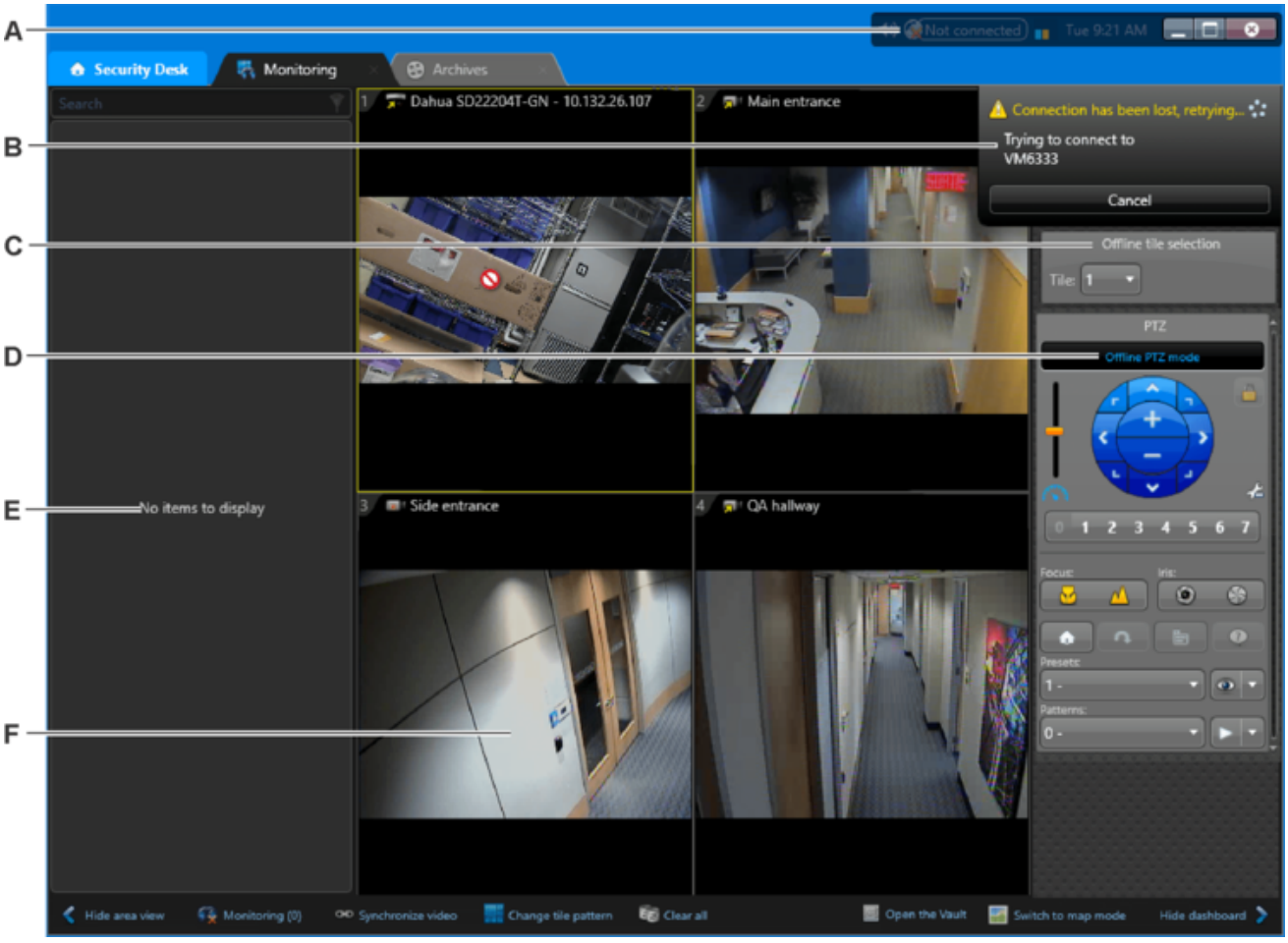
2.2.18 | Affichage de la vidéo en cas de déconnexion du rôle Répertoire

Le rôle Security Center *Répertoire* gère l'intégralité du système. Sans lui, vous ne pouvez pas vous connecter au système. Si le rôle Répertoire est déconnecté du reste du système, Security Desk fonctionne en mode dégradé.

Si vous visionnez une caméra, vous restez connecté à son flux en temps réel, même si vous êtes déconnecté du système. Vous pouvez également visionner de la vidéo enregistrée si la vidéo en temps réel a été mise en cache sur votre poste de travail. La vidéo mise en cache est indiquée par la barre orange au sommet de la frise chronologique.

La vidéo n'a pas été mise en cache La vidéo a été mise en cache

Security Desk essaie de se reconnecter au Répertoire. Une fois reconnecté, le mode de fonctionnement normal est rétabli. Quand Security Desk est hors ligne, vous pouvez toujours contrôler vos caméras PTZ à l'aide des widgets affichés dans le tableau de bord. La figure suivante illustre le mode dégradé en cas de défaillance du Répertoire.



A	L'icône d'état de la connexion indique que la connexion est perdue.
B	Un message contextuel indique que le Security Desk tente de se reconnecter
C	Utilisez le widget Tuile pour sélectionner la caméra PTZ que vous souhaitez contrôler.
D	Les commandes PTZ intégrées à la tuile ne fonctionnent pas. Vous devez utiliser le widget PTZ, avec les limitations suivantes :

	• Vous ne pouvez pas expressément verrouiller le PTZ, et vous ne pouvez pas non plus voir qui détient le verrou. • Vous ne pouvez ni modifier ni afficher le nom des préréglages et parcours PTZ. • Les commandes spécifiques ne fonctionnent pas. • Le zoom numérique n'est pas disponible. S'il est activé, vous devez le désactiver avant d'utiliser le zoom PTZ.
E	La vue secteur est indisponible.
F	Les caméras déjà affichées restent connectées.

2.2.18.1 | Activer le mode PTZ hors ligne sur un poste Security Desk

Pour permettre aux opérateurs de contrôler les caméras PTZ lorsque Security Desk est hors ligne (déconnecté du Répertoire), vous pouvez activer le mode PTZ hors ligne.

Procédure

1. Sur l'ordinateur qui exécute Security Desk, ouvrez le fichier App.SecurityDesk.config situé dans le dossier ConfigurationFiles du dossier d'installation de Security Center (par défaut C:\Program Files (x86)\Genetec Security Center 5.9\ sur un poste 64 bits).
2. Ajoutez le sous-élément suivant à l'élément `<configuration/>`.

   ```
   <?xml version="1.0" encoding="utf-8"?>
   <configuration>
      ...
      <Ptz DisableThrottling="False" ThrottlingDelay="75" AllowOfflineMode="True"/>
      ...
   </configuration>
   ```

   Si le sous-élément `<Ptz/>` existe déjà, ajoutez seulement l'attribut `AllowOfflineMode`.

   REMARQUE : La syntaxe est sensible à la casse.
3. Enregistrez les modifications et redémarrez Security Desk.

Sujet parent : Affichage de la vidéo en cas de déconnexion du rôle Répertoire

2.2.19 | Afficher les réglages de caméras

Vous pouvez afficher la liste de toutes les caméras Security Center locales et fédérées ainsi que leurs réglages qui font partie de votre système à l'aide du rapport Configuration des caméras.

À savoir

Le rapport Configuration des caméras est utile pour comparer les réglages de caméras et vérifier que vos caméras sont correctement configurées. Si la caméra est configurée pour plusieurs flux vidéo ou plusieurs horaires de streaming, chaque flux et chaque horaire est affiché en tant qu'élément distinct.
REMARQUE : Ce rapport ne prend pas en charge les caméras Omnicast™ fédérées.

Procédure

1. Ouvrez la tâche Configuration des caméras.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Caméras
   Sélectionnez la caméra à examiner.

Champs personnalisés
Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

3. Cliquez sur Générer le rapport.
   Les réglages de caméra suivants sont affichés dans le volet de rapport :

Caméra
Nom de la caméra.

Propriétaire
Archiveur qui gère la caméra.

Résolution
Résolution du flux vidéo de la caméra.

Qualité de l'image
Réglage de qualité de l'image de la caméra.

Images par seconde
Réglage de vitesse en images par seconde de la caméra.

Utilisation des flux
Utilisation du flux vidéo (vidéo en direct, enregistrement, et ainsi de suite).

Paramètre réseau
Type de connexion utilisé par la caméra.

Débit binaire
Réglage de débit binaire de la caméra.

Flux
Le flux vidéo de la caméra.

Intervalle d'image clé
Réglage d'intervalle d'image clé de la caméra.

Mode d’enregistrement
Réglages d'enregistrement de la caméra.

Type
Type de caméra (fixe ou PTZ).

Horaire de streaming
Horaire de diffusion vidéo de la caméra.

Fabricant
Fabricant de l'unité.

Type de produit
Modèle ou gamme de l'unité vidéo.

Chemin du secteur
Liste de tous les secteurs parents, en partant de l'entité système. Lorsque la caméra a plusieurs secteurs parents, le chemin est représenté par « *\ ».

Description
Description de l'entité.

Transfert sur périphérique
Indique si la caméra est configurée pour le transfert sur périphérique (oui ou non).

Version du micrologiciel
Version du micrologiciel de la caméra.

Adresse IP
Adresse IP de la caméra.

ID logique
ID logique de la caméra.

Adresse de multidiffusion
Adresse de multidiffusion de la caméra.

Port de multidiffusion
Port de connexion de l'unité vidéo.

Période de rétention
Période de rétention de la caméra.

4. Pour modifier les réglages d'une caméra, faites un clic droit sur un élément du volet de rapport, puis cliquez sur Configurer () pour basculer vers la page de configuration de l'entité dans Config Tool.
   REMARQUE : Vous devez disposer du privilège d'utilisateur de modification d'entités pour utiliser cette commande.

2.2.20 | Enregistrer de la vidéo manuellement sur un Archiveur auxiliaire

Avec les caméras locales et fédérées contrôlées par un Archiveur auxiliaire, vous pouvez démarrer manuellement l'enregistrement vidéo sur l'Archiveur auxiliaire depuis Security Desk lorsque vous observez un incident.

Avant de commencer

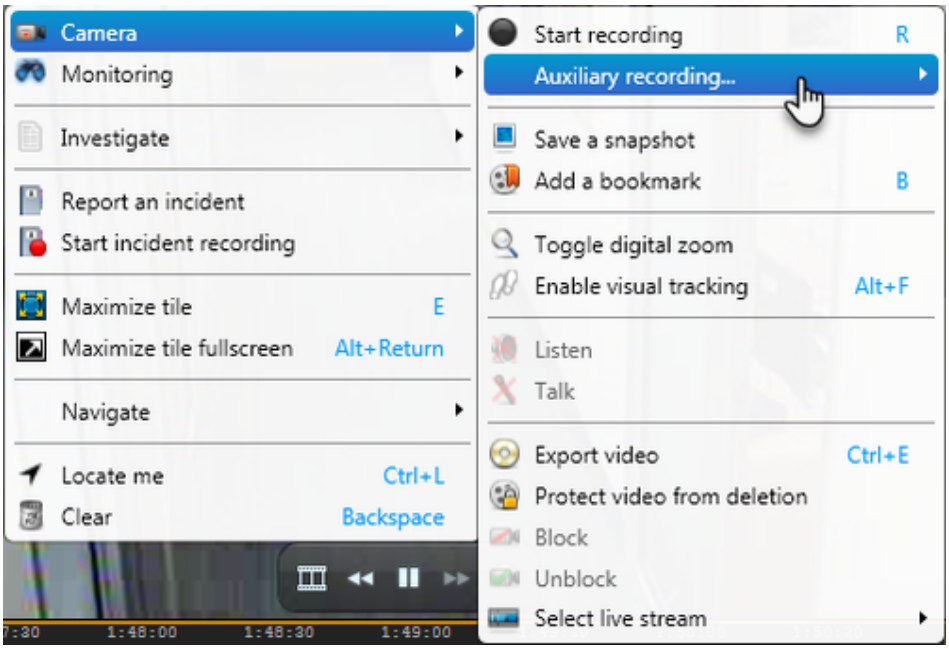
Vérifiez que la caméra est contrôlée par un Archiveur auxiliaire, et réglez le mode d'enregistrement de l'Archiveur auxiliaire sur *manuel*.

Procédure

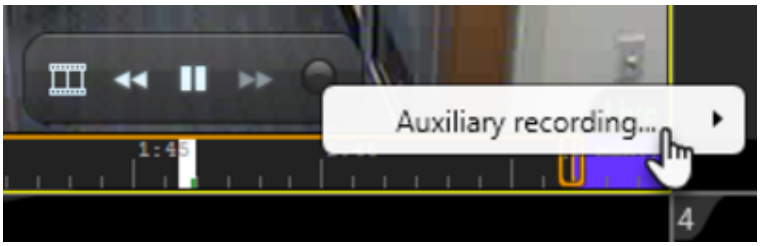
1. Sélectionnez une caméra affichée dans une tuile.
2. Procédez de l'une des manières suivantes :

- Effectuez un clic droit dans la tuile pour afficher le menu contextuel de la tuile, puis cliquez sur Caméra > Enregistrement auxiliaire.

  Vous pouvez également appuyer sur `Maj+F10` pour afficher le menu contextuel. Appuyez ensuite sur la touche `Tab` jusqu'à ce que l'option Caméra soit sélectionnée et appuyez sur `Entrée`, puis appuyez sur la touche `Tab` jusqu'à ce que l'option Enregistrement auxiliaire soit sélectionnée, puis appuyez sur `Entrée`.

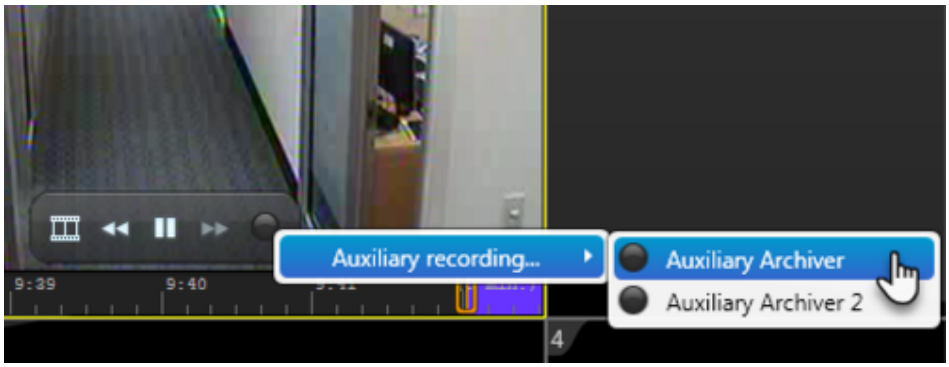


- Faites un clic droit sur l'icône de l'état d'enregistrement dans la tuile, puis cliquez sur Enregistrement auxiliaire.



- Faites un clic droit sur le bouton d'état d'enregistrement dans le widget Caméra, puis cliquez sur Enregistrement auxiliaire.

3. Cliquez sur le bouton enregistrer ( ) en regard du nom du rôle Archiveur auxiliaire.
   Si la caméra est associée à plusieurs rôles Archiveur auxiliaire, sélectionnez l'Archiveur auxiliaire qui doit enregistrer.



Résultats

L'enregistrement vidéo démarre sur l'Archiveur auxiliaire que vous avez sélectionné, et il est stocké dans la base de données de l'Archiveur auxiliaire.

2.2.21 | Optimiser les performances de décodage vidéo sur votre ordinateur

Security Desk peut détecter et exploiter les équipements compatibles pour accélérer le décodage vidéo. L'accélération matérielle améliore les performances, surtout lorsque vous visionnez plusieurs flux H.264 haute définition.

À savoir

Pour en savoir plus sur les cartes vidéo recommandées et les tests de performances, voir Security Center 5.9 Configuration requise pour les postes client.
REMARQUE : Security Desk ne prend pas en charge l'accélération matérielle sous Windows XP.

Procédure

1. Les conditions suivantes sont requises pour optimiser le fonctionnement avec les cartes vidéo NVIDIA :
   - La carte vidéo est un modèle pris en charge.
   - Le moniteur ou projecteur utilisé pour afficher la vidéo est branché sur cette carte vidéo.
   - Le dernier pilote fourni par NVIDIA sur son site est installé.
2. Les conditions suivantes sont requises pour optimiser le fonctionnement avec les cartes vidéo Intel Quick Sync :
   - Le processeur est compatible Quick Sync (voir http://ark.intel.com pour confirmer).
   - La carte vidéo intégrée au processeur est un modèle pris en charge.
   - Un moniteur est branché sur la sortie intégrée de la carte mère.
   - Les graphismes intégrés Intel sont activés dans le BIOS.
   - Le dernier pilote fourni par Intel sur son site est installé.

   REMARQUE : Sur les ordinateurs hautes performances, le décodage par le processeur graphique NVIDIA fonctionne mieux lorsque Quick Sync est désactivé.
3. Pour dépanner les problèmes lors de l'utilisation de plusieurs écrans et processeurs graphiques :
   - Si le mode SLI (Scalable Link Interface) est disponible, désactivez-le.
   - Si vous avez plusieurs cartes vidéo NVIDIA, connectez chaque moniteur à une carte distincte pour les utiliser en parallèle.
   - Si vous avez des cartes vidéo qui utilisent différents pilotes (AMD, NVIDIA, Intel), configurez un moniteur relié à une carte NVIDIA en tant que moniteur principal.
   - Si vous avez des cartes vidéo distinctes et intégrées et si votre carte vidéo NVIDIA est conforme à la configuration requise, désactivez les graphismes intégrés dans le BIOS. L'exploitation des graphismes intégrés diminue les performances de la carte vidéo distincte.
   - Après l'installation de Security Center sur les portables équipés de la technologie NVIDIA OPTIMUS (cartes graphiques Intel et NVIDIA combinées), vous devez lancer chaque application exigeante en matière de vidéo (Security Desk, Genetec™ Video Player, et ainsi de suite) afin de les s'inscrire en tant qu'applications qui exigent le processeur graphique NVIDIA. Après cette première configuration, l'application utilise systématiquement le processeur graphique NVIDIA.

2.3 | Archives vidéo dans Security Desk

2.3.1 | Modes vidéo en temps réel et enregistrée

Lorsque vous affichez une caméra sur le canevas, vous pouvez basculer entre les modes vidéo *en direct* et *enregistrée* depuis la frise chronologique ou le widget Caméra dans le volet Commandes.

Utilisez le widget Caméra pour mettre en pause ou rembobiner la vidéo ou revoir instantanément un passage. Lorsque vous avez fini de visionner la reprise instantanée, vous pouvez rebasculer vers la vidéo en temps réel. Lorsqu'une caméra est affichée, le mode vidéo actuel est indiqué dans le coin inférieur droit de la tuile.

Lorsque vous visionnez de la vidéo en direct, l'état actuel de l'enregistrement de la caméra est également indiqué :

- Vert avec un point rouge (

) - La caméra enregistre.
- Vert (

) - La caméra n'enregistre pas.

Lorsque vous affichez de la vidéo enregistrée, la date et l'heure de l'enregistrement sont indiquées, en mode absolu ou relatif. Cliquez sur l'horodatage pour basculer entre ces deux modes d'affichage.

- 

Horodatage incrusté en mode *relatif*.
- 

Horodatage incrusté en mode *absolu*.

Choix du mode vidéo par défaut

Si vous choisissez de visionner une autre caméra sur le canevas, le mode vidéo par défaut est hérité de celui de la tuile actuellement sélectionnée. Par exemple, si la tuile sélectionnée affiche de la vidéo enregistrée, la caméra que vous ajoutez à une autre tuile affiche également de la vidéo enregistrée.

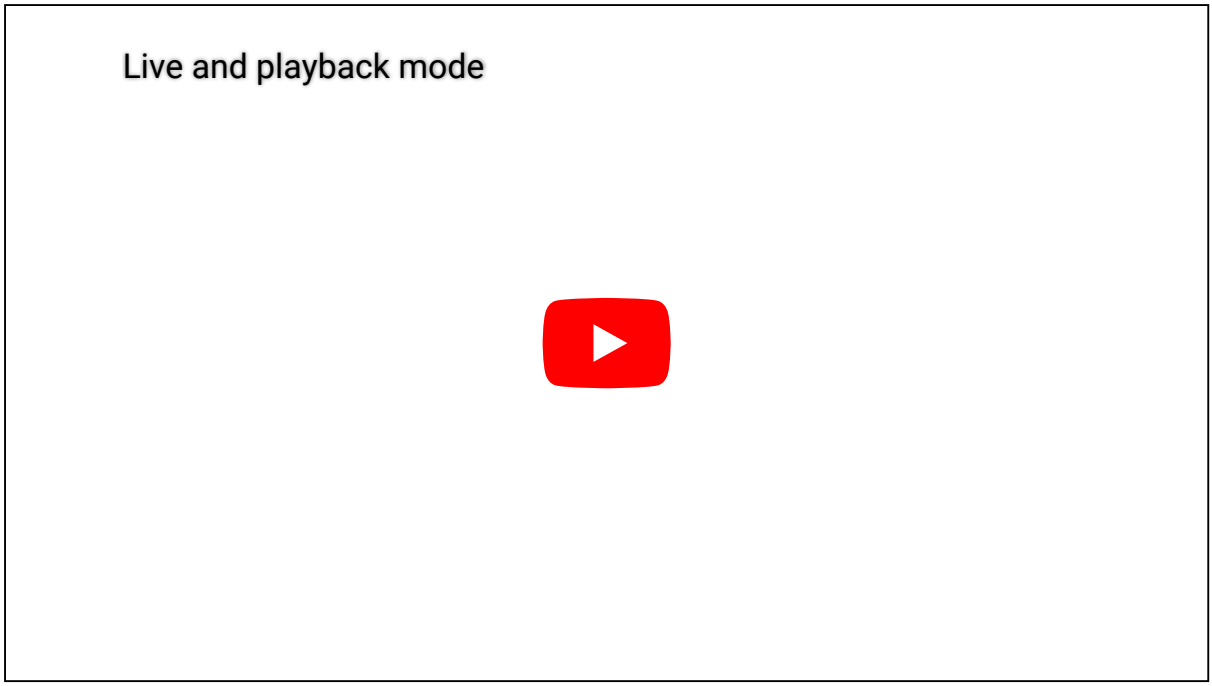
Si la tuile sélectionnée n'affiche pas actuellement de caméra, le mode vidéo hérité dépend du type de tâche. Pour une tâche de type *Surveillance*, le mode vidéo par défaut est Vidéo en direct. Le mode vidéo utilisé par défaut pour les tâches d'investigation est Vidéo enregistrée.

États de l'exportation vidéo

Lorsque vous visionnez de la vidéo enregistrée, une zone bleue apparaît en incrustation dans le coin inférieur gauche de l'image dès lors que l'état est autre que la lecture normale à vitesse x1. Dans la figure suivante, la vidéo est rembobinée à 10 fois la vitesse normale.

États de lecture	
	Pause
	Ralenti
	Avance rapide (2x, 4x, 6x, 8x, 10x, 20x, 40x ou 100x)
	Lecture arrière (-2x, -4x, -6x, -8x, -10x, -20x, -40x ou -100x)

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



Explorer

- Basculer entre les modes vidéo

2.3.2 | Basculer entre les modes vidéo

Vous pouvez basculer entre les modes vidéo *en direct* et *enregistrée* depuis la frise chronologique ou le widget Caméra du volet Commandes.

À savoir

Si la caméra n'enregistre pas actuellement (indiqué par le bouton vert ), c'est peut-être que l'Archiveur est indisponible. Toutefois, même si la caméra n'enregistre pas sur l'Archiveur, la barre orange en haut de la frise chronologique indique que la vidéo a été mise en mémoire tampon sur votre disque dur en local. Vous pouvez lire la vidéo mise en mémoire tampon en local.

Procédure

1. Basculez vers le mode vidéo *enregistrée* de l'une des manières suivantes :

- Dans la frise chronologique, cliquez sur la tête de lecture et faites-la glisser vers la gauche.
  CONSEIL : Pour modifier l'échelle de la frise chronologique, utilisez la molette de la souris en survolant la frise.
- Pour lancer la lecture arrière, cliquez sur Rembobiner ( ) dans le widget Caméra.

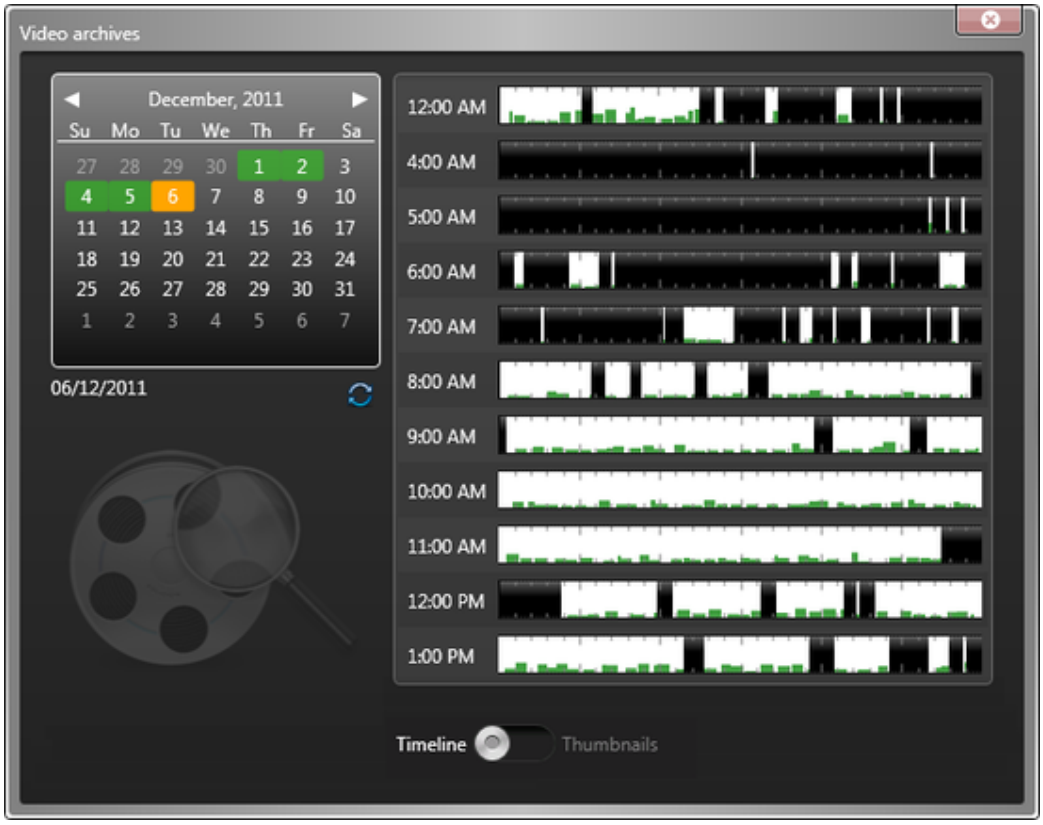
  Cliquez plusieurs fois pour régler la vitesse de -1 à -100x.

- Pour effectuer un saut arrière de 15 secondes, cliquez sur Saut arrière ( ) dans le widget Caméra.

  La valeur par défaut est de 15 secondes. Vous pouvez la modifier dans la boîte de dialogue Options.

- Pour atteindre une heure spécifique de la vidéo, procédez comme suit :
  a. Dans le widget Caméra, cliquez sur Aller à l'heure spécifique ( ).
  b. Dans la boîte de dialogue Archives vidéo, utilisez le calendrier pour parcourir les mois et les années et sélectionner une date.

     Les heures de la journée dotées d'archives vidéo sont indiquées par un arrière-plan blanc dans la frise chronologique.



  c. (Facultatif) Basculez entre les vues Frise chronologique et Vignettes.
  d. Cliquez sur un endroit de la frise chronologique pour basculer vers l'endroit correspondant de l'enregistrement vidéo.

2. Basculez vers le mode vidéo *en direct* de l'une des manières suivantes :
   - Dans les commandes vidéo de la tuile, cliquez sur Caméra > Basculer vers le direct ( ).
   - Dans le widget Caméra, cliquez sur Basculer vers le direct ( ).

Explorer

- Modes vidéo en temps réel et enregistrée
- Options vidéo dans Security Desk

2.3.3 | À propos de la frise chronologique

La frise chronologique apparaît en dessous de l'image vidéo dans les tuiles du canevas.

La frise chronologique permet d'effectuer les tâches suivantes :

- Déplacer la fenêtre de frise chronologique vers la gauche ou vers la droite en cliquant sur la frise et en la faisant glisser latéralement.
- Réduire ou élargir la frise chronologique en la survolant avec la souris, puis en actionnant la molette de la souris.

A	Un fond blanc indique la présence d'un enregistrement.
B	Un fond noir indique l'absence d'enregistrement durant cette plage.
C	Barres de mouvement vertes. La taille de la barre correspond à la quantité de mouvement.
D	L'icône avec le ruban orange indique la présence d'un signet. Survolez le signet pour afficher le texte et l'horodatage associés.
E	La barre orange au sommet de la frise chronologique indique que la vidéo a été mise en cache sur le disque dur de votre poste de travail.
F	Curseur de lecture. Faites glisser le curseur pour lire une autre section de la frise chronologique.
G	Marque d'horodatage. Cliquez pour basculer entre l'heure relative et absolue.
H	Durée/échelle de la frise chronologique. Survolez la frise chronologique avec la souris, et utilisez la molette de la souris pour modifier l'échelle.
I	Le fond violet indique « le futur ».

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

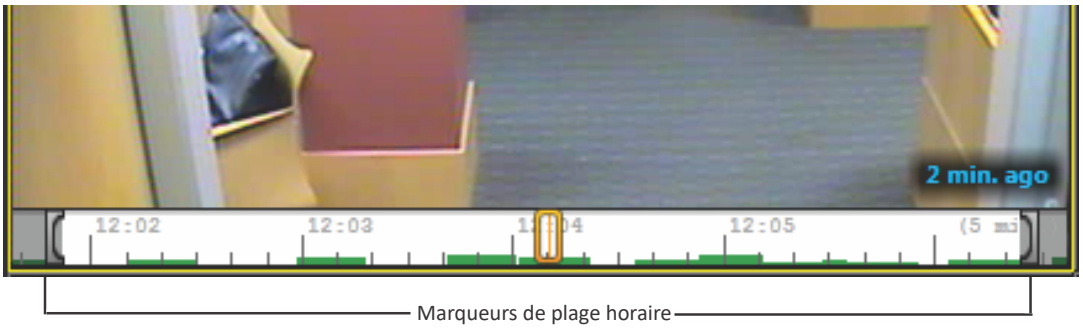
2.3.4 | Créer une boucle de lecture

Pour lire une séquence de vidéo de manière répétée, vous pouvez définir une boucle de lecture dans la frise chronologique vidéo.

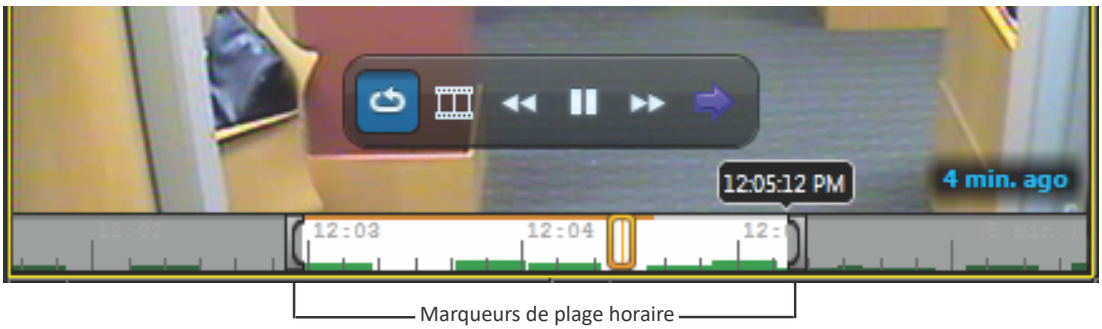
Procédure

1. Procédez de l'une des manières suivantes :
   - Dans le widget Caméra, cliquez sur Lecture en boucle ( ).
   - Faites un clic droit dans la frise chronologique.

   Un marqueur de plage horaire apparaît à chaque extrémité de la frise chronologique.



2. Faites glisser les marqueurs aux emplacements souhaités. Lorsque vous déplacez un marqueur avec la souris, la valeur temporaire précise est affichée.



   La lecture en boucle démarre instantanément. Toutes les commandes de lecture sont disponibles durant la lecture en boucle.
3. Pour annuler la lecture en boucle, cliquez sur Lecture en boucle ( ) dans les commandes vidéo de la tuile ou dans le widget Caméra.

2.3.5 | Effectuer des recherches vidéo ciblées

Si une caméra a enregistré un événement et si vous savez où l'événement est situé dans le champ de vision de la caméra, comme dans le cas d'un sac ôté d'une table, vous pouvez utiliser la *Recherche rapide* dans la vidéo enregistrée pour retrouver la séquence vidéo particulière qui contient la preuve.

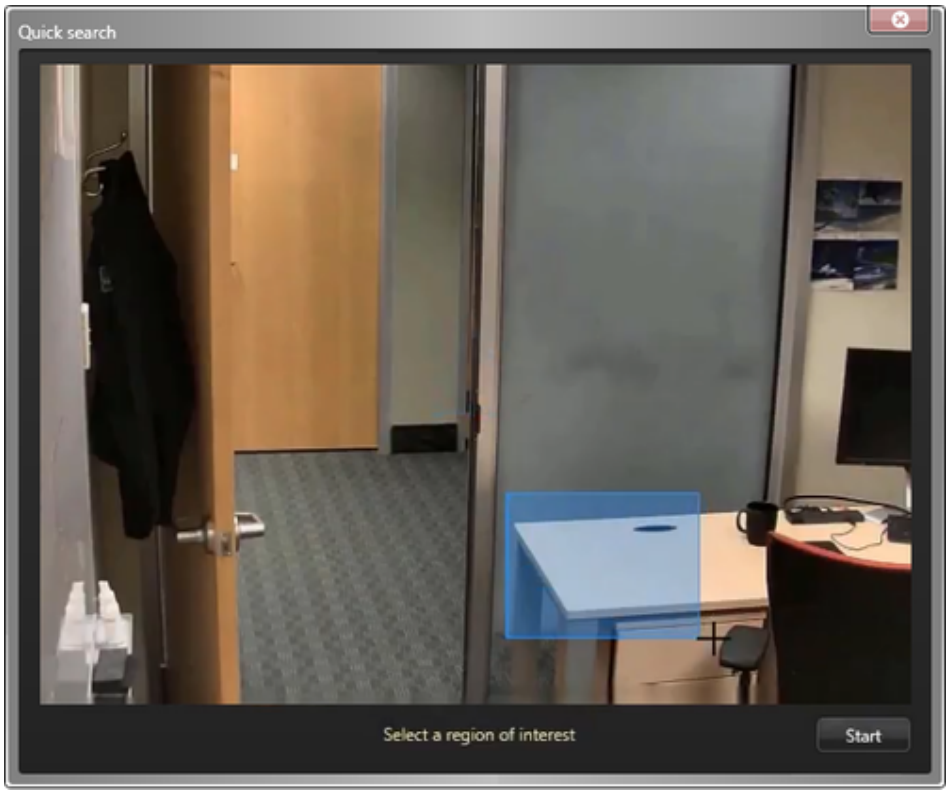
À savoir

L'option *Recherche rapide* prend uniquement en charge la vidéo enregistrée.

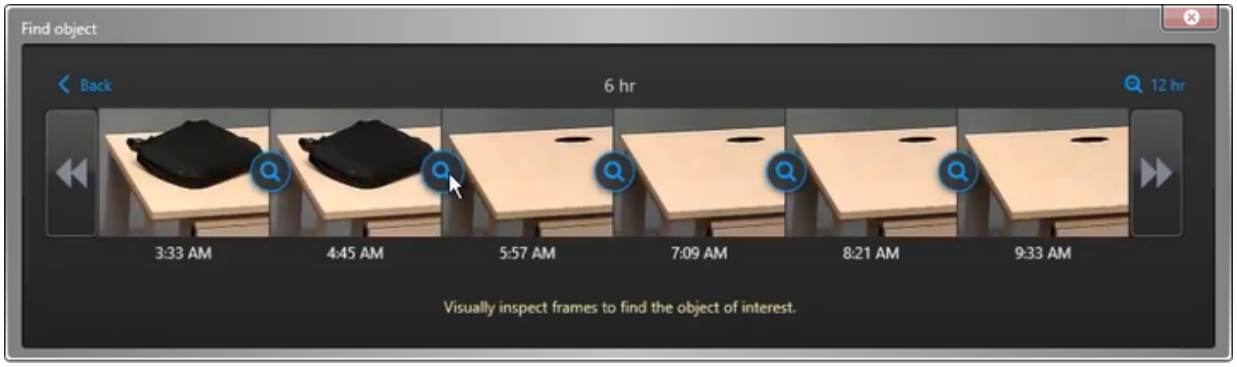
Procédure

1. Sur la page d'accueil, ouvrez la tâche Surveillance.
2. Dans la vue secteur, faites glisser la caméra qui vous intéresse dans une tuile.

3. Dans le widget Caméra, cliquez sur Recherche rapide ( ).
   La caméra sélectionnée est affichée dans la boîte de dialogue Recherche rapide.
4. Tracez un rectangle autour de la zone dans laquelle vous voulez effectuer la recherche.
   Par exemple, si vous tentez de savoir qui a retiré un objet d'une table, entourez la partie de la table où l'objet était présent.



5. Cliquez sur Démarrer.
   Un aperçu des six dernières heures d'enregistrements vidéo est affiché sous forme de vignettes représentant la partie sélectionnée.



6. Inspectez les vignettes et cliquez sur le bouton entre les deux images correspondant au moment où l'objet a été retiré.
7. Si aucune image ne correspond au moment recherché, cliquez sur ou pour avancer ou reculer dans la frise chronologique.
8. Poursuivez la recherche jusqu'à ce que vous repériez le moment précis de l'événement.
9. Lorsque vous l'avez repéré, cliquez sur l'image correspondante pour lancer la lecture à partir de ce moment.

10. (Facultatif) Exportez la séquence vidéo en tant que preuve.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

2.3.6 | Afficher des archives vidéo

Le rapport Archives vous permet de rechercher et de visionner les archives vidéo sur votre système par caméra et plage de temps.

À savoir

Si un événement de sécurité important se produit, vous pouvez effectuer les opérations suivantes dans le rapport Archives :

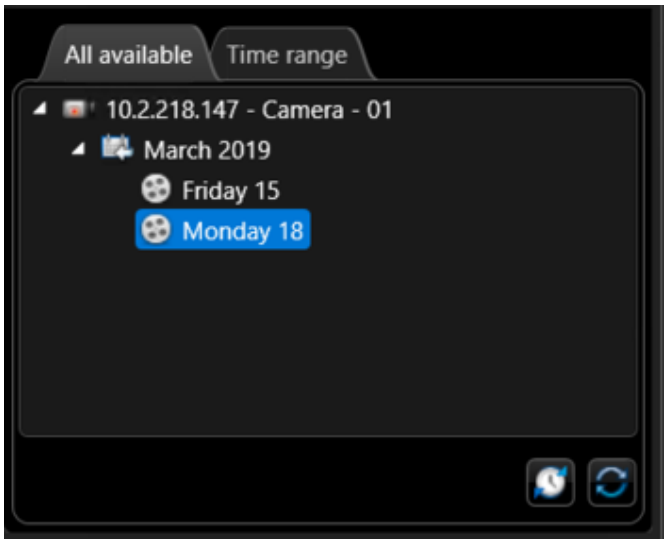
- Recherchez des *archives vidéo* disponibles pour une plage de temps ou une caméra donnée à une date spécifiée.
- Recherchez des archives vidéo pour examiner un enregistrement vidéo.
- Exportez un enregistrement vidéo pour le partager avec vos collègues ou les forces de l'ordre.

Procédure

1. Sur la page d'accueil de Security Desk, ouvrez la tâche Archives.
2. Cliquez sur l'onglet Filtres et sélectionnez les caméras que vous souhaitez examiner.

3. Recherchez des archives vidéo par date ou plage horaire :
   - Pour rechercher des archives vidéo par date :
     a. Cliquez sur l'onglet Toutes les archives, puis sélectionnez les caméras qui vous intéressent.

        Tous les jours qui comportent des archives vidéo pour les caméras sélectionnées sont affichés par mois et par jour.

     b. Pour afficher la plage horaire pour chaque jour comprenant des archives vidéo, cliquez sur .
     c. Sélectionnez une date.
   - Pour rechercher des archives par plage horaire :
     a. Clique sur le filtre Caméras et sélectionnez les caméras à examiner.
     b. Cliquez sur l'onglet Plage horaire et sélectionnez la plage horaire.
4. Cliquez sur Générer le rapport.
   Les enregistrements vidéo associés sont répertoriés dans le volet de rapport :
   - Si vous avez recherché par date, le rapport affiche les heures du jour sélectionné qui contiennent de la vidéo.
   - Si vous avez effectué une recherche par plage horaire, seules les caméras comportant des archives vidéo sont affichées, et l'en-tête de colonne *Aperçu* est remplacé par un curseur chronologique.
     REMARQUE : Si les résultats du rapport comprennent des caméras dans différents fuseaux horaires et que votre système affiche l'heure en fonction du fuseau horaire de chaque appareil, le curseur chronologique est masqué.

   La colonne *Aperçu* indique les plages vidéo disponibles au sein de la séquence de chaque caméra. Vous pouvez placer le curseur de la souris sur cette chronologie pour afficher des horodatages spécifiques.

5. Pour afficher la séquence vidéo dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser vers le canevas.
   La lecture de la séquence sélectionnée débute.
   REMARQUE : Si vous recevez un message indiquant `Aucune vidéo disponible pour l'instant`, vérifiez que vous disposez des éléments suivants :
   - Un certificat valide si le flux vidéo est chiffré.
   - Le privilège requis pour afficher cette caméra spécifique. Il se peut que la caméra soit bloquée et qu'un privilège spécifique soit nécessaire pour afficher les archives associées.
6. Pour contrôler l'enregistrement vidéo, utilisez le widget Caméra.
7. Pour exporter une archive vidéo importante, sélectionnez l'élément souhaité dans le volet de rapport, puis cliquez sur Exporter ( ).

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l’icône Sous-titres (CC) pour activer les sous-titres dans l’une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s’affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Exporter de la vidéo
- Exporter un rapport
- Widget Caméra
- Présentation de la tâche Archives

2.3.6.1 | Colonnes du volet de rapport pour la tâche Archives

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Caméra
Nom de la caméra.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Heure de début
Début de la plage horaire, séquence d'enregistrement ou séquence vidéo.

Heure de fin
Fin de la plage horaire, séquence d'enregistrement ou séquence vidéo.

Aperçu
Frise chronologique qui indique la présence de données vidéo dans la plage horaire sélectionnée.

Vignettes
Images miniatures de la vidéo enregistrée durant la plage horaire sélectionnée. Les vignettes n'apparaissent que pour les vidéos enregistrées par un Archiveur ou Archiveur auxiliaire, pas pour les vidéos enregistrées sur périphérique.

Sujet parent : Afficher des archives vidéo

2.3.7 | Afficher les statistiques d'Archiveur

Vous pouvez afficher les statistiques de fonctionnement de tous les rôles d'archivage (Archiveur et Archiveur auxiliaire) de votre système à l'aide du rapport Statistiques de l'Archiveur.

À savoir

Vous pouvez afficher des détails supplémentaires sur chaque rôle d'archivage, comme l'utilisation moyenne des disques par jour, les statistiques sur les fichiers vidéo protégés et sur chaque caméra individuelle en ouvrant la page Ressources du rôle d'archivage dans Config Tool, puis en cliquant sur Statistiques ( ).

Procédure

1. Sur la page d'accueil, ouvrez la tâche Statistiques de l'Archiveur.
2. Dans le filtre Archiveur, sélectionnez les rôles d'archivage que vous souhaitez examiner.
3. Cliquez sur Générer le rapport.
   Les statistiques de fonctionnement des rôles d'archivage sélectionnés sont affichées dans le volet de rapport.

Explorer

- Présentation de la tâche État du système

2.3.7.1 | Colonnes du volet de rapport dans la tâche Statistiques de l'Archiveur

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Entité
Nom de l'entité.

Serveur
Nom du serveur qui héberge ce rôle.

Caméras actives
Nombre de caméras détectées par l'Archiveur.

Caméras d'archivage
Nombre de caméras sur lesquelles l'archivage est activé (En continu, Sur mouvement ou Manuel) et qui ne présentent pas de problèmes d'archivage.

Afficher les détails : Affichez l'*état d'enregistrement* et les statistiques de chaque caméra dans la boîte de dialogue Caméras d'archivage. Les statistiques proviennent de la dernière actualisation de la boîte de dialogue Statistiques. Ce rapport permet de voir si chaque codeur diffuse actuellement des flux vidéo (et audio) et si l'Archiveur enregistre actuellement ces données.

Nombre total de caméras
Nombre de caméras affectées à ce rôle.

Espace utilisé
Quantité d'espace utilisé par les archives vidéo.

Espace libre
Espace libre sur le disque.

Espace disponible
Espace disque disponible pour les archives vidéo (égal à *Espace libre sur le disque* moins *Espace libre min.*).

Pourcentage de charge
Pourcentage d'espace utilisé sur le disque comparé à l'espace alloué.

Débit de réception de l'Archiveur
Débit de réception des données par l'Archiveur.

Débit d'écriture de l'Archiveur
Débit d'écriture sur le disque par l'Archiveur.

Estimation de la durée d'enregistrement
Estimation de la durée d'enregistrement restante en jours, heures et minutes calculée en fonction du taux moyen d'utilisation des disques et la charge actuelle.

Trafic réseau entrant
Débit binaire du trafic réseau entrant sur cet ordinateur.

Trafic réseau sortant
Débit binaire du trafic réseau sortant sur cet ordinateur.

Étendue de l'archivage
Plage horaire couverte par les archives vidéo.
Sujet parent : Afficher les statistiques d'Archiveur

2.3.8 | Analyser les événements d'Archiveur

Vous pouvez rechercher les événements relatifs aux rôles d'archivage (Archiveur et Archiveur auxiliaire) à l'aide du rapport Événements d'Archiveur.

À savoir

Vous pouvez vérifier l'état d'un Archiveur en le sélectionnant, en réglant la plage horaire sur une semaine, puis en vérifiant qu'il n'y a pas d'événements critiques dans le rapport. Vous pouvez également diagnostiquer un Archiveur en recherchant des événements importants, comme *Seuil de saturation des disques dépassé* ou *Impossible d'écrire sur aucun disque*, pour voir quand ils sont survenus.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Événements d'Archiveur.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Archiveur
   Sélectionnez les rôles d'archivage (Archiveur et Archiveur auxiliaire) que vous souhaitez analyser.

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

   Événements
   Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

3. Cliquez sur Générer le rapport.
   Les événements d'Archiveur sont affichés dans le volet de rapport.

2.3.8.1 | Colonnes du volet de rapport dans la tâche Événements d'Archiveur

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Description
Description de l'événement, activité, entité ou incident.
IMPORTANT : Pour respecter la réglementation des États, si l'option Rapport généré est utilisée pour un rapport Historiques d'activité qui contient des données de RAPI, le motif de la recherche RAPI est inclus dans le champ Description.

Événement
Nom de l'événement.

Heure de l'événement
Date et heure de l'événement.

Source (entité)
Nom du système auquel appartient la caméra.
Sujet parent : Analyser les événements d'Archiveur

2.3.9 | Rechercher des événements de mouvement dans les archives vidéo

Utilisez le rapport *Recherche de mouvement* pour rechercher des séquences vidéo dans les archives vidéo qui contiennent du mouvement dans certaines zones du champ d'une caméra.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Recherche de mouvement.
2. Dans l'onglet Filtres, sélectionnez une caméra dans la liste déroulante.
   Lorsqu'une caméra est sélectionnée, un aperçu correspondant à la plage horaire par défaut est affiché. Si la caméra sélectionnée ne prend pas en charge la recherche de mouvement, le message « La recherche de mouvement n'est pas disponible pour cette caméra » est affiché à la place de l'aperçu.
3. Cliquez sur le bouton  pour actualiser l'aperçu basé sur la nouvelle plage horaire.
4. Cliquez sur  pour visionner la vidéo plutôt qu'une image fixe.
5. Définissez la plage horaire pour la recherche de mouvement.
6. Pour définir une zone de détection de mouvement sur l'image d'aperçu, tracez des blocs de détection de mouvement (rectangles bleus) sur les zones où il convient de rechercher du mouvement à l'aide des outils suivants :
   - Pour recouvrir l'image entière de blocs de détection de mouvement, utilisez l'outil Remplissage ().
   - Pour dessiner un groupe de blocs de détection de mouvement, utilisez l'outil Rectangle ().
   - Pour dessiner des blocs de détection de mouvement individuels, utilisez l'outil Crayon ().
   - Pour inverser les zones de détection de mouvement et la zone en dehors des blocs, utilisez l'outil Inverser ().
   - Pour effacer tous les blocs de détection de mouvement de l'image, utilisez l'outil Effacer tout ().
   - Pour effacer des blocs de détection de mouvement superflus, utilisez l'outil Gomme ().
7. Pour régler la vitesse et la précision de la recherche de mouvement, configurez les options de critères de détection de mouvement :

   Seuil minimum
   Définit le nombre minimum de blocs qui doivent être activés pour qu'un résultat de détection de mouvement soit inclus dans la requête. Le nombre total de blocs dans la zone de détection de mouvement correspond à la valeur maximale du seuil. Un seuil de zéro signifie que tout mouvement détecté dans l'aire définie est pris en compte lors de la recherche.

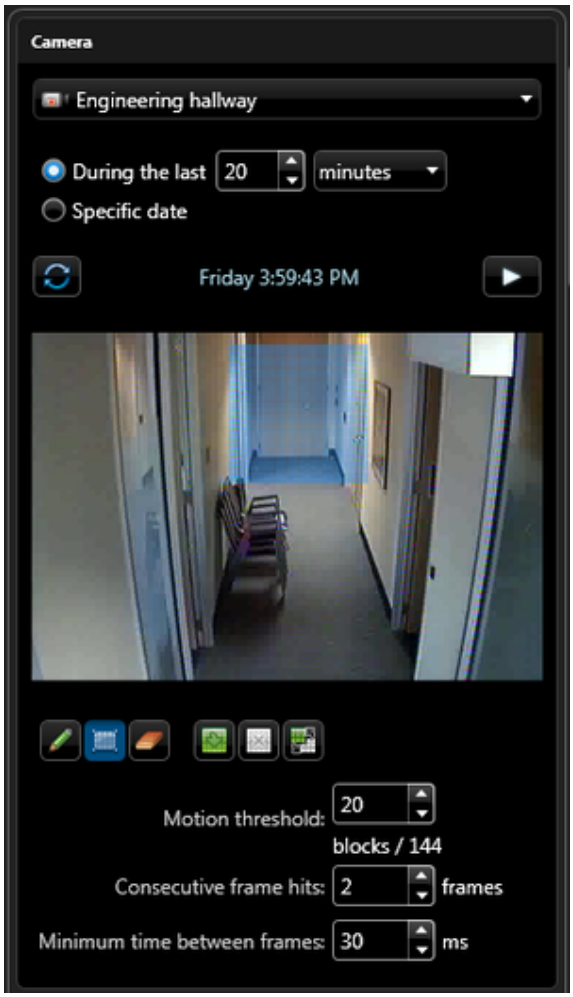
   Nombre d'occurrences consécutives
   Applique le seuil minimum à un nombre d'images vidéo particulier. Ce paramètre permet d'éviter les faux positifs dans la détection de mouvement (comme les interférences présentes dans une seule image). Le mouvement est ainsi détecté lorsque le seuil est atteint pour un nombre prédéterminé d'images consécutives (au lieu d'une seule image).

Durée minimum entre les images
Contrôle la fréquence d'échantillonnage de la recherche en indiquant au système de ne pas examiner chaque image vidéo. Plus la valeur est *élevée*, plus le système saute d'images au cours de la recherche, effectuant ainsi la recherche plus rapidement. Pour examiner chaque image, réglez la valeur sur 33 ms ou moins. La vitesse d'archivage la plus élevée est de 30 images/s. À cette vitesse, l'intervalle séparant deux images est de 33 ms.

8. Cliquez sur Générer le rapport.
   Les événements de mouvement sont affichés dans le volet de rapport.
9. Pour afficher la séquence vidéo associée à un événement de mouvement dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas.
   La lecture de la séquence sélectionnée débute immédiatement.
10. Pour contrôler l'enregistrement vidéo, utilisez le widget Caméra.
11. Pour exporter une archive vidéo importante, sélectionnez-la dans le volet de rapport, puis cliquez sur Exporter ( ).

Exemple

Pour consulter l'activité d'une porte particulière, recherchez du mouvement pour une caméra orientée vers la porte. Dans la figure suivante, une zone de détection de mouvement est définie pour la porte d'entrée. Le mouvement des personnes au fond du couloir est ainsi ignoré par la recherche.



Explorer

- Exporter de la vidéo
- Sélectionner la plage horaire d'un rapport
- Widget Caméra
- Présentation de la tâche Recherche de mouvement

2.3.9.1 | Colonnes du volet de rapport pour la tâche Recherche de mouvement

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Caméra
Nom de la caméra.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Heure de fin
Fin de la plage horaire, séquence d'enregistrement ou séquence vidéo.

Source (entité)
Nom du système auquel appartient la caméra.

Heure de début
Début de la plage horaire, séquence d'enregistrement ou séquence vidéo.
Sujet parent : Rechercher des événements de mouvement dans les archives vidéo

2.3.10 | Rechercher des événements de caméra dans les archives vidéo

You can find events related to selected cameras that were recorded by an Archiver, using the *Événements de caméra* report.

À savoir

Ce rapport est utile si vous connaissez le nom de la caméra qui vous intéresse. Vous pouvez ainsi voir les événements déclenchés par la caméra. Vous pouvez également analyser des événements particuliers, comme un enregistrement démarré en réaction à une alarme.

Pour que le rapport contienne des résultats, la vidéo et les métadonnées d'analyse doivent être enregistrées par un Archiveur.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Événements de caméra.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Caméras
   Sélectionnez la caméra à examiner.

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Événements
   Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

3. Cliquez sur Générer le rapport.
   Les événements de caméra sont affichés dans le volet de rapport.
4. Pour afficher la séquence vidéo associée à un événement dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas.
5. Pour contrôler l'enregistrement vidéo, utilisez le widget Caméra.

Explorer

- Widget Caméra

2.3.10.1 | Colonnes du volet de rapport pour la tâche Événements de caméra

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Archiveur
Nom du rôle Archiveur.

Caméra
Nom de la caméra.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Description
Description de l'événement, activité, entité ou incident.
IMPORTANT : Pour respecter la réglementation des États, si l'option Rapport généré est utilisée pour un rapport Historiques d'activité qui contient des données de RAPI, le motif de la recherche RAPI est inclus dans le champ Description.

Événement
Nom de l'événement.

Heure de l'événement
Date et heure de l'événement.

Sujet parent : Rechercher des événements de caméra dans les archives vidéo

2.3.11 | Préparer les unités Bosch à enregistrer les événements d'analyse vidéo

Avant de pouvoir rechercher des événements d'analyse vidéo enregistrés par une unité Bosch avec le rapport Recherche analytique, les unités doivent être configurées pour enregistrer la vidéo en local, et Bosch Video SDK doit être installé sur les postes Security Desk.

À savoir

Pour en savoir plus sur l'installation et la configuration des unités vidéo Bosch, consultez la documentation Bosch.

Procédure

1. Installez les unités vidéo Bosch sur le réseau.
   Les appareils Bosch doivent prendre en charge l'analyse vidéo intelligente (IVA).
2. Sur la page web de l'unité, configurez l'unité afin d'enregistrer en local sur l'appareil, ou sur un disque réseau iSCSI.
3. Sur la page web de l'unité, configurez les réglages *Bosch IVA*.
   REMARQUE : Les unités vidéo Bosch qui prennent en charge l'analyse IVA enregistrent les images vidéo et des métadonnées brutes, non traitées. Dès lors, la configuration de l'analyse peut être modifiée à tout instant à des fins de recherche historique. Par exemple, si vous configurez initialement l'analyse pour l'événement « *ligne franchie* » et que vous décidez plus tard de modifier la configuration pour l'événement « *présence prolongée* », vous pouvez quand même rechercher le nouvel événement d'analyse.
4. Installez *Bosch Video SDK* sur tout poste Security Desk qui doit utiliser la tâche Recherche analytique.
   Vous pouvez télécharger le pack d'installation Bosch Video SDK sur http://ipp.boschsecurity.com/en/.
5. Ajoutez vos unités vidéo Bosch (caméras ou codeurs vidéo IP) dans Security Center.
   L'Archiveur doit être connecté à l'appareil pour pouvoir envoyer des signaux de commandes à l'unité vidéo. Toutefois, puisque l'unité enregistre de manière autonome, l'Archiveur ne fournit qu'une duplication des enregistrements, et parfois une plus longue période de rétention des archives. Vous ne pouvez rechercher des événements d'analyse vidéo que parmi les enregistrements stockés sur la caméra.

Lorsque vous avez terminé

Recherchez les événements d'analyse vidéo stockés sur les unités Bosch.

2.3.12 | Rechercher des événements d'analyse vidéo stockés sur les unités Bosch

Utilisez le rapport *Recherche analytique* pour rechercher des événements d'analyse vidéo enregistrés en local sur les unités vidéo Bosch.

Avant de commencer

Configurez les unités Bosch pour l'enregistrement des analyses vidéo pour pouvoir rechercher les événements avec la tâche Recherche analytique.

À savoir

Pour que le rapport contienne des résultats, l'analyse vidéo doit être effectuée par l'unité vidéo elle-même, et l'unité doit enregistrer la vidéo et les métadonnées d'analyse en local (disque dur interne, disque dur USB, carte mémoire ou lecteur connecté iSCSI).

Vous n'avez pas besoin d'une licence spécifique pour utiliser le rapport Recherche analytique. Pour l'instant, seules les unités vidéo Bosch qui gèrent l'analyse Bosch IVA sont prises en charge pour ce rapport.

REMARQUE : Pour rechercher des événements d'analyse vidéo enregistrés par un Archiveur, utilisez le rapport *Événements de caméra*.

Procédure

1. Lancez Security Desk sur un poste sur lequel le *Bosch Video SDK* est installé.
2. Sur la page d'accueil, ouvrez la tâche Recherche analytique.
3. Dans l'onglet Filtres, configurez le filtre de recherche Caméras pour sélectionner une caméra à analyser.
   Lorsqu'une caméra une sélectionnée, un aperçu vidéo en temps réel est affiché.
4. Pour réinitialiser la configuration d'analyse, cliquez sur  .
5. Pour afficher ou modifier la configuration d'analyse, cliquez sur  .
6. Configurez le filtre de recherche Plage horaire pour sélectionner une plage horaire.
7. Cliquez sur Générer le rapport.
   Les événements d'analyse vidéo sont affichés dans le volet de rapport.
8. Pour afficher la séquence vidéo associée à un événement dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas.
9. Pour contrôler l'enregistrement vidéo, utilisez le widget Caméra.
10. Pour exporter une archive vidéo importante, sélectionnez-la dans le volet de rapport, puis cliquez sur Exporter ().

Explorer

- Exporter de la vidéo
- Sélectionner la plage horaire d'un rapport
- Widget Caméra

2.3.12.1 | Colonnes du volet de rapport pour la tâche Recherche analytique

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

ID d'algorithme
Valeur analytique Bosch. Pour en savoir plus, voir la documentation du fabricant.

Caméra
Nom de la caméra.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Heure de fin
Fin de la plage horaire, séquence d'enregistrement ou séquence vidéo.

Événement
Nom de l'événement.

Type d'événement
Valeur analytique Bosch. Pour en savoir plus, voir la documentation du fabricant.

Heure de début
Début de la plage horaire, séquence d'enregistrement ou séquence vidéo.

ID de piste
Valeur analytique Bosch. Pour en savoir plus, voir la documentation du fabricant.
Sujet parent : Rechercher des événements d'analyse vidéo stockés sur les unités Bosch

2.3.13 | Gérer les effets de l'heure d'été sur les archives vidéo

Les changements d'heure annuels, lors du passage à l'heure d'hiver ou l'heure d'été, peuvent affecter la consultation et les recherches des archives vidéo dans Security Center.

Les changements d'heure n'empêchent pas vos caméras d'enregistrer des données vidéo. Le rôle *Archiveur* enregistre toujours en utilisant le temps universel coordonné (UTC), qui ne décale pas l'heure en fonction de l'heure d'été, et les requêtes d'archivage sont toujours envoyées au serveur avec des horodatages UTC.

L'utilisation de l'heure UTC isole les archives des effets du changement d'heure. Cependant, puisque Security Desk et Config Tool peuvent être configurés pour utiliser (et afficher) un fuseau horaire autre qu'UTC ou GMT, différents effets sont observables selon que l'heure est avancée ou reculée.
REMARQUE : Le fuseau horaire EST (côte est des États-Unis, GMT-5) est utilisé en tant qu'exemple, mais tous les fuseaux horaires qui appliquent l'heure d'été sont concernés.

2.3.13.1 | Effets du recul de l'heure

Lorsque l'heure est reculée, elle passe de l'heure d'été à l'heure normale (GMT-5 ou EST).

Le passage de l'heure d'été à l'heure EST survient à 2h00. Avant 2h00, Security Center utilise l'heure d'été (GMT-4). À partir de 2h00, il utilise l'heure EST (GMT-5), comme le montre le tableau suivant :

	Heure d'été		Changement d'heure	EST	
Heure locale	00:00	01:00	02:00 = 01:00	02:00	03:00
Décalage (heures)	-4	-4	-5	-5	-5
UTC	04:00	05:00	06:00	07:00	08:00

En raison du recul de l'heure, les effets suivants se produisent lors de la lecture vidéo ou de l'exportation d'archives.

- L'heure recule d'une heure dans la frise chronologique. À 1:59:59, l'heure affichée repasse à 1:00:00.
- L'heure de fin d'une séquence vidéo peut être avant son heure de début.
- L'exportation d'archives entre 1:00 et 2:00 intègre toujours une heure de vidéo supplémentaire. Par exemple, si vous exportez des archives de 1h50 à 2h00 la nuit du changement d'heure, la séquence contient 1 heure et 10 minutes de vidéo, car la requête contient de la vidéo de 5h50 à 7h00 UTC.

Pour éviter que l'heure recule d'une heure pendant la lecture vidéo, ou pour exporter de la vidéo sans l'heure de métrage supplémentaire, vous devez configurer Security Desk pour qu'il utilise UTC. Une fois la séquence exportée, vous pouvez rétablir le fuseau horaire précédent pour visionner la séquence de manière relative à la référence temporelle locale.
Sujet parent : Gérer les effets de l'heure d'été sur les archives vidéo

2.3.13.2 | Effets de l'avancement de l'heure

Lorsque l'heure est avancée, elle passe de l'heure standard (EST ou GMT-5) à l'heure d'été.

Le passage de l'heure EST à l'heure d'été survient à 2h00. Avant 2h00, Security Center utilise l'heure EST (GMT-5). À partir de 2h00, il utilise l'heure d'été (GMT-4), comme le montre le tableau suivant :

	EST		Changement d'heure	Heure d'été	
Heure locale	00:00	01:00	02:00 = 03:00	04:00	05:00
Décalage (heures)	-5	-5	-4	-4	-4
UTC	05:00	06:00	07:00	08:00	09:00

En raison de l'avancement de l'heure, les effets suivants se produisent lors de la lecture vidéo ou de l'exportation d'archives :

- L'heure avance d'une heure dans la frise chronologique. À 1:59:59, l'heure affichée passe à 3:00:00.
- Il n'y a pas d'archives à exporter entre 2h00 et 3h00, puisque cette période est sautée.

Pour éviter que l'heure avance d'une heure pendant la lecture vidéo, vous devez configurer Security Desk pour qu'il utilise UTC.
Sujet parent : Gérer les effets de l'heure d'été sur les archives vidéo

2.3.14 | Régler le fuseau horaire sur UTC

Si vous manipulez des archives enregistrées durant le changement d'heure d'été et que vous souhaitez supprimer les effets sur la frise chronologique, vous pouvez régler le fuseau horaire sur UTC (temps universel coordonné) dans Security Desk avant de lancer votre tâche.

À savoir

Security Desk et Config Tool affichent l'heure relative au fuseau horaire sélectionné. Toutefois, le serveur utilise l'heure UTC (ou GMT), et l'application client convertit l'horodatage UTC du serveur vers le fuseau horaire sélectionné. Vous pouvez configurer les applications client afin qu'elles utilisent l'heure UTC pour éviter la conversion de l'heure et éviter les effets du changement d'heure.
REMARQUE : Les réglages de date et heure ne s'appliquent qu'à l'application client que vous configurez. Chaque application doit être configurée séparément.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Date et heure.
2. Le cas échéant, sélectionnez Afficher les abréviations de fuseaux horaires pour afficher le fuseau horaire sélectionné en regard de l'heure dans la zone de notification.
3. Cliquez sur Afficher l'heure en fonction du fuseau horaire suivant, puis sélectionnez UTC (temps universel coordonné).

4. Cliquez sur Enregistrer.

Résultats

L'application client affiche désormais l'heure actuelle et l'horodatage des archives en fonction du fuseau horaire UTC.

2.4 | Exportation vidéo dans Security Desk

2.4.1 | Formats d'exportation vidéo

Les formats d'exportation vidéo disponibles dans Security Desk déterminent le lecteur multimédia à utiliser pour visionner les fichiers vidéo exportés. Vous pouvez exporter la vidéo au format G64x, G64, ASF et MP4.

Formats G64x et G64

Les formats vidéo G64x et G64 Security Center prennent en charge l'audio, les signets, les horodatages, l'incrustation des métadonnées et les indicateurs de mouvement. Tous les marqueurs d'événement sont inclus dans le fichier exporté, sauf les marqueurs de métadonnées. Ces formats prennent également en charge les débits binaires variables et les résolutions d'image variables.

REMARQUE : Le format G64 est obsolète et a été remplacé par le format G64x. Utilisez uniquement le format G64 pour garantir la compatibilité avec Security Center version 5.2 et antérieures ou Omnicast™ version 4.8 et antérieures.

Le cas échéant, les fichiers G64x héritent automatiquement de la *signature de données* de la vidéo d'origine. Une seule signature peut exister par fichier. Si une séquence vidéo exportée dispose de plusieurs signatures, un fichier distinct est généré pour chaque signature. En outre, le format G64x est le seul pouvant être réexporté, si cette option est sélectionnée lors de l'exportation.

Lorsque vous exportez plusieurs séquences vidéo en même temps depuis le canevas, vous pouvez les combiner dans un seul fichier G64x. Des fichiers G64x sont également créés lorsque vous exportez un pack d'incident avec la fonction d'enregistrement d'incident dans une tuile. Selon la manière d'exporter la vidéo, les séquences sont lues dans les mêmes tuiles qu'elles occupaient au moment de l'exportation, ou dans une seule tuile, selon l'ordre d'enregistrement.

REMARQUE : Les caméras Omnicast™ fédérées ne peuvent pas être exportées au format G64x. Si vous sélectionnez le format G64x, les séquences vidéo provenant de caméras Omnicast™ fédérées sont exportées sous forme de plusieurs fichiers G64, au lieu du format groupé G64x. Ces fichiers G64 hériteront de la signature numérique de la vidéo d'origine, le cas échéant.

Vous devez utiliser Security Desk ou le Genetec™ Video Player pour visionner les fichiers vidéo G64x et G64.

format ASF

Le format ASF (Advanced Systems Format) est un format de données propriétaire de Microsoft. Il prend en charge les données audio ainsi que les débits d'image variables, mais pas les métadonnées associées à la séquence vidéo. Les informations concernant la date et l'heure ne sont pas non plus prises en charge, mais elles peuvent être ajoutées par incrustation sur la vidéo à l'exportation.

Si la séquence vidéo que vous souhaitez exporter comporte plusieurs résolutions d'image (CIF, 2CIF, 4CIF, et ainsi de suite), la séquence exportée utilise la résolution de la première image de la séquence vidéo d'origine. En outre, les métadonnées associées à la séquence vidéo et aux signatures numériques ne sont pas exportées. Cette option est utile si vous devez faire une copie d'un enregistrement vidéo pour les forces de l'ordre, votre service juridique, ou d'autres membres de votre équipe de sécurité.

Quand vous exportez plusieurs séquences vidéo ASF à partir du canevas en même temps, un fichier ASX unique est créé, pour que vous puissiez visionner les fichiers ASF dans l'ordre selon lequel ils ont été enregistrés.

Vous devez utiliser Windows Media Player pour lire les fichiers vidéo ASF.

format MP4

Format standard qui stocke le son et les vidéos et qui peut être lu sur de multiples lecteurs multimédias tels que Windows Media Player et QuickTime.

Quand vous exportez plusieurs séquences vidéo MP4 à partir du canevas en même temps, un fichier ASX unique est créé, pour que vous puissiez visionner les fichiers MP4 dans l'ordre selon lequel ils ont été enregistrés.

L'exportation MP4 prend en charge les formats vidéo H.264 et MPEG-4 et le format audio AAC. Le chiffrement flux fusion, les incrustations et les signatures numériques ne sont pas pris en charge actuellement.

Explorer

- Exporter de la vidéo
- Configurer les réglages d'exportation vidéo

2.4.2 | Configurer les réglages d'exportation vidéo

Avant d'exporter de la vidéo dans Security Desk, vous devez choisir un emplacement pour les fichiers exportés et configurer les réglages de chaque format d'exportation.

À savoir

Quand vous exportez une vidéo G64x, le système peut inclure des informations supplémentaires sur les fichiers, comme le nom de la caméra, la date de création et les coordonnées de la caméra, qui peuvent être utiles lors des analyses. Pour afficher des informations supplémentaires sur les fichiers, effectuez un clic droit dans le Coffre-fort, puis sélectionnez Afficher les propriétés.
REMARQUE : Le système n'inclut ces informations supplémentaires que si un administrateur active la fonctionnalité dans vos réglages utilisateur.
IMPORTANT : Les fichiers vidéo exportés sont enregistrés en tant qu'instantanés dans le même dossier et sont disponibles dans le *Coffre-fort*. Si vous modifiez l'emplacement du dossier, vous ne pourrez plus afficher les vidéos et instantanés existants avec l'outil Coffre-fort.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Vidéo.
2. Dans la section Coffre-fort, configurez les options suivantes :

   Emplacement
   Le chemin Windows vers le dossier de stockage des fichiers vidéo et instantanés. Le chemin par défaut est : C:\Users\Username\AppData\Local\Genetec Security Center version #\Vault.

   Nettoyage automatique
   La période de rétention en jours des vidéos et des instantanés exportés dans le Coffre-fort. Lorsque cette option est désactivée, les vidéos et les instantanés exportés dans le coffre-fort ne sont jamais supprimés automatiquement.

3. Dans la section Exporter, sélectionnez un Format de fichier par défaut pour l'exportation vidéo :

   G64x
   Fichier qui contient plusieurs séquences vidéo pouvant être lues dans Security Desk ou avec Genetec™ Video Player.

   G64 (mode compatibilité)
   Format Security Center qui peut être lu dans Security Desk ou avec Genetec™ Video Player.

   Advanced Systems Format
   Format propriétaire de Microsoft qui peut être lu avec Windows Media Player.

   MP4
   Format standard qui stocke le son et les vidéos et qui peut être lu sur de multiples lecteurs multimédias tels que Windows Media Player et QuickTime.

4. Cliquez sur Avancé ( ) et configurez les options suivantes :
   REMARQUE : Les options pour le format G64x peuvent être remplacées au moment de l'exportation.

Option	Description	S'applique à
Est protégé par mot de passe	Activez cette option pour protéger les fichiers vidéo exportés, puis entrez un mot de passe dans le champ Mot de passe. Toute personne qui souhaite lire les fichiers vidéo exportés devra saisir ce mot de passe.	G64x
Supprimer les fichiers intermédiaires	Activez cette option si vous souhaitez supprimer les fichiers d'origine (non protégés). Si vous ne protégez pas les fichiers vidéo exportés par mot de passe, cette option est sans effet. REMARQUE : Le nom du fichier protégé par mot de passe est celui du fichier d'origine, avec le suffixe « _1 ».	G64x
Autoriser la réexportation du fichier vidéo	Activez cette option pour permettre à la personne qui visionne la vidéo exportée de *réexporter* tout ou partie de la vidéo au même format ou dans un autre format. REMARQUE : L'ajout d'un mot de passe désactive automatiquement cette option.	G64x
Utiliser le profil suivant	Sélectionnez le profil de compression vidéo. Le débit binaire (indiqué entre parenthèses) est une indication de la qualité de la vidéo exportée. Plus il est élevé, meilleure est la qualité d'image (et plus les fichiers convertis sont volumineux). La description sous le profil fournit des informations utiles pour vous guider dans votre choix.	ASF (Advanced Systems Format)
Exporter l'audio	Activez cette option pour inclure les données audio dans les fichiers ASF et MP4.	ASF, MP4
Afficher la date et l'heure sur l'image vidéo	Activez cette option pour incruster la date et l'heure sur l'image vidéo exportée.	ASF (Advanced Systems Format)
Supprimer les fichiers intermédiaires	Activez cette option pour supprimer les fichiers d'origine après conversion en fichiers ASF ou MP4.	ASF, MP4

5. Cliquez sur Enregistrer.

Explorer

- Formats d'exportation vidéo

2.4.3 | Exporter de la vidéo

Pour créer des fichiers vidéo autonomes lisibles sans connexion au Répertoire Security Center, vous pouvez exporter la vidéo depuis n'importe quelle tâche de Security Desk dotée d'une séquence de vidéo enregistrée sur le canevas.

Avant de commencer

- Vérifiez que vous disposez du privilège *Exporter la vidéo*.

À savoir

- Quand vous exportez une vidéo G64x, le système peut inclure des informations supplémentaires sur les fichiers, comme le nom de la caméra, la date de création et les coordonnées de la caméra, qui peuvent être utiles lors des analyses. Pour afficher des informations supplémentaires sur les fichiers, effectuez un clic droit dans le Coffre-fort, puis sélectionnez Afficher les propriétés.
  REMARQUE : Le système n'inclut ces informations supplémentaires que si un administrateur active la fonctionnalité dans vos réglages utilisateur.
- Si vous avez activé le tatouage numérique de la vidéo, les signatures numériques et le chiffrement de la vidéo sont exclus du fichier exporté.
- Si vous ne disposez pas du privilège *Exportation par un seul utilisateur*, un deuxième utilisateur doté du privilège *Exporter la vidéo* doit autoriser l'exportation.
- Les nouvelles exportations sont placées en file d'attente et démarrent lorsque l'exportation en cours prend fin.

Procédure

1. Sur la page d'accueil de Security Desk, ouvrez n'importe quelle tâche disposant d'un canevas vidéo.
2. Ouvrez la vidéo enregistrée sur le canevas.
3. Sélectionnez la vidéo à exporter.
   - Dans le volet de rapport, sélectionnez un élément et cliquez sur Exporter ( ).
     REMARQUE : Si la protection de la confidentialité est activée, mais que vous souhaitez exporter la vidéo d'origine sans floutage ni anonymisation, sélectionnez le flux *Vidéo confidentielle* dans la liste du rapport. Vous devez disposer du privilège *Supprimer la protection de la confidentialité* pour exporter un flux vidéo confidentiel.
   - Effectuez un clic droit sur une tuile, puis cliquez sur Caméra > Exporter la vidéo.

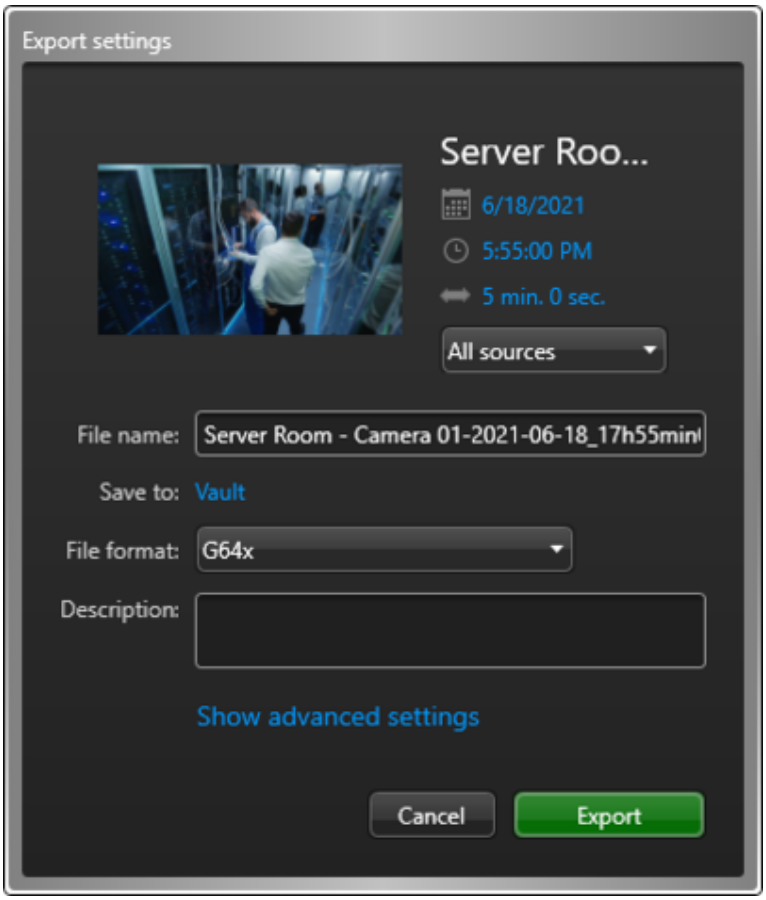
     Le format vidéo actuellement lu dans la tuile est exporté.

   - Dans le widget Caméra, cliquez sur Exporter ( ).

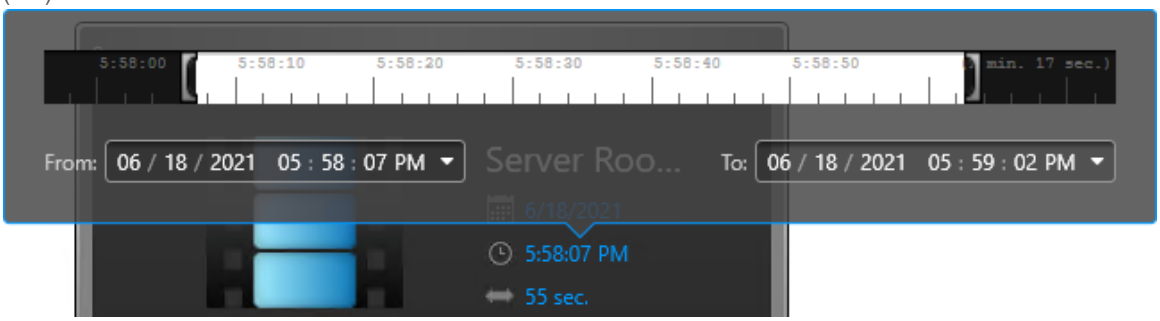
     Vous pouvez exporter la vidéo depuis la tuile sélectionnée ou depuis toutes les tuiles. Le format vidéo actuellement lu dans la tuile sélectionnée ou dans toutes les tuiles est exporté.

     REMARQUE : Si la séquence vidéo a plusieurs sources, cliquez sur Toutes les sources et sélectionnez la source particulière que vous souhaitez exporter.

   La boîte de dialogue Paramètres d'exportation s'ouvre :



4. Définissez la date, l'heure et la durée des séquences vidéo sélectionnées :
   a. Cliquez sur le réglage de date, heure ou durée.
   b. Saisissez la date et l'heure du début et de la fin de la séquence, ou faites glisser les marqueurs de plage de temps ( ) sur la durée souhaitée.



   REMARQUE : Vous pouvez configurer une plage horaire de 24 heures maximum.
5. (Facultatif) Dans le champ Nom de fichier, donnez un nom au fichier vidéo.
   Par défaut, le nom du fichier inclut le nom de la caméra, la date et la durée de la séquence vidéo.
6. Pour enregistrer le fichier dans un sous-dossier du Coffre-fort, cliquez sur Coffre-fort et créez ou sélectionnez un sous-dossier.
7. Dans la liste Format de fichier, sélectionnez un format d'exportation :

G64x
Fichier qui contient plusieurs séquences vidéo pouvant être lues dans Security Desk ou avec Genetec™ Video Player.

G64 (mode compatibilité)
Format Security Center qui peut être lu dans Security Desk ou avec Genetec™ Video Player.

Advanced Systems Format
Format propriétaire de Microsoft qui peut être lu avec Windows Media Player.

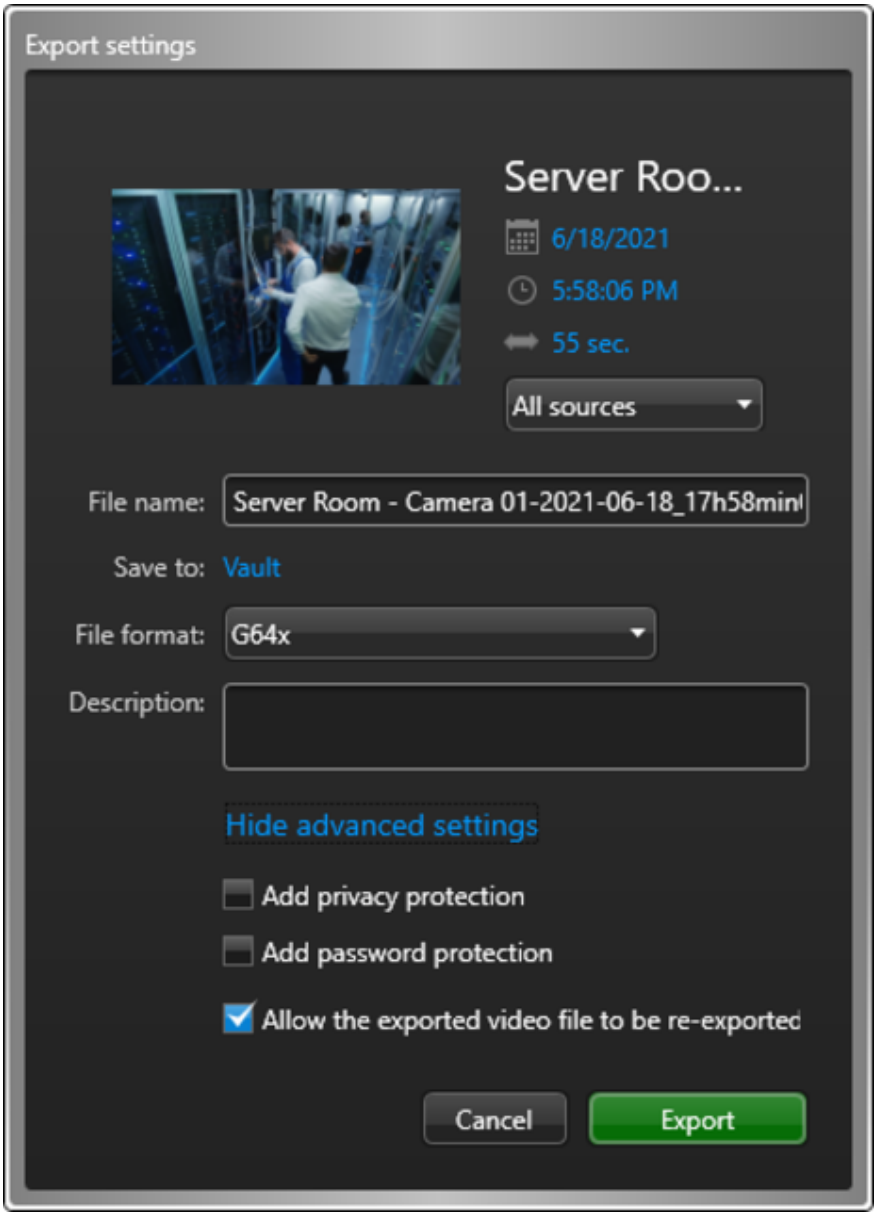
MP4
Format standard qui stocke le son et les vidéos et qui peut être lu sur de multiples lecteurs multimédias tels que Windows Media Player et QuickTime.

8. (Facultatif) Dans le champ Description, saisissez une description pour la vidéo exportée.
   La description s'affiche dans les rapports Historiques de configuration et dans les propriétés de fichier du Coffre-fort.
   REMARQUE : Une description doit être saisie pour les utilisateurs ne disposant pas du privilège *Exportation par un seul utilisateur*. Pour les autres utilisateurs, le champ est uniquement disponible si le format G64x est sélectionné et que l'option Inclure les propriétés supplémentaires pour exportation/instantané est activée dans l'onglet Avancé de l'utilisateur dans Config Tool.
9. Si exportez la vidéo depuis toutes les tuiles, procédez comme suit :
   a. Si vous exportez la vidéo au format G64x, sélectionnez un mode de lecture.

      En même temps
      Lit les séquences dans les tuiles où elles s'affichaient lors de l'exportation.

      En séquence
      Lit la vidéo en séquence sur une même tuile.

   b. Pour modifier l'ordre de lecture d'une séquence vidéo, sélectionnez-la, puis utilisez les boutons et .
10. Si vous exportez la vidéo au format G64x, pour afficher les paramètres supplémentaires, cliquez sur Afficher les paramètres avancés et configurez-les comme requis.



   a. SélectionnezEst protégé par mot de passe, puis saisissez un mot de passe pour chiffrer le fichier vidéo. Toute personne souhaitant consulter ce fichier doit saisir ce mot de passe.
   b. (Facultatif) Sélectionnez Autoriser la réexportation du fichier vidéo.
      Si vous sélectionnez cette option, la personne visionnant la vidéo exportée dans Security Desk ou Genetec™ Video Player peut la réexporter partiellement ou en totalité, au même format ou dans un format différent.

11. Cliquez sur Exporter.
    Si vous ne disposez pas du privilège *Exportation par un seul utilisateur*, la fenêtre Autorisation s'ouvre et un deuxième utilisateur disposant du privilège *Exporter la vidéo* doit saisir ses identifiants pour autoriser l'exportation.
    REMARQUE : Le nom d'utilisateur des deux personnes s'affiche dans le rapport Historiques d'activité, mais dans un système fédéré, seul le nom de l'utilisateur fédéré s'affiche.
    La progression de l'exportation est affichée dans la zone de notification ( ). Pour afficher la progression ou résoudre des erreurs d'exportation, cliquez sur Plus ou Afficher les détails pour ouvrir la boîte de dialogue Exporter.

    Lorsque l'exportation est terminée, les fichiers vidéo sont créés dans le dossier d'exportation que vous avez spécifié, et les fichiers sont disponibles dans l'outil Coffre-fort.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Lorsque vous avez terminé

Procédez de l'une des manières suivantes :

- Lancez la lecture des fichiers vidéo G64 et G64x en local sur votre ordinateur.
- Copiez les fichiers vidéo exportés pour les partager sur un autre ordinateur.

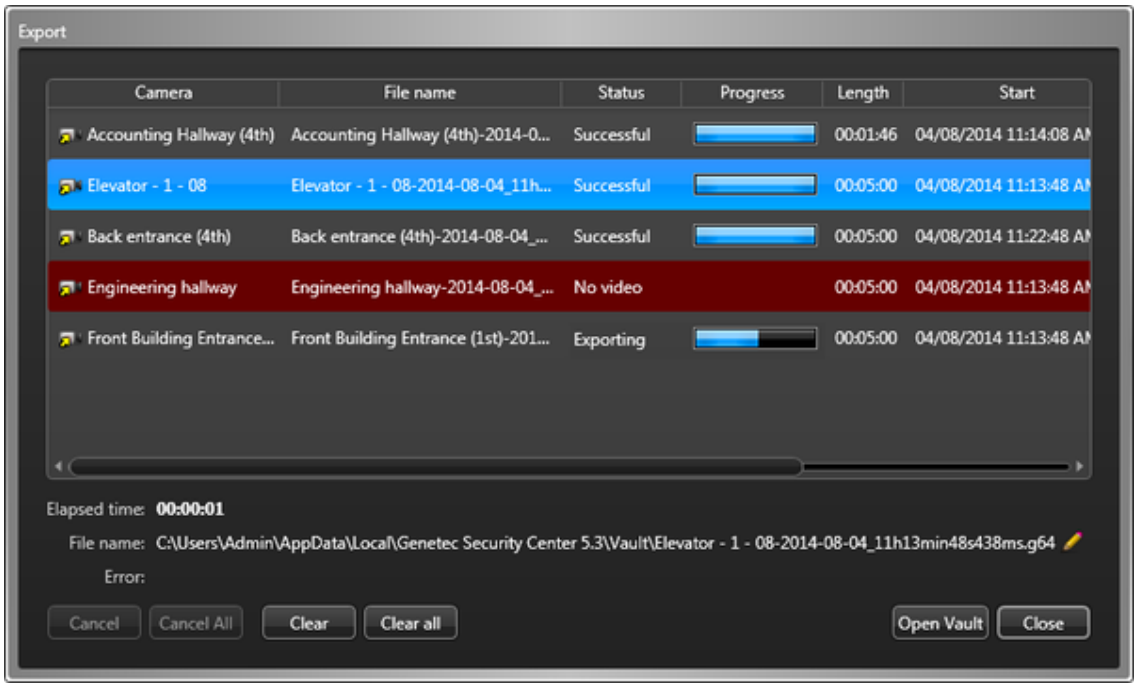
Explorer

- Formats d'exportation vidéo
- Chiffrer les fichiers vidéo exportés

2.4.4 | Boîte de dialogue Exporter de la vidéo

La boîte de dialogue Exporter la vidéo apparaît lorsque vous exportez de la vidéo depuis une tâche Security Desk qui affiche une séquence vidéo enregistrée sur le canevas.

La figure suivante illustre la boîte de dialogue Exporter la vidéo durant le processus d'exportation vidéo.



La boîte de dialogue Exportation affiche les informations suivantes sur le processus d'exportation :

Caméra
Nom de la caméra.

Nom de fichier
Le nom du fichier en cours d'exportation.

État
États possibles de l'exportation :

En file d'attente
L'opération d'exportation est placée en attente, mais n'est pas lancée.

Exportation
L'exportation est en cours. La progression est indiquée par le nombre d'octets transférés.

Conversion en cours
Si vous avez choisi de chiffrer le fichier vidéo ou de l'exporter au format ASF, cette étape suit l'étape Exportation. La progression est indiquée par le pourcentage du travail effectué.

Aucune vidéo
Aucun enregistrement vidéo n'est associé à cette caméra pour la période sélectionnée.

Exportation partielle
Un problème imprévu a interrompu l'exportation. Cliquez sur la séquence pour afficher une description du problème dans le champ État situé dans la partie inférieure de la boîte de dialogue. En cas d'exportation partielle, le reste de la vidéo est exportée dans un fichier vidéo distinct.

Le serveur Archiveur n'est pas lancé
L'Archiveur qui gère l'enregistrement vidéo que vous cherchez à exporter n'est pas actif.

Annulé
L'opération d'exportation a été annulée par l'utilisateur.

Réussie
La séquence vidéo complète a été exportée avec succès.

Une erreur est survenue
L'exportation a échoué. Cliquez sur la séquence pour consulter la raison de l'échec dans le champ Erreur au bas de la boîte de dialogue.

Progression
Progression de l'exportation

Durée
Longueur du fichier vidéo.

Début
Heure de début de la séquence vidéo contenue dans le fichier.

Fin
Heure de fin de la séquence vidéo contenue dans le fichier.

Source
La source d'archivage de la séquence vidéo.

Temps passé
Temps écoulé depuis le début de l'opération d'exportation.

Nom de fichier
Le nom du fichier en cours d'exportation. Vous pouvez cliquer sur Renommer () pour modifier le nom de fichier.

Erreur
Message d'erreur décrivant la raison de l'échec ou de l'interruption (exportation partielle) de l'exportation sélectionnée.

Annuler
Interrompt l'exportation avant la fin de l'opération. Les parties de séquences déjà exportées sont enregistrées en tant que fichiers vidéo.

Tout annuler
Interrompt l'exportation de tous les fichiers vidéo restants. Les séquences déjà exportées (mention *Réussie*) sont enregistrées en tant que fichiers vidéo.

2.4.5 | Afficher les fichiers vidéo exportés

Vous pouvez utiliser l'outil Coffre-fort dans Security Desk pour lire vos fichiers vidéo exportés sur votre ordinateur.

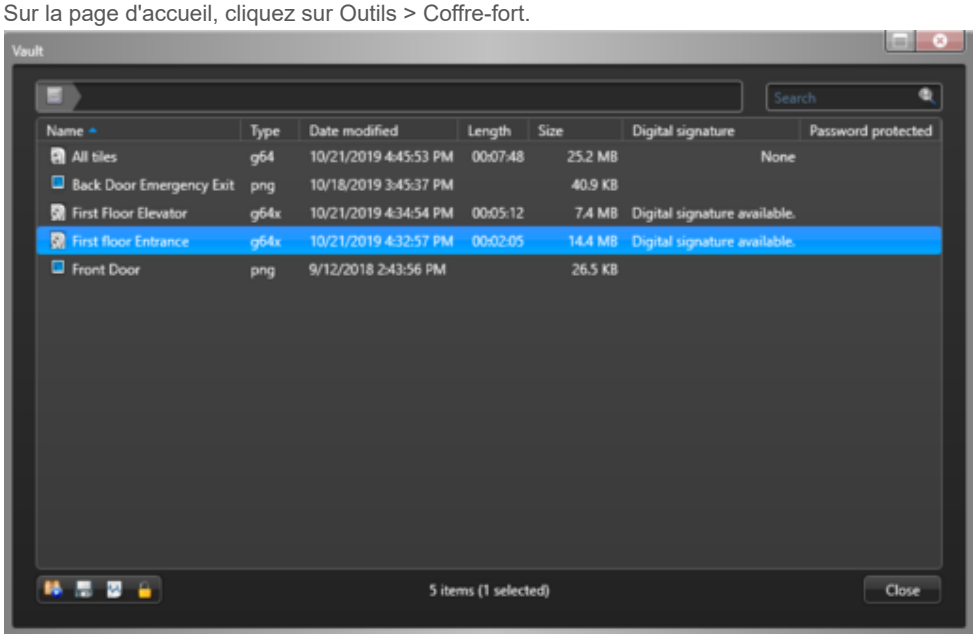
À savoir

- Si vous avez exporté plusieurs séquences vidéo en même temps sous forme de fichier G64x, elles sont soit affichées dans les tuiles utilisées lors de l'exportation, soit de manière séquentielle dans une seule tuile.
- Si vous modifiez l'emplacement d'enregistrement des fichiers vidéo exportés, les fichiers exportés vers l'emplacement précédent ne sont plus visibles depuis le Coffre-fort. Vous ne pouvez pas faire glisser un fichier vidéo depuis Windows vers le Coffre-fort.
- Les fichiers ASF ne peuvent être visionnés qu'avec Windows Media Player.
- Les fichiers MP4 peuvent être visualisés dans de nombreux lecteurs multimédias tels que Windows Media Player et QuickTime.
  REMARQUE : Certains lecteurs multimédias exigent l'installation d'un codec particulier pour lire correctement les fichiers.
- Quand vous exportez une vidéo G64x, le système peut inclure des informations supplémentaires sur les fichiers, comme le nom de la caméra, la date de création et les coordonnées de la caméra, qui peuvent être utiles lors des analyses. Pour afficher des informations supplémentaires sur les fichiers, effectuez un clic droit dans le Coffre-fort, puis sélectionnez Afficher les propriétés.
  REMARQUE : Le système n'inclut ces informations supplémentaires que si un administrateur active la fonctionnalité dans vos réglages utilisateur.

Procédure

Pour lire un fichier vidéo exporté depuis le Coffre-fort :

1. Sur la page d'accueil, cliquez sur Outils > Coffre-fort.



   Le coffre-fort affiche tous les fichiers exportés.

2. Cliquez deux fois sur le fichier que vous souhaitez lire.
   (G64x seulement) Si le fichier est protégé par mot de passe, entrez le mot de passe.

Voici les cas de figure :

- S'il s'agit d'un fichier G64x, le fichier est ouvert dans Security Desk et affiché sur le canevas de la tâche Surveillance.
- S'il s'agit d'un fichier ASF ou MP4, le fichier est ouvert dans le lecteur multimédia installé sur votre système.

Pour lire les fichiers vidéo exportés depuis Genetec™ Video Player :

1. Sur la page d'accueil, cliquez sur Outils > Genetec™ Video Player .
2. Cliquez sur Fichier > Ouvrir un fichier, puis sélectionnez le fichier vidéo.
   La lecture de la vidéo démarre. Vous pouvez contrôler la lecture à l'aide des commandes situées au bas de la fenêtre.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Widget Caméra

2.4.5.1 | Visionner les fichiers vidéo exportés avec l'Explorateur de fichiers vidéo

Vous pouvez utiliser la tâche Explorateur de fichiers vidéo pour rechercher et lire des fichiers vidéo G64 et G64x exportés afin de valider leur authenticité.

À savoir

Il n'est pas nécessaire d'être connecté à Security Center pour utiliser la tâche Explorateur de fichiers vidéo. Vous pouvez donc lire un fichier vidéo important, même lorsque vous ne pouvez pas vous connecter.
CONSEIL : Lorsque vous cliquez deux fois sur un fichier exporté dans l'Explorateur Windows, une nouvelle tâche Explorateur de fichiers vidéo est automatiquement ouverte dans Security Desk. Vous pouvez également faire glisser un fichier depuis l'Explorateur Windows sur une tuile de Security Desk.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Explorateur de fichiers vidéo.
2. Dans le Sélecteur, sélectionnez un dossier.
   Si le dossier contient des fichiers vidéo, ceux-ci sont affichés dans le volet de rapport avec les informations suivantes :

Nom de fichier
Nom du fichier vidéo.

Caméra
Nom de la caméra ayant capturé la vidéo.

Début
Heure de début de la séquence vidéo contenue dans le fichier.

Fin
Heure de fin de la séquence vidéo contenue dans le fichier.

Fuseau horaire
Le fuseau horaire de la caméra.

Durée
Durée de la séquence vidéo (Heure de fin moins Heure de début).

Taille du fichier
Taille du fichier vidéo.

Signature électronique
Indique si le fichier vidéo a été signé numériquement ou non.

Chiffrement
Indique si le fichier vidéo est chiffré. Si c'est le cas, vous devez le déchiffrer avant de le lire.

Date de modification
Date de la dernière modification du fichier vidéo.

3. Cliquez deux fois sur un fichier vidéo dans le volet de rapport, ou faites-le glisser sur le canevas.
   La lecture de la séquence sélectionnée démarre immédiatement, et le nom et l'horodatage du fichier sont affichés. L'heure indiquée sur la frise chronologique représente toujours l'heure locale de la vidéo enregistrée.
   REMARQUE : Vous ne pouvez pas basculer vers la vidéo en direct lorsque vous visionnez un fichier exporté, car Security Desk ne peut pas savoir à quelle caméra le fichier est associé.

Sujet parent : Afficher les fichiers vidéo exportés
Explorer

- Présentation de la tâche Explorateur de fichiers vidéo

2.4.6 | Partager des fichiers vidéo exportés

Pour partager des fichiers vidéo exportés au format G64 ou G64x avec quelqu'un qui n'a pas installé Security Desk, vous pouvez les associer au lecteur Genetec™ Video Player, puis copier les fichiers vidéo sur un CD, un DVD ou une clé USB.

À savoir

Pour partager des fichiers ASF ou MP4, copiez-les sur un CD ou un DVD.

Procédure

1. Sur la page d'accueil, cliquez sur Outils > Coffre-fort.
2. Sélectionnez le fichier vidéo, puis cliquez sur Inclure avec Genetec Video Player ( ).
3. Dans le champ Destination, sélectionnez l'emplacement d'enregistrement des fichiers et de Genetec Video Player.exe.
4. Cliquez sur Empaqueter.
5. Naviguez jusqu'au dossier dans lequel vous avez enregistré les fichiers, puis copiez-les sur un CD, DVD ou clé USB.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

2.4.7 | Convertir des fichiers vidéo au format ASF ou MP4

Security Desk vous permet de convertir des fichiers vidéo G64 ou G64x précédemment exportés aux formats ASF ou MP4 de sorte qu'ils puissent être vus à l'aide de lecteurs multimédias pour Windows.

Avant de commencer

Configurez vos réglages d'exportation vidéo

À savoir

Les fichiers vidéo exportés au format *ASF* ou *MP4* peuvent être lus avec des logiciels comme Windows Media Player. Security Desk n'est pas nécessaire. Cette option est utile si vous devez faire une copie d'un enregistrement vidéo pour les forces de

l'ordre, votre service juridique, ou d'autres membres de votre équipe de sécurité.

Procédure

1. Sur la page d'accueil, procédez de l'une des manières suivantes :
   - Cliquez sur Outils > Coffre-fort.
   - Ouvrez la tâche Explorateur de fichiers vidéo et sélectionnez le dossier qui contient le fichier vidéo à convertir.
2. Sélectionnez le fichier vidéo, et cliquez sur le bouton Enregistrer sous ( ).
   REMARQUE : Pour sélectionner plusieurs fichiers vidéo, appuyez sur les touches Ctrl ou Maj.
3. Dans la boîte de dialogue Enregistrer sous, vous pouvez saisir un nouveau Nom de fichier ou conserver le nom existant.
4. Dans le champ Format de fichier, sélectionnez ASF ou MP4.
5. Cliquez sur Enregistrer pour démarrer la conversion.
   CONSEIL : Vous pouvez suivre la progression de la conversion à tout moment en cliquant deux fois sur l'icône Conversion vidéo ( ) dans la zone de notification.

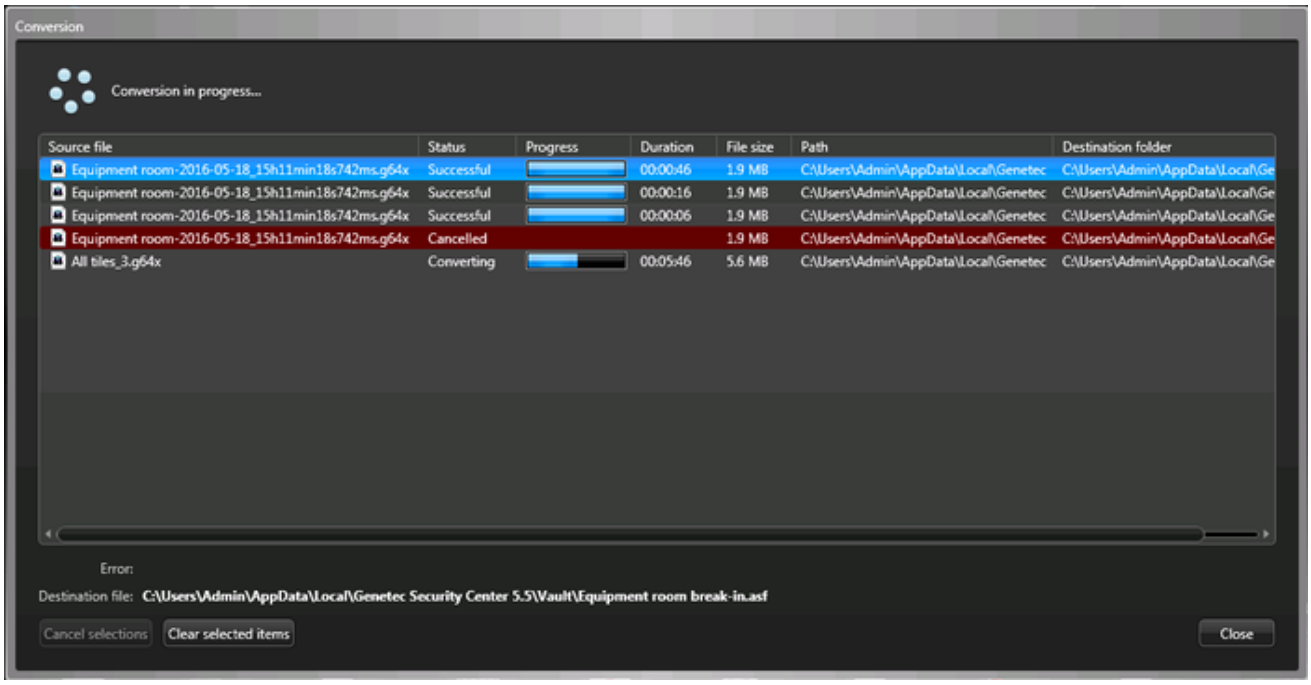
Explorer

- Formats d'exportation vidéo

2.4.7.1 | Boîte de dialogue de la conversion

Dans Security Desk, vous pouvez surveiller l'état de conversion des fichiers vidéo G64 et G64x au format ASF ou MP4 dans la boîte de dialogue Conversion.

Vous pouvez également ouvrir la boîte de dialogue Conversion en double cliquant sur l'icône Conversion vidéo ( ) dans la zone de notification.



La boîte de dialogue affiche la file d'attente de conversion (fichiers en attente de conversion) et le journal des conversions (fichiers ayant déjà été convertis). Chaque fichier est identifié par son Nom de fichier, l'État de la conversion, un indicateur de Progression, la Durée de la conversion, la Taille de fichier d'origine, le Chemin du fichier et le Dossier de destination du fichier converti. Le fichier converti conserve le nom du fichier d'origine, mais utilise l'extension ASF.

Les états de conversion possibles sont les suivants :

En file d'attente
Le fichier est en attente de conversion.

Conversion en cours
La conversion est en cours. La progression de la conversion est indiquée dans la colonne Progression.

Réussie
La conversion s'est terminée avec succès. La durée de conversion est indiquée dans la colonne durée.

Une erreur est survenue
La conversion a échoué. Sélectionnez le fichier pour connaître la raison de l'échec, indiquée dans le champ Erreur situé en dessous.

Annulé
La conversion a été annulée par l'utilisateur. Si la conversion a été annulée après avoir démarré, la durée de conversion est indiquée dans la colonne Durée.
Les boutons d'action suivants sont disponibles dans la boîte de dialogue :

Effacer les éléments sélectionnés
Supprime les éléments sélectionnés du journal de conversion. Seules les conversions *réussies*, *échouées* et *annulées* peuvent être supprimées du journal. L'historique de conversion est supprimé lorsque vous quittez .Security Desk

Annuler les sélections
Retire les éléments sélectionnés de la file d'attente de conversion. Seules les conversions *en attente* ou *en cours* de conversion peuvent être annulées. Lorsque vous annulez une conversion ayant débuté, la partie déjà convertie est enregistrée.

Fermer
Ferme la fenêtre de suivi de conversion. Le processus de conversion continue en tâche de fond. La fermeture de cette fenêtre permet d'ajouter d'autres fichiers à convertir.
Sujet parent : Convertir des fichiers vidéo au format ASF ou MP4

2.4.8 | Ré-exportation de fichiers vidéo G64 et G64x

Les fichiers G64 et G64x déjà exportés peuvent être exportés à nouveau pour créer des fichiers dans Security Desk. Cela s'avère utile quand vous voulez vous concentrer sur un segment spécifique de la vidéo précédemment exportée, parce que vous pouvez définir une heure de début et de fin pour la nouvelle exportation. Vous pouvez également vouloir enregistrer le fichier sous un format différent. Vous pouvez réexporter un fichier vidéo depuis une tuile Security Desk ou depuis le Coffre-fort.

Avant de commencer

- Configurez les réglages de chaque format d'exportation vidéo.
- Vérifiez que vous avez le privilège d'utilisateur *Exporter de la vidéo*.

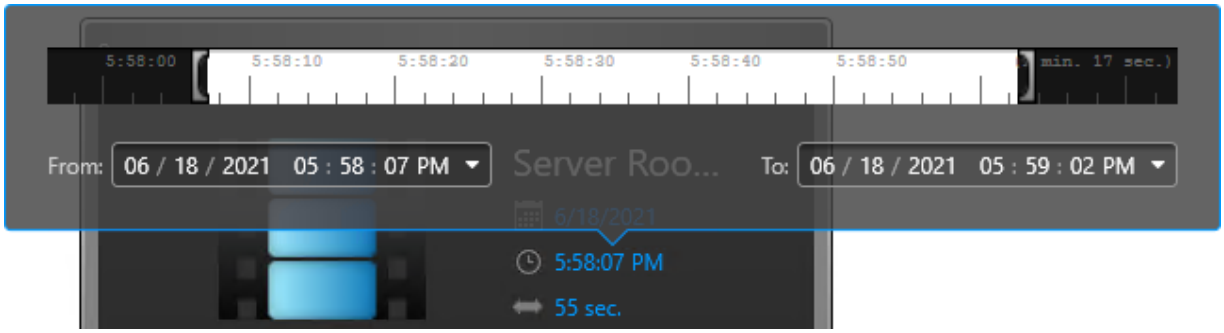
À savoir

- Seuls les fichiers G64x exportés avec l'option Autoriser la réexportation du fichier vidéo exporté peuvent être réexportés.
  REMARQUE : Genetec™ Video Player peut également réexporter les fichiers G64x lorsque la réexportation est autorisée.
- À compter de Security Center 5.8 GA, les fichiers GEK ne sont plus utilisés pour stocker la vidéo chiffrée. Les fichiers vidéo chiffrés et non chiffrés sont désormais stockés dans des fichiers G64x.
  REMARQUE : Les dernières applications Security Center (5.8 GA et ultérieur) peuvent lire les anciens fichiers GEK créés avec la version 5.7 ou antérieure, mais les anciennes applications ne peuvent pas lire les nouveaux fichiers G64x protégés par mot de passe créés par la version 5.8 ou ultérieure.
- Les réexportations sont placées en file d'attente et démarrent lorsque l'exportation en cours prend fin.

Procédure

1. Procédez de l'une des manières suivantes :
   - Ouvrez un fichier vidéo précédemment exporté dans une tuile de tâche Surveillance.
   - Ouvrez l'outil Coffre-fort et sélectionnez le fichier que vous voulez ré-exporter.
2. Si vous réexportez le fichier dans une tuile de tâche Surveillance, procédez de l'une des manières suivantes :
   - Effectuez un clic droit sur la tuile, puis cliquez sur Caméra > Enregistrer sous.
   - Dans le widget Caméra, cliquez sur le bouton Enregistrer sous ().

3. Si vous réexportez un fichier depuis le Coffre-fort, sélectionnez le fichier et cliquez sur Enregistrer sous ( ).
4. Dans la boîte de dialogue Enregistrer sous, effectuez les opérations suivantes :
   a. Cliquez sur le réglage de date, heure ou durée.
   b. Dans la frise chronologique affichée, faites glisser les marqueurs de plage ( ) pour sélectionner la durée voulue.
   c. Pour régler la plage horaire, cliquez sur le widget Date-heure.



5. (Facultatif) Dans le champ Nom de fichier, donnez un nom au fichier vidéo.
   Par défaut, le nom du fichier inclut le nom de la caméra, la date et la durée de la séquence vidéo.
6. Dans le champ Format de fichier, sélectionnez un des formats d'exportation suivants :

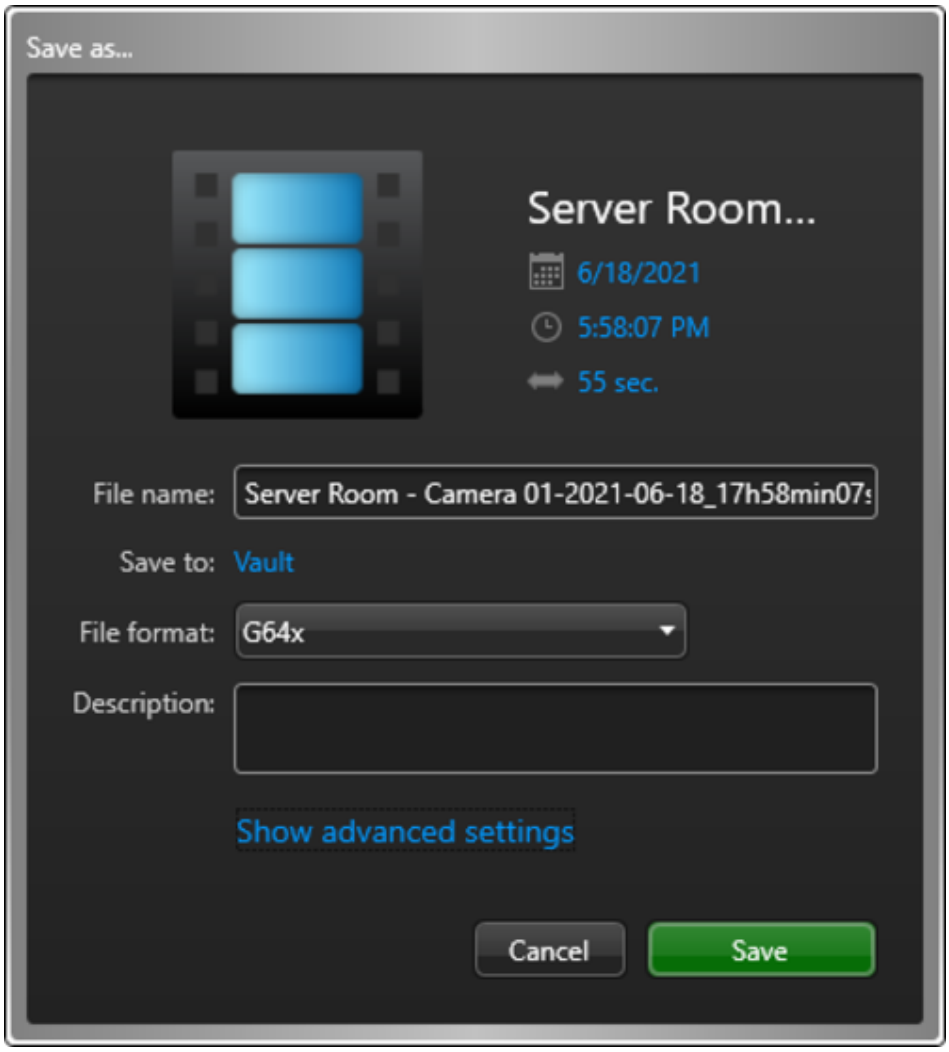
   G64x
   Fichier qui contient plusieurs séquences vidéo pouvant être lues dans Security Desk ou avec Genetec™ Video Player.

   G64 (mode compatibilité)
   Format Security Center qui peut être lu dans Security Desk ou avec Genetec™ Video Player.

   Advanced Systems Format
   Format propriétaire de Microsoft qui peut être lu avec Windows Media Player.

   MP4
   Format standard qui stocke le son et les vidéos et qui peut être lu sur de multiples lecteurs multimédias tels que Windows Media Player et QuickTime.

   REMARQUE : Les fichiers G64x ne peuvent pas être ré-exportés au format G64.
7. (Facultatif) Dans le champ Description, saisissez une description pour la vidéo exportée.
   La description s'affiche dans les rapports Historiques de configuration et dans les propriétés de fichier du Coffre-fort.
   REMARQUE : Une description doit être saisie pour les utilisateurs ne disposant pas du privilège *Exportation par un seul utilisateur*. Pour les autres utilisateurs, le champ est uniquement disponible si le format G64x est sélectionné et que l'option Inclure les propriétés supplémentaires pour exportation/instantané est activée dans l'onglet Avancé de l'utilisateur dans Config Tool.
8. Pour afficher les paramètres supplémentaires, cliquez sur Afficher les paramètres avancés et configurez-les comme requis.



a. SélectionnezEst protégé par mot de passe, puis saisissez un mot de passe pour chiffrer le fichier vidéo. Toute personne souhaitant consulter ce fichier doit saisir ce mot de passe.
b. (Facultatif) Sélectionnez Autoriser la réexportation du fichier vidéo.
Si vous sélectionnez cette option, la personne visionnant la vidéo exportée dans Security Desk ou Genetec™ Video Player peut la réexporter partiellement ou en totalité, au même format ou dans un format différent.

9. Cliquez sur Enregistrer.
La progression de l'exportation est affichée sur l'icône Conversion vidéo ( ) de la zone de notification.

Une fois l'exportation terminée, le fichier est disponible dans le Coffre-fort.

Lorsque vous avez terminé

Procédez de l'une des manières suivantes :

- Lancez la lecture des fichiers vidéo G64 et G64x en local sur votre ordinateur.
- Copiez les fichiers vidéo exportés pour les partager sur un autre ordinateur.

2.4.9 | Afficher les propriétés des fichiers vidéo

Vous pouvez consulter les propriétés des fichiers vidéo, comme leur nom, heure de début et de fin, taille du fichier, état de la protection, etc. dans le rapport *Détails de stockage d'archive*. Vous pouvez également modifier l'état de la protection des fichiers vidéo.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Détails de stockage d'archive.

2. Définissez les filtres de recherche pour votre rapport. Sélectionnez un ou plusieurs des filtres suivants :

Caméras
Sélectionnez la caméra à examiner.

Champs personnalisés
Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Heure de l'événement
Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

Type de support
Sélectionnez le type de support que vous recherchez :

Vidéo
Fichiers contenant des enregistrements vidéo.

Audio
Fichiers contenant des enregistrements audio.

Métadonnées
Fichiers contenant des métadonnées, comme des incrustations.

Type d'origine
Affinez votre recherche en sélectionnant l'origine des fichiers :

Téléchargé depuis le stockage interne de l'unité
Fichiers créés par la caméra, téléchargés depuis la caméra par un Archiveur et actuellement stockés sur le disque de ce dernier.

Copie depuis un autre Archiveur
Fichiers créés par un Archiveur et transmis à un autre.

Sur le stockage interne de l'unité
Fichiers créés par la caméra et actuellement stockés sur celle-ci.

Enregistré par l'Archiveur
Fichiers créés et actuellement stockés par un Archiveur.

Restauration depuis une sauvegarde
Fichiers restaurés depuis un jeu de sauvegarde hors ligne ; c'est-à-dire un fichier de sauvegarde contenant des archives qui n'ont pas été accessibles depuis Security Center avant leur restauration.

Source
Nom du système auquel appartient la caméra.

État
Sélectionnez les détails de fichiers vidéo que vous souhaitez examiner :

Non protégé
Fichiers vidéo qui ne sont pas protégés des routines de nettoyage de l'Archiveur. Ces fichiers peuvent être supprimés à l'expiration de leur période de rétention, ou lorsque l'Archiveur manque d'espace, selon les réglages de votre rôle Archiveur.

Protection à échéance
Fichiers vidéo dont vous avez supprimé la protection il y a moins de 24 heures.

Protégé
Fichiers vidéo qui sont protégés. Ils ne sont pas supprimés, même lorsque le disque est saturé. Vous pouvez également spécifier une date de fin de protection pour ces fichiers.

3. Cliquez sur Générer le rapport.
   Les fichiers vidéo associés aux caméras sélectionnées ainsi que leurs propriétés sont affichés dans le volet de rapport.
4. Pour afficher une séquence vidéo dans une tuile, cliquez deux fois sur un fichier vidéo, ou faites-le glisser du volet de rapport vers le canevas.
   La lecture de la séquence sélectionnée débute immédiatement.

Lorsque vous avez terminé

- Pour exporter une archive vidéo dans Security Desk, sélectionnez-la dans le volet de rapport, puis cliquez sur Exporter de la vidéo ( ).
- Pour supprimer un fichier vidéo, sélectionnez-le dans le volet de rapport, puis cliquez sur Supprimer ( ).
- Pour protéger une archive vidéo contre la suppression automatique, sélectionnez-la dans le volet de rapport, puis cliquez sur Protéger ( ).
- Pour déprotéger une archive vidéo, sélectionnez-la dans le volet de rapport, puis cliquez sur Annuler la protection ( ).

Explorer

- Protéger les fichiers vidéo contre l'effacement
- Présentation de la tâche Détails de stockage d'archive

2.4.9.1 | Colonnes du volet de rapport dans la tâche Détails de stockage d'archive

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Caméra
Nom de la caméra.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Lecteur
Le disque du serveur qui héberge le rôle Archiveur.

Heure de fin
Fin de la plage horaire, séquence d'enregistrement ou séquence vidéo.

Nom de fichier
Nom du fichier vidéo.

Taille du fichier
Taille du fichier vidéo.

Durée
Durée en heures, minutes et secondes de la séquence vidéo contenue dans le fichier vidéo.

Type de support
Type de contenu multimédia (vidéo, vidéo confidentielle, audio, métadonnées) contenu dans le fichier.

Type d'origine
L'origine du fichier :

Téléchargement depuis le stockage interne de l'unité
Fichiers créés par la caméra, téléchargés depuis la caméra par un Archiveur et actuellement stockés sur le disque de ce dernier.

Copie depuis un autre Archiveur
Fichiers créés par un Archiveur et transmis à un autre.

Sur le stockage interne de l'unité
Fichiers créés par la caméra et actuellement stockés sur celle-ci.

Enregistré par l'Archiveur
Fichiers créés et actuellement stockés par un Archiveur.

Restauration depuis une sauvegarde
Fichiers restaurés depuis un jeu de sauvegarde hors ligne ; c'est-à-dire un fichier de sauvegarde contenant des archives qui n'ont pas été accessibles depuis Security Center avant leur restauration.

État de la protection
État de la protection du fichier vidéo.

Serveur
Nom du serveur qui héberge ce rôle.

Source (entité)
Nom du système auquel appartient la caméra.

Heure de début
Début de la plage horaire, séquence d'enregistrement ou séquence vidéo.
Sujet parent : Afficher les propriétés des fichiers vidéo

2.4.10 | Protéger les fichiers vidéo contre l'effacement

Vous pouvez protéger les fichiers vidéo importants contre la suppression par le système lorsque l'espace de stockage de l'Archiveur est saturé, ou lorsque la période de rétention normale du fichier arrive à échéance.

À savoir

La vidéo peut être protégée contre la suppression. La protection est appliquée à tous les fichiers vidéo nécessaires au stockage de la séquence vidéo protégée. Puisqu'un fichier vidéo doit être protégé en entier, la longueur réelle de la séquence vidéo protégée dépend de la granularité des fichiers vidéo.

L'Archiveur ne peut pas protéger les fichiers partiels. Par conséquent, vous protégerez parfois un segment plus long que le segment voulu.

ATTENTION :
Une quantité trop importante de fichiers vidéo protégés sur un disque peut réduire l'espace disponible pour l'enregistrement de nouveaux fichiers. Pour éviter de gâcher de l'espace disque, vérifiez régulièrement le taux d'occupation des fichiers vidéo protégés sur chaque disque.

Pour libérer de l'espace de stockage, vous pouvez sauvegarder les fichiers vidéo protégés ou dupliquer les fichiers protégés sur un autre Archiveur avec *transfert d'archive*, puis déprotéger les fichiers vidéo d'origine.

Procédure

1. Ouvrez la tâche Détails de stockage d'archive.
2. Créez votre rapport.
   Les fichiers vidéo associés aux caméras sélectionnées sont affichés dans le volet de rapport.
3. Dans le volet de rapport, sélectionnez le fichier vidéo à protéger, puis cliquez sur Protéger ( ).
   Pour sélectionner plusieurs fichiers vidéo, appuyez sur les touches Ctrl ou Maj.
4. Dans la boîte de dialogue Protéger les archives, spécifiez l'heure de début et l'heure de fin de la vidéo à protéger.

5. Sélectionnez la durée de protection du fichier vidéo avec l'une des options suivantes :

   Indéfiniment
   Pas de date de fin. Vous devez supprimer la protection manuellement en sélectionnant la vidéo dans le volet de rapport, puis en cliquant sur Annuler la protection ( ).
   REMARQUE : Lorsque la période de rétention est dépassée, les fichiers vidéo déprotégés ne sont pas supprimés immédiatement. Vous avez 24 heures pour restaurer la protection vidéo. Pour en savoir plus sur le stockage d'archives, voir le *Guide de l'administrateur Security Center*.

   Pendant x jours
   Le fichier vidéo est protégé durant le nombre de jours sélectionné.

   Jusqu'au
   Le fichier vidéo est protégé jusqu'à la date spécifiée.

6. Cliquez sur Protéger.

Résultats

Le fichier vidéo est protégé.

2.4.11 | Chiffrer les fichiers vidéo exportés

Pour protéger les fichiers vidéo exportés, vous pouvez créer des versions protégées par mot de passe des fichiers, puis supprimer les fichiers non protégés.

À savoir

Vous pouvez également choisir de protéger toutes les vidéos exportées par mot de passe par défaut, ou de chiffrer les fichiers au moment de l'exportation.

Procédure

1. Sur la page d'accueil, procédez de l'une des manières suivantes :
   - Cliquez sur Outils > Coffre-fort.
   - Ouvrez la tâche Explorateur de fichiers vidéo et sélectionnez le dossier qui contient le fichier vidéo G64 non chiffré.
2. Sélectionnez le fichier vidéo chiffré, puis cliquez sur Chiffrer les fichiers ( ).
   REMARQUE : Pour sélectionner plusieurs fichiers vidéo, appuyez sur les touches Ctrl ou Maj.
3. Dans la boîte de dialogue Réglages de chiffrement, sélectionnez un dossier de Destination.
4. Entrez un Mot de passe fort, confirmez-le, puis cliquez sur Chiffrer.
   Une version chiffrée du fichier sélectionné est créée.
5. (Facultatif) Pour renforcer la sécurité, supprimez le fichier non chiffré d'origine.
   Dans le coffre-fort, faites un clic droit sur le fichier d'origine et cliquez sur Supprimer.

Explorer

- Configurer les réglages d'exportation vidéo
- Exporter de la vidéo

2.5 | Options vidéo dans Security Desk

2.5.1 | Configurer une manette de jeu

Vous pouvez configurer n'importe quelle manette de jeu (ou autre contrôleur avec au moins un axe de mouvement) reliée à votre ordinateur, afin de contrôler l'affichage des caméras dans Security Desk.

Avant de commencer

Connectez une manette à votre ordinateur.

BONNE PRATIQUE : Ne connectez pas deux manettes d'un même modèle. Elles sont présentées avec le même nom, et vous risquez de ne pas pouvoir les distinguer. En outre, vous ne pouvez avoir qu'une seule manette active à la fois.

À savoir

Vous pouvez affecter deux commandes Security Desk différentes à chaque bouton : l'une à l'événement bouton enfoncé et l'autre à l'événement bouton relâché. La *Commande enfoncée* est facultative. Le nombre de boutons que vous pouvez configurer dépend du type de manette.

La valeur de Zone morte de la manette détermine la quantité de mouvement nécessaire avant de déplacer la caméra PTZ. Lorsque vous ramenez la manette à sa position d'origine, cette valeur détermine la proximité à la position d'origine nécessaire pour que la caméra PTZ cesse de bouger.

Les réglages de manette s'appliquent au poste Security Desk local pour tous les utilisateurs.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Périphériques.
2. Cliquez sur l'onglet Manette.
3. Dans la liste déroulante Manette active, sélectionnez la marque et le modèle de votre manette.
   Vous pouvez cliquer sur à tout moment pour actualiser la liste.
   Tous les axes pris en charge par votre manette sont affichés.
4. (Facultatif) Pour importer une configuration de manette préalablement enregistrée, cliquez sur Importer.
5. Pour associer les commandes d'axe aux commandes PTZ de votre choix, procédez de la manière suivante :
   a. Sélectionnez un Axe dans la liste.
   b. Dans la liste déroulante de la colonne Commandes, sélectionnez une commande de PTZ.
   c. Pour inverser la commande, sélectionnez l'option dans la colonne Inverser.
      Si vous avez associé la commande *Inclinaison* à l'axe des Y et que vous inversez les commandes, la caméra se déplace vers le haut lorsque vous tirez la manette vers vous et vers le bas lorsque vous poussez la manette vers

l'avant.

d. Pour effacer l'association sélectionnée, cliquez sur Effacer ( ).

6. Pour associer les boutons de la manette aux commandes Security Desk de votre choix, procédez de la manière suivante :
   a. Sélectionnez un Bouton dans la liste.
   b. Pour associer une commande à un événement bouton enfoncé, sélectionnez une commande dans la liste déroulante de la colonne Commande enfoncée.
   c. Pour associer une commande à un événement bouton relâché, sélectionnez une commande dans la liste déroulante de la colonne Commande relâchée.
   d. Si la commande sélectionnée requiert un argument, comme la sélection d'un réglage PTZ prédéfini, ajoutez-le dans le champ Args.
7. Pour effacer les associations sélectionnées et recommencer, cliquez sur Effacer ( ).
8. Pour définir le seuil de détection de mouvement relatif à la position d'origine, ou zone au repos, spécifiez un pourcentage dans l'option Zone morte de la manette.
9. Pour enregistrer la configuration de la manette sur disque, cliquez sur Exporter.
10. Cliquez sur Enregistrer.

2.5.2 | Configurer un clavier CCTV

Vous pouvez configurer n'importe quel clavier CCTV (par exemple, un Axis T8310 Video Surveillance Control Board) relié à votre ordinateur, afin de contrôler l'affichage des caméras dans Security Desk.

Avant de commencer

Connectez un clavier CCTV à votre ordinateur.

À savoir

Une fois que vous avez connecté un clavier CCTV, vous pouvez contrôler les caméras PTZ, basculer entre les caméras, contrôler la lecture et ainsi de suite avec le clavier, plutôt qu'avec la souris.

Les réglages de clavier CCTV s'appliquent au poste Security Desk local pour tous les utilisateurs.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Périphériques > Clavier.
2. Dans la liste déroulante Protocole du clavier, sélectionnez la marque et le modèle de votre clavier CCTV.
3. Dans la section Port série, configurez les caractéristiques du port série auquel le clavier CCTV est connecté.
   Cela n'est nécessaire que pour certains claviers CCTV. Suivez les indications fournies par le fabricant du clavier.
4. Pour vous connecter automatiquement au clavier CCTV au démarrage de Security Desk, sélectionnez l'option Connexion automatique au clavier.
   Si vous désactivez cette option, vous devez connecter le clavier manuellement à chaque fois que vous souhaitez l'utiliser.
5. Cliquez sur Connexion.
   Pour certains claviers CCTV, l'état de la connexion est affiché dans la section État du clavier.
6. Pour déconnecter le clavier CCTV, cliquez sur Options > Périphériques > Clavier > Déconnecter.

2.5.3 | Personnaliser les options de flux vidéo

La boîte de dialogue Options vous permet de personnaliser les options de flux vidéo, comme le flux par défaut pour l'affichage de la vidéo en direct, la source d'archivage par défaut pour afficher la vidéo enregistrée et l'affichage de messages concernant les flux.

À savoir

Les options Flux en temps réel et Source de lecture s'appliquent au poste Security Desk local pour tous les utilisateurs. L'option Afficher un avertissement si la sélection du flux n'est pas automatique est enregistrée dans votre profil utilisateur.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Vidéo > Options par défaut.
2. Dans la liste déroulante Flux en temps réel, sélectionnez le flux vidéo par défaut pour la vidéo en temps réel.

   En direct
   Flux par défaut utilisé pour afficher la vidéo en direct.

   Enregistrement
   Flux enregistré par l'Archiveur pour une analyse différée.

   Distant
   Flux utilisé pour la vidéo en direct lorsque la bande passante est limitée.

   Basse résolution
   Flux utilisé à la place du flux *en direct* lorsque la tuile utilisée pour afficher le flux dans Security Desk est petite.

   Haute résolution
   Flux utilisé à la place du flux *en direct* lorsque la tuile utilisée pour afficher le flux dans Security Desk est grande.

   Automatique
   Security Desk utilise le flux *Basse résolution* ou *Haute résolution* en fonction de la taille de la tuile.

3. Dans la liste déroulante Source de lecture, sélectionnez la source d'archivage par défaut pour afficher la vidéo enregistrée.

   Toute source de lecture
   Déléguez au système le choix de la source d'archivage à utiliser.

   Archiveur
   Vidéo enregistrée par l'Archiveur.

   Archiveur auxiliaire
   Vidéo enregistrée par l'Archiveur auxiliaire.

   Toute source de lecture fédérée
   Déléguez au système le choix de la source d'archivage fédéré à utiliser.

   Archiveur fédéré
   Vidéo enregistrée par l'Archiveur fédéré.

   Archiveur auxiliaire fédéré
   Vidéo enregistrée par l'Archiveur fédéré auxiliaire.

   Lecture sur périphérique
   Vidéo enregistrée sur un périphérique.

4. Cliquez sur l'onglet Interaction utilisateur.
5. Pour recevoir un message d'avertissement lorsque la résolution de l'image vidéo affichée dans la tuile est trop grande et que la sélection de flux vidéo n'est pas *Automatique*, sélectionnez l'option Afficher un avertissement si la sélection du flux n'est pas automatique.
   Le message qui apparaît indique que vous devez régler le flux vidéo sur *Automatique*.
6. Cliquez sur Enregistrer.

2.5.4 | Configuration du nettoyage automatique du Coffre-fort

Vous pouvez configurer la suppression automatique des fichiers antérieurs à un nombre défini de jours.

Avant de commencer

Assurez-vous que votre compte utilisateur Windows dispose des privilèges de suppression des fichiers dans le dossier Coffre-fort.

À savoir

- Les fichiers du coffre-fort sont supprimés automatiquement uniquement si l'option Nettoyage automatique est activée.
- Seuls les types de fichiers suivants peuvent être supprimés automatiquement :
  - Images : .png, .jpg, .bmp et .gif
  - Vidéos : .g64, .g64x, .gek, .asf, .asx et .mp4

  Les dossiers ne sont pas supprimés du Coffre-fort.
- Le système recherche les fichiers à supprimer lors de la connexion à Security Desk, puis à toutes les heures suivantes. Les fichiers ne peuvent pas être supprimés s'ils sont ouverts lors d'une vérification.

Procédure

1. Sur la page d'accueil de Security Desk, cliquez sur Options > Vidéo.
2. Dans la section Coffre-fort, définissez l'option Nettoyage automatique sur Activé, puis entrez une période de rétention de 1 à 999 jours.
3. Cliquez sur Enregistrer.

2.5.5 | Options vidéo dans Security Desk

Une fois familiarisé avec l'utilisation des vidéos dans Security Center, vous pouvez personnaliser la gestion vidéo dans le système via l'onglet Vidéo de la boîte de dialogue Options.

Temps de recul, options

Sélectionnez les valeurs par défaut lorsque vous parcourez la vidéo. Ces réglages sont conservés dans votre profil utilisateur.

Décalage de lecture
Lorsque vous affichez un événement dans une tuile, cette valeur spécifie la quantité de vidéo, en secondes, qui est lue en amont de l'événement. La valeur de décalage par défaut est de 15 secondes. Vous pouvez spécifier une valeur comprise entre 0 et 90 secondes.
REMARQUE : Si l'option *Durée d'enregistrement avant un événement* dans Config Tool a une valeur inférieure au temps de recul, vous n'obtiendrez pas forcément de vidéo. Demandez la valeur de *Durée d'enregistrement avant un événement* à votre administrateur.

Durée de lecture
Lorsque vous affichez un événement dans une tuile, cette valeur spécifie la quantité de vidéo, en secondes, qui est lue. Si vous exportez l'événement, cette valeur détermine la longueur de la séquence vidéo exportée.

Saut avant/arrière
Détermine la longueur du saut avant ou arrière au sein d'un enregistrement vidéo lorsque vous cliquez sur les boutons Saut arrière () ou Saut avant () dans le widget Caméra.

Options par défaut

Sélectionnez les valeurs par défaut pour la lecture vidéo. Ces réglages s'appliquent au poste Security Desk local pour tous les utilisateurs.

Flux en direct
Flux vidéo à demander pour afficher la vidéo en direct.

Source de lecture
La source vidéo prioritaire en cas de demande de lecture d'enregistrement vidéo.

Afficher les surimpressions
Activez cette option pour afficher les incrustations vidéo par défaut.

Options de cache vidéo

Le cache vidéo sert à mettre en cache les flux vidéo reçus par Security Desk. La vidéo enregistrée est mise en mémoire tampon avant le démarrage de la lecture pour assurer la disponibilité d'une quantité de vidéo suffisante. Le cache aide à réduire le nombre de transmissions de la vidéo et assure un accès plus rapide à la vidéo enregistrée, une lecture arrière plus fluide et des vitesses de lecture supplémentaires. Le cache est vidé à la fermeture de Security Desk ou de votre session.

Ces réglages s'appliquent au poste Security Desk local pour tous les utilisateurs.

Emplacement du cache
Sélectionnez l'emplacement de stockage du cache. Vous pouvez utiliser le dossier par défaut proposé par Windows ou spécifier celui de votre choix.

Taille maximale
Définir la taille du cache.

Mise en cache vidéo en direct
Les flux vidéo en direct sont mis en cache séparément de la vidéo enregistrée. Lorsque l'emplacement du cache est indisponible, la vidéo en direct n'est pas affectée.

Vider le cache à la déconnexion
Activez cette option pour effacer le cache à la déconnexion de Security Desk.

Vider le cache
Cliquez pour effacer le cache maintenant.

Options avancées

Ces réglages vidéo avancés s'appliquent au poste local et affectent Security Desk et Config Tool pour tous les utilisateurs.

REMARQUE : Lorsque vous modifiez les options avancées, vous devez redémarrer Security Desk.

Délai de mémoire tampon antisaccade
La Mémoire tampon antisaccade sert à empêcher les problèmes de rendu des flux vidéo entraînés par les variations de débit sur le réseau, et à fournir une vidéo plus fluide en cas de transmission irrégulière d'images vidéo de la source. Il est recommandé d'utiliser une taille minimale pour éviter des effets secondaires, comme des retards lors de la manipulation PTZ ou une attente exagérée au démarrage d'un flux vidéo.

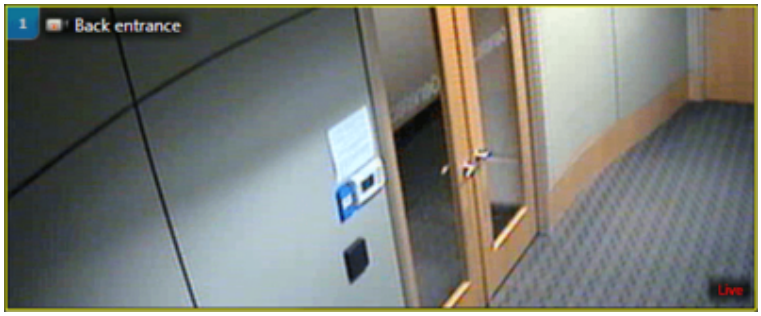
Activer le désentrelacement
Sélectionnez cette option pour réduire l'effet de brèches lors des mouvements.

Activer la dégradation de la qualité vidéo
Sélectionnez cette option pour empêcher Security Desk de consommer trop de temps processeur sur votre ordinateur en réduisant le débit d'images de la vidéo affichée. Lorsque l'utilisation du processeur dépasse 90 %, Security Desk diminue le débit d'image affiché sur le canevas, en commençant avec la tuile 1. Les flux MJPEG sont réduits jusqu'à 5 i/s ou moins, tandis que les flux vidéo qui utilisent d'autres types de compression n'affichent plus que les images clés. Les tuiles vidéo affectées par cette option sont signalées par une icône clignotante ( ). Pour rétablir le débit normal de votre vidéo, videz la tuile puis restaurez son contenu (dans le widget de tuile, cliquez sur , puis sur).
REMARQUE : Lorsque vous modifiez le contenu affiché sur le canevas, Security Desk recommence à réduire le débit vidéo, en partant de la tuile N°1.

Tuile de caméra
Sélectionnez la manière d'afficher les caméras dans les tuiles.

Afficher l'image entière (avec barres)
Des barres noires peuvent apparaître autour de l'image si ses proportions ne correspondent pas aux proportions de la tuile.

Remplir la tuile (rogner)
L'image vidéo remplit la tuile. L'image peut être rognée si ses proportions ne correspondent pas à celles de la tuile.



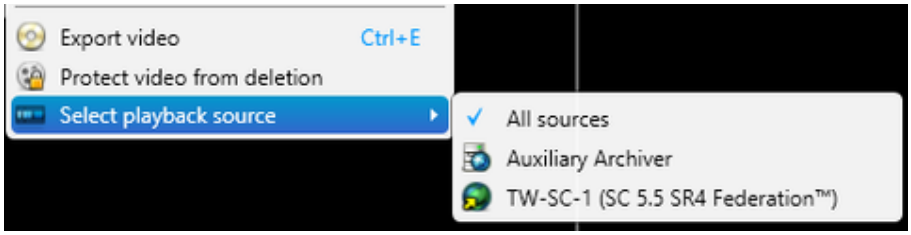
Mode audio
Sélectionnez le mode audio.

Bidirectionnel simultané
Permet de parler et d'écouter en même temps.

Bidirectionnel alternatif (PTT)
Ne permet pas de parler et d'écouter en même temps. Lorsque vous cliquez sur le bouton *Parler* ( ) dans le widget Caméra, le bouton *Écouter* ( ) est désactivé. Le mode bidirectionnel à l'alternat est nécessaire lorsque deux unités sont connectées, ou lorsque les données audio doivent être contrôlées par le biais d'entrées numériques.

Type de filtre de lecture (menu contextuel)
Indiquez la manière dont Security Desk doit demander la source de lecture sélectionnée par l'utilisateur.

Source de streaming
(Valeur par défaut) L'utilisateur sélectionne le rôle qui doit diffuser la vidéo. Security Desk n'interroge que les serveurs qui hébergent le rôle sélectionné. Avec cette option, l'utilisateur peut constater des blancs dans la vidéo si des parties de l'archive vidéo ont été déplacées (transférées) vers d'autres rôles.



Source originale de l'archive
L'utilisateur sélectionne les rôles qui ont enregistré la vidéo. Security Desk interroge tous les rôles qui ont une copie de la vidéo d'origine enregistrée par le rôle sélectionné. Avec cette option, l'utilisateur ne verra pas de blancs dans la vidéo, même si des parties de l'archive vidéo ont été transférées vers d'autres rôles.

Accélération matérielle
Activez cette option pour permettre à Security Desk de déléguer le décodage vidéo du processeur vers les cartes vidéo. Pour afficher les cartes vidéo installées sur votre ordinateur, cliquez sur Afficher les informations matérielles. Suivez également ces conseils pour optimiser les performances de décodage vidéo.

Optimisation du délai d'affichage
Activez cette option pour réduire le délai d'affichage d'un groupe de caméras Lorsque vous activez cette fonctionnalité dans Security Desk, vous devez sélectionner une séquence de caméras dans la liste de Délai d'affichage de caméra. Security Desk diffuse en continu de la vidéo en direct depuis les caméras sélectionnées, ce qui permet un accès plus rapide à la vidéo. REMARQUE : L'activation de cette fonctionnalité taxe le système, entraînant une augmentation de la consommation de bande passante sur les serveurs de redirection et une augmentation des demandes de flux auprès du serveur de l'Archiveur.
Explorer

- Personnalisation des options d'instantané dans Security Center
- Configurer les réglages d'exportation vidéo

3 | Présentation du contrôle d'accès dans Security Desk

3.1 | Présentation rapide du contrôle d'accès dans Security Desk

3.1.1 | À propos de Security Center Synergis™

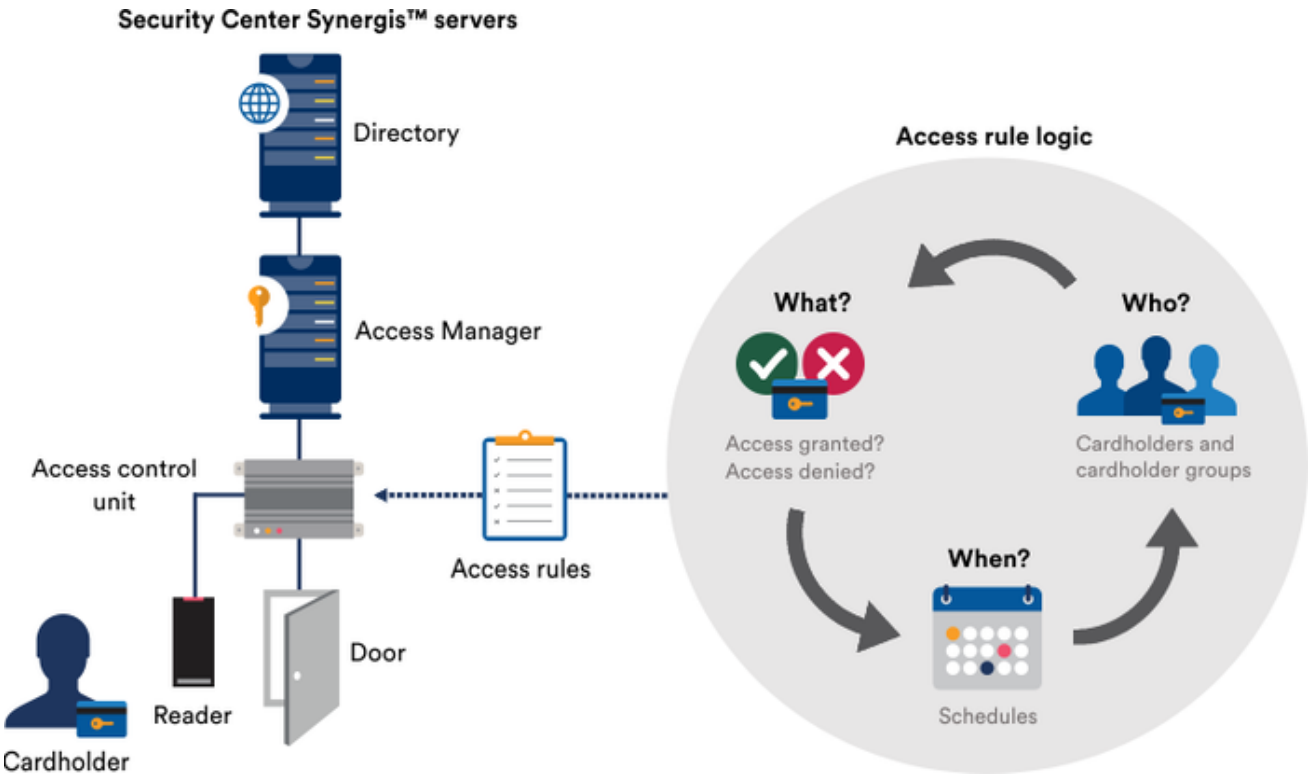
Security Center Synergis™ est le système de contrôle d'accès (SCA) sur IP qui renforce la sécurité physique de votre organisation ainsi que votre capacité à réagir aux menaces. Prenant en charge un éventail en constante évolution de dispositifs tiers de contrôle de porte et de verrous électroniques, il vous permet d'exploiter vos investissements existants en matière d'équipements réseau et de sécurité.

Synergis™ est conçu sur la base d'une architecture ouverte et distribuée. Bâtissez votre système avec de nouveaux lecteurs IP ou utilisez ceux que vous avez déjà. Intégrez votre système de contrôle d'accès avec des systèmes d'autres fournisseurs, tels que ceux de détection d'intrusion ou de gestion d'immeubles, et distribuez les composants serveur de Synergis™ sur plusieurs machines du réseau pour optimiser la bande passante et la charge de travail.

Synergis™ *Enterprise* peut prendre en charge un nombre illimité de portes, de contrôleurs et de postes de travail client. Vous pouvez faire croître votre système porte par porte, ou étendre votre système sur plusieurs bâtiments avec la fonction Federation™.

Fonctionnement de Synergis™

Synergis™ est doté d'une architecture basée sur le rôle de serveur appelé *Gestionnaire d'accès*, qui gère les contrôleurs physiques de porte.



Vous trouverez ci-dessous une description générale du fonctionnement de l'architecture de Synergis™ :

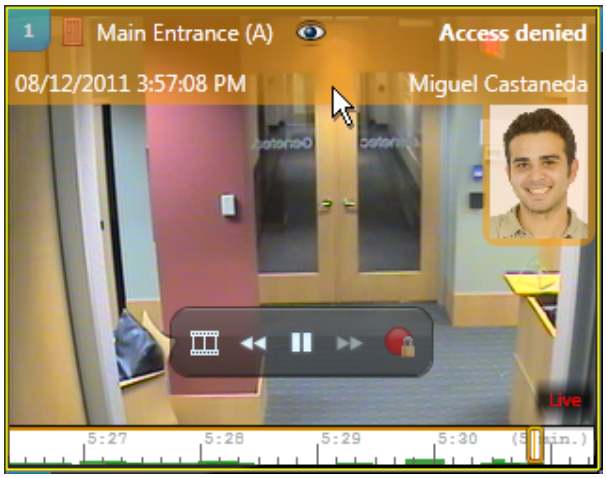
- Les configurations système sont enregistrées par le rôle Répertoire.
- Le Répertoire transmet les configurations au Gestionnaire d'accès.
- Le rôle Gestionnaire d'accès communique directement avec les contrôleurs de porte physiques (ou unités de contrôle d'accès) par TCP/IP.
- Le rôle Gestionnaire d'accès envoie les horaires, les données de titulaires de cartes ainsi que les règles d'accès aux contrôleurs de porte.
- Lorsqu'un titulaire de cartes présente son identifiant à un lecteur, le contrôleur consulte la règle d'accès pour savoir s'il doit accorder ou refuser l'accès.
- Une fois que les contrôleurs ont été synchronisés avec le Gestionnaire d'accès, ils peuvent fonctionner de façon autonome, même en cas de perte de connexion au Gestionnaire d'accès.

Avec des configurations supplémentaires, un titulaire de cartes peut appartenir à un groupe de titulaires de cartes, ou une porte peut être intégrée à un secteur, et plusieurs horaires et règles peuvent être envoyés vers une unité.

3.1.2 | Affichage des événements d'accès dans les tuiles

Un événement d'accès (*Accès autorisé*, *Accès refusé : Code PIN non valable* , et ainsi de suite) est un événement impliquant un *point d'accès*. Lorsqu'un événement d'accès survient pour une entité surveillée, les informations associées à l'événement sont affichées dans une tuile de la tâche *Surveillance*.

La figure suivante est un exemple d'événement Accès refusé. La description d'événement est affichée en haut de la tuile dans la zone de couleur en incrustation. D'autres informations comme la date et l'heure de l'événement et le nom du titulaire de cartes sont affichées lorsque vous survolez la zone colorée. Vous pouvez également agrandir la photo du titulaire de cartes en survolant l'image. Cela permet par exemple de comparer la photo du titulaire de cartes avec le visage que vous voyez dans la vidéo.



Fonctionnement de l'antiretour

Une *violation antiretour* survient lorsqu'un titulaire de cartes entre dans un secteur qu'il n'a jamais quitté ou lorsqu'il quitte un secteur dans lequel il n'est jamais entré. Cela peut survenir lorsqu'un titulaire de cartes autorisé déverrouille une porte, puis passe sa carte à une autre personne en entrant.

L'administrateur Security Center peut configurer le système pour refuser l'accès au titulaire de cartes. Lorsque cette situation se produit, vous devez cliquer sur le bouton Pardonner une violation antiretour ( ) pour autoriser le titulaire de cartes à entrer ou sortir.

3.2 | Titulaires de cartes et visiteurs dans Security Center dans Security Desk

3.2.1 | À propos des titulaires de cartes

Type d'entité qui représente un individu autorisé à pénétrer et à quitter des secteurs sécurisés en fonction de ses identifiants (généralement des cartes d'accès), et dont les activités peuvent être surveillées. Ils correspondent au *qui* dans le cadre d'une règle d'accès.

Groupes de titulaires de cartes

L'entité *groupe de titulaires de cartes* sert à configurer des *droits d'accès* et des propriétés communs à un ensemble de titulaires de cartes.

Dans le cadre d'un système de contrôle d'accès de taille importante, les titulaires de cartes et les règles d'accès sont bien plus faciles à gérer quand les titulaires de cartes sont membres de groupes de titulaires.

3.2.2 | Affichage des titulaires de cartes sur le canevas de Security Desk

Les titulaires de cartes représentent des individus, comme des employés, autorisés à pénétrer et quitter des secteurs sécurisés à l'aide de cartes d'accès, et dont les activités peuvent être surveillées.

Pour afficher les informations sur un titulaire de cartes, faites glisser un événement associé aux titulaires depuis le volet de rapport des tâches Droits d'accès de titulaire de cartes ou Configuration de titulaires de cartes vers une tuile du canevas.

A	Nom du titulaire de cartes.
B	Affiche des informations complémentaires.
C	Photo du titulaire de cartes.
D	Détails du titulaire de carte.

3.2.3 | Créer des titulaires de cartes

La tâche Gestion des titulaires de cartes vous permet d'ajouter les nouveaux employés qui doivent pouvoir accéder à des secteurs sécurisés avec des cartes d'accès, et de suivre leurs activités.

Avant de commencer

- Pour ajouter des informations personnalisées aux titulaires de cartes, créez des champs personnalisés dans Config Tool (voir le *Guide de l'administrateur Security Center*).
- Créez des groupes de titulaires de cartes dans Config Tool si vous souhaitez affecter des droits d'accès différents à différents groupes de titulaires de cartes (voir le *Guide de l'administrateur Security Center*).
- Pour modifier le niveau d'accès d'un titulaire de carte, vous devez disposer des privilèges *Modifier les options du titulaire de carte* et *Modifier le niveau d'accès*.

Procédure

1. Ouvrez la tâche Gestion des titulaires de cartes, et cliquez sur Nouveau ( ).
2. En haut de la boîte de dialogue, entrez le nom et le prénom du titulaire de cartes.
3. Pour affecter une photo au titulaire de cartes, cliquez sur la silhouette et choisissez l'une des options suivantes :

   Charger depuis un fichier
   Choisir une image à partir du disque. Les principaux formats d'image sont pris en charge.

   Charger depuis une webcam
   Prendre une photo avec une webcam. Cette option n'apparaît que si votre poste est équipé d'une webcam.

   Charger depuis une caméra
   Prendre une photo avec une caméra gérée par Security Center. Lorsque vous cliquez sur Charger depuis une caméra, une boîte de dialogue de capture distincte apparaît. Sélectionnez la source vidéo, et cliquez sur Prendre un instantané ( ).

Charger depuis le presse-papiers
Charger l'image copiée dans le presse-papiers. Cette option n'apparaît que si vous utilisez la commande Copier de Windows pour placer une image dans le presse-papiers.

4. Si vous souhaitez modifier l'image, cliquez sur celle-ci pour ouvrir l'*Éditeur d'image*, et utilisez les outils de modification en haut de la boîte de dialogue.
5. Dans la section État, procédez de la manière suivante :

État
Réglez l'état sur *Actif* ou *Inactif*. Pour que les identifiants fonctionnent et qu'ils puissent accéder à un secteur, leur état doit être réglé sur *Actif*.

Activation
Spécifiez la modalité d'activation de leur profil :

Jamais
(Disponible après la désactivation d'un titulaire de cartes) La date et l'heure du clic sur Nouveau () pour créer le titulaire de cartes.

Date spécifique
Expire à une date et heure particulières.

Expiration
Spécifiez un délai d'expiration pour le profil :

Jamais
N'expire jamais.

Date spécifique
Expire à une date et heure particulières.

Expiration après la première utilisation
Expire un certain nombre de jours après sa première utilisation.

En cas d'inutilisation
Expire s'il n'a pas été utilisé durant un certain nombre de jours.

6. Affectez un identifiant au titulaire de cartes pour qu'il puisse accéder aux secteurs sécurisés.
   REMARQUE : Vous pouvez affecter un identifiant maintenant ou une fois que tous les identifiants ont été inscrits au sein du système.
7. Affectez le titulaire de cartes à un groupe de titulaires de cartes.
   REMARQUE : Un titulaire de cartes peut appartenir à plusieurs groupes de titulaires de cartes.
   a. Pour affecter le premier groupe de titulaires de cartes, cliquez sur la liste déroulante Groupe de titulaires de cartes et sélectionnez un groupe.
   b. Pour affecter des groupes de titulaires de cartes supplémentaires, cliquez sur Avancé (), puis cliquez sur Ajouter un élément (). Dans la boîte de dialogue qui apparaît, sélectionnez les groupes de titulaires de cartes et cliquez sur OK.
8. Entrez l'adresse e-mail du titulaire de cartes.
   Une adresse e-mail valable est nécessaire si vous voulez affecter des *identifiants mobiles* au titulaire de cartes.
9. (Facultatif) Lorsque des champs personnalisés sont définis pour les titulaires (service, numéros de téléphone, et ainsi de suite), saisissez les informations personnalisées dans les champs correspondants.
10. (Facultatif) Dans la section Avancé, configurez les propriétés de titulaire de cartes suivantes :
    REMARQUE : Certaines de ces propriétés peuvent être héritées des groupes de titulaires de cartes parents. Lorsqu'une valeur particulière est spécifiée pour le titulaire de cartes, cliquez sur Rétablir la valeur héritée () pour récupérer la propriété des groupes de titulaires de cartes parents. Si le titulaire appartient à plusieurs groupes de titulaires de cartes, il hérite du niveau d'accès le plus élevé.
    a. Si un identifiant a été affecté au titulaire de cartes, accordez des privilèges d'accès au titulaire :

Utiliser le délai d’accès prolongé
Lorsque le paramètre *Délai d'accès prolongé* est défini pour une porte, l'usager dispose de plus de temps pour la franchir. Utilisez cette option pour les personnes à mobilité réduite.

Contourner les règles d’antiretour
Exempte le visiteur de toutes les restrictions antiretour.

Peut escorter les visiteurs
Indique si le titulaire de cartes peut agir en tant qu’hôte de visiteur.

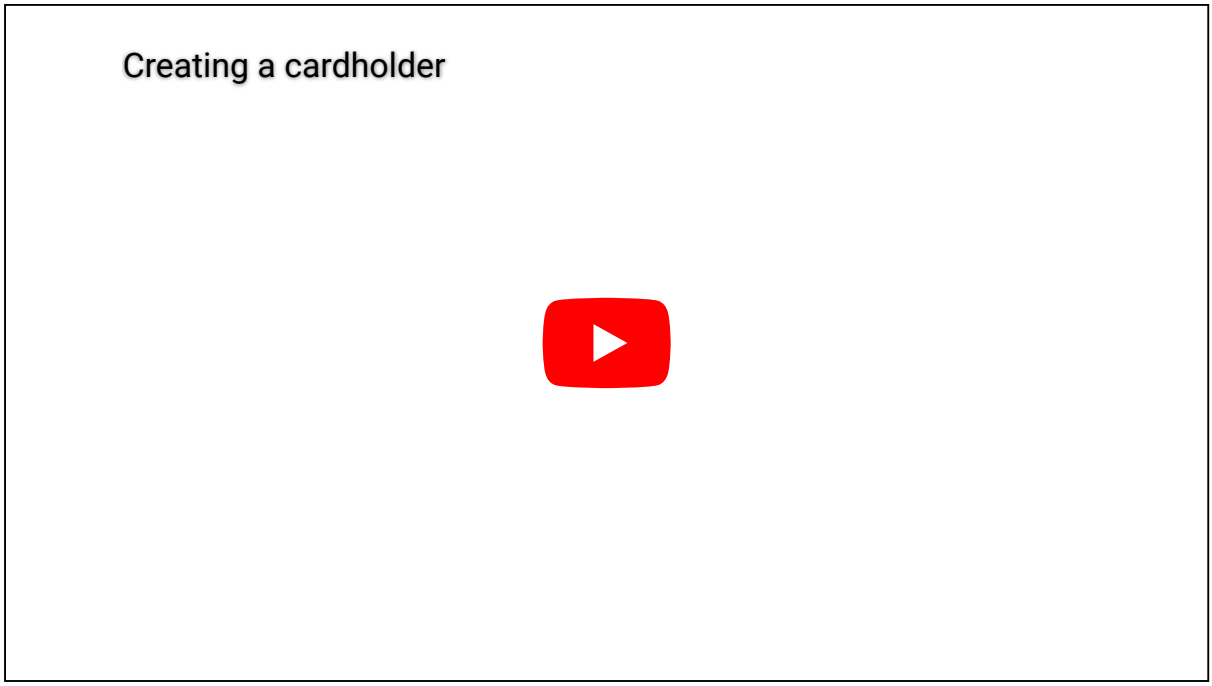
Pour en savoir plus sur la configuration des secteurs et des portes avec les règles de délai d'accès prolongé et d'antiretour, voir le *Guide de l'administrateur Security Center*.

b. Dans la section Niveau d'accès, sélectionnez le niveau d'accès du titulaire de cartes. Le niveau d'accès définit ses droits d'accès aux secteurs lorsqu'un niveau de risque est activé dans Security Center. Le Niveau 0 est le niveau d'accès le plus élevé, qui confère le plus de privilèges.
c. Dans le champ Nom de l'entité, donnez un nom à l'entité titulaire de cartes si vous ne souhaitez pas utiliser le nom du titulaire.
Par défaut, le Nom de l’entité utilise les champs Prénom et Nom.
d. Décrivez le titulaire de cartes dans le champ Description.
e. Affectez le titulaire de cartes à une partition.
Les partitions déterminent quels utilisateurs Security Center ont accès à cette entité. Seuls les utilisateurs ayant accès à la partition peuvent voir le titulaire de cartes.

11. Cliquez sur Enregistrer.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l’icône Sous-titres (CC) pour activer les sous-titres dans l’une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s’affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



Explorer

- Rogner une photo
- Appliquer un arrière-plan transparent à une photo
- Présentation de la tâche Gestion des titulaires de cartes

3.2.3.1 | Affecter des règles d'accès aux titulaires de cartes

Pour accorder ou refuser l'accès aux secteurs, portes et ascenseurs, vous devez affecter des règles d'accès aux titulaires de cartes.

Avant de commencer

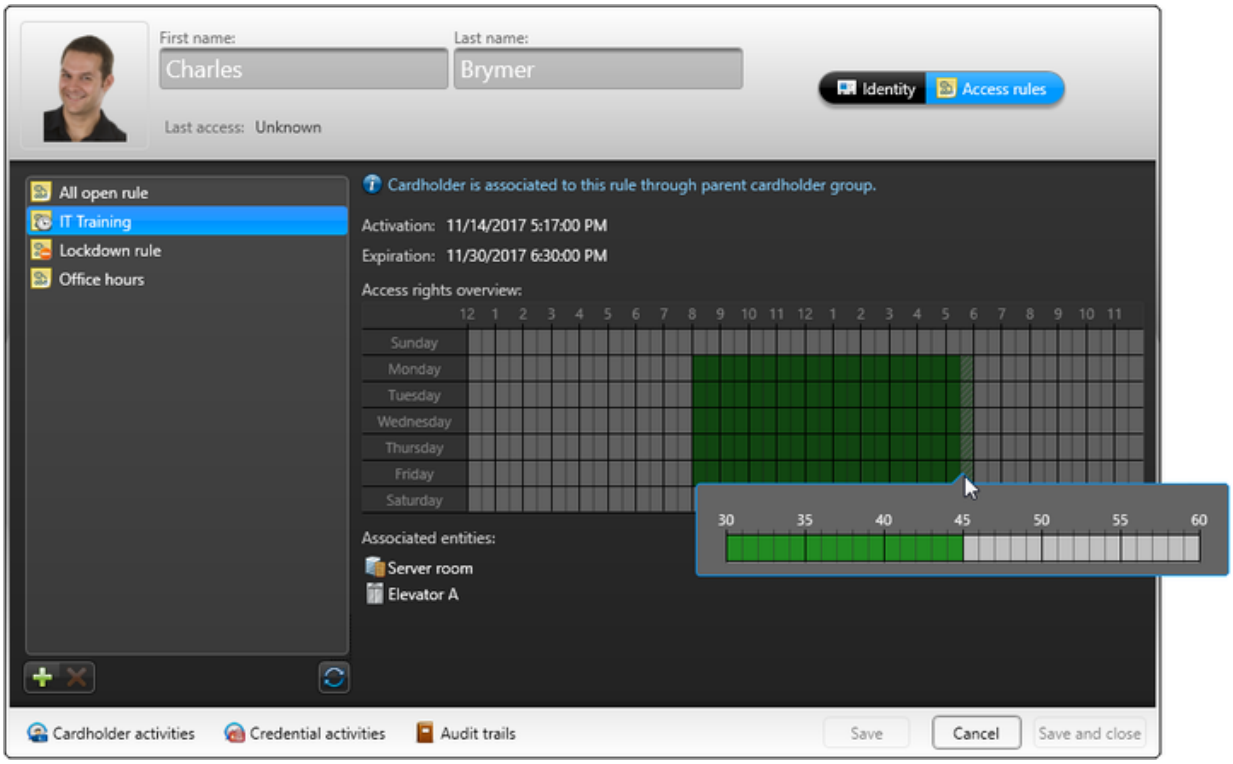
Créez des règles d'accès dans Config Tool (voir le *Guide de l'administrateur Security Center*).

À savoir

Vous pouvez affecter les règles d'accès lors de la création des titulaires de cartes, ou après leur création. Dans la procédure suivante, le titulaire de cartes a déjà été créé.
BONNE PRATIQUE : Affectez des règles d'accès aux groupes de titulaires de cartes plutôt qu'aux titulaires de cartes individuels. N'affectez des règles d'accès aux titulaires de cartes individuels qu'à titre temporaire. Si vous l'utilisez trop souvent, le système de contrôle d'accès peut rapidement devenir ingérable. Pour accorder un accès temporaire ou à court terme à un titulaire de cartes, créez une *règle d'accès temporaire*.

Procédure

1. Dans la tâche Gestion des titulaires de cartes, sélectionnez un titulaire, puis cliquez sur Modifier ( ).
2. Cliquez sur l'onglet Règles d'accès ( ) > Ajouter ( ).
   La boîte de dialogue qui apparaît affiche toutes les règles d'accès qui ne sont pas affectées à ce titulaire de cartes.
3. Procédez de l'une des manières suivantes :
   - Sélectionnez une règle et cliquez sur Ajouter.
   - Créez et affectez une règle d'accès temporaire.
4. Sélectionnez la règle d'accès dans la liste.
   L'horaire appliqué à la règle d'accès s'affiche dans une grille sur la droite. Chaque bloc de temps représente 30 minutes. Les zones vertes indiquent les périodes durant lesquelles l'accès est accordé par la règle. Les zones rouges indiquent les périodes durant lesquelles l'accès est refusé par la règle. Les zones en gris correspondent à des périodes non précisées par la règle et donc à un accès refusé. S'il s'agit d'une règle d'accès temporaire ( ), les heures d'activation et d'expiration sont indiquées. Les zones, portes et ascenseurs auxquels la règle est associée sont répertoriés en bas.



5. Pour voir un bloc de temps partiel (hachuré) en minutes, cliquez et maintenez le bouton gauche de la souris enfoncé.
6. Pour affecter une autre règle d'accès au titulaire de cartes, cliquez sur .

7. Pour supprimer une règle d'accès affectée directement à un titulaire de cartes, cliquez sur .
   Vous ne pouvez pas supprimer les règles *Admission générale* et *Aucune admission*.
8. Cliquez sur Enregistrer.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Sujet parent : Créer des titulaires de cartes

3.2.3.2 | Affecter des règles d'accès temporaires aux titulaires de cartes

Pour accommoder les titulaires de cartes saisonniers, comme les étudiants inscrits pour un semestre, ou des titulaires de carte permanents qui ont besoin d'un accès à court terme à une zone restreinte, vous pouvez créer et affecter des règles d'accès temporaire.

À savoir

Règle d'accès doté d'une heure d'activation et d'une heure d'expiration. Les règles d'accès temporaires sont adaptées aux situations qui nécessitent d'accorder aux titulaires de cartes un accès temporaire ou saisonnier à des secteurs sécurisés. Ces règles d'accès sont automatiquement supprimées sept jours après leur expiration afin d'éviter d'encombrer le système.
REMARQUE : Dans la tâche Gestion des titulaires de cartes, vous ne pouvez attribuer une règle d'accès temporaire qu'à un titulaire de cartes à la fois. Pour attribuer une règle d'accès temporaire à plusieurs titulaires de cartes ou groupes de titulaires de cartes, vous devez modifier les propriétés de la règle d'accès dans Config Tool.

Procédure

1. Dans la tâche Gestion des titulaires de cartes, sélectionnez un titulaire, puis cliquez sur Modifier ( ).
2. Cliquez sur l'onglet Règles d'accès ( ) > Ajouter ( ).
   La boîte de dialogue qui apparaît affiche toutes les règles d'accès qui ne sont pas affectées à ce titulaire de cartes.
3. Procédez de l'une des manières suivantes :

- Sélectionnez une règle d’accès temporaire existante ( ) et cliquez sur Ajouter.
- Cliquez sur Règle d'accès temporaire ( ).

L'assistant de création de règles d'accès temporaire s'ouvre.

4. Sur la page Informations de base, nommez et décrivez la règle, puis cliquez sur Suivant.
5. Sur la page Informations sur la règle d'accès, procédez de l'une des manières suivantes :
   - Cliquez sur Utiliser une règle d’accès existante en tant que modèle, puis sélectionnez la règle d'accès qui doit servir de modèle dans la liste déroulante Règle d'accès.

     L'horaire et les entités associées seront copiées sur votre règle d'accès temporaire.

   - Cliquez sur Spécifier les paramètres d'accès personnalisés, et précisez les éléments suivants :

     Accès à
     Développez la vue secteur et sélectionnez les entités auxquelles vous souhaitez accorder l'accès.

     Activation
     Date et heure d’activation, ou l’horaire d’application de la règle.

     Expiration
     Date et heure d’expiration, ou l'horaire de fin d'application de la règle.

     Horaire
     Période durant laquelle la règle d'accès est en vigueur.

6. Cliquez sur Suivant > Créer.

   Une règle d’accès temporaire ( ) est créée et affectée au titulaire de cartes.
7. Cliquez sur Enregistrer.

Lorsque vous avez terminé

(Facultatif) Affectez la règle d’accès temporaire que vous venez de créer à d'autres titulaires de cartes.
Sujet parent : Créer des titulaires de cartes

3.2.4 | Inscrire de nouveaux visiteurs

Pour pouvoir surveiller les allées et venues d'un visiteur, vous devez l'inscrire avec la tâche Gestion des visiteurs. Vous pouvez soit inscrire les visiteurs à l’avance, soit créer un visiteur et l’inscrire immédiatement.

Avant de commencer

Les règles d'accès ne peuvent pas être directement associées aux visiteurs. Par conséquent, pour accorder des *droits d'accès* à un visiteur, vous devez créer un groupe de titulaires de cartes réservé aux visiteurs dans Config Tool, puis affecter les règles d'accès au groupe. Créez le groupe de titulaires de cartes.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Gestion des visiteurs.
2. Cliquez sur Nouveau ( ).
3. En haut de la boîte de dialogue, entrez le nom et le prénom du visiteur.
4. Pour affecter une photo au visiteur, cliquez sur la silhouette et choisissez l'une des options suivantes :

   Charger depuis un fichier
   Choisir une image à partir du disque. Les principaux formats d'image sont pris en charge.

   Charger depuis une webcam
   Prendre une photo avec une webcam. Cette option n'apparaît que si votre poste est équipé d'une webcam.

Charger depuis une caméra
Prendre une photo avec une caméra gérée par Security Center. Lorsque vous cliquez sur Charger depuis une caméra, une boîte de dialogue de capture distincte apparaît. Sélectionnez la source vidéo, et cliquez sur Prendre un instantané ( ).

Charger depuis le presse-papiers
Charger l'image copiée dans le presse-papiers. Cette option n'apparaît que si vous utilisez la commande Copier de Windows pour placer une image dans le presse-papiers.

5. Si vous souhaitez modifier l'image, cliquez sur celle-ci pour ouvrir l'*Éditeur d'image*, et utilisez les outils de modification en haut de la boîte de dialogue.
6. Dans la section État, définissez les éléments suivants :
   REMARQUE : La date *d'activation* est identique à la date d'inscription. Vous pouvez régler la date d'activation dans le futur, ce qui permet de créer des profils de visiteurs à l'avance.

   État
   Pour que les identifiants d'un visiteur fonctionnent, leur état doit être *Actif*. Vous pouvez régler leur état sur *Actif* immédiatement en cliquant sur Enregistrer et inscrire ( ).

   Activation
   Spécifiez la modalité d'activation de leur profil :

   Jamais
   La valeur par défaut. Utilisez cette option si vous comptez inscrire un visiteur manuellement, ou si vous ne savez pas quand il arrivera.

   Date spécifique
   Expire à une date et heure particulières.

   Expiration
   Spécifiez un délai d'expiration pour le profil :

   Jamais
   N'expire jamais.

   Date spécifique
   Expire à une date et heure particulières.

   Expiration après la première utilisation
   Expire un certain nombre de jours après sa première utilisation.

   En cas d'inutilisation
   Expire s'il n'a pas été utilisé durant un certain nombre de jours.

7. Affectez un identifiant au visiteur pour que ses déplacements puissent être suivis par le système.
   REMARQUE : Vous pouvez affecter un identifiant maintenant ou plus tard.
8. Affectez le visiteur à un groupe de titulaires de cartes.
   Les groupes de titulaires de cartes déterminent les règles d'accès qui s'appliquent au visiteur.
   a. Pour affecter le premier groupe de titulaires de cartes, cliquez sur la liste Groupe de titulaires de cartes et sélectionnez un groupe.
      REMARQUE : Seuls les groupes de titulaires de cartes configurés pour les visiteurs apparaissent dans la liste. Un visiteur peut appartenir à plusieurs groupes de titulaires de cartes.
   b. Pour affecter des groupes de titulaires de cartes supplémentaires, cliquez sur Avancé ( ), puis cliquez sur Ajouter un élément ( ). Dans la boîte de dialogue qui apparaît, sélectionnez les groupes de titulaires de cartes et cliquez sur OK.
9. Entrez l'adresse e-mail du visiteur.
10. (Facultatif) Affectez un ou deux accompagnateurs (ou hôtes ou escortes) au visiteur de la manière suivante :
    a. Cliquez sur la liste Hôte du visiteur et sélectionnez le titulaire de cartes qui sera l'hôte du visiteur.

b. (Facultatif) Pour affecter un deuxième hôte, cliquez sur Avancé (), puis cliquez sur Ajouter un élément (). Dans la boîte de dialogue qui apparaît, sélectionnez le titulaire de cartes qui sera l'hôte, puis cliquez sur OK.
c. Cochez l'option Escorte obligatoire si le visiteur n'est pas autorisé à accéder à certains secteurs si son hôte attitré ne présente pas son identifiant après lui sous un certain délai.
REMARQUE : L'ordre de présentation des identifiants par les hôtes n'a pas d'importance.

11. (Facultatif) Entrez une date dans le champ Arrivée prévue.
12. (Facultatif) Lorsque des champs personnalisés sont définis pour les visiteurs, saisissez les informations complémentaires.
13. (Facultatif) Dans la section Avancé, définissez les propriétés de visiteur suivantes :
REMARQUE : Certaines de ces propriétés peuvent être héritées des groupes de titulaires de cartes parents. Lorsqu'une valeur particulière est spécifiée pour le visiteur, cliquez sur Rétablir la valeur héritée () pour récupérer la propriété des groupes de titulaires de cartes parents. Si le titulaire appartient à plusieurs groupes de titulaires de cartes, il hérite du niveau d'accès le plus élevé.
    a. Si un identifiant a été affecté au visiteur, accordez des privilèges d'accès au visiteur.

    Utiliser le délai d'accès prolongé
    Lorsque le paramètre *Délai d'accès prolongé* est défini pour une porte, l'usager dispose de plus de temps pour la franchir. Utilisez cette option pour les personnes à mobilité réduite.

    Contourner les règles d'antiretour
    Exempte le visiteur de toutes les restrictions antiretour.

    b. Dans la section Niveaux d'accès, sélectionnez le niveau d'accès du visiteur. Le niveau d'accès définit ses droits d'accès aux secteurs lorsqu'un niveau de risque est activé dans Security Center. Le Niveau 0 est le niveau d'accès le plus élevé, qui confère le plus de privilèges.
    c. Dans le champ Nom d'entité, saisissez un nouveau nom pour l'entité visiteur, si vous ne souhaitez pas utiliser le prénom et le nom du visiteur.
    Par défaut, le Nom d'entité utilise les champs Prénom et Nom.
    d. (Facultatif) Dans le champ Description, saisissez une description pour le visiteur.
    e. Affectez le visiteur à une *partition*.
    Les partitions déterminent quels utilisateurs Security Center ont accès à cette entité. Seuls les utilisateurs ayant accès à la partition peuvent voir le visiteur.
14. Procédez de l'une des manières suivantes :
    - Pour inscrire un visiteur à l'avance, cliquez sur Enregistrer.
    - Pour inscrire le visiteur immédiatement, cliquez sur Enregistrer et inscrire.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Présentation de la tâche Gestion des visiteurs

3.2.4.1 | Inscrire un visiteur connu

Lorsqu'un visiteur revient sur votre site, vous pouvez l'inscrire sans saisir à nouveau ses informations, car tous les visiteurs radiés sont conservés dans la base de données.

À savoir

Si un identifiant avait été affecté au visiteur, vous devez affecter un nouvel identifiant après inscription du visiteur.

Procédure

1. Dans la tâche Gestion des visiteurs, cliquez sur Nouveau ( ).
2. En haut de la boîte de dialogue, entrez le nom ou le prénom du visiteur.
   En cas de correspondance dans la base de données des visiteurs, un bouton vert indiquant le nombre de correspondances potentielles apparaît ( ).
3. Cliquez sur le bouton vert.
   La boîte de dialogue Visiteurs apparaît et présente la liste des correspondances potentielles trouvées dans la base de données.
4. (Facultatif) Pour filtrer la liste des visiteurs, procédez de l'une des manières suivantes :
   - Saisissez le nom ou le prénom d'un visiteur, puis cliquez sur Rechercher.
   - Sélectionnez la date d'inscription, d'expiration ou d'arrivée prévue du visiteur, puis cliquez sur Rechercher.
   - Cliquez sur Cliquer pour modifier, sélectionnez un champ personnalisé de visiteur, cliquez sur OK, puis cliquez sur Rechercher.
5. Sélectionnez un visiteur, puis cliquez sur Sélectionner.
   Les informations du visiteur sélectionné sont chargées dans la boîte de dialogue Visiteur.
6. Modifiez les informations sur le visiteur si nécessaire, puis procédez de l'une des manières suivantes :
   - Pour inscrire un visiteur à l'avance, cliquez sur Enregistrer.
   - Pour inscrire le visiteur immédiatement, cliquez sur Enregistrer et inscrire ( ).

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Lorsque vous avez terminé

Si le visiteur a besoin d'un identifiant, affectez-en un.
Sujet parent : Inscrire de nouveaux visiteurs

3.2.5 | Affecter un hôte de visiteur supplémentaire aux secteurs avec tourniquets

Vous pouvez définir un deuxième hôte de délégations de visiteurs pour les secteurs accessibles par des tourniquets. Cette fonctionnalité vous permet de désigner un hôte comme tête de délégation et un autre comme queue de délégation. Pour une délégation avec une limite définie, un deuxième hôte est requis si le nombre de visiteurs dépasse cette limite.

À savoir

Si la délégation de visiteurs a atteint la limite configurée pour un seul hôte, l'ajout d'un visiteur supplémentaire déclenche l'avertissement « Limite pour un seul hôte atteinte. Affectez un autre hôte ou ajoutez un deuxième hôte » et vous oblige soit à démarrer une nouvelle délégation, soit à affecter un deuxième hôte à la délégation élargie.
REMARQUE : Une délégation est composée d'un ou deux hôtes et d'un ou plusieurs visiteurs.

Procédure

1. Cliquez sur Avancé ( ), puis cliquez sur la liste déroulante Hôte du visiteur.
2. Effectuez l'une des tâches suivantes :
   - Ajouter un deuxième hôte à la délégation
     a. Dans la liste Hôte du visiteur, sélectionnez un titulaire de cartes en tant que deuxième hôte.
     b. Sélectionnez l'option Escorte obligatoire.
     c. Cliquez sur Enregistrer. Dans la boîte de dialogue qui apparaît, confirmez que vous souhaitez ajouter un deuxième hôte à la délégation.
     REMARQUE : Lorsque vous ajoutez un deuxième hôte à une délégation existante, celui-ci est affecté à tous les titulaires de cartes de la délégation.
   - Démarrer une nouvelle délégation
     a. Supprimez l'hôte affecté en cliquant sur Effacer la sélection au bas de la liste Hôtes de visiteurs.
     b. Sélectionnez un nouvel hôte dans la liste.

3.2.5.1 | Fonctionnement des escortes de visiteurs avec les tourniquets sécurisés

Avec la règle d'escorte de visiteur, l'hôte et le visiteur doivent badger au tourniquet dans un ordre précis.

Sur les tourniquets compatibles avec la règle d'escorte de visiteur, voici la séquence de lecture des badges et d'entrée de l'escorte et du visiteur :

1. L'hôte badge et entre.
2. Le premier visiteur badge et entre.
3. Le visiteur suivant badge et entre. La séquence se poursuit jusqu'au passage du dernier visiteur.
4. S'il y a un deuxième hôte, celui-ci badge et entre.

Si l'ordre de lecture des badges de l'hôte et du visiteur n'est pas respecté, les événements suivants peuvent être déclenchés :

- *Accès refusé : un hôte valable est requis* est déclenché si le visiteur badge avant l'hôte.
- *Visiteur égaré* : si l'hôte badge et entre sans le ou les visiteurs, cet événement est déclenché pour chaque visiteur, ainsi qu'un événement *Hôte de queue manquant* si un deuxième hôte est configuré.
    - *Visiteur égaré* est également déclenché si un visiteur ne badge pas après le passage de l'hôte, ou si l'hôte de queue badge avant le dernier visiteur.
- *Hôte de queue manquant* est déclenché si l'hôte de queue d'une délégation à deux hôtes ne badge pas.

REMARQUE : L'ordre de lecture des badges des hôtes n'est pas important, dès lors qu'un hôte badge et entre avant le premier visiteur, et que l'autre hôte badge et entre en dernier.
Sujet parent : Affecter un hôte de visiteur supplémentaire aux secteurs avec tourniquets

3.2.6 | Rogner une photo

Pour rogner la photo d'un titulaire de cartes ou d'un visiteur et isoler la partie de l'image à conserver, vous pouvez utiliser l'*Éditeur d'image*.

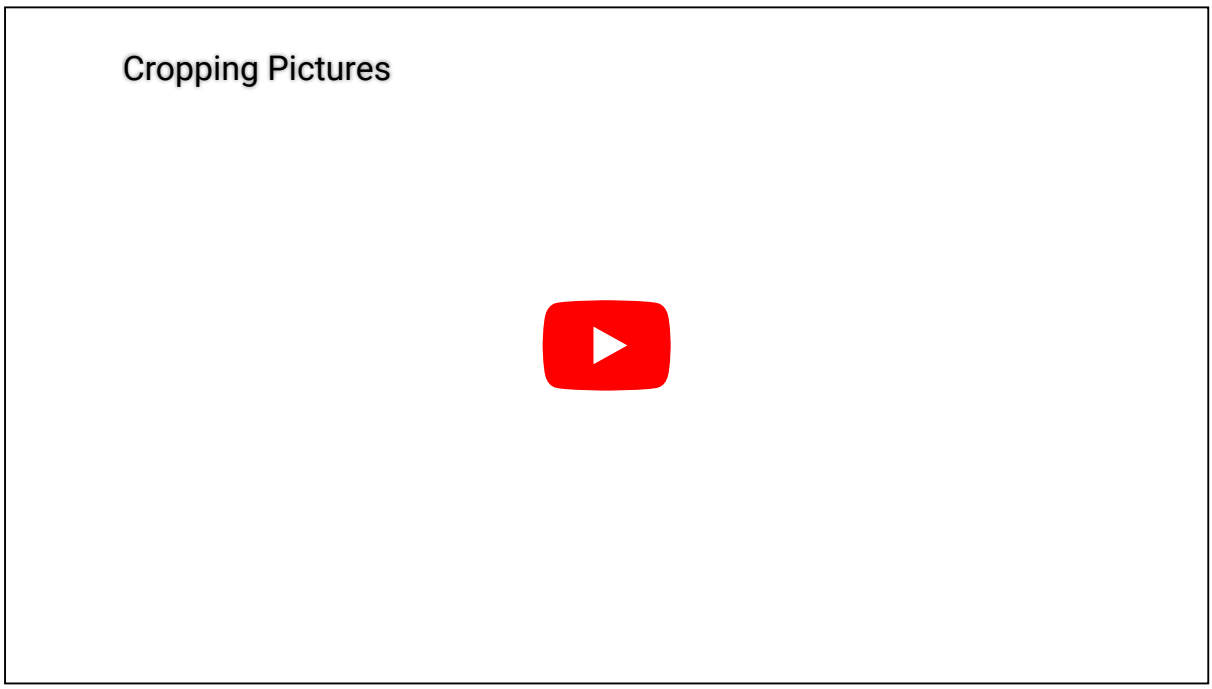
Procédure

1. Cliquez sur l'image.
2. Dans l'*Éditeur d'image*, cliquez sur l'onglet Rogner ( ).
3. Cliquez sur l'image et faites glisser l'icône pour rogner l'image.
4. Pour modifier la zone de rognage, procédez de l'une des manières suivantes :
    - Utilisez les icônes bleues sur l'image pour définir la zone de rognage.
    - Au bas de la boîte de dialogue *Éditeur d'image*, utilisez les valeurs de Largeur et de Hauteur pour redimensionner la zone de rognage. La largeur et la hauteur peuvent être spécifiées en pixels, pouces ou millimètres.

5. Pour rétablir l'image d'origine, cliquez sur Réinitialiser.
6. Cliquez sur Appliquer.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



3.2.7 | Appliquer un arrière-plan transparent à une photo

Si la photo d'un titulaire de cartes a été prise devant un « écran vert », vous pouvez rendre l'arrière-plan de la photo transparent. Cela peut s'avérer utile si vous créez un modèle de badge doté d'une image en arrière-plan.

Procédure

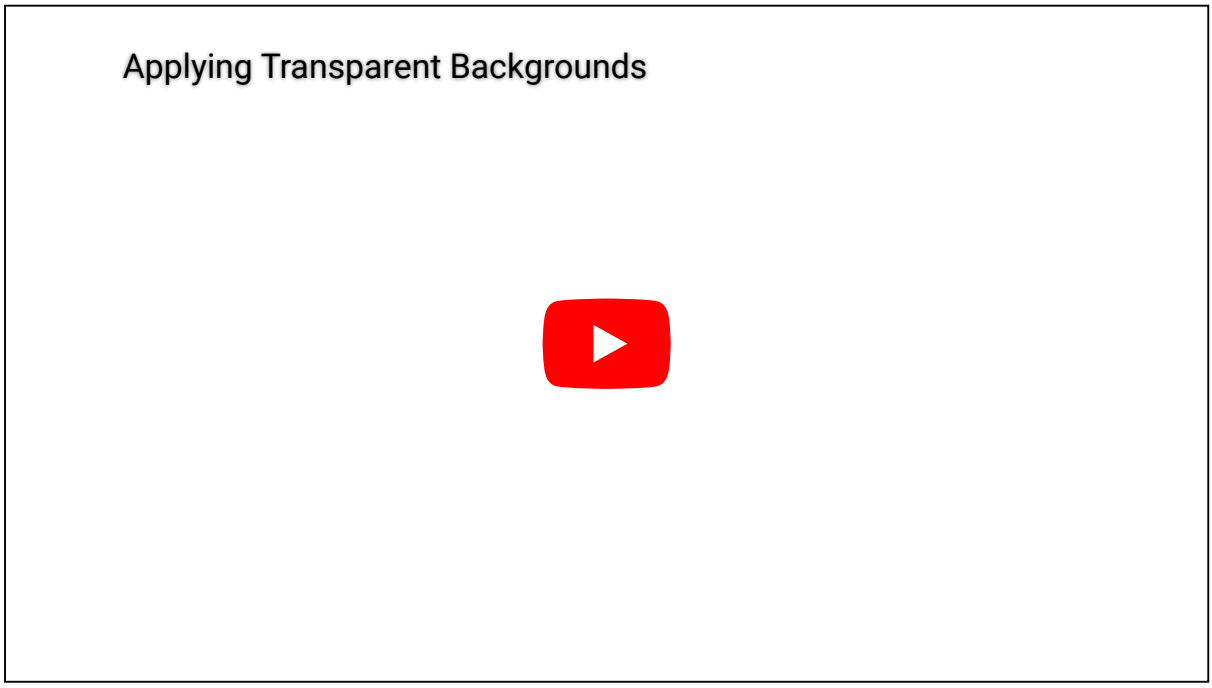
1. Cliquez sur l'image.
2. Dans l'*Éditeur d'image*, cliquez sur l'onglet Transparence.
   Le curseur se transforme en pipette lorsque vous survolez l'image.
3. Cliquez sur une zone de l'arrière-plan pour sélectionner la couleur de transparence (généralement verte ou bleue).

4. Utilisez le curseur Tolérance pour régler le pourcentage de transparence.

5. Pour rétablir l'image d'origine, cliquez sur Réinitialiser.
6. Cliquez sur Enregistrer.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



3.2.8 | Affecter des identifiants

Pour accorder l'accès à des secteurs sécurisés aux titulaires de cartes ou aux visiteurs, vous devez d'abord leur affecter des identifiants.

À savoir

Les titulaires de cartes et visiteurs peuvent se voir affecter plusieurs *identifiants*. Vous pouvez affecter un identifiant lorsque vous créez un titulaire de cartes ou un visiteur (à l'exception des *identifiants mobiles*) ou plus tard. Dans la procédure suivante, les titulaires de cartes ont déjà été créés.

Procédure

1. Procédez de l'une des manières suivantes :
   - Dans la tâche Gestion des titulaires de cartes, sélectionnez un titulaire, puis cliquez sur Modifier ( ).
   - Pour les visiteurs, ouvrez la tâche Gestion des visiteurs, sélectionnez un visiteur, puis cliquez sur Modifier ( ).
2. Dans la section Identifiant, cliquez sur Ajouter un identifiant ( ).
3. Sélectionnez l'une des options suivantes :

   Saisie automatique
   Passez la carte sur un lecteur.

   Saisie manuelle
   Entrez manuellement les données de carte. Utilisez cette méthode lorsque vous n'avez pas de lecteur de cartes à proximité.

   Identifiant existant
   Sélectionnez un identifiant déjà inscrit, mais non affecté.

   Code PIN
   Créer un code PIN.

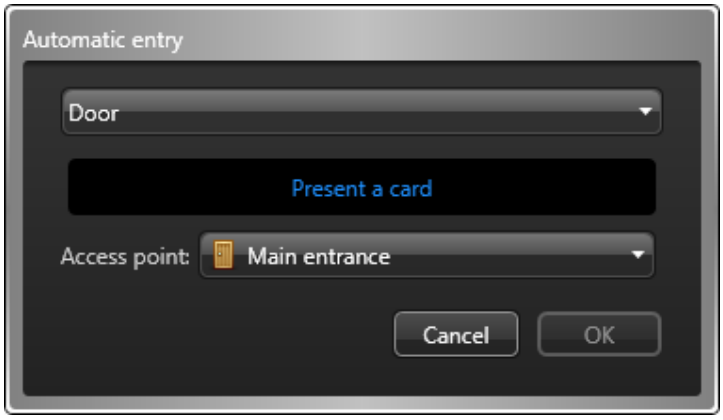
   Plaque d'immatriculation
   Entrez le numéro de plaque d'immatriculation d'un titulaire de cartes. Utilisez cette méthode si une caméra Sharp sert à utiliser une barrière d'accès pour véhicules. Dans ce cas, la plaque d'immatriculation du titulaire de cartes peut servir d'identifiant.

   Demander une carte
   Demandez une carte d'identification pour le titulaire de cartes ou visiteur. Utilisez cette méthode si vous n'avez pas d'imprimante sur site.

   Identifiant mobile
   Demander un identifiant mobile pour le titulaire de cartes ou visiteur. Un fournisseur d'identifiants mobiles doit être configuré et des lecteurs d'identifiants mobiles doivent être installés. Le titulaire de cartes doit avoir une adresse e-mail valable.

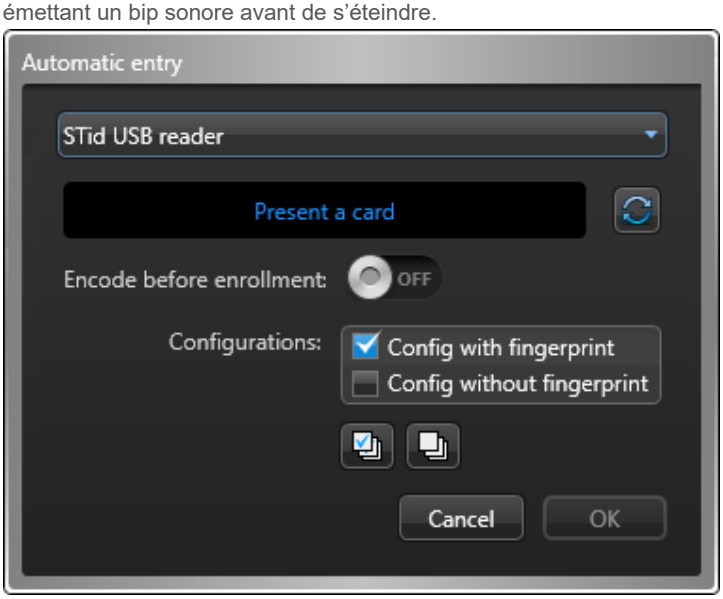
   Identifiant papier (impression)
   Imprimez un badge (étiquette ou carte d'identification) sans affecter d'identifiant. L'identifiant papier ne peut pas servir à ouvrir les portes. Il ne sert qu'à identifier le titulaire de cartes ou visiteur de visu.

4. Si vous sélectionnez Saisie automatique, vous devez sélectionner un lecteur (USB ou porte), et passer la carte sur le lecteur.

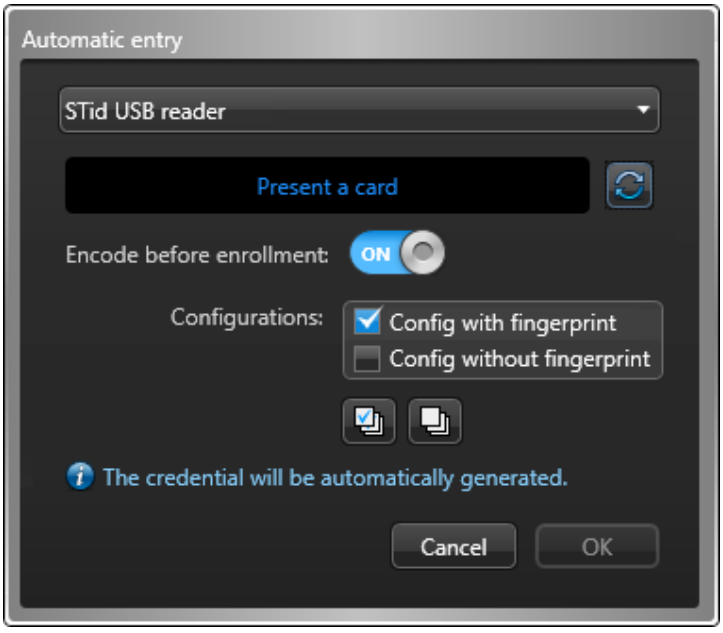


   Si vous avez un lecteur qui permet de coder les cartes à puce, procédez de l'une des manières suivantes :

- Pour lire une carte préconfigurée, désactivez l'option Coder avant l’inscription. Lorsque le témoin DEL du lecteur vire au vert (prêt à la lecture), placez la carte à puce sur le lecteur. Le témoin DEL passe au jaune puis au vert en émettant un bip sonore avant de s’éteindre.

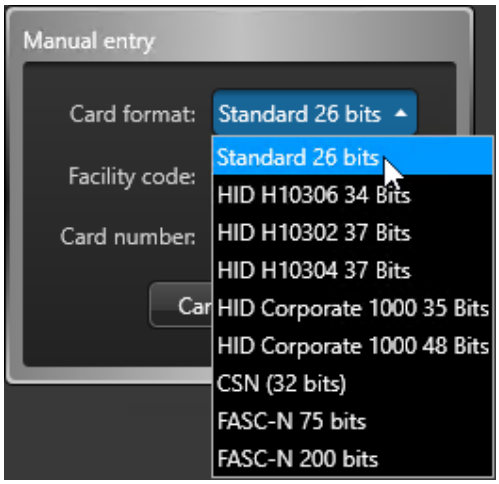


- Pour générer et coder un identifiant 128 bits aléatoire MIFARE DESFire avant de l’inscrire, réglez l’option Coder avant l’inscription sur Activé. Lorsque le témoin DEL du lecteur vire au vert (prêt au codage), placez la carte à puce sur le lecteur pendant environ 2 secondes. Le témoin DEL passe au jaune puis au vert en émettant un bip sonore avant de s’éteindre. Si vous entendez un bip long et que le témoin DEL reste rouge, réessayez.
  REMARQUE : Votre licence Security Center doit prendre en charge le codage de cartes à puce.



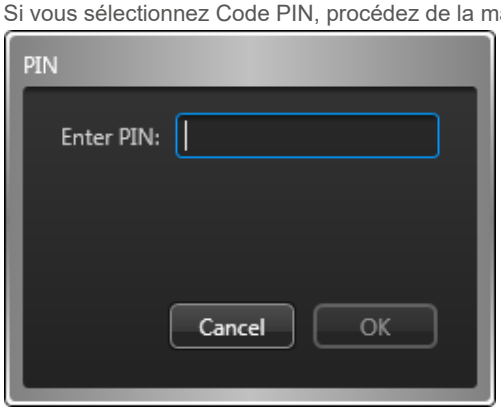
La boîte de dialogue se ferme automatiquement lorsqu'une carte valable est présentée. La carte est automatiquement inscrite si ce n'était pas déjà le cas. Si la carte est déjà affectée à quelqu'un, elle est refusée.

5. Si vous sélectionnez Saisie manuelle, vous devez sélectionner un format de carte, renseigner les champs de données requis, puis cliquer sur OK.

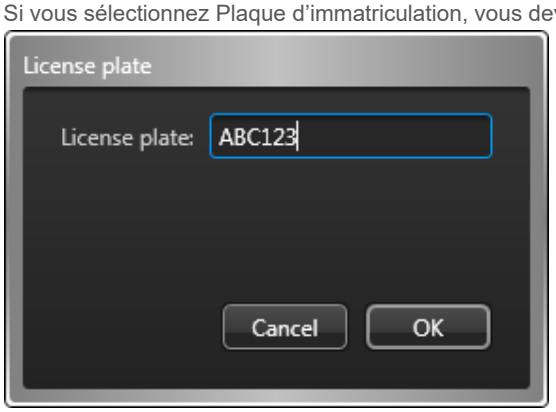


ATTENTION :
Saisissez les données de carte soigneusement, car le système ne peut pas savoir si les données saisies correspondent ou non à une carte physique.
La carte est automatiquement inscrite si ce n'était pas déjà le cas. Si la carte est déjà affectée à quelqu'un, elle est refusée.

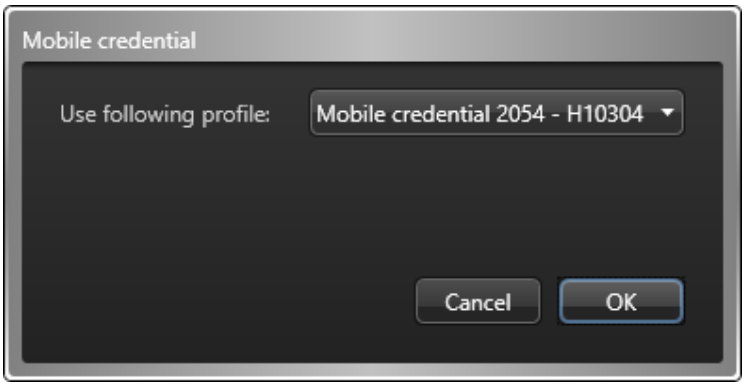
6. Lorsque vous sélectionnez Identifiant existant, une boîte de dialogue apparaît et présente la liste de tous les identifiants non affectés. Sélectionnez un identifiant non attribué dans la liste et cliquez sur OK.
7. Si vous sélectionnez Code PIN, procédez de la manière suivante :



   a. Entrez le code PIN sous forme de valeur numérique.
      REMARQUE : Veillez à ne pas dépasser le nombre de chiffres accepté par vos lecteurs. Un code PIN est généralement composé de cinq chiffres. Toutefois, certains modèles acceptent jusqu'à 15 chiffres.
   b. Cliquez sur OK.
8. Si vous sélectionnez Plaque d'immatriculation, vous devez procéder de la manière suivante :



   a. Entrez le numéro de plaque d'immatriculation.
      REMARQUE : Il est inutile de saisir les espaces qui apparaissent dans le numéro de plaque d'immatriculation. Pour le système, « ABC123 » et « ABC 123 » sont équivalents.
   b. Cliquez sur OK.
9. Si vous sélectionnez Identifiant mobile, vous devez procéder de la manière suivante :



a. Sélectionnez le profil d'identifiant (s'il y en a plusieurs).
Vous pouvez affecter un identifiant mobile de chaque profil au titulaire de cartes.
b. Cliquez sur OK.

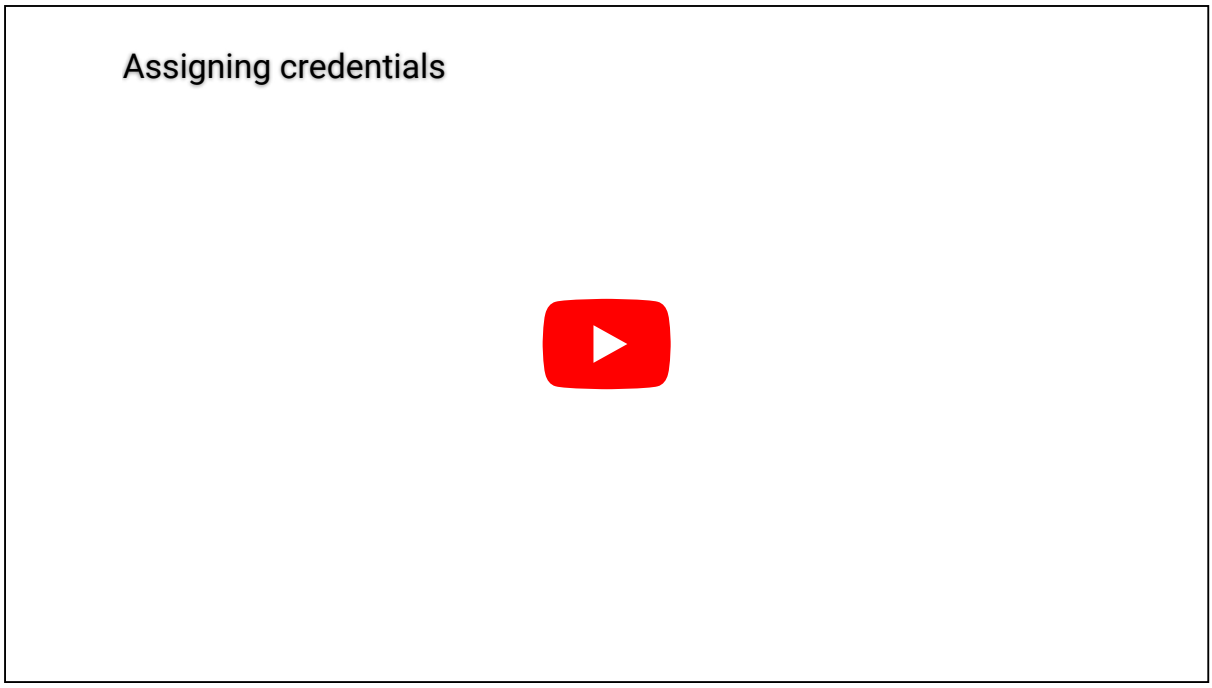
REMARQUE : Une invitation est envoyée par e-mail au titulaire de cartes avec un lien pour télécharger l'app d'identifiant mobile. Le titulaire de cartes doit accepter l'invitation pour que l'identifiant soit *activé* sur son téléphone. Si le titulaire de cartes décline l'invitation ou si l'invitation expire, l'identifiant reste *inutilisé*, et le fournisseur d'identifiants mobiles peut l'affecter à un autre titulaire de cartes. Security Center ne sait pas que l'identifiant mobile demandé n'a pas été accepté par le titulaire de cartes jusqu'à ce que l'identifiant mobile soit affecté à quelqu'un d'autre. Security Center le supprime alors automatiquement du titulaire de cartes actuel.

IMPORTANT : Un identifiant mobile activé (associé à un téléphone) ne peut jamais être réutilisé sur un autre téléphone. Si un titulaire de cartes perd son téléphone ou doit changer de téléphone, il doit informer l'opérateur Security Center, qui devra supprimer l'identifiant ou le marquer comme *perdu*. Ensuite, l'opérateur doit se connecter sur le portail du fournisseur d'identifiants et *révoquer* l'identifiant mobile.

10. Une fois que l'identifiant est affecté, il apparaît dans la section Identifiant.
Le nom et l'état de l'identifiant sont affichés. *Actif* indique que l'identifiant est affecté.
REMARQUE : Si l'identifiant est un code PIN, l'icône de pavé numérique est affichée. Si l'identifiant est une plaque d'immatriculation, une icône de plaque d'immatriculation est affichée. Si l'identifiant est une carte, un *modèle de badge* par défaut est affecté, et un aperçu du badge est affiché à la place de l'icône.
11. (Facultatif) Si l'identifiant est une carte, vous pouvez sélectionner un autre modèle de badge de la manière suivante.
    a. Dans la section Identifiant, cliquez sur l'image de badge.
    b. Sélectionnez un modèle de badge, puis cliquez sur OK.
    Les modèles de badge sont créés dans Config Tool.
    Un aperçu avant impression du badge apparaît, avec données du titulaire ou visiteur et de l'identifiant concernés.
12. Cliquez sur Enregistrer.
Vous devez enregistrer toutes les modifications avant de pouvoir imprimer le badge.
13. Pour imprimer le badge, cliquez sur Imprimer un badge en regard de l'aperçu du badge.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



3.2.8.1 | Demander une carte d'identification

Lorsque vous n'êtes pas en possession des cartes d'identification, vous pouvez demander à quelqu'un d'autre d'affecter les cartes aux titulaires de cartes et visiteurs que vous gérez.

À savoir

Vous pouvez demander une carte lorsque vous créez un titulaire de cartes ou un visiteur ou plus tard. Dans la procédure suivante, le titulaire de cartes ou visiteur a déjà été créé.

Procédure

1. Procédez de l'une des manières suivantes :
   - Dans la tâche Gestion des titulaires de cartes, sélectionnez un titulaire, puis cliquez sur Modifier ( ).
   - Pour les visiteurs, ouvrez la tâche Gestion des visiteurs, sélectionnez un visiteur, puis cliquez sur Modifier ( ).
2. Dans la section Identifiant, cliquez sur Ajouter un identifiant ( ).
3. Dans le menu déroulant, cliquez sur Demander une carte.
4. Dans la boîte de dialogue Demander une carte, sélectionnez le motif de la demande.
   REMARQUE : Les motifs de demande de carte n'apparaissent que si l'administrateur les a créés dans Config Tool.
5. Sélectionnez un modèle dans la liste déroulante Modèle de badge.
   Il n'est pas nécessaire de sélectionner un modèle de badge si vous n'allez pas imprimer le badge. Les modèles de badge sont créés dans .
   Un aperçu avant impression du badge est affiché.
6. Dans l'option Activer, sélectionnez quand activer l'identifiant.

   Jamais
   L'identifiant ne sera jamais activé.

   Après l'inscription
   Après qu'un autre utilisateur a répondu à la demande de carte.

   Activé
   Sélectionnez une date particulière pour l'activation de l'identifiant.

7. Pour recevoir un e-mail lorsque l'identifiant a été imprimé, sélectionnez l'option Me prévenir par e-mail lorsque la carte est prête.
   REMARQUE : Pour que cette option fonctionne, l'utilisateur doit avoir une adresse e-mail valable.

8. Cliquez sur OK.
   L'identifiant est affiché avec la mention Demandé dans la section Identifiant de la fenêtre des détails de titulaire de cartes ou de visiteur.
9. Cliquez sur Enregistrer.

Résultats

L'icône Demandes de cartes () apparaît dans la zone de notification.
Sujet parent : Affecter des identifiants
Explorer

- Répondre aux demandes de cartes d'identification

3.2.8.2 | Imprimer des cartes d'identification par lots

Pour gagner du temps lorsque vous imprimez des cartes d'identification, vous pouvez les imprimer par lots.

À savoir

Tous les identifiants que vous sélectionnez doivent être associés à un modèle de badge.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Gestion des identifiants.
2. Sélectionnez les identifiants que vous souhaitez imprimer :
   - Appuyez sur la touche Ctrl pour sélectionner des identifiants particuliers dans la liste.
   - Appuyez sur la touche Maj pour sélectionner une plage d'identifiants dans la liste.
3. Cliquez sur Imprimer.

Résultats

Les identifiants sélectionnés sont imprimés dans l'ordre d'affichage dans la tâche Gestion des identifiants.
Sujet parent : Affecter des identifiants

3.2.8.3 | Imprimer un identifiant papier

Lorsque vous n'avez pas d'identifiants affectés aux titulaires de cartes ou aux visiteurs, vous pouvez imprimer un identifiant papier (badge sans données d'identifiant) qui servira d'étiquette ou de carte d'identification visuelle.

À savoir

Pour imprimer un badge, vous devez utiliser un modèle de badge. Un modèle de badge est généralement associé à un identifiant de type carte afin qu'il puisse servir à déverrouiller les portes, mais vous pouvez également imprimer un badge sans données d'identifiant (appelé identifiant papier) qui peut servir d'étiquette ou de carte d'identité pour une identification visuelle.

Vous pouvez imprimer un badge lorsque vous créez un titulaire de cartes ou un visiteur, ou l'imprimer plus tard.

Procédure

1. Procédez de l'une des manières suivantes :
   - Dans la tâche Gestion des titulaires de cartes, sélectionnez un titulaire, puis cliquez sur Modifier ().
   - Pour les visiteurs, ouvrez la tâche Gestion des visiteurs, sélectionnez un visiteur, puis cliquez sur Modifier ().
2. Dans la section Identifiant, cliquez sur Ajouter un identifiant ().

3. Dans le menu qui apparaît, cliquez sur Identifiant papier (impression).
4. Dans la boîte de dialogue Impression de badges, sélectionnez un badge dans la liste.
   Un aperçu avant impression du badge est affiché. Les informations de titulaire de cartes ou de visiteur peuvent figurer sur le badge (en fonction de la mise en page du modèle de badge). Aucune donnée d'identifiant n'est affichée sur le badge.
5. Pour imprimer l'identifiant papier, cliquez sur Imprimer un badge.

Sujet parent : Affecter des identifiants

3.2.9 | Affecter une carte temporaire

En cas de perte ou de vol de l'identifiant d'un titulaire de cartes ou d'un visiteur, vous pouvez le remplacer par une carte temporaire, et signaler la perte de la carte d'origine.

Avant de commencer

Vous devez disposer des éléments suivants :

- Un lecteur de cartes à proximité.
- Des cartes supplémentaires préalablement inscrites. Vous pouvez inscrire un grand nombre de cartes à la fois avec la tâche Gestion des identifiants.

Procédure

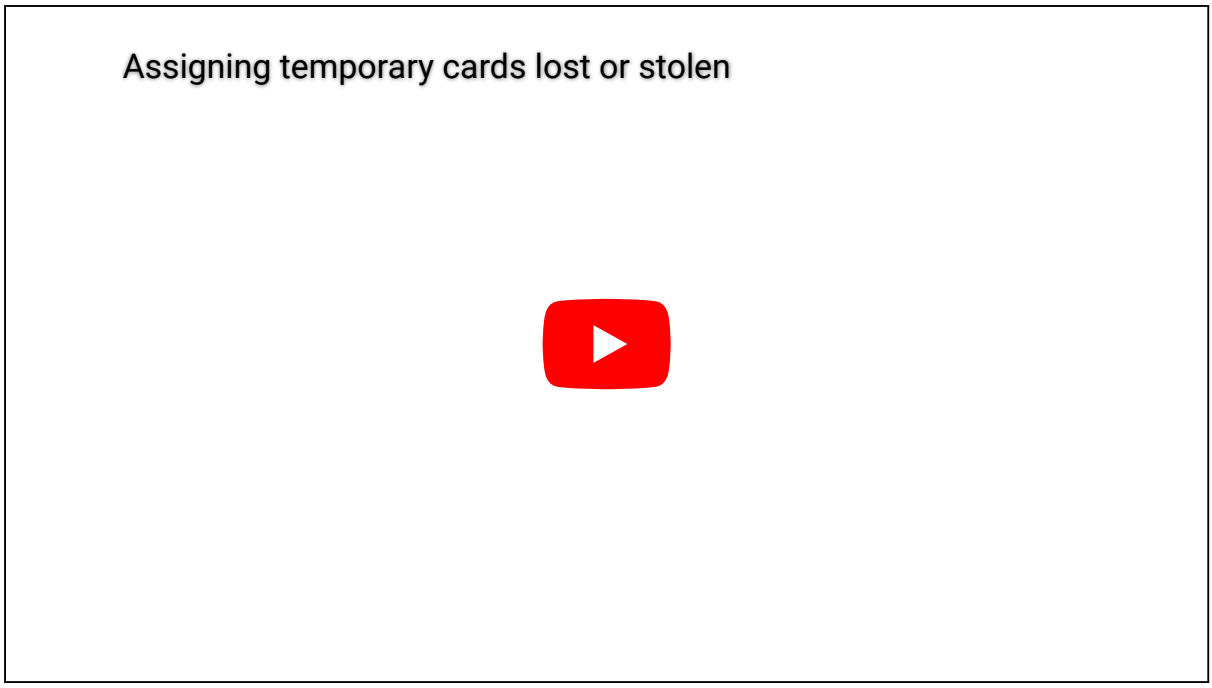
1. Procédez de l'une des manières suivantes :
   - Dans la tâche Gestion des titulaires de cartes, sélectionnez un titulaire, puis cliquez sur Modifier ( ).
   - Pour les visiteurs, ouvrez la tâche Gestion des visiteurs, sélectionnez un visiteur, puis cliquez sur Modifier ( ).
2. Dans la section Identifiant, cliquez sur Affecter la carte temporaire.
3. Dans la liste déroulante, sélectionnez un lecteur de cartes à proximité.
   Le lecteur de carte peut être un appareil USB connecté à votre ordinateur ou vous pouvez utiliser un Point d'accès (porte).
4. Présentez une carte disponible et préalablement inscrite.
5. Définissez le nombre de jours de validité de la carte temporaire et cliquez sur Affecter la carte temporaire.
6. Cliquez sur Enregistrer.

Résultats

La carte d'origine est alors signalée comme perdue, mais reste affectée au titulaire de cartes. La carte temporaire est activée pour la période définie et affectée au même titulaire de cartes. Le titulaire de cartes dispose alors d'au moins deux cartes. La carte d'origine perdue et la carte temporaire active.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



3.2.9.1 | Rétablir la carte d'origine d'un titulaire de cartes ou visiteur

Si la carte perdue est retrouvée, vous pouvez rétablir la carte d'origine et supprimer l'affectation de la carte temporaire.

Avant de commencer

Vous devez disposer d'un lecteur de cartes à proximité.

À savoir

Pour rétablir la carte d'origine, le titulaire de cartes ou visiteur doit retourner la carte d'origine et la carte temporaire.
ATTENTION :
Lorsqu'un titulaire de cartes a plusieurs cartes temporaires, le retour de la carte temporaire ne rétablit pas la carte d'origine du titulaire. La fonction de retour de carte temporaire ne peut être utilisée qu'une seule fois par titulaire.

Procédure

1. Dans la tâche Gestion des titulaires de cartes ou Gestion des visiteurs, cliquez sur Retourner une carte ( ).
2. Dans la liste déroulante, sélectionnez un lecteur de cartes à proximité.
   Le lecteur de cartes peut être un Lecteur USB relié à votre ordinateur, ou vous pouvez utiliser un Point d'accès (porte).
3. Passez la carte d'origine et la carte temporaire dans le lecteur (l'ordre n'a pas d'importance).
4. Si les deux cartes sont affectées au même titulaire de cartes, cliquez sur Restaurer la carte d'origine pour rétablir l'état Actif de la carte d'origine et désactiver la carte temporaire.
   La carte temporaire peut alors être affectée à quelqu'un d'autre.

Sujet parent : Affecter une carte temporaire

3.2.10 | Utiliser une tablette de signature

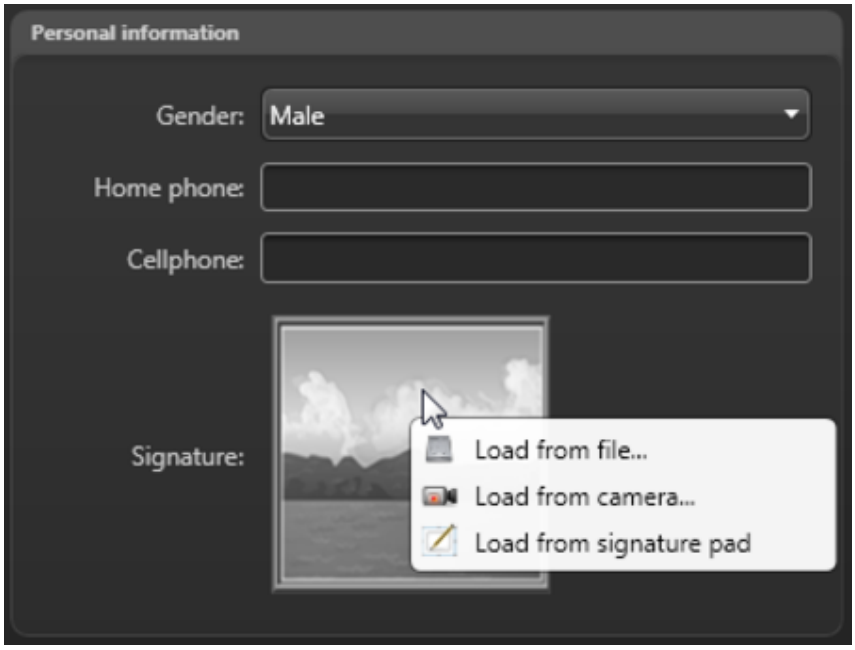
Si vous avez une tablette de signature connectée à votre ordinateur, vous pouvez l'utiliser pour capturer la signature des titulaires de cartes et des visiteurs, puis l'enregistrer directement dans un champ personnalisé préalablement créé.

Avant de commencer

- Vérifiez que les champs de signature pour les titulaires de cartes et visiteurs sont de type *Image*.
- Reliez une tablette de signature Topaz à votre ordinateur, et activez-la dans Security Desk.

Procédure

1. Ouvrez la tâche *Gestion des titulaires de cartes* ou la tâche *Gestion des visiteurs* pour créer ou modifier le titulaire de cartes ou le visiteur.
2. Dans la boîte de dialogue Propriétés, cliquez sur le champ personnalisé réservé à la signature, puis sélectionnez Charger depuis la tablette de signature.



3. Tendez la tablette au titulaire de cartes ou au visiteur, et invitez-le à signer.
   La signature capturée apparaît dans le champ signature.
4. Cliquez sur Enregistrer.

3.2.11 | Radier les visiteurs

Vous devez radier les visiteurs lorsqu'ils s'en vont.

Procédure

1. Dans la tâche Gestion des visiteurs, sélectionnez le visiteur dans la liste des visiteurs.
   Si la liste des visiteurs est longue, utilisez les fonctions de recherche pour trouver le visiteur.
   REMARQUE : Vous pouvez radier plusieurs visiteurs en même temps en appuyant sur la touche Maj. tout en sélectionnant les visiteurs que vous souhaitez radier.
2. Cliquez sur Radier ( ).

Résultats

Le visiteur radié est supprimé de la liste des visiteurs, mais il reste disponible pour les rapports d'investigation. Les informations sur le visiteur sont conservées dans la base de données, et peuvent être utilisées s'il revient.

Si un identifiant était associé à ce visiteur, l'état de l'identifiant est réglé sur *Non affecté* et l'identifiant peut être affecté à autre visiteur ou titulaire de cartes. L'identifiant est également supprimé de tous les contrôleurs d'accès avec lesquels il a été synchronisé. Cela peut prendre quelques secondes.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Analyser les événements de visiteurs
- Présentation de la tâche Gestion des visiteurs

3.2.11.1 | Supprimer des visiteurs

Les visiteurs pré-inscrits ne peuvent pas être radiés, mais ils peuvent être supprimés.

Procédure

1. Dans la tâche Gestion des visiteurs, sélectionnez le visiteur dans la liste des visiteurs.
   Si la liste des visiteurs est longue, utilisez les fonctions de recherche pour trouver le visiteur.
   REMARQUE : Vous pouvez supprimer plusieurs visiteurs en même temps en appuyant sur la touche Maj. tout en sélectionnant les visiteurs que vous souhaitez supprimer.
2. Cliquez sur Supprimer ( ).

Résultats

Le visiteur est supprimé de la base de données.
Sujet parent : Radier les visiteurs

3.2.12 | Analyser les événements de titulaires de cartes

Vous pouvez analyser les événements relatifs aux titulaires de cartes (Accès refusé : Code PIN non valable , Premier entré, Dernier sorti, Violation antiretour, et ainsi de suite) à l'aide du rapport *Activités de titulaires de cartes*.

À savoir

Par exemple, pour connaître les secteurs, portes et ascenseurs empruntés par un titulaire durant la journée ou la semaine écoulée, vous pouvez rechercher le titulaire concerné, puis définir une plage horaire pour le rapport. En cas d'activité suspecte sur votre site durant la journée écoulée, vous pouvez rechercher les titulaires de cartes dont l'accès à un secteur a été refusé en sélectionnant le secteur, puis l'événement *Accès refusé*.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Activités de titulaires de cartes.

2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Titulaires de cartes
   Limitez votre recherche à des titulaires de cartes ou groupes de titulaires de cartes spécifiques
   REMARQUE : Si vous ne sélectionnez que le groupe de titulaires de cartes *Tous les titulaires de cartes*, les titulaires de cartes fédérés ne sont pas inclus. En effet, *Tous les titulaires de cartes* est un groupe local qui ne prend en compte que les titulaires de cartes locaux.

   Identifiant
   Limitez la recherche à certains identifiants.

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Portes - Secteurs - Ascenseurs
   Restreindre la recherche aux activités survenues à certaines portes, certains secteurs ou ascenseurs.

   Événements
   Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

3. Cliquez sur Générer le rapport.
   Les événements de titulaire de cartes sont affichés dans le volet de rapport.
4. Pour afficher la séquence vidéo associée à un événement dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas depuis le volet de rapport.
   Lorsqu'aucune caméra n'est associée à l'entité, une icône de porte, d'ascenseur ou de secteur est affichée, selon le type d'événement de titulaire de cartes.
5. Utilisez les widgets du volet Commandes pour contrôler les tuiles.

3.2.12.1 | Colonnes du volet de rapport dans la tâche Activités de titulaires de cartes

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Événement
Nom de l'événement.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Photo
Photo du titulaire de cartes ou du visiteur.

Emplacement
Emplacement (secteur) où l'activité a eu lieu.

Point d'accès
Point d'accès concerné (ne s'applique qu'aux secteurs, portes et ascenseurs).

Identifiant
Nom d'identifiant utilisé par le titulaire de cartes.

Identifiant complémentaire
Un deuxième identifiant est parfois exigé. Par exemple, un badge et un code PIN peuvent être requis pour l'accès à une porte ou à un ascenseur.

Heure de l'événement
Date et heure de l'événement.

Format de carte
Format de carte de l'identifiant.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

Code de l'identifiant
Numéro de carte ou code de l'installation.

Appareil
Périphérique utilisé par l'unité (lecteur, entrée REX, module d'E/S, relais de pêne, et ainsi de suite).

Adresse e-mail
L'adresse e-mail du titulaire de cartes ou du visiteur.

Adresse IP
L'adresse IP de l'unité ou de l'ordinateur.

Période d'occurrence
Période durant laquelle l'événement est survenu.

Type de produit
Modèle de l'unité.

Fuseau horaire
Le fuseau horaire de l'unité.

Sous contrainte
Indique que le titulaire de cartes est sous contrainte.

Unité
Nom de l'unité.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.
Sujet parent : Analyser les événements de titulaires de cartes

3.2.13 | Analyser les événements de visiteurs

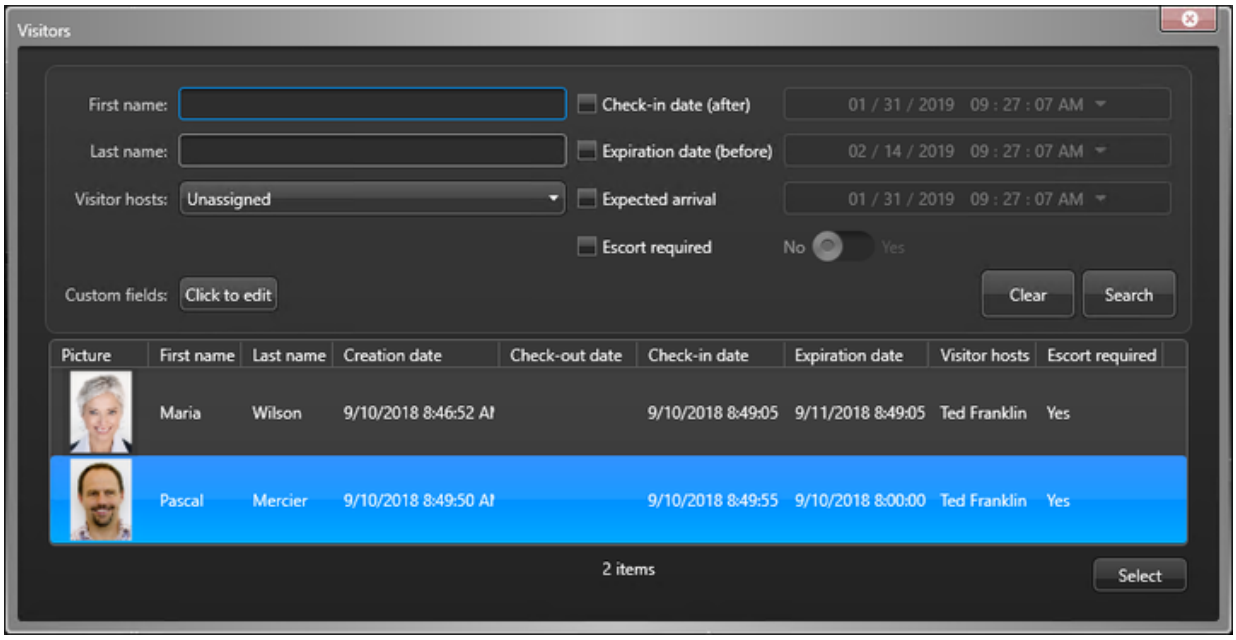
Utilisez le rapport *Activités de visiteurs* pour analyser les activités liées aux visiteurs (accès refusé, premier entré, dernier sorti, violation antiretour, et ainsi de suite).

À savoir

Dans Security Desk, vous pouvez voir tous les secteurs et toutes les portes empruntées par un visiteur durant son séjour. Si vous voulez savoir si des événements critiques associés aux visiteurs sont survenus sur votre site durant la journée écoulée, vous pouvez appliquer une plage horaire au rapport.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Activités de visiteurs.
2. Dans le filtre de requête Visiteur de l'onglet Filtres, cliquez sur .
3. Dans la boîte de dialogue Visiteurs, filtrez la liste des visiteurs de l'une des manières suivantes :
   - Saisissez le nom ou le prénom d'un visiteur, puis cliquez sur Rechercher.
   - Sélectionnez la date d'activation, d'expiration ou d'arrivée prévue du visiteur, puis cliquez sur Rechercher.
   - Sélectionnez l'hôte du visiteur, puis cliquez sur Rechercher.
   - Cliquez sur Cliquer pour modifier, sélectionnez un champ personnalisé de visiteur, cliquez sur OK, puis cliquez sur Rechercher.
4. Sélectionnez un visiteur à examiner.
   Vous ne pouvez spécifier qu'un visiteur à la fois.



5. Cliquez sur Sélectionner.
6. Définissez les autres filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Portes - Secteurs - Ascenseurs
   Restreindre la recherche aux activités survenues à certaines portes, certains secteurs ou ascenseurs.

   Événements
   Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

7. Cliquez sur Générer le rapport.
   Les événements de visiteur sont affichés dans le volet de rapport.
8. Pour afficher la séquence vidéo associée à un événement dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas.
   Lorsqu'aucune caméra n'est connectée à l'entité, une icône de porte, d'ascenseur ou de secteur est affichée, selon le type d'événement de visiteur.
9. Utilisez les widgets du volet Commandes pour contrôler les tuiles.

3.2.13.1 | Colonnes du volet de rapport dans la tâche Activités de visiteurs

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Événement
Nom de l'événement.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Emplacement
Emplacement (secteur) où l'activité a eu lieu.

Point d'accès
Point d'accès concerné (ne s'applique qu'aux secteurs, portes et ascenseurs).

Heure de l'événement
Date et heure de l'événement.

Photo
Photo du titulaire de cartes ou du visiteur.

Format de carte
Format de carte de l'identifiant.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

Identifiant
Nom d'identifiant utilisé par le titulaire de cartes.

Code de l'identifiant
Numéro de carte ou code de l'installation.

Appareil
Périphérique utilisé par l'unité (lecteur, entrée REX, module d'E/S, relais de pêne, et ainsi de suite).

Adresse e-mail
L'adresse e-mail du titulaire de cartes ou du visiteur.

Adresse IP
L'adresse IP de l'unité ou de l’ordinateur.

Période d'occurrence
Période durant laquelle l'événement est survenu.

Type de produit
Modèle de l'unité.

Identifiant complémentaire
Un deuxième identifiant est parfois exigé. Par exemple, un badge et un code PIN peuvent être requis pour l'accès à une porte ou à un ascenseur.

Fuseau horaire
Le fuseau horaire de l'unité.

Unité
Nom de l'unité.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.
Sujet parent : Analyser les événements de visiteurs

3.2.14 | Compter les individus

Vous pouvez voir le nombre de titulaires de cartes actuellement présents dans des secteurs sécurisés de votre système avec la tâche *Comptage d'individus*. Cela peut également servir à supprimer les personnes d'un secteur dans lesquels ils apparaissent par erreur.

À savoir

Le nombre de titulaires de cartes présents dans un secteur donné est mis à jour en temps réel au fil des entrées et sorties.

Pour que ce rapport soit précis, le secteur sélectionné doit être entièrement sécurisé, c'est-à-dire que pour entrer et sortir du secteur, les personnes doivent impérativement passer leur badge dans un lecteur. Les lecteurs doivent être installés des deux côtés des portes (pas de *REX*), et les titulaires de cartes doivent franchir la porte les uns après les autres (pas de *talonnage*). Les tourniquets sont souvent utilisés à cette fin.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Comptage d'individus.
2. Dans le *Sélecteur*, sélectionnez un secteur.

   Les titulaires de cartes présents dans le secteur sont affichés à droite.

3. Pour lancer un rapport d'investigation sur un titulaire de cartes sélectionné, cliquez sur Analyser ().
4. Pour supprimer un titulaire de cartes sélectionné du secteur que vous consultez, cliquez sur Supprimer du secteur ().
5. Pour réinitialiser le comptage d'individus du secteur, cliquez sur Effacer tout.

Résultats

Les titulaires de cartes supprimés avec la commande Supprimer du secteur ou la commande Effacer tout sont automatiquement exemptés d'une violation antiretour lors du passage suivant de leur badge. Ils peuvent ainsi revenir dans le secteur dont ils ont été supprimés.

Exemple

Si vous remarquez une activité suspecte en surveillant un flux vidéo, vous pouvez utiliser le *comptage d'individus* pour afficher la liste des titulaires de cartes présents dans le secteur concerné. En cas d'incendie, vous pouvez utiliser le *comptage d'individus* pour vérifier que tout le monde a quitté le bâtiment.
Explorer

- Suivre les titulaires de cartes présents dans un secteur

3.2.14.1 | Utiliser le comptage d'individus pour suivre et supprimer les titulaires de cartes dans un secteur

Si un titulaire de cartes sort d'un secteur par talonnage, ou s'il est indiqué comme présent par erreur, vous pouvez le supprimer du secteur à l'aide du champ Rechercher de la tâche *Comptage d'individus*.

À savoir

La recherche de titulaires de cartes permet de chercher par nom du secteur et par le nom et le prénom des titulaires.

Procédure

1. Dans la tâche Comptage d'individus, entrez le nom du titulaire de cartes dans le champ Rechercher en haut du canevas.
   La recherche intègre une fonction de remplissage automatique.
   Vous pouvez également saisir du texte partiel. Par exemple, « art » renvoie « Martin ».
2. Sélectionnez le titulaire de cartes et cliquez sur Supprimer du secteur.
   Le titulaire de cartes est supprimé du secteur, et il est exempté d'une violation antiretour la prochaine fois qu'il badgera.

Sujet parent : Compter les individus

3.2.15 | Suivre les titulaires de cartes présents dans un secteur

Vous pouvez voir le nombre de titulaires de cartes et de visiteurs présents dans un secteur donné, ainsi que la durée de leur séjour, avec le rapport *Présence dans un secteur*.

À savoir

Pour que ce rapport soit précis, le secteur sélectionné doit être entièrement sécurisé, c'est-à-dire que pour entrer et sortir du secteur, les personnes doivent impérativement passer leur badge dans un lecteur. Les lecteurs doivent être installés des deux côtés des portes (pas de *REX*), et les titulaires de cartes doivent franchir la porte les uns après les autres (pas de *talonnage*). Les tourniquets sont souvent utilisés à cette fin.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Présence dans un secteur.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

Secteurs
Sélectionnez les secteurs à examiner.
REMARQUE : Vous devez sélectionner un secteur entièrement sécurisé.

Titulaires de cartes
Limitez votre recherche à des titulaires de cartes ou groupes de titulaires de cartes spécifiques

Champs personnalisés
Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

3. Cliquez sur Générer le rapport.
   Les titulaires de cartes et les visiteurs actuellement présents dans le secteur sont affichés dans le volet de rapport.
4. Pour afficher la séquence vidéo associée à un événement dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas.
   Si le secteur n'est pas associé à une URL ou à une carte par le biais d'un module externe de tuile, seule l'icône du secteur est affichée.
5. Pour contrôler les secteurs, utilisez le widget Secteur.

Explorer

- Compter les individus

3.2.15.1 | Colonnes du volet de rapport dans la tâche Présence dans un secteur

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Secteur
Nom du secteur.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Dernier accès
Heure à laquelle le titulaire de cartes est entré dans le secteur.

Photo
Photo du titulaire de cartes ou du visiteur.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

Adresse e-mail
L'adresse e-mail du titulaire de cartes ou du visiteur.

Groupes de titulaires de cartes
Groupes de titulaires de cartes auxquels appartient l'utilisateur.

Hôtes de visiteurs
Titulaires de cartes affectés en tant qu'escortes de visiteurs.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Sujet parent : Suivre les titulaires de cartes présents dans un secteur

3.2.16 | Suivre la présence dans un secteur

Utilisez le rapport *Présence* pour savoir quelles personnes ont accédé à un secteur donné et la durée totale de leur séjour sur une période donnée.

À savoir

Le rapport affiche le temps passé par chaque titulaire de cartes et visiteur sélectionné dans le secteur concerné, pour chaque date couverte par la plage de dates. Par exemple, si un événement est survenu dans le secteur il y a deux jours, vous pouvez savoir qui était dans le secteur concerné au moment de l'incident en sélectionnant le secteur et la plage de dates.

Pour que ce rapport soit précis, le secteur sélectionné doit être entièrement sécurisé, c'est-à-dire que pour entrer et sortir du secteur, les personnes doivent impérativement passer leur badge dans un lecteur. Les lecteurs doivent être installés des deux côtés des portes (pas de *REX*), et les titulaires de cartes doivent franchir la porte les uns après les autres (pas de *talonnage*). Les tourniquets sont souvent utilisés à cette fin.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Présence.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Secteurs
   Sélectionnez les secteurs à examiner.
   REMARQUE : Vous devez sélectionner un secteur entièrement sécurisé.

   Titulaires de cartes
   Limitez votre recherche à des titulaires de cartes ou groupes de titulaires de cartes spécifiques

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Plage horaire
   La plage de dates pour le rapport.

3. Cliquez sur Générer le rapport.
   Le volet de rapport affiche le temps passé par chaque titulaire de cartes et visiteur sélectionné dans le secteur concerné, pendant la plage de dates spécifiée.

3.2.16.1 | Colonnes du volet de rapport dans la tâche Présence

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Date
La date.

Jour de la semaine
Jour de la semaine correspondant à la date.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Photo
Photo du titulaire de cartes ou du visiteur.

Secteur
Nom du secteur.

Temps total
Temps total passé par le titulaire de cartes dans ce secteur à cette date.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.
Sujet parent : Suivre la présence dans un secteur

3.2.17 | Afficher la durée de séjour d'un visiteur

Vous pouvez consulter la durée de séjour des visiteurs actuels et passés, entre l'inscription et la radiation, avec le rapport *Détails de visite*.

À savoir

Si vous souhaitez savoir si un visiteur a été radié avant son départ, vous pouvez analyser ce visiteur, puis voir si la colonne *Date de radiation* est remplie dans le volet de rapport. Vous pouvez également voir les visiteurs qui ont été ajoutés ou supprimés durant la semaine écoulée.

Procédure

1. Sur la page d'accueil, ouvrez la tâche *Détails de visite*.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Date d'inscription
   Date et heure d'activation du profil du visiteur, qui peut correspondre à l'heure d'arrivée.

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Escorte obligatoire
   Indiquez qu'un hôte est obligatoire.

   Arrivée prévue
   Spécifiez la plage horaire d'arrivée supposée du visiteur.

   Date d'expiration
   Spécifiez la plage horaire d'expiration du profil du titulaire de cartes ou du visiteur.

   Prénom
   Prénom du titulaire de cartes ou visiteur.

   Nom
   Nom du titulaire de cartes ou visiteur.

   État
   L'état du profil du titulaire de cartes ou du visiteur : *Actif* ou *Archivé*.

   Hôtes de visiteurs
   Sélectionnez l'hôte du visiteur.

3. Cliquez sur Générer le rapport.
   Les événements de visiteur sont affichés dans le volet de rapport.

4. Pour afficher la photo, le nom et les champs personnalisés d'un visiteur dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas depuis le volet de rapport.
5. Pour afficher des informations supplémentaires sur le visiteur dans la tuile, cliquez sur  .

3.2.17.1 | Colonnes du volet de rapport dans la tâche Détails de visite

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Photo
Photo du titulaire de cartes ou du visiteur.

Date d'inscription
Date et heure d'activation du profil du visiteur (peut correspondre à l'heure d'arrivée).

Date d'expiration
Date et heure d'expiration du profil du titulaire de cartes ou du visiteur.

Date de création
Date et heure de création du profil du visiteur.

Date de radiation
Date et heure de radiation du visiteur (peut correspondre à l'heure de départ).

Hôtes de visiteurs
Titulaires de cartes affectés en tant qu'escortes de visiteurs.

Escorte obligatoire
Indique si un hôte de visiteur est requis.

Arrivée prévue
Date et heure d'arrivée présumées du visiteur.

Durée de la visite
Le temps écoulé entre l'inscription et maintenant pour un visiteur inscrit ; le temps écoulé entre l'arrivée et le départ d'un visiteur qui a été radié. Pour les visiteurs pré-inscrits qui ne sont pas encore arrivés, cette colonne est vide.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Sujet parent : Afficher la durée de séjour d'un visiteur

3.2.18 | Afficher les propriétés des membres d'un groupe de titulaires de cartes

Pour afficher les membres d'un groupe de titulaires de cartes et consulter les propriétés associées aux titulaires (prénom, nom, état, propriétés personnalisées, et ainsi de suite), utilisez la tâche Configuration de titulaires de cartes.

À savoir

Vous pouvez rechercher un groupe de titulaires de cartes particulier pour voir les titulaires qui le composent. Vous pouvez également rechercher les titulaires de cartes expirés ou inactifs au sein de votre système.

Procédure

1. Sur la page d'accueil, ouvrez la tâche *Configuration de titulaires de cartes*.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

\Date d'activation
Spécifiez une plage horaire pour l'activation du profil de titulaire de carte.

Date d'expiration
Spécifiez la plage horaire d'expiration du profil du titulaire de cartes ou du visiteur.

Titulaires de carte non utilisés
Recherchez les titulaires de cartes ou visiteurs dont les identifiants n'ont pas généré d'événement *accès accordé* au cours d'une plage de dates donnée.
REMARQUE : Pour que le rapport produise des résultats, tous les rôles Gestionnaire d'accès doivent être actifs et en ligne.

État
L'état du profil du titulaire de cartes ou du visiteur : *Actif*, *Expiré* ou *Inactif*.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Adresse e-mail
L'adresse e-mail du titulaire de cartes ou du visiteur.

Description
Restreindre la recherche aux entités qui contiennent cette chaîne de caractères.

Photo
Photo du titulaire de cartes ou du visiteur.

Partition
Partition à laquelle appartient l'entité.

Groupes de titulaires de cartes
Limitez votre recherche à des groupes de titulaires de cartes particuliers.

Identifiant
Limitez la recherche à certains identifiants.

État de l'identifiant
L'état de l'identifiant du titulaire de cartes ou du visiteur : Actif ; Expiré ; Inactif ; Perdu ; Volé. Tous les états ne sont pas disponibles dans toutes les tâches.

Informations sur l'identifiant
Limitez la recherche à certains formats de cartes, codes d'installation, numéros de cartes ou plaques d'immatriculation.

Champs personnalisés
Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Peut escorter les visiteurs
Indique si le titulaire de cartes peut agir en tant qu'hôte de visiteur (peut être activé ou désactivé).

3. Cliquez sur Générer le rapport.
   Les titulaires de cartes qui appartiennent au groupe sélectionné sont affichés dans le volet de rapport.
4. Pour afficher un titulaire de cartes dans une tuile, cliquez deux fois sur le titulaire ou faites-le glisser sur le canevas.
5. Pour afficher des informations supplémentaires dans la tuile, cliquez sur  .

3.2.18.1 | Colonnes du volet de rapport dans la tâche Configuration de titulaires de cartes

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Photo
Photo du titulaire de cartes ou du visiteur.

État du titulaire
L'état du profil du titulaire de cartes.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

Groupes de titulaires de cartes
Groupes de titulaires de cartes auxquels appartient l'utilisateur.

Adresse e-mail
L'adresse e-mail du titulaire de cartes ou du visiteur.

Dernier accès
Heure du dernier événement d'accès impliquant le titulaire de cartes, le visiteur ou l'identifiant.

Dernier lieu d'accès
Lieu du dernier événement d'accès impliquant le titulaire de cartes, le visiteur ou l'identifiant.

Dernière décision d'accès
Résultat du dernier événement d'accès impliquant le titulaire de cartes, le visiteur ou l'identifiant.

Peut escorter les visiteurs
Indique si le titulaire de cartes peut agir en tant qu'hôte de visiteur (peut être activé ou désactivé).

Niveau d'accès
Niveau d'accès du titulaire de cartes.

\Date d'activation
Date et heure d'activation du profil du titulaire de carte.

Date d'expiration
Date et heure d'expiration du profil du titulaire de carte.

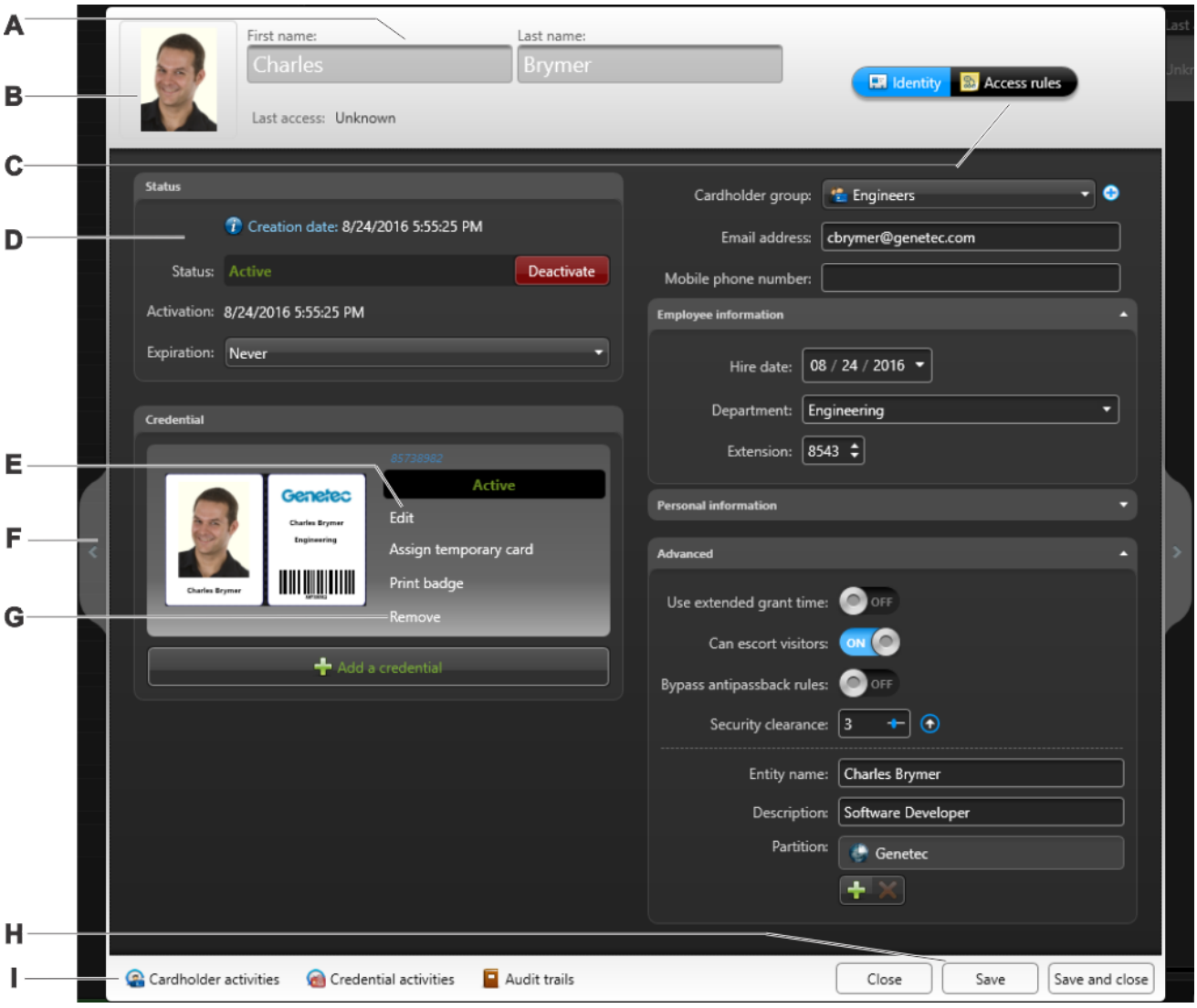
Rôle
Type de rôle qui gère l'entité sélectionnée.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.
Sujet parent : Afficher les propriétés des membres d'un groupe de titulaires de cartes

3.2.19 | Boîte de dialogue Modifier le titulaire de cartes

Une fois que vous avez créé un titulaire de cartes, vous pouvez revenir et modifier ses propriétés, identifiants et droits d'accès en le sélectionnant dans la tâche *Gestion des titulaires de cartes* , puis en cliquant sur *Modifier* ( ).

Les propriétés que vous pouvez modifier dépendent de vos *privilèges d'utilisateur*. La figure suivante montre la boîte de dialogue de modification de titulaire de cartes.



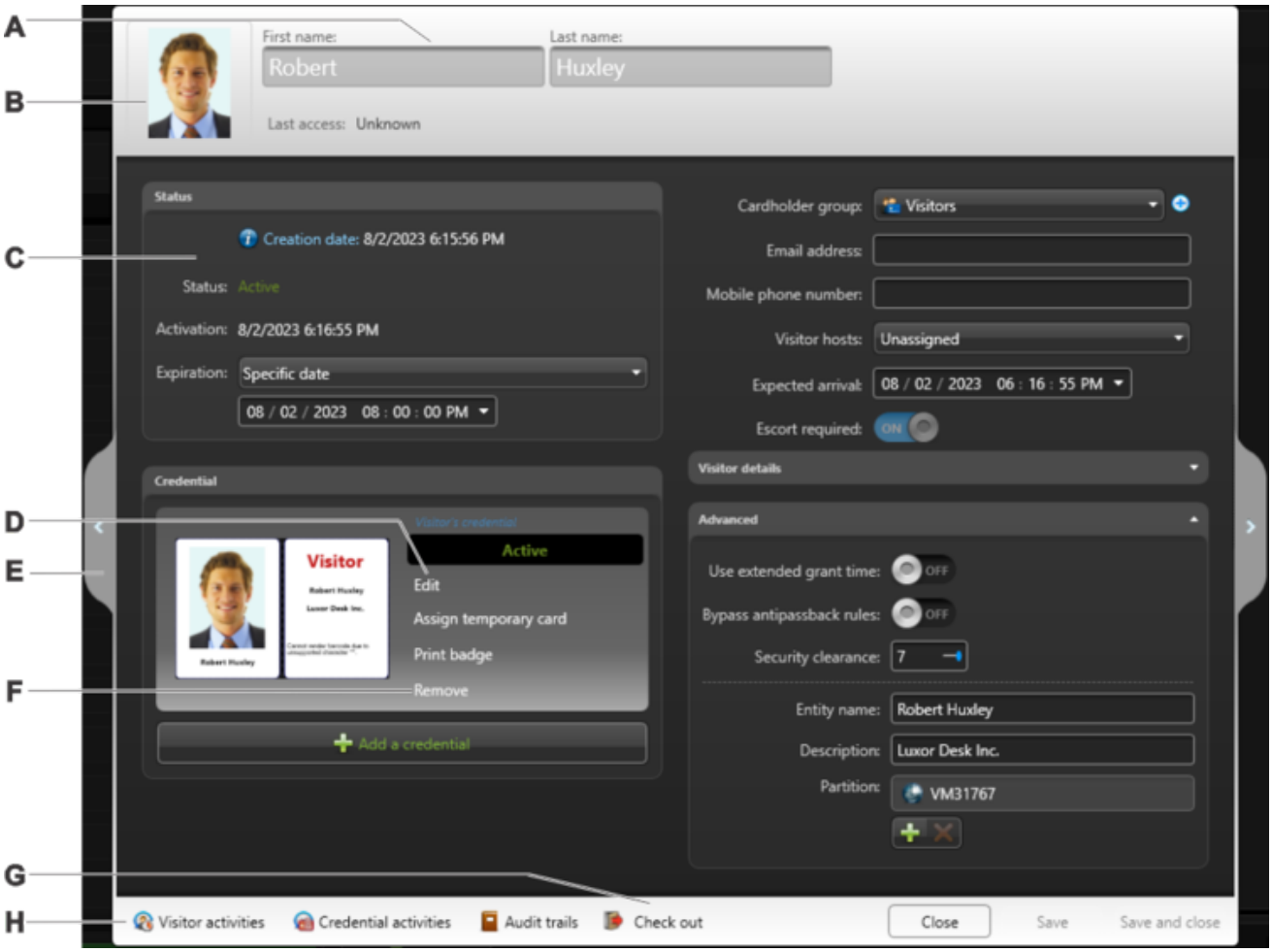
A	Propriétés de base du titulaire de cartes. Les propriétés de titulaire de cartes sont décrites dans Créer des titulaires de cartes.
B	Modifier la photo du titulaire (voir Appliquer un arrière-plan transparent à une photo et Rogner une photo). Pour supprimer la photo du titulaire de cartes, faites un clic droit, puis cliquez sur Effacer l'image.

C	Affectez des droits d'accès supplémentaires au titulaire de cartes dans l'onglet Règles d'accès (voir Affecter des identifiants).
D	Informations complémentaires sur le titulaire de cartes. Ces propriétés sont décrites dans Créer des titulaires de cartes.
E	Modifier l'identifiant du titulaire. Les propriétés d'identifiant sont décrites dans Affecter des identifiants.
F	Supprimer l'identifiant du titulaire.
G	Basculer entre les titulaires de cartes.
H	Enregistrer ou annuler les modifications.
I	•  - Créer un rapport sur le titulaire de cartes (voir Analyser les événements de titulaires de cartes). •  - Créer un rapport sur l'identifiant du titulaire de cartes (voir Analyser les événements d'identifiants). •  - Créer un rapport sur les modifications apportées au titulaire de cartes (voir Rechercher les modifications apportées à la configuration du système).

3.2.20 | Boîte de dialogue Modifier le visiteur

Une fois que vous avez inscrit un visiteur, vous pouvez revenir et modifier ses propriétés en le sélectionnant dans la tâche *Gestion des visiteurs*, puis en cliquant sur *Modifier* ().

Les propriétés que vous pouvez modifier dépendent de vos privilèges d'utilisateur. La figure suivante montre la boîte de dialogue de modification de visiteur.



A	Propriétés de base du visiteur. Les propriétés de visiteur sont décrites dans Inscrire de nouveaux visiteurs.
B	Modifier la photo du visiteur (voir Appliquer un arrière-plan transparent à une photo et Rogner une photo). Pour supprimer la photo du visiteur, faites un clic droit, puis cliquez sur Effacer l'image.
C	Informations complémentaires sur le visiteur. Ces propriétés sont décrites dans Inscrire de nouveaux visiteurs.
D	Modifier l'identifiant du visiteur. Les propriétés d'identifiant sont décrites dans Affecter des identifiants.
E	Basculer entre les visiteurs.
F	Supprimer l'identifiant du visiteur.
G	Enregistrez ou annulez vos modifications, ou radiez le visiteur.
H	• - Créer un rapport sur le visiteur (voir Analyser les événements de visiteurs). • - Créer un rapport sur l'identifiant du visiteur (voir Analyser les événements d'identifiants). • - Créer un rapport sur les modifications apportées au visiteur (voir Rechercher les modifications apportées à la configuration du système).

3.2.21 | Rechercher des titulaires de cartes

Si vous avez un système de contrôle d'accès de taille importante et que vous ne parvenez pas à retrouver un titulaire de cartes, vous pouvez le rechercher par nom, ou utiliser la recherche avancée en appliquant des filtres.

Procédure

1. Sur la page d'accueil, ouvrez la tâche *Gestion des titulaires de cartes*.
2. Pour lancer une recherche par nom d'entité, tapez le nom dans le champ de Recherche ().
   Toutes les entités dont le nom contient le texte saisi sont affichées.
3. Pour rechercher une entité avec la recherche avancée :
   a. Cliquez sur Recherche avancée dans le volet de gauche.
   b. Définissez les filtres de recherche pour votre rapport. Les filtres de recherche ne sont pas tous disponibles dans toutes les tâches. Faites votre sélection parmi les éléments suivants, selon la tâche utilisée :

\Date d'activation
Spécifiez une plage horaire pour l'activation du profil de titulaire de carte.

Date d'expiration
Spécifiez la plage horaire d'expiration du profil du titulaire de cartes ou du visiteur.

Titulaires de carte non utilisés
Recherchez les titulaires de cartes ou visiteurs dont les identifiants n'ont pas généré d'événement *accès accordé* au cours d'une plage de dates donnée.
REMARQUE : Pour que le rapport produise des résultats, tous les rôles Gestionnaire d'accès doivent être actifs et en ligne.

État
L'état du profil du titulaire de cartes ou du visiteur : *Actif*, *Expiré* ou *Inactif*.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Adresse e-mail
L'adresse e-mail du titulaire de cartes ou du visiteur.

Description
Restreindre la recherche aux entités qui contiennent cette chaîne de caractères.

Photo
Photo du titulaire de cartes ou du visiteur.

Partition
Partition à laquelle appartient l'entité.

Groupes de titulaires de cartes
Limitez votre recherche à des groupes de titulaires de cartes particuliers.

Identifiant
Limitez la recherche à certains identifiants.

État de l'identifiant
L'état de l'identifiant du titulaire de cartes ou du visiteur : Actif ; Expiré ; Inactif ; Perdu ; Volé. Tous les états ne sont pas disponibles dans toutes les tâches.

Informations sur l'identifiant
Limitez la recherche à certains formats de cartes, codes d'installation, numéros de cartes ou plaques d'immatriculation.

Peut escorter les visiteurs
Indique si le titulaire de cartes peut agir en tant qu'hôte de visiteur (peut être activé ou désactivé).

c. Cliquez sur Rechercher.

Résultats

Les titulaires de cartes qui correspondent aux critères de recherche sont affichés à l'écran.

Exemple

Imaginons que le titulaire de cartes que vous recherchez a une carte qui a été activée il y a moins d'une semaine. Dans le filtre Date d'activation, saisissez 7 jours dans la zone *Au cours du dernier*.

3.2.21.1 | Colonnes du volet de rapport dans la tâche Gestion des titulaires de cartes

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Photo
Photo du titulaire de cartes ou du visiteur.

État du titulaire
L'état du profil du titulaire de cartes.

Groupes de titulaires de cartes
Groupes de titulaires de cartes auxquels appartient l'utilisateur.

Adresse e-mail
L'adresse e-mail du titulaire de cartes ou du visiteur.

Dernier accès
Heure du dernier événement d'accès impliquant le titulaire de cartes, le visiteur ou l'identifiant.

Dernier lieu d'accès
Lieu du dernier événement d'accès impliquant le titulaire de cartes, le visiteur ou l'identifiant.

Dernière décision d'accès
Résultat du dernier événement d'accès impliquant le titulaire de cartes, le visiteur ou l'identifiant.

Peut escorter les visiteurs
Indique si le titulaire de cartes peut agir en tant qu'hôte de visiteur (peut être activé ou désactivé).

Niveau d'accès
Niveau d'accès du titulaire de cartes.

Date d'expiration
Date et heure d'expiration du profil du titulaire de cartes ou du visiteur.

\Date d'activation
Date et heure d'activation du profil du titulaire de carte.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

Description
Description de l'événement, activité, entité ou incident.
IMPORTANT : Pour respecter la réglementation des États, si l'option Rapport généré est utilisée pour un rapport Historiques d'activité qui contient des données de RAPI, le motif de la recherche RAPI est inclus dans le champ Description.

Rôle
Type de rôle qui gère l'entité fédérée ou importée depuis Active Directory qui est sélectionnée.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.
Sujet parent : Rechercher des titulaires de cartes

3.2.22 | Rechercher des visiteurs

Si vous avez un système de contrôle d'accès de taille importante et que vous ne parvenez pas à retrouver un visiteur, vous pouvez le rechercher par nom, ou utiliser la recherche avancée en appliquant des filtres.

Procédure

1. Sur la page d'accueil, ouvrez la tâche *Gestion des visiteurs*.
2. Pour lancer une recherche par nom d'entité, tapez le nom dans le champ de Recherche ( ).
   Toutes les entités dont le nom contient le texte saisi sont affichées.
3. Pour rechercher une entité avec la recherche avancée :
   a. Cliquez sur Recherche avancée dans le volet de gauche.
   b. Définissez les filtres de recherche pour votre rapport. Les filtres de recherche ne sont pas tous disponibles dans toutes les tâches. Faites votre sélection parmi les éléments suivants, selon la tâche utilisée :

      Date d'inscription
      Date et heure d'activation du profil du visiteur, qui peut correspondre à l'heure d'arrivée.

      Date d'expiration
      Spécifiez la plage horaire d'expiration du profil du titulaire de cartes ou du visiteur.

      Titulaires de carte non utilisés
      Recherchez les titulaires de cartes ou visiteurs dont les identifiants n'ont pas généré d'événement *accès accordé* au cours d'une plage de dates donnée.
      REMARQUE : Pour que le rapport produise des résultats, tous les rôles Gestionnaire d'accès doivent être actifs et en ligne.

      État
      L'état du profil du titulaire de cartes ou du visiteur : *Actif*, *Expiré* ou *Inactif*.

      Prénom
      Prénom du titulaire de cartes ou visiteur.

      Nom
      Nom du titulaire de cartes ou visiteur.

      Adresse e-mail
      L'adresse e-mail du titulaire de cartes ou du visiteur.

      Description
      Restreindre la recherche aux entités qui contiennent cette chaîne de caractères.

      Photo
      Photo du titulaire de cartes ou du visiteur.

Partition
Partition à laquelle appartient l'entité.

Groupes de titulaires de cartes
Limitez votre recherche à des groupes de titulaires de cartes particuliers.

Date de création
Date et heure de création du profil du visiteur.

Identifiant
Limitez la recherche à certains identifiants.

Arrivée prévue
Spécifiez la plage horaire d'arrivée supposée du visiteur.

État de l'identifiant
L'état de l'identifiant du titulaire de cartes ou du visiteur : Actif ; Expiré ; Inactif ; Perdu ; Volé. Tous les états ne sont pas disponibles dans toutes les tâches.

Informations sur l'identifiant
Limitez la recherche à certains formats de cartes, codes d'installation, numéros de cartes ou plaques d'immatriculation.

Champs personnalisés
Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Escorte obligatoire
Indiquez qu'un hôte est obligatoire.

Hôtes de visiteurs
Sélectionnez l'hôte du visiteur.

c. Cliquez sur Rechercher.

Résultats

Les visiteurs qui correspondent aux critères de recherche sont affichés à l'écran.

3.2.22.1 | Colonnes du volet de rapport dans la tâche Gestion des visiteurs

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Photo
Photo du titulaire de cartes ou du visiteur.

État
L'état du profil du visiteur.

Date d’inscription
Date et heure d’activation du profil du visiteur, qui peut correspondre à l’heure d'arrivée.

Date d'expiration
Date et heure d'expiration du profil du titulaire de cartes ou du visiteur.

Date de création
Date et heure d'activation de l'identifiant du visiteur (peut correspondre à l'heure d'arrivée).

Hôtes de visiteurs
Titulaires de cartes affectés en tant qu'escortes de visiteurs.

Dernier accès
Heure du dernier événement d'accès impliquant le titulaire de cartes, le visiteur ou l'identifiant.

Dernier lieu d'accès
Lieu du dernier événement d'accès impliquant le titulaire de cartes, le visiteur ou l'identifiant.

Dernière décision d'accès
Résultat du dernier événement d'accès impliquant le titulaire de cartes, le visiteur ou l'identifiant.

Arrivée prévue
Date et heure d'arrivée présumées du visiteur.

Description
Description de l'événement, activité, entité ou incident.
IMPORTANT : Pour respecter la réglementation des États, si l'option Rapport généré est utilisée pour un rapport Historiques d'activité qui contient des données de RAPI, le motif de la recherche RAPI est inclus dans le champ Description.

Escorte obligatoire
Indique si un hôte de visiteur est requis.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.
Sujet parent : Rechercher des visiteurs

3.2.23 | Rechercher un titulaire de cartes ou visiteur à l'aide de son identifiant

Si vous trouvez une carte non identifiée, vous pouvez rechercher son propriétaire en passant la carte sur un lecteur USB ou de porte.

Avant de commencer

Vérifiez qu'un lecteur USB est connecté à votre ordinateur ou que vous disposez d'un lecteur de porte à proximité pour lire la carte.

Procédure

1. Ouvrez l'une des tâches suivantes depuis la page d'accueil :
   - Pour les titulaires de cartes, cliquez sur Gestion des titulaires de cartes.
   - Pour les visiteurs, cliquez sur Gestion des visiteurs.
2. Au sommet de la fenêtre de la tâche, cliquez sur  .
3. Dans la liste déroulante de la fenêtre de recherche, sélectionnez un des éléments suivants :

   Lecteur USB
   Un lecteur USB connecté à votre ordinateur.

   Porte
   Un point d'accès à proximité.

4. Lisez la carte avec l'appareil sélectionné à l'étape précédente.

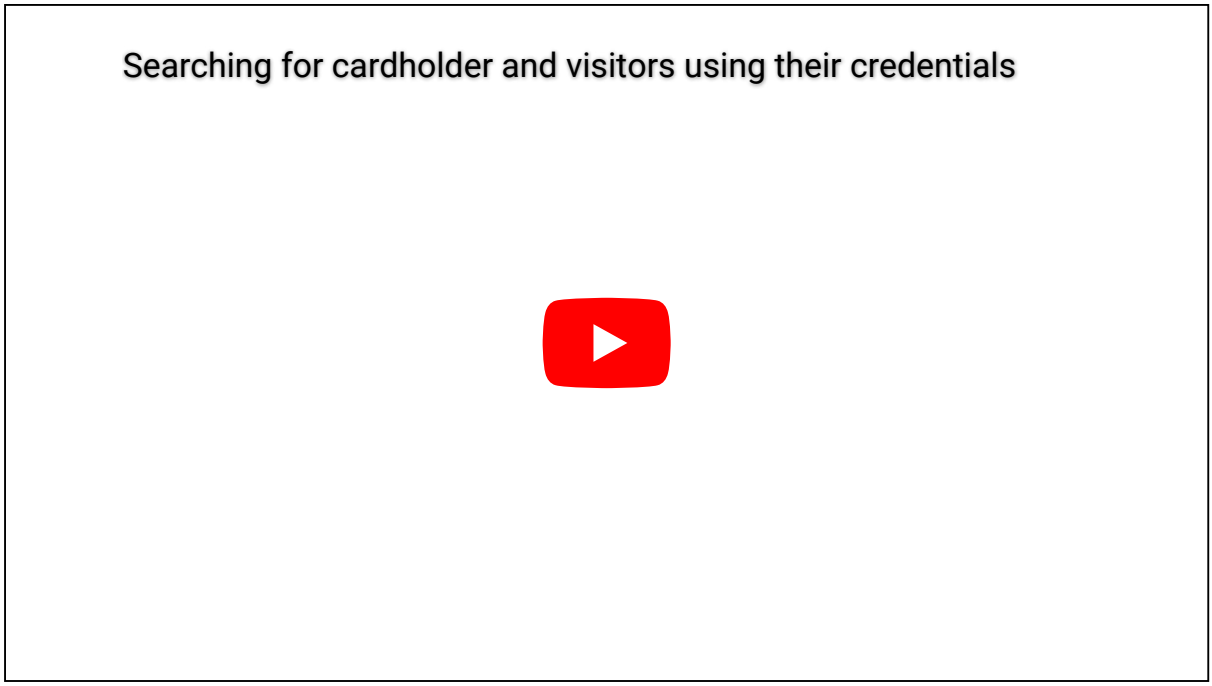
Résultats

Si la carte est affectée à un titulaire de cartes ou visiteur, la boîte de dialogue de recherche se referme et l'individu est affiché dans la liste des titulaires de cartes ou des visiteurs. Si la carte n'est pas affectée à un titulaire de cartes ou visiteur, le motif de refus de la carte est affiché dans la boîte de dialogue de recherche. Vous pouvez lire une autre carte ou cliquer sur Annuler pour interrompre l'opération.

Exemple

Si vous trouvez une carte sans nom ni photo dans un bureau ou un parking, vous pouvez identifier à qui elle appartient.

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.



3.3 | Identifiants Security Center dans Security Desk

3.3.1 | À propos des identifiants

Type d'entité qui représente une carte de proximité, un modèle biométrique ou un code PIN exigé pour accéder à un secteur sécurisé. Un identifiant ne peut être affecté qu'à un titulaire à la fois.

L'entité identifiant représente une carte de proximité, un modèle biométrique ou un code PIN. Les identifiants permettent à Security Center d'identifier les individus qui demandent le passage par un point d'accès sécurisé. Les identifiants sont en quelque sorte des *preuves d'identité*. Les identifiants distinguent les titulaires de cartes les uns des autres. Pour que le contrôle d'accès soit efficace, chaque titulaire de cartes doit avoir au moins un identifiant. Il s'agit le plus souvent (mais non pas exclusivement) de cartes de contrôle d'accès.

L'identifiant nécessaire dépend du type de lecteur installé sur la porte.

Security Center Formats de carte natifs

Security Center prend en charge plusieurs formats de carte standard.

Pour les formats de type carte, un numéro de carte est obligatoire. Selon le format de carte, le code d'installation est obligatoire ou non. Le tableau suivant décrit les formats de carte standard pris en charge par Security Center, et les plages valables pour le code d'installation (également appelé *Company ID Code*) et le numéro de carte (également appelé *Card ID Number*).

Format de carte	Plage de code d'installation	Plage de numéro de carte
Standard 26 bits	0 à 255	0 à 65 535
HID H10306 34 Bits	0 à 65 535	0 à 65 535
HID H10302 37 bits	Non requis[1]	0 à 34 359 738 367
HID H10304 37 Bits	0 à 65 535	0 à 524 287
HID Corporate 1000 35 bits	0 à 4095	0 à 1 048 575
HID Corporate 1000 48 bits	0 à 4 194 303	0 à 8 388 607
CSN 32 bits	Non requis	0 à FFFFFFFF
FASC-N 75 bits[2]	-	-
FASC-N 200 bits[2]	-	-

[1]Si le format HID H10302 37 bits est le seul format référencé dans votre fichier CSV, il est préférable d'associer le numéro de carte au champ Données de la carte de Security Center plutôt qu'au champ Numéro de carte, puisque le code d'installation n'est pas requis. Et puisqu'une seule valeur est stockée dans le champ Données de la carte, il est inutile de spécifier un séparateur.

Les formats de carte personnalisés sont également pris en charge, dès lors qu'ils ont été prédéfinis dans votre système. Pour en savoir plus sur la création de formats de carte personnalisés, voir le *Guide de l'administrateur Security Center*.

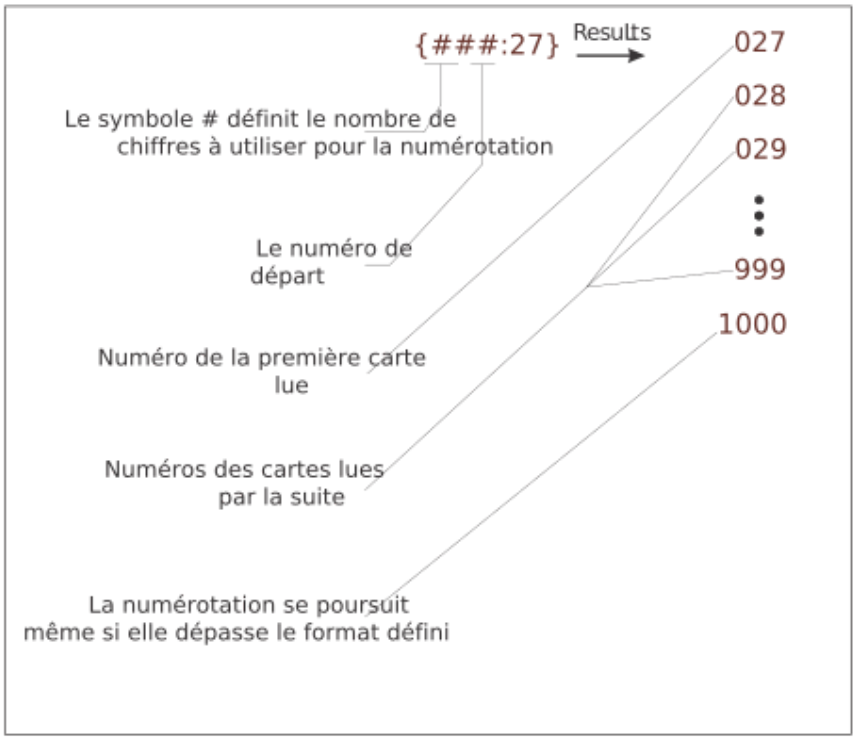
[2] Pour en savoir plus sur les formats FASC-N 75 bits et FASC-N 200 bits, voir Fonctionnement des formats de cartes avec Active Directory dans Security Center.

Le préfixe d'identifiant et le compteur

Le Préfixe d'identifiant détermine le nom des identifiants inscrits. La tâche Gestion des identifiants assure que tous les identifiants inscrits ont un nom unique en leur ajoutant automatiquement un numéro défini dans Préfixe de l'identifiant. Vous pouvez contrôler le compteur en ajoutant un format de numérotation automatique (entre accolades) au préfixe des identifiants.

Le format de numérotation automatique détermine le style du compteur. Le format de numérotation automatique peut être placé n'importe où au sein du préfixe d'identifiant. Un seul format de numérotation automatique peut être utilisé dans le préfixe d'identifiant à la fois.

Le format de numérotation automatique est expliqué ci-dessous.



Voici des exemples de format de numérotation automatique.

Préfixe de l'identifiant	Séquence d'identifiants générée	Commentaires
Identifiant_	Identifiant_0 Identifiant_1 Identifiant_2	Lorsque le format de numérotation n'est pas précisé, le numéro automatique est ajouté à la fin du préfixe, et démarre à 0.
Identifiant #{##:1}	Identifiant #01 Identifiant #02 Identifiant #03	Une numérotation automatique de base ajoutée au préfixe d'identifiant.
1{####:46} 11203162-2	10046 11203162-2 10047 11203162-2 10048 11203162-2	Les identifiants inscrits peuvent être numérotés automatiquement dans Security Center afin que leur nom corresponde au numéro de série imprimé au verso d'une série de cartes.

Recommandation de code PIN

Lorsque vous utilisez un code PIN en tant qu'identifiant, vous pouvez l'utiliser seul (Carte ou code PIN) ou avec une carte (Carte et code PIN). Les capacités et la configuration du lecteur déterminent les exigences relatives au code PIN.

Si vous comptez utiliser vos lecteurs en mode Carte ou code PIN, veillez à ce que les codes PIN soient uniques pour tous les titulaires de cartes et vérifiez qu'il n'y a pas de doublons dans le système. Un code PIN en double peut créer de la confusion puisqu'il est impossible de savoir à quel titulaire de cartes il appartient lorsqu'il est saisi à une porte.

Identifiants bruts

Dans Security Center 5.8 ou ultérieur, toute lecture d'identifiant qui ne correspond pas à un format de carte natif ou personnalisé est affichée sous la forme Brut [n] bits, où *[n]* est la longueur en bits de la carte.

3.3.1.1 | À propos du format de carte FASC-N et des identifiants bruts

Un numéro FASC-N (Federal Agency Smart Credential Number) est un identifiant utilisé dans les justificatifs d'identité personnels (Personal Identity Verification ou PIV) émis par les agences fédérales américaines. La longueur en bits des identifiants FASC-N varie en fonction de la configuration du lecteur. Security Center prend en charge nativement les formats de 75 ou 200 bits.

Les identifiants FASC-N peuvent être créés manuellement dans Config Tool ou Security Desk à l'aide de la liste de définitions des Formats de carte natifs ou en utilisant l'Inscription par lots dans la tâche Gestion des identifiants de Security Desk.

Vous pouvez également importer des identifiants FASC-N et au format brut depuis un fichier CSV à l'aide de l'outil Importation dans Config Tool ou le SDK Security Center. Lorsque vous sélectionnez Données brutes des identifiants sur la page Associations pendant l'importation, Security Center reconnaît automatiquement les identifiants et les formats.

Les identifiants non gouvernementaux PIV-I (Personal Identity Verification-Interoperable) et CIV (Commercial Identity Verification) génèrent l'identifiant CHUID.GUID, qui est reconnu par Security Center en tant qu'identifiant brut de 128 bits, et l'identifiant peut aussi être associé à un format de carte personnalisé.

Sujet parent : À propos des identifiants

3.3.2 | Méthodes d'inscription des identifiants

Si votre système de contrôle d'accès requiert de nombreuses cartes d'identification, vous pouvez inscrire plusieurs cartes en même temps.

Les deux méthodes d'inscription suivantes sont disponibles dans la tâche *Gestion des identifiants* :

Saisie automatique
La saisie automatique est la méthode d'inscription recommandée lorsque vous disposez des cartes à inscrire, et que les données de carte n'appartiennent pas à une plage de données connue. Il convient également d'utiliser cette méthode d'inscription lorsque vous utilisez différents formats de carte.

Saisie manuelle
La saisie manuelle est la méthode d'inscription conseillée lorsque toutes les cartes à inscrire sont du même format et que l'un des champs de données (généralement, le *Numéro de carte*) contient une série de valeurs consécutives. Il n'est pas nécessaire de disposer des cartes physiques ni d'un lecteur pour utiliser cette méthode d'inscription, qui peut s'avérer pratique pour inscrire un grand nombre de cartes à l'avance.

Vous pouvez également inscrire les identifiants à l'aide de l'*Outil Importation*. Pour en savoir plus sur l'importation d'identifiants avec l'*Outil d'importation*, voir le *Guide de l'administrateur Security Center*.

3.3.3 | Inscrire plusieurs identifiants automatiquement

Si votre système de contrôle d'accès requiert de nombreuses cartes d'identification, vous pouvez inscrire plusieurs cartes automatiquement en les passant dans un lecteur.

Avant de commencer

Vous devez avoir accès à un lecteur de cartes. Le format des cartes que vous souhaitez inscrire doit être prédéfini dans votre système.

Vérifiez qu'il s'agit de la méthode d'inscription adaptée à vos besoins.

À savoir

Tous les identifiants à inscrire doivent être inconnus du système Security Center. Tout identifiant préalablement enregistré est rejeté car un même identifiant ne peut pas être enregistré deux fois dans Security Center.

Pour en savoir plus sur comment coder un identifiant sur une carte avant de l'inscrire, voir Affecter des identifiants.

Procédure

1. Dans la tâche Gestion des identifiants, cliquez sur Inscription par lots.
2. Cliquez sur l'onglet Saisie automatique.
3. Indiquez si vous souhaitez passer la carte sur un lecteur USB connecté en local ou sur une porte à proximité :
   - Sélectionnez Lecteur USB RF IDeas ou Lecteur USB Omnikey dans la liste, connectez un lecteur de cartes correspondant au poste local, et cliquez sur Actualiser ( ).
   - Sélectionnez Porte dans la liste, puis sélectionnez une entité porte en tant que Point d'accès.
4. Dans la section Préfixe d'identifiant, entrez le format que vous souhaitez affecter au nom des identifiants inscrits.
5. Dans la section État de l'identifiant, configurez l'état, la date d'activation et d'expiration des identifiants à inscrire.

   État
   Toutes les valeurs possibles sont acceptées.

   Activation
   Peut être réglée sur *Jamais* ou sur une date particulière.

   Expiration
   Spécifiez un délai d'expiration pour l'identifiant :

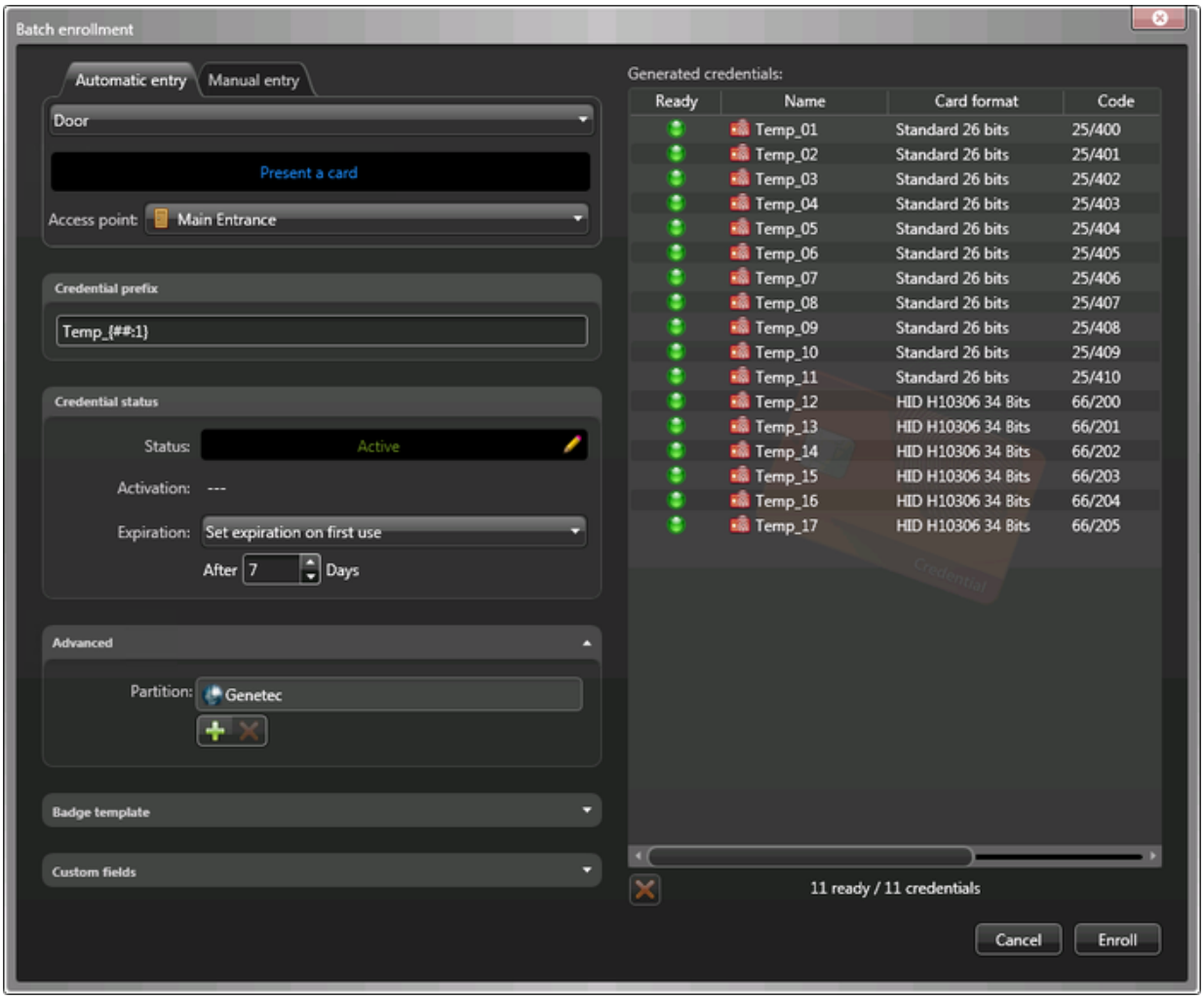
   Jamais
   L'identifiant n'expire jamais.

   Date spécifique
   L'identifiant expire à une date et heure particulières.

   Expiration après la première utilisation
   L'identifiant expire un certain nombre de jours après sa première utilisation.

   En cas d'inutilisation
   L'identifiant expire s'il n'a pas été utilisé durant un certain nombre de jours.

6. Dans la section Avancé, sélectionnez la partition à laquelle les identifiants inscrits doivent être affectés.
   Ce champ détermine quels utilisateurs peuvent voir et modifier les identifiants.
   - Pour ajouter une partition, cliquez sur Ajouter ( ).
   - Pour supprimer une partition, sélectionnez-la, puis cliquez sur Supprimer ( ).
7. Dans la liste Modèle de badge, sélectionnez le modèle de badge par défaut utilisé pour représenter l'identifiant.
8. Dans la section Champs personnalisés, spécifiez les valeurs par défaut des champs personnalisés.
   Cette section n'est disponible que si des champs personnalisés ont été créés pour les identifiants.
9. Passez les cartes sur le lecteur sélectionné.
   Les cartes lues sont affichées dans la section Identifiants générés. Si certains identifiants sont déjà inscrits, ils sont rejetés, et sont affichés dans la liste avec un bouton rouge.



10. Pour supprimer un identifiant rejeté de la liste, sélectionnez-le et cliquez sur .
11. Cliquez sur Inscrire.

Lorsque vous avez terminé

Affectez les identifiants aux titulaires de cartes.

Explorer

- À propos des identifiants

3.3.4 | Inscrire plusieurs identifiants manuellement

Si votre système de contrôle d'accès requiert de nombreuses cartes d'identification, vous pouvez inscrire plusieurs cartes à la fois en saisissant manuellement le format et les données de carte.

Avant de commencer

Vous devez connaître la plage exacte de valeurs représentées dans les données de cartes. Puisque les cartes ne sont pas passées sur un lecteur, l'application n'a aucun moyen de les valider.

Vérifiez qu'il s'agit de la méthode d'inscription adaptée à vos besoins.

À savoir

Tous les identifiants à inscrire doivent être inconnus du système Security Center. Tout identifiant préalablement enregistré est rejeté car un même identifiant ne peut pas être enregistré deux fois dans Security Center. 5000 identifiants peuvent être créés à la fois.

Procédure

1. Dans la tâche Gestion des identifiants, cliquez sur Inscription par lots.
2. Cliquez sur l'onglet Saisie manuelle.
3. Dans la liste Format de carte, sélectionnez le format de carte des cartes que vous souhaitez inscrire.
   Cette option détermine les champs de données que vous devez remplir ainsi que leur plage de valeurs.
4. Dans les champs Code d'installation et Numéro de carte, entrez les valeurs de début et de fin pour les numéros de carte.
   Le champ Numéro de carte sert de générateur de séquence.
   REMARQUE : Si la plage de Numéro de carte spécifiée contient plus de 5000 valeurs, la valeur de fin est automatiquement réglée sur la valeur de début plus 5000.
5. Dans la section Préfixe d'identifiant, entrez le format que vous souhaitez affecter au nom des identifiants inscrits.
6. Dans la section État de l'identifiant, configurez l'état, la date d'activation et d'expiration des identifiants à inscrire.

   État
   Toutes les valeurs possibles sont acceptées.

   Activation
   Peut être réglée sur *Jamais* ou sur une date particulière.

   Expiration
   Spécifiez un délai d'expiration pour l'identifiant :

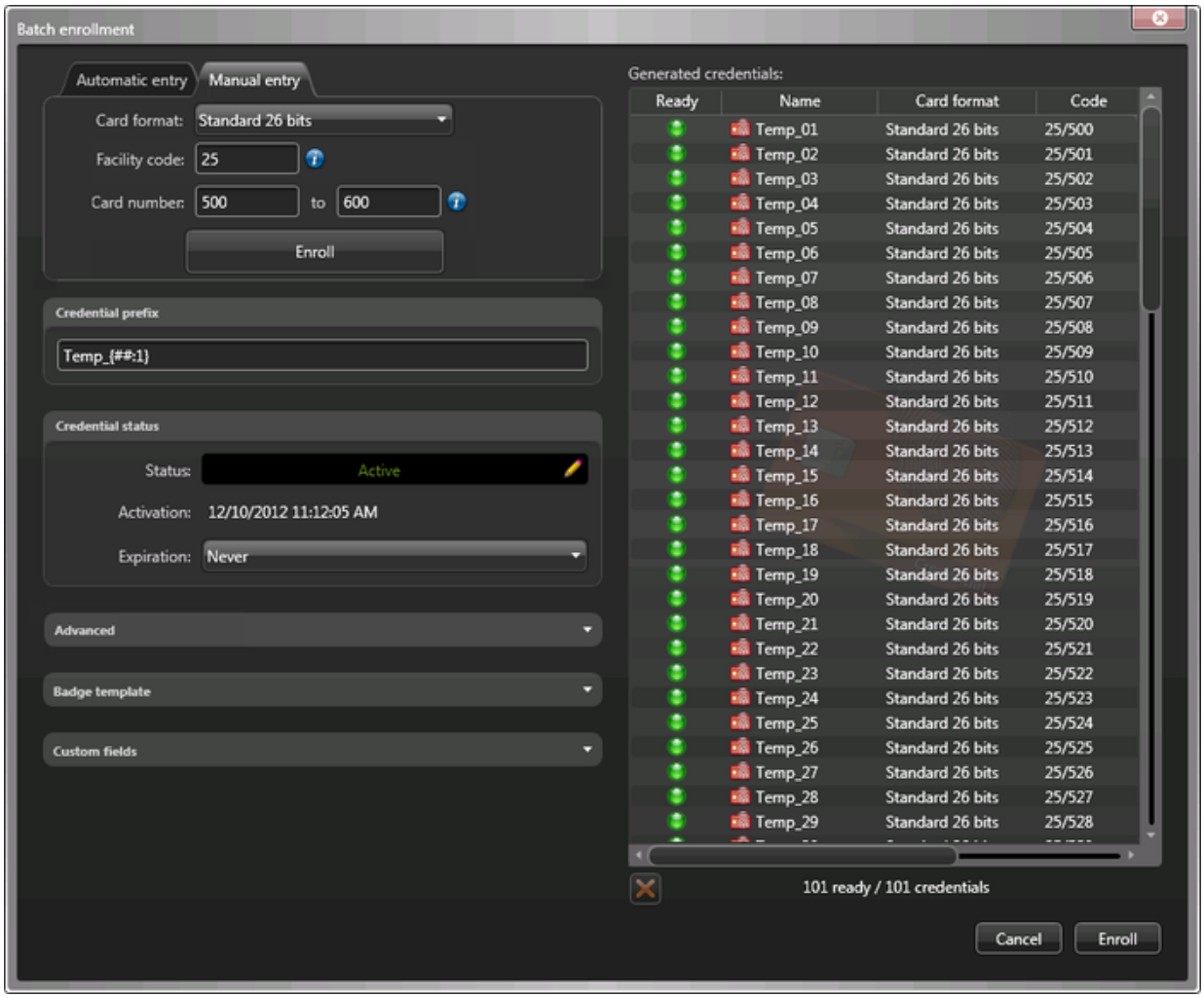
   Jamais
   L'identifiant n'expire jamais.

   Date spécifique
   L'identifiant expire à une date et heure particulières.

   Expiration après la première utilisation
   L'identifiant expire un certain nombre de jours après sa première utilisation.

   En cas d'inutilisation
   L'identifiant expire s'il n'a pas été utilisé durant un certain nombre de jours.

7. Dans la section Avancé, sélectionnez la partition à laquelle les identifiants inscrits doivent être affectés.
   Ce champ détermine quels utilisateurs peuvent voir et modifier les identifiants.
   - Pour ajouter une partition, cliquez sur Ajouter ().
   - Pour supprimer une partition, sélectionnez-la, puis cliquez sur Supprimer ().
8. Dans la liste Modèle de badge, sélectionnez le modèle de badge par défaut utilisé pour représenter l'identifiant.
9. Dans la section Champs personnalisés, spécifiez les valeurs par défaut des champs personnalisés.
   Cette section n’est disponible que si des champs personnalisés ont été créés pour les identifiants.
10. Cliquez sur Inscrire.
    Les identifiants que vous allez créer sont affichés dans la section Identifiants générés. Si certains identifiants sont déjà inscrits, ils sont rejetés, et sont affichés dans la liste avec un bouton rouge.



11. Pour supprimer un identifiant rejeté de la liste, sélectionnez-le et cliquez sur .
12. Cliquez sur Inscrire.

Lorsque vous avez terminé

Affectez les identifiants aux titulaires de cartes.

Explorer

- À propos des identifiants

3.3.5 | Créer un identifiant

Vous pouvez créer un identifiant, configurer ses propriétés, et l'affecter à un titulaire de carte ou visiteur avec la tâche *Gestion des identifiants*.

À savoir

Au lieu de créer les identifiants manuellement, vous pouvez les importer depuis un fichier CSV ou depuis l'annuaire Active Directory de votre société. Pour en savoir plus, voir le *Guide de l'administrateur Security Center*).

Procédure

1. Dans la tâche Gestion des identifiants, cliquez sur Créer un identifiant ( ).
2. Sélectionnez l'une des options suivantes :

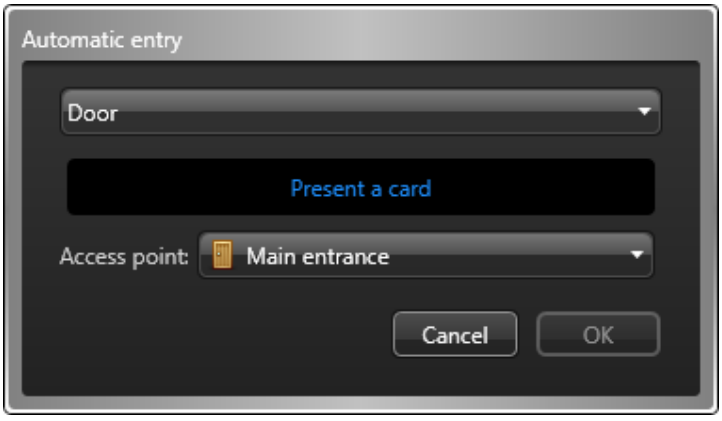
   Saisie automatique
   Passez la carte sur un lecteur.

Saisie manuelle
Entrez manuellement les données de carte. Utilisez cette méthode lorsque vous n'avez pas de lecteur de cartes à proximité.

Code PIN
Créer un code PIN.

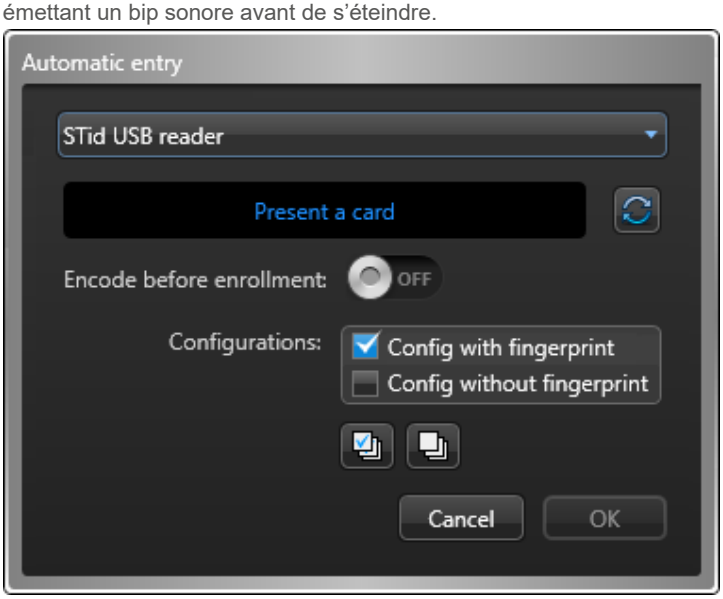
Plaque d’immatriculation
Entrez le numéro de plaque d'immatriculation d'un titulaire de cartes. Utilisez cette méthode si une caméra Sharp sert à utiliser une barrière d'accès pour véhicules. Dans ce cas, la plaque d'immatriculation du titulaire de cartes peut servir d'identifiant.

3. Si vous sélectionnez Saisie automatique, vous devez sélectionner un lecteur (USB ou porte), et passer la carte sur le lecteur.

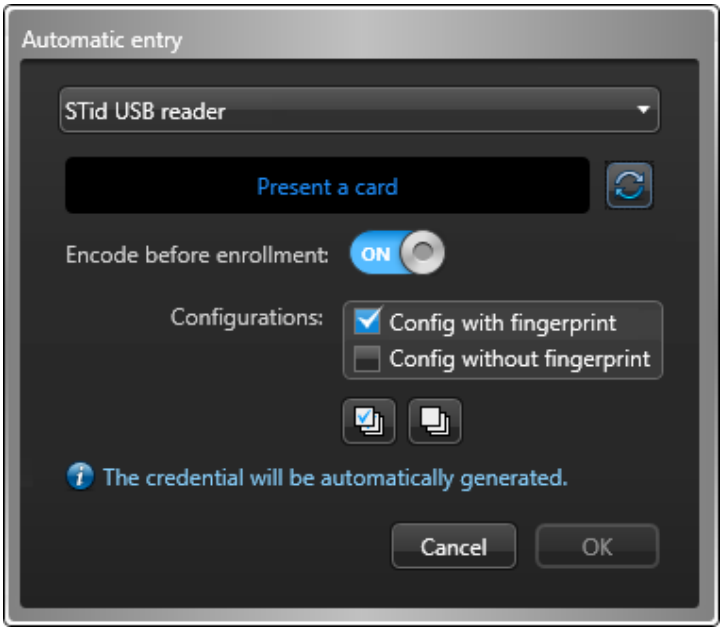


Si vous avez un lecteur qui permet de coder les cartes à puce, procédez de l’une des manières suivantes :

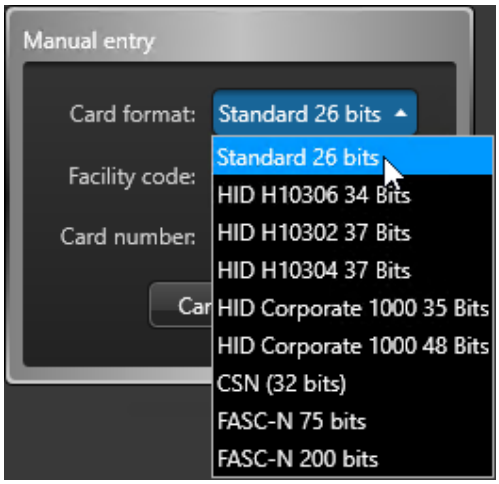
- Pour lire une carte préconfigurée, désactivez l'option Coder avant l’inscription. Lorsque le témoin DEL du lecteur vire au vert (prêt à la lecture), placez la carte à puce sur le lecteur. Le témoin DEL passe au jaune puis au vert en émettant un bip sonore avant de s’éteindre.



- Pour générer et coder un identifiant 128 bits aléatoire MIFARE DESFire avant de l’inscrire, réglez l’option Coder avant l’inscription sur Activé. Lorsque le témoin DEL du lecteur vire au vert (prêt au codage), placez la carte à puce sur le lecteur pendant environ 2 secondes. Le témoin DEL passe au jaune puis au vert en émettant un bip sonore avant de s’éteindre. Si vous entendez un bip long et que le témoin DEL reste rouge, réessayez.
  REMARQUE : Votre licence Security Center doit prendre en charge le codage de cartes à puce.

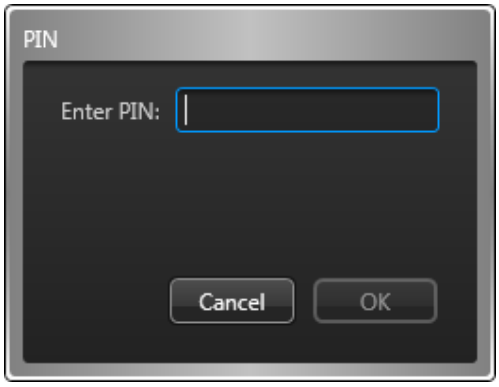


4. Si vous sélectionnez Saisie manuelle, vous devez sélectionner un format de carte, renseigner les champs de données requis, puis cliquer sur OK.



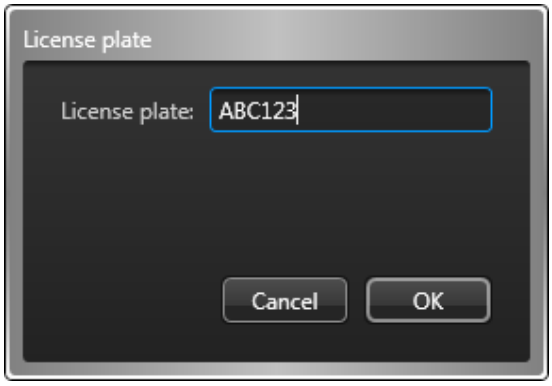
ATTENTION :
Saisissez les données de carte soigneusement, car le système ne peut pas savoir si les données saisies correspondent ou non à une carte physique.

5. Si vous sélectionnez Code PIN, vous devez procéder de la manière suivante :



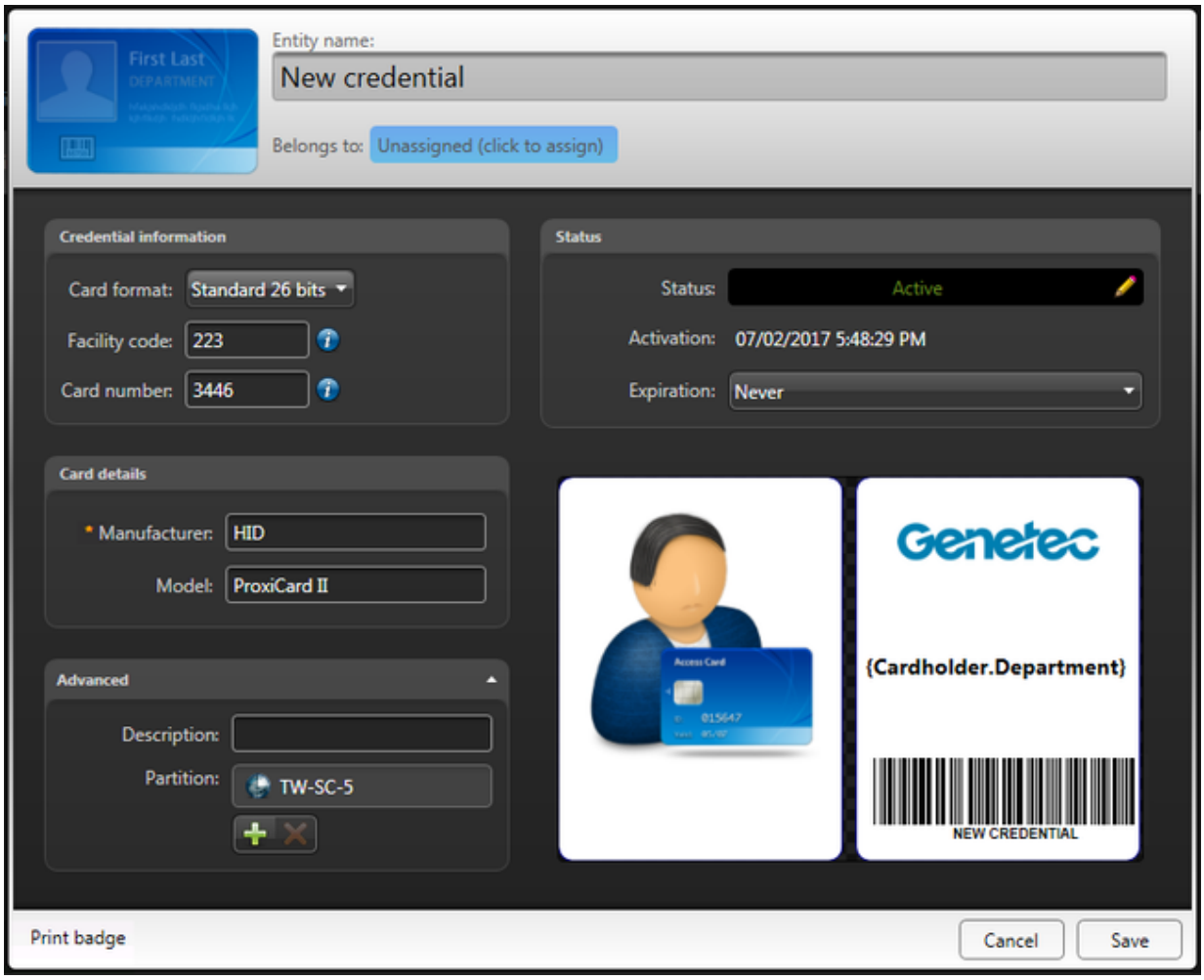
   a. Entrez le code PIN sous forme de valeur numérique.
      REMARQUE : Veillez à ne pas dépasser le nombre de chiffres accepté par vos lecteurs. Un code PIN est généralement composé de cinq chiffres. Toutefois, certains modèles acceptent jusqu'à 15 chiffres.
   b. Cliquez sur OK.

6. Si vous sélectionnez Plaque d'immatriculation, vous devez procéder de la manière suivante :



   a. Entrez le numéro de plaque d'immatriculation.
      REMARQUE : Il est inutile de saisir les espaces qui apparaissent dans le numéro de plaque d'immatriculation. Pour le système, « ABC123 » et « ABC 123 » sont équivalents.
   b. Cliquez sur OK.

7. Dans le champ Nom de l'entité, donnez un nom à l'entité identifiant.
   La capture d'écran suivante représente des identifiants de type carte. La boîte de dialogue n'a pas le même aspect si vous sélectionnez des identifiants de type Code PIN ou Plaque d'immatriculation.



8. Cliquez dans le champ Appartient à, sélectionnez un titulaire de cartes ou un visiteur à qui affecter la carte, puis cliquez sur OK.
   Si vous n'affectez pas d'identifiant, vous ne pouvez pas suivre les activités du titulaire ou visiteur, ni créer de rapport d'activité pour celui-ci.
9. Dans la section État, modifiez l'état et la période d'activation de l'identifiant.
   Si l'identifiant est inactif, le titulaire de cartes ou visiteur n'a pas accès au secteur.

   État
   Réglez l'état du titulaire de cartes sur Actif.

   Activation
   Affiche la date actuelle.

   Expiration
   Spécifiez un délai d'expiration pour l'identifiant :

   Jamais
   L'identifiant n'expire jamais.

   Date spécifique
   L'identifiant expire à une date et heure particulières.

   Expiration après la première utilisation
   L'identifiant expire un certain nombre de jours après sa première utilisation.

   En cas d'inutilisation
   L'identifiant expire s'il n'a pas été utilisé durant un certain nombre de jours.

10. Si des champs personnalisés sont définis pour les identifiants, comme le fabricant, le modèle de carte, etc., entrez les informations personnalisées de l'identifiant dans la section concernée.

11. (Facultatif) Dans la section Avancé, configurez les propriétés d'identifiant suivantes :
    a. Décrivez l'identifiant dans le champ Description.
    b. Affectez l'identifiant à une *partition*.
    Les partitions déterminent quels utilisateurs Security Center ont accès à cette entité. Seuls les utilisateurs qui ont un accès à la partition peuvent voir l'identifiant.
12. (Facultatif) Si l'identifiant est une carte (pas un code PIN), sélectionnez un modèle de badge.
    a. Cliquez sur l'image de badge dans le coin inférieur droit de la boîte de dialogue Détails de l'identifiant.
    b. Sélectionnez un modèle de badge, puis cliquez sur OK.
    Les modèles de badge sont créés dans Config Tool. Pour plus de détails, voir le *Guide de l'administrateur Security Center*.
    Un aperçu avant impression du badge apparaît, avec données de l'identifiant concerné.
    REMARQUE : Le modèle de badge reste associé à l'identifiant même si vous supprimez l'identifiant du titulaire de cartes ou du visiteur.
13. Pour imprimer le badge, cliquez sur Imprimer un badge dans le coin inférieur gauche de la boîte de dialogue Détails sur l'identifiant.
14. Lorsque vous avez terminé de modifier l'identifiant, cliquez sur Enregistrer.

Résultats

Le nouvel identifiant est ajouté à la liste de la tâche Gestion des identifiants.

Lorsque vous avez terminé

Pour modifier un identifiant, sélectionnez-le dans la liste, puis cliquez sur Modifier ( ).
Explorer

- Affecter des identifiants
- Demander une carte d'identification
- Présentation de la tâche Gestion des identifiants

3.3.6 | Répondre aux demandes de cartes d'identification

En cas de demande de carte d'identification, vous pouvez répondre en affectant l'identifiant au demandeur ou en refusant la demande.

À savoir

Le nombre de demandes de cartes en attente est affiché sur l'icône Demandes de cartes ( ) dans la zone de notification, et en haut de la tâche Gestion des identifiants.

Les demandes d'identifiants sont envoyées lorsqu'un utilisateur crée un titulaire de carte, mais ne peut pas affecter un identifiant ou imprimer une carte pour le titulaire (par exemple, parce qu'aucune imprimante n'est disponible). Une fois la carte affectée et imprimée, elle peut être envoyée à un autre site si nécessaire.

Procédure

1. Procédez de l'une des manières suivantes :
    - Dans la zone de notification, cliquez sur Demandes de cartes ( ).
    - En haut de la tâche Gestion des identifiants, cliquez sur Demandes de cartes.
2. Dans la boîte de dialogue Demandes de cartes, sélectionnez la demande à laquelle vous souhaitez répondre.
   Appuyez sur `Maj` pour sélectionner plusieurs demandes.
3. Pour modifier la demande, cliquez sur Modifier ( ), apportez vos modifications, puis cliquez sur OK.
4. Pour refuser la demande, cliquez sur Refuser la demande ( ).
5. Pour affecter un identifiant de type carte, cliquez sur Associer une carte ( ).
   Dans la boîte de dialogue Associer des cartes, procédez de l'une des manières suivantes :

- Pour affecter un identifiant automatiquement, cliquez sur Saisie automatique, sélectionnez un lecteur (USB ou porte), et passez la carte sur le lecteur.

  Si une carte éligible est présentée, elle est immédiatement affectée. La carte est automatiquement inscrite si ce n'était pas déjà le cas. Si la carte est déjà affectée à quelqu'un, elle est refusée.

  Pour en savoir plus sur comment coder un identifiant sur une carte avant de l'inscrire, voir Affecter des identifiants.

- Pour affecter un identifiant manuellement, cliquez sur Saisie manuelle, puis sélectionnez un format de carte, renseignez les champs obligatoires, et cliquez sur Inscrire.

  Si une carte éligible est saisie, elle est immédiatement affectée. La carte est automatiquement inscrite si ce n'était pas déjà le cas. Si la carte est déjà affectée à quelqu'un, elle est refusée.

  ATTENTION :
  Saisissez les données de carte soigneusement, car le système ne peut pas savoir si les données saisies correspondent ou non à une carte physique.
- Pour affecter un identifiant existant, cliquez sur Identifiant existant, puis cliquez deux fois sur un identifiant dans la liste des identifiants éligibles.

6. Pour imprimer le badge ou la carte, cliquez sur Imprimer des cartes ( ) et suivez les instructions.
7. Cliquez sur Fermer pour terminer la demande.

Résultats

Une fois que la demande de carte est terminée ou refusée, un e-mail est envoyé au demandeur s'il a sélectionné l'option Me prévenir par e-mail lorsque la carte est prête lors de sa demande.
Explorer

- Créer un identifiant
- Demander une carte d'identification

3.3.7 | Analyser l'historique des demandes d'identifiants

Utilisez le rapport *Historique de demande d'identifiants* pour voir quels utilisateurs ont demandé, annulé et imprimé des cartes d'identification.

Avant de commencer

Pour obtenir des résultats dans le rapport Historique de demande d'identifiants, vous devez déjà être en train de surveiller les activités de demande d'identifiants des utilisateurs. Vous pouvez sélectionner les activités à surveiller et enregistrer dans la base de données depuis la tâche *Système*.

À savoir

Les badges d'identification sont généralement demandés lorsqu'aucune imprimante n'est disponible sur site. Vous pouvez créer un rapport sur les badges imprimés durant le mois écoulé dans le cadre de votre facturation.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Historique de demande d'identifiants.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

Activités
Sélectionnez les activités de badge à analyser.

Demande d'identifiant
Lorsqu'un utilisateur demande l'impression d'un badge.

Demande d'identifiant annulée
Lorsqu'un utilisateur annule l'impression d'un badge.

Demande d'identifiant terminée
Lorsqu'un utilisateur imprime un badge en file d'attente.

Titulaires de cartes
Limitez votre recherche à des titulaires de cartes ou groupes de titulaires de cartes spécifiques

Identifiant
Limitez la recherche à certains identifiants.

Champs personnalisés
Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Utilisateurs qui impriment
Restreindre la recherche à des utilisateurs ayant imprimé un badge.

Utilisateurs demandeurs
Restreindre la recherche à des utilisateurs ayant demandé l'impression d'un badge.

3. Cliquez sur Générer le rapport.
   Les événements d'impression d'identifiants sont affichés dans le volet de rapport.

Explorer

- Demander une carte d'identification

3.3.7.1 | Colonnes du volet de rapport pour la tâche Historique de demande d'identifiants

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Date/heure de mise en file d'attente
Date et heure de la demande d'impression du badge.

Nom d'activité
Type de l'activité.

Demander un motif
Motif de refus du nouvel identifiant.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Photo
Photo du titulaire de cartes ou du visiteur.

Identifiant
Nom d'identifiant utilisé par le titulaire de cartes.

Utilisateur
Nom de l'utilisateur ayant déclenché l'événement. Le nom d'utilisateur est vide si l'événement n'a pas été déclenché depuis Security Desk.

E-mail du demandeur
Adresse e-mail de l'utilisateur ayant demandé l'impression du badge.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.
Sujet parent : Analyser l'historique des demandes d'identifiants

3.3.8 | Analyser les événements d'identifiants

Vous pouvez analyser les événements relatifs aux identifiants (Accès refusé : Identifiant expiré, Accès refusé : Identifiant inactif, Accès refusé : Identifiant volé, et ainsi de suite) à l'aide du rapport *Activités d'identifiants*.

À savoir

Utilisez les *Activités d'identifiants* pour examiner les secteurs fréquentés par un titulaire de carte en sélectionnant l'identifiant, puis la plage horaire. Vous pouvez également rechercher par événements d'identifiant critiques. Par exemple, en cas d'événement *Accès refusé : Identifiant volé*, vous pouvez voir qui a essayé d'utiliser l'identifiant volé en examinant la vidéo associée à l'événement.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Activités d'identifiants.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Identifiant
   Limitez la recherche à certains identifiants.

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Portes - Secteurs - Ascenseurs
   Restreindre la recherche aux activités survenues à certaines portes, certains secteurs ou ascenseurs.

   Événements
   Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

3. Cliquez sur Générer le rapport.
   Les événements d'identifiants sont affichés dans le volet de rapport.
4. Pour afficher la séquence vidéo associée à un événement dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas.
   Lorsqu'aucune caméra n'est connectée à l'entité, une icône de porte, d'ascenseur ou de secteur est affichée, selon le type d'événement d'identifiant.
5. Utilisez les widgets du volet Commandes pour contrôler les tuiles.

3.3.8.1 | Colonnes du volet de rapport pour la tâche Activités d'identifiants

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Point d'accès
Point d'accès concerné (ne s'applique qu'aux secteurs, portes et ascenseurs).

Format de carte
Format de carte de l'identifiant.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

Identifiant
Nom d'identifiant utilisé par le titulaire de cartes.

Code de l'identifiant
Numéro de carte ou code de l'installation.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Appareil
Périphérique utilisé par l'unité (lecteur, entrée REX, module d'E/S, relais de pêne, et ainsi de suite).

Adresse e-mail
L'adresse e-mail du titulaire de cartes ou du visiteur.

Événement
Nom de l'événement.

Heure de l'événement
Date et heure de l'événement.

Prénom
Prénom du titulaire de cartes ou visiteur.

Adresse IP
L'adresse IP de l'unité ou de l’ordinateur.

Nom
Nom du titulaire de cartes ou visiteur.

Emplacement
Emplacement (secteur) où l'activité a eu lieu.

Période d'occurrence
Période durant laquelle l'événement est survenu.

Photo
Photo du titulaire de cartes ou du visiteur.

Type de produit
Modèle de l'unité.

Fuseau horaire
Le fuseau horaire de l'unité.

Unité
Nom de l'unité.
Sujet parent : Analyser les événements d'identifiants

3.3.9 | Afficher les propriétés d'identifiants d'un titulaire de cartes

Pour afficher les propriétés d'identifiants (état, titulaire de cartes affecté, format de carte, code d'identifiant, propriétés personnalisées, et ainsi de suite) d'un titulaire de cartes, utilisez le rapport *Configuration d'identifiant* .

À savoir

Par exemple, le rapport Configuration d'identifiants est utile si vous avez demandé un identifiant pour un titulaire de cartes et que vous souhaitez savoir s'il a été activé. Si vous faites une recherche par titulaire de cartes, la colonne *État de l'identifiant* indique si l'état de l'identifiant est égal à *Demandé* ou *Actif*. Vous pouvez également voir si des identifiants sont actuellement signalés comme perdus ou volés.

Procédure

1. Ouvrez la tâche *Gestion des identifiants*.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Description
   Restreindre la recherche aux entités qui contiennent cette chaîne de caractères.

   Partition
   Partition à laquelle appartient l'entité.

   État
   L'état du profil du titulaire de cartes ou du visiteur : *Actif*, *Expiré*, *Inactif Perdu*, *Volé*.

   Identifiants non utilisés
   Recherchez les identifiants qui n'ont pas généré d'événement accès accordé au cours d'une plage de dates donnée.
   REMARQUE : Pour que le rapport produise des résultats, tous les rôles Gestionnaire d'accès doivent être actifs et en ligne.

   Identifiant
   Spécifiez si l'identifiant est affecté ou non.

   Titulaires de cartes
   Limitez votre recherche à des titulaires de cartes ou groupes de titulaires de cartes spécifiques

   Date d'expiration
   Spécifiez la plage horaire d'expiration du profil du titulaire de cartes ou du visiteur.

   Informations sur l'identifiant
   Limitez la recherche à certains formats de cartes, codes d'installation, numéros de cartes ou plaques d'immatriculation.

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

3. Cliquez sur Générer le rapport.
   Les propriétés d'identifiants du titulaire de cartes sélectionné sont affichées dans le volet de rapport.
4. Pour afficher un titulaire de cartes dans une tuile, cliquez deux fois sur le titulaire ou faites-le glisser sur le canevas.
5. Pour afficher des informations supplémentaires dans la tuile, cliquez sur  .

3.3.9.1 | Colonnes du volet de rapport dans la tâche Configuration d'identifiants

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Format de carte
Format de carte de l'identifiant.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

Date d'activation du titulaire de cartes
Date et heure d'activation du profil du titulaire de carte.

Date d'expiration du titulaire de cartes
Date et heure d'expiration du profil du titulaire de carte.

État du titulaire
L'état du profil du titulaire de cartes.

Identifiant
Nom d'identifiant utilisé par le titulaire de cartes.

Date d'activation de l'identifiant
Date et heure d'activation de l'identifiant du titulaire de cartes.

Code de l'identifiant
Numéro de carte ou code de l'installation.

Date d'expiration de l'identifiant
Date et heure d'expiration de l'identifiant du titulaire de cartes.

État de l'identifiant
L'état de l'identifiant du titulaire de cartes ou du visiteur : Actif ; Inactif.

Description
Description de l'événement, activité, entité ou incident.
IMPORTANT : Pour respecter la réglementation des États, si l'option Rapport généré est utilisée pour un rapport Historiques d'activité qui contient des données de RAPI, le motif de la recherche RAPI est inclus dans le champ Description.

Adresse e-mail
L'adresse e-mail du titulaire de cartes ou du visiteur.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Photo
Photo du titulaire de cartes ou du visiteur.

Code PIN
Code PIN d'identifiant.

Rôle
Type de rôle qui gère l'entité fédérée ou importée depuis Active Directory qui est sélectionnée.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.
Sujet parent : Afficher les propriétés d'identifiants d'un titulaire de cartes

3.3.10 | Rechercher un identifiant

Si vous avez un système de contrôle d'accès de taille importante et que vous ne parvenez pas à retrouver un identifiant, vous pouvez le rechercher par nom, ou utiliser la recherche avancée en appliquant des filtres.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Gestion des identifiants.
2. Pour lancer une recherche par nom d'entité, tapez le nom dans le champ de Recherche ( ).
   Toutes les entités dont le nom contient le texte saisi sont affichées.
3. Pour rechercher une entité avec la recherche avancée :
   a. Cliquez sur Recherche avancée dans le volet de gauche.
   b. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

      Titulaires de cartes
      Limitez votre recherche à des titulaires de cartes ou groupes de titulaires de cartes spécifiques

      Identifiant
      Spécifiez si l'identifiant est affecté ou non.

      Informations sur l'identifiant
      Limitez la recherche à certains formats de cartes, codes d'installation, numéros de cartes ou plaques d'immatriculation.

      Champs personnalisés
      Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

      Description
      Restreindre la recherche aux entités qui contiennent cette chaîne de caractères.

      Date d'expiration
      Spécifiez la plage horaire d'expiration de l'identifiant.

      Partition
      Partition à laquelle appartient l'entité.

      État
      L'état du profil du titulaire de cartes ou du visiteur : *Actif*, *Expiré*, *Inactif Perdu*, *Volé*.

      Identifiants non utilisés
      Recherchez les identifiants qui n'ont pas généré d'événement accès accordé au cours d'une plage de dates donnée.
      REMARQUE : Pour que le rapport produise des résultats, tous les rôles Gestionnaire d'accès doivent être actifs et en ligne.

   c. Cliquez sur Rechercher.

Résultats

Les identifiants qui correspondent aux critères de recherche sont affichés à l'écran.

3.3.10.1 | Colonnes du volet de rapport pour la tâche Gestion des identifiants

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Date d'activation de l'identifiant
Date à laquelle l'identifiant a été activé.

Format de carte
Format de carte de l'identifiant.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

\Date d'activation
Date et heure d'activation du profil du titulaire de carte.

Date d'expiration
Date et heure d'expiration du profil du titulaire de carte.

État du titulaire
L'état du profil du titulaire de cartes.

Identifiant
Nom d'identifiant utilisé par le titulaire de cartes.

Code de l'identifiant
Numéro de carte ou code de l'installation.

Date d'expiration de l'identifiant
Date et heure d'expiration de l'identifiant du titulaire de cartes.

État de l'identifiant
L'état de l'identifiant du titulaire de cartes ou du visiteur : Actif ; Inactif.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Description
Description de l'événement, activité, entité ou incident.
IMPORTANT : Pour respecter la réglementation des États, si l'option Rapport généré est utilisée pour un rapport Historiques d'activité qui contient des données de RAPI, le motif de la recherche RAPI est inclus dans le champ Description.

Adresse e-mail
L'adresse e-mail du titulaire de cartes ou du visiteur.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Photo
Photo du titulaire de cartes ou du visiteur.

Code PIN
Code PIN d'identifiant.

Rôle
Type de rôle qui gère l'entité sélectionnée.
Sujet parent : Rechercher un identifiant

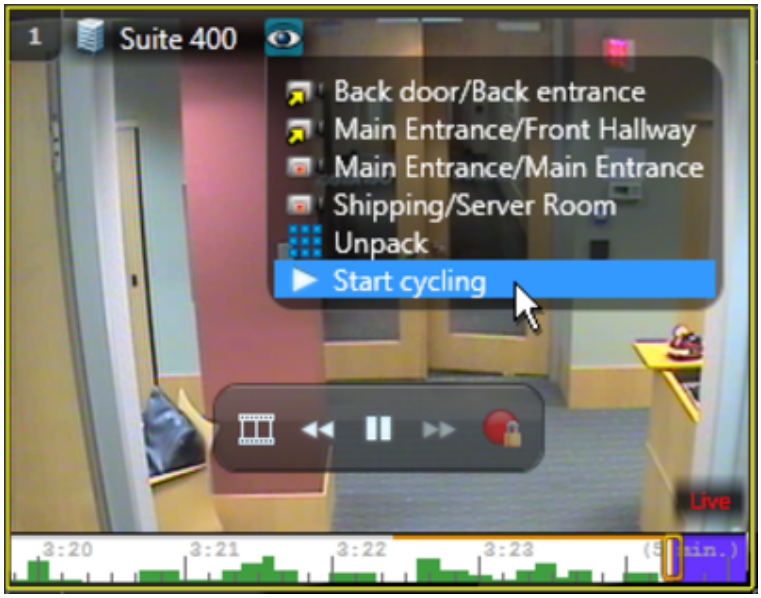
3.4 | Zones, portes et ascenseurs dans Security Desk

3.4.1 | Affichage des secteurs sur le canevas

Lorsque vous affichez un *secteur* ( ) ou un secteur sécurisé ( ) dans une tuile du canevas, le widget Secteur apparaît dans volet Commandes pour que vous puissiez contrôler le secteur.

Les secteurs sont généralement associés à plusieurs caméras. Lorsque vous affichez un secteur, la première caméra associée au secteur est affichée.

Cliquez sur l'icône œil ( ) dans la barre d'outils de la tuile pour sélectionner l'entité à afficher, ou *développez* le secteur pour afficher toutes les entités associées dans une tuile distincte. Vous pouvez également démarrer le *cycle des tâches*, pour afficher successivement les entités dans la tuile.

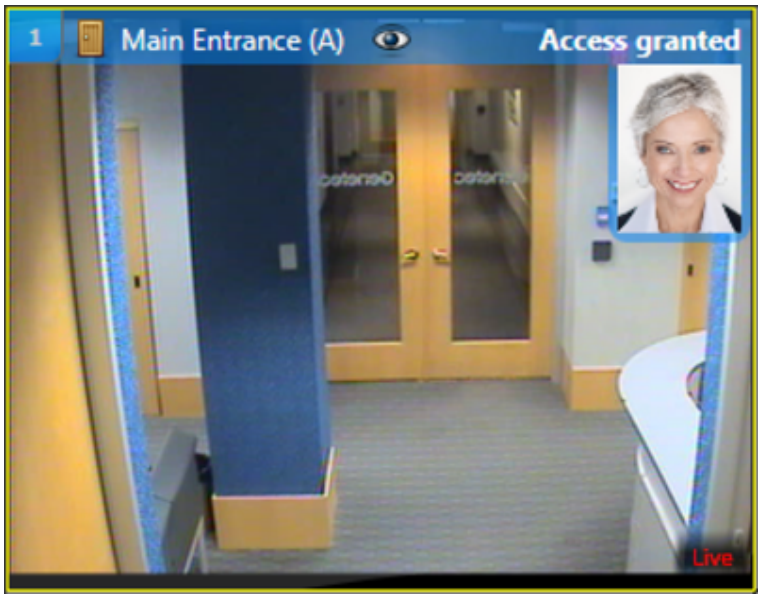


Si aucune caméra n'est associée au secteur, seule l'icône du secteur est affichée.

3.4.2 | Affichage des portes sur le canevas de Security Desk

Lorsque vous affichez une *porte* ( ) dans une tuile du canevas, le widget Porte apparaît dans le volet Commandes pour que vous puissiez contrôler la porte.

Si la porte est associée à une caméra, le flux vidéo de la caméra est affiché dans la tuile.



Si la porte n'est pas associée à une caméra, seule l'icône de la porte est affichée. L'image de la porte est statique. Elle reste ouverte.

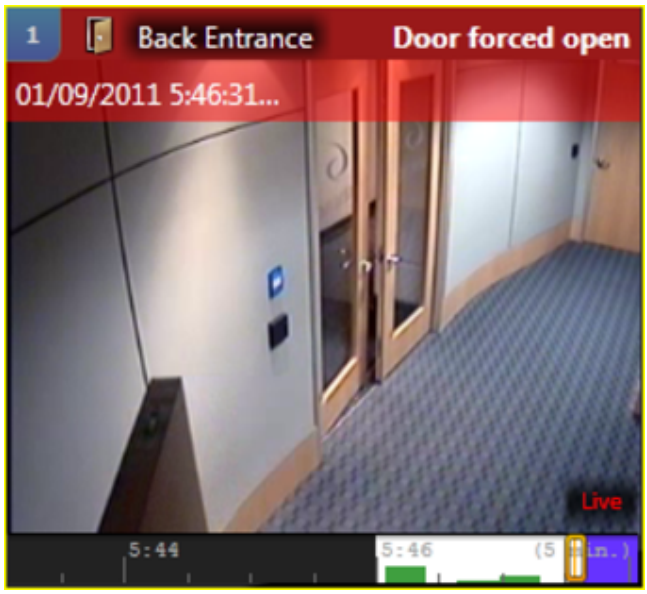
3.4.3 | Autoriser le franchissement d'une porte

Pour déverrouiller une porte ou ignorer les horaires de verrouillage et déverrouillage, utilisez le widget *Porte* pour contrôler le franchissement de la porte. Le widget Porte est activé lorsqu'une entité porte est affichée dans la tuile sélectionnée sur le canevas.

À savoir

Les portes à accès contrôlé sont verrouillées par défaut, à moins qu'un horaire de déverrouillage soit en vigueur. Seuls les titulaires de cartes disposant des identifiants appropriés peuvent les ouvrir. Lorsqu'une porte est affichée dans une tuile du canevas, l'icône de l'entité porte est actualisée en temps réel pour indiquer si la porte est ouverte ( ) ou fermée ( ).

En l'absence de caméra associée à la porte, une image statique de porte ouverte est affichée dans la tuile du canevas. La figure suivante montre une porte ouverte et l'icône de porte correspondante.



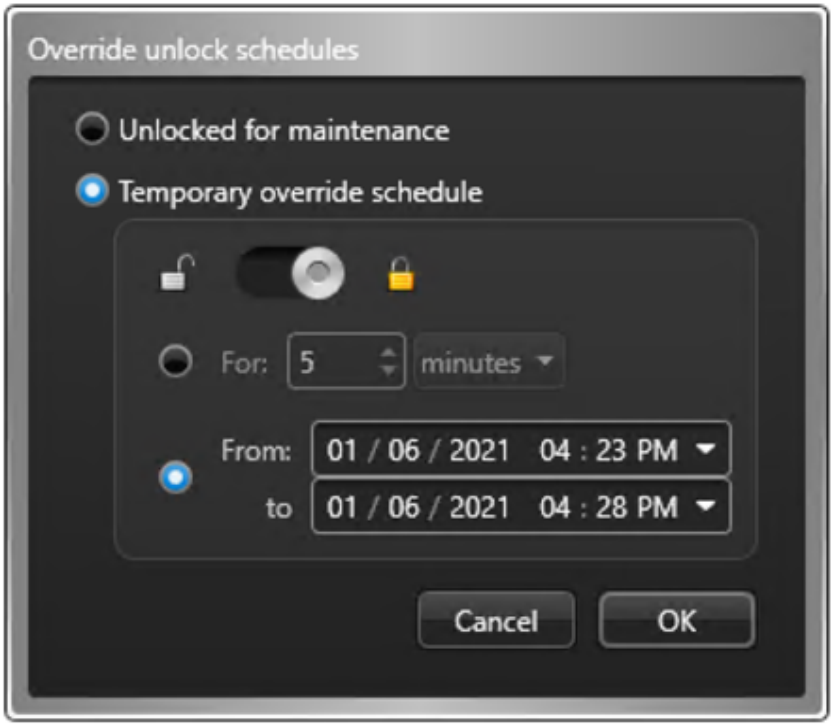
Procédure

1. Dans la tâche Surveillance, sélectionnez une tuile qui affiche une porte.
   Le widget *Porte* est affiché dans le volet Commandes.
2. Dans le widget Porte, procédez de l'une des manières suivantes :

- Pour déverrouiller la porte et accorder un accès temporaire, cliquez sur Déverrouiller ( ).

  Le délai d'accès est configuré par l'administrateur système. Le widget indique que la porte est ouverte et déverrouillée.

- Pour supplanter l'horaire de déverrouillage de la porte, cliquez sur Ignorer les horaires de déverrouillage ( ), puis sélectionnez l'une des options suivantes :



Déverrouillée pour maintenance

Déverrouiller la porte indéfiniment à des fins de maintenance. Pour annuler ce déverrouillage, cliquez sur dans le widget Porte.

Annuler temporairement l'horaire de déverrouillage

Verrouillez ( ) ou déverrouillez ( ) la porte pour une durée spécifiée, maintenant ou plus tard. L'état normal de la porte est rétabli à l'expiration de ce délai.

3. Cliquez sur OK.

Exemple

En définissant un horaire de déverrouillage d'une porte, un administrateur Security Center peut programmer la porte afin qu'elle accorde l'accès à tous durant certains créneaux horaires (comme lorsqu'une personne est présente à l'accueil). Si vous disposez des droits adéquats, vous pouvez ignorer ces horaires de déverrouillage en verrouillant la porte lorsque les horaires prévoient son ouverture et inversement.

3.4.4 | Empêcher le franchissement d'une porte

Pour empêcher à titre temporaire tous les accès par une porte, vous pouvez désactiver (ou contourner) le lecteur du côté de porte auquel vous souhaitez bloquer l'accès.

À savoir

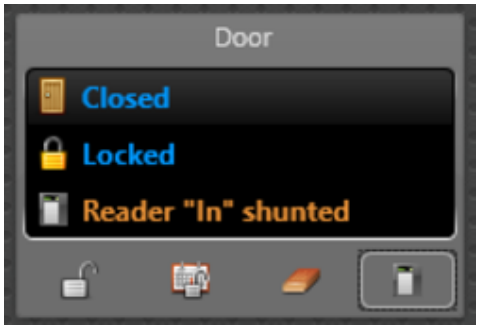
Les lecteurs ne peuvent pas tous être désactivés depuis Security Desk. La possibilité de contourner un lecteur dépend de votre équipement de contrôle d'accès. Contourner un lecteur équivaut à couper sa source d'alimentation. Un titulaire de cartes qui présente un identifiant valable ne peut alors plus déverrouiller la porte. Toutefois, cela n'empêche pas le déverrouillage de la porte avec une clé.

CONSEIL : Vous pouvez également contourner un lecteur défaillant, pour l'empêcher d'émettre des sons ou de générer des événements.

Procédure

Pour empêcher le franchissement d'une porte :

1. Dans la tâche Surveillance, sélectionnez une tuile qui affiche une porte.
   Le widget *Porte* est affiché dans le volet Commandes.
2. Dans le widget Porte, cliquez sur le bouton Lecteur ( ), puis sélectionnez le lecteur que vous souhaitez désactiver.
   Le lecteur désactivé est indiqué dans le widget Porte.



Pour réactiver un lecteur :

1. Cliquez à nouveau sur le bouton Lecteur ( ), puis sélectionnez le lecteur que vous souhaitez activer.

3.4.5 | Configurer et utiliser une action éclair pour déverrouiller plusieurs portes de périmètre d'un secteur

Vous pouvez déverrouiller toutes les portes du périmètre d'un secteur en même temps à l'aide d'un raccourci clavier en configurant une action éclair.

À savoir

Lorsque vous configurez une *action éclair* pour déverrouiller les portes du périmètre d'un secteur, l'action est affectée à une touche de fonction. L'action éclair est ensuite déclenchée en appuyant sur Ctrl et la touche de fonction correspondante, ou depuis la zone de notification.

Procédure

1. Dans la zone de notification, cliquez sur Actions éclair ( ).
2. Dans la boîte de dialogue Actions éclair, cliquez sur Modifier.
3. Cliquez sur Ajouter ( ).
4. Nommez l'action éclair dans le champ Nom.
5. Dans la liste Action, sélectionnez Déverrouiller expressément les portes du périmètre.
6. Dans la liste Secteur, sélectionnez le secteur dont vous souhaitez déverrouiller les portes.
7. Cliquez sur Terminé.
   L'action éclair que vous avez créée est présentée avec sa touche de fonction associée.

Lorsque vous avez terminé

Vérifiez que l'action éclair que vous avez configurée fonctionne en ouvrant les portes du secteur de l'une des deux façons suivantes :

- Sélectionnez l'action éclair que vous avez créée, puis cliquez sur Exécuter.
- Appuyez sur Ctrl+*Fn*.

3.4.6 | Contrôler l’accès aux étages d'ascenseur

Pour autoriser ou refuser l’accès aux étages d'ascenseur à titre temporaire, vous pouvez utiliser le widget *Ascenseur* pour ignorer l'horaire de l’ascenseur ou contourner le lecteur de la cabine. Le widget Ascenseur est activé lorsqu'une entité ascenseur est affichée dans la tuile sélectionnée sur le canevas.

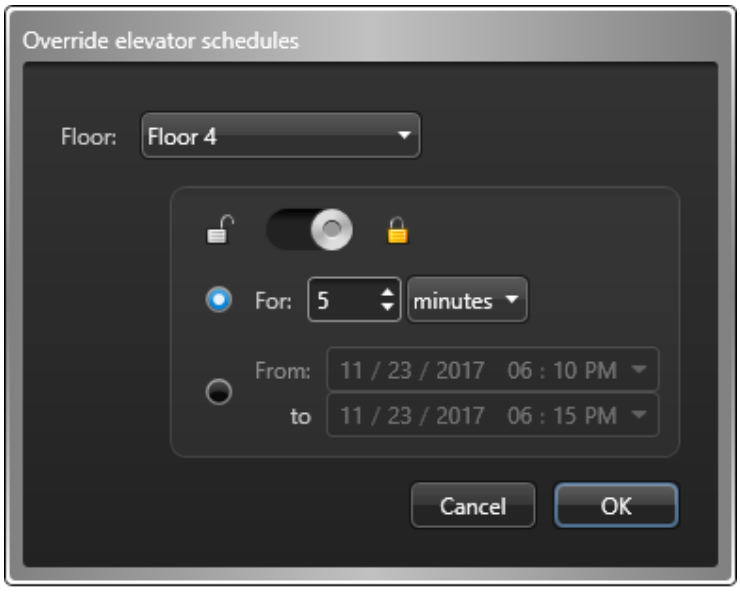
À savoir

Les ascenseurs ne peuvent pas tous être contrôlés depuis Security Desk, et les lecteurs ne peuvent pas être tous désactivés depuis le widget. La possibilité de contourner un lecteur dépend de votre équipement de contrôle d'accès. Contourner un lecteur équivaut à couper sa source d'alimentation. Un titulaire de cartes qui présente un identifiant valable dans la cabine d'ascenseur ne peut alors plus utiliser l'ascenseur en appuyant sur un bouton d'étage.
CONSEIL : Vous pouvez également contourner un lecteur défaillant, pour l'empêcher d'émettre des sons ou de générer des événements.

Procédure

Pour contrôler l’accès à un étage d'ascenseur :

1. Dans la tâche Surveillance, sélectionnez une tuile qui affiche un ascenseur ( ).
2. Dans le widget ascenseur, cliquez sur Ignorer les horaires d'ascenseur ( ).
   la boîte de dialogue Ignorer les horaires d'ascenseur apparaît.



3. Dans la liste déroulante Étage, sélectionnez les étages pour lesquels vous souhaitez remplacer les horaires.
4. Verrouillez ( ) ou déverrouillez ( ) les étages sélectionnés pour une durée déterminée.
   - Cliquez sur le premier choix et entrez la durée de remplacement, effective immédiatement.
   - Cliquez sur le deuxième choix et entrez la durée du remplacement et son heure de début.
5. Cliquez sur OK.

Pour empêcher l’accès à tous les étages d'ascenseur :

1. Dans le widget Ascenseur, cliquez sur le bouton Lecteur ( ), et cliquez sur Contourner.
   l’état du lecteur est indiqué dans le widget Ascenseur.

   CONSEIL : Pour lire la description complète de l'état, survolez le bouton Lecteur ( ).

Pour réactiver le lecteur de la cabine d'ascenseur :

1. Cliquez à nouveau sur le bouton Lecteur () et sélectionnez Activer.

Explorer

- Widget Ascenseur

3.4.7 | Analyser les événements de secteurs

Utilisez le rapport *Accès autorisé* pour analyser les événements relatifs aux *secteurs* (Premier entré, Violation antiretour, Activités de secteurs, et ainsi de suite).

Procédure

1. Sur la page d'accueil, ouvrez la tâche Activités de secteurs.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Secteurs
   Sélectionnez les secteurs à examiner.

   Titulaires de cartes
   Limitez votre recherche à des titulaires de cartes ou groupes de titulaires de cartes spécifiques

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Événements
   Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

3. Cliquez sur Générer le rapport.
   Les événements de secteurs sont affichés dans le volet de rapport.
4. Pour afficher la séquence vidéo associée à un événement dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas.
   Si le secteur n'est pas associé à une URL ou à une carte par le biais d'un module externe de tuile, seule l'icône du secteur est affichée.
5. Pour contrôler les secteurs, utilisez le widget Secteur.

Exemple

Si vous souhaitez afficher l'activité d'un secteur particulier durant le week-end ou depuis votre dernière connexion, vous pouvez sélectionner le secteur et une plage horaire pour le rapport. Vous pouvez rechercher les événements critiques survenus dans un secteur (comme *Accès autorisé* ou *Accès refusé : Identifiant volé*), puis analyser la vidéo associée à l'événement pour voir ce qui s'est passé et réunir des preuves.

Explorer

- Widget Secteur

3.4.7.1 | Colonnes du volet de rapport pour la tâche Activités de secteurs

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Secteur
Nom du secteur.

Format de carte
Format de carte de l'identifiant.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

Identifiant
Nom d'identifiant utilisé par le titulaire de cartes.

Code de l'identifiant
Numéro de carte ou code de l'installation.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Appareil
Périphérique utilisé par l'unité (lecteur, entrée REX, module d'E/S, relais de pêne, et ainsi de suite).

Adresse e-mail
L'adresse e-mail du titulaire de cartes ou du visiteur.

Événement
Nom de l'événement.

Heure de l'événement
Date et heure de l'événement.

Prénom
Prénom du titulaire de cartes ou visiteur.

Adresse IP
L'adresse IP de l'unité ou de l’ordinateur.

Nom
Nom du titulaire de cartes ou visiteur.

Période d'occurrence
Période durant laquelle l'événement est survenu.

Photo
Photo du titulaire de cartes ou du visiteur.

Type de produit
Modèle de l'unité.

Niveau d'accès
Niveau d'accès du titulaire de cartes.

Côté - Direction
Entrée ou sortie.

Identifiant complémentaire
Un deuxième identifiant est parfois exigé. Par exemple, un badge et un code PIN peuvent être requis pour l'accès à une porte ou à un ascenseur.

Fuseau horaire
Le fuseau horaire de l'unité.

Unité
Nom de l'unité.
Sujet parent : Analyser les événements de secteurs

3.4.8 | Analyser les événements de portes

Utilisez la tâche *Activités de portes* pour analyser les événements relatifs aux *portes* (Porte forcée, Porte entrebâillée trop longtemps, Sabotage matériel, et ainsi de suite).

Procédure

1. Sur la page d'accueil, ouvrez la tâche Activités de portes.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Titulaires de cartes
   Limitez votre recherche à des titulaires de cartes ou groupes de titulaires de cartes spécifiques

   Identifiant
   Limitez la recherche à certains identifiants.

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Portes
   Sélectionnez les portes à examiner.

   Événements
   Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

3. Cliquez sur Générer le rapport.
   Les événements de porte sont affichés dans le volet de rapport.
4. Pour afficher la séquence vidéo associée à un événement dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas.
   Si aucune caméra n'est associée à la porte, l'icône de porte est affichée.
5. Pour contrôler les portes, utilisez le widget Porte.

Exemple

À l'aide du rapport *Activités de portes*, vous pouvez consulter le nombre d'événements accès refusé survenus durant la semaine écoulée ou depuis votre dernière ronde. Vous pouvez également rechercher les autres événements critiques, comme *Porte forcée*. Si vous observez un comportement suspect de la part d'un titulaire de cartes en surveillant de la vidéo, vous pouvez analyser les autres portes franchies par le titulaire de cartes durant la journée. Si vous souhaitez vérifier que les équipes de maintenance ont terminé une intervention sur une porte, vous pouvez analyser la porte concernée, et sélectionner l'événement *Maintenance de porte terminée*.
Explorer

- Widget Porte

3.4.8.1 | Colonnes du volet de rapport pour la tâche Activités de portes

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

REMARQUE : Si vous avez généré le rapport Activités de portes avec Web Client, les colonnes de rapport ne sont pas toutes disponibles.

Format de carte
Format de carte de l'identifiant.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

Identifiant
Nom d'identifiant utilisé par le titulaire de cartes.

Code de l'identifiant
Numéro de carte ou code de l'installation.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Appareil
Périphérique utilisé par l'unité (lecteur, entrée REX, module d'E/S, relais de pêne, et ainsi de suite).

Porte
Nom de la porte.

Adresse e-mail
L'adresse e-mail du titulaire de cartes ou du visiteur.

Événement
Nom de l'événement.

Heure de l'événement
Date et heure de l'événement.

Prénom
Prénom du titulaire de cartes ou visiteur.

Adresse IP
L'adresse IP de l'unité ou de l’ordinateur.

Nom
Nom du titulaire de cartes ou visiteur.

Période d'occurrence
Période durant laquelle l'événement est survenu.

Photo
Photo du titulaire de cartes ou du visiteur.

Type de produit
Modèle de l'unité.

Côté
Nom du côté de porte.

Identifiant complémentaire
Un deuxième identifiant est parfois exigé. Par exemple, un badge et un code PIN peuvent être requis pour l'accès à une porte ou à un ascenseur.

Fuseau horaire
Le fuseau horaire de l'unité.

Unité
Nom de l'unité.
Sujet parent : Analyser les événements de portes

3.4.9 | Analyser les événements d'ascenseur

Utilisez le rapport *Activités d'ascenseurs* pour analyser les événements relatifs aux ascenseurs (Accès à un étage, Ascenseur hors ligne : L'appareil est hors ligne, Sabotage matériel, et ainsi de suite).

À savoir

Utilisez les *Activités d'ascenseurs* pour voir les titulaires de cartes ou les identifiants qui ont accédé aux différents ascenseurs et étages sur une période donnée. Ou recherchez tous les événements Accès refusé associés à un ascenseur pour voir qui a tenté d'accéder à un étage non autorisé.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Activités d'ascenseurs.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Titulaires de cartes
   Limitez votre recherche à des titulaires de cartes ou groupes de titulaires de cartes spécifiques

   Identifiant
   Limitez la recherche à certains identifiants.

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Ascenseurs
   Sélectionnez les ascenseurs à examiner.

   Événements
   Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

3. Cliquez sur Générer le rapport.
   Les événements d'ascenseur sont affichés dans le volet de rapport.
4. Pour afficher la séquence vidéo associée à un événement dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas.
   Si l'ascenseur n'est pas associé à une URL ou à une carte par le biais d'un module externe de tuile, seule l'icône de l'ascenseur est affichée.
5. Utilisez les widgets du volet Commandes pour contrôler les tuiles.

3.4.9.1 | Colonnes du volet de rapport pour la tâche Activités d'ascenseurs

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Format de carte
Format de carte de l'identifiant.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

Identifiant
Nom d'identifiant utilisé par le titulaire de cartes.

Code de l'identifiant
Numéro de carte ou code de l'installation.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Appareil
Périphérique utilisé par l'unité (lecteur, entrée REX, module d'E/S, relais de pêne, et ainsi de suite).

Ascenseur
Nom de l'ascenseur.

Adresse e-mail
L'adresse e-mail du titulaire de cartes ou du visiteur.

Événement
Nom de l'événement.

Heure de l'événement
Date et heure de l'événement.

Prénom
Prénom du titulaire de cartes ou visiteur.

Étage
Nom de l'étage de l'ascenseur.

Adresse IP
L'adresse IP de l'unité ou de l’ordinateur.

Nom
Nom du titulaire de cartes ou visiteur.

Période d'occurrence
Période durant laquelle l'événement est survenu.

Photo
Photo du titulaire de cartes ou du visiteur.

Type de produit
Modèle de l'unité.

Identifiant complémentaire
Un deuxième identifiant est parfois exigé. Par exemple, un badge et un code PIN peuvent être requis pour l'accès à une porte ou à un ascenseur.

Fuseau horaire
Le fuseau horaire de l'unité.

Unité
Nom de l'unité.
Sujet parent : Analyser les événements d'ascenseur

3.4.10 | Identifier les personnes autorisées ou non à franchir un point d'accès

Utilisez le rapport Droits d'accès de titulaire de cartes pour savoir quels titulaires de cartes ont accès ou non à certains secteurs, portes et ascenseurs.

À savoir

Ce rapport est utile pour savoir où un titulaire de cartes peut aller et à quels moments, et pour décider s'il convient de modifier ses règles d'accès.

CONSEIL : Effectuez la recherche sur un point d'accès à la fois pour obtenir un rapport plus spécifique.

Procédure

1. Sur la page d'accueil de , ouvrez la tâche Droits d'accès de titulaire de cartes.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Portes - Secteurs - Ascenseurs
   Restreindre la recherche aux activités survenues à certaines portes, certains secteurs ou ascenseurs.

3. Cliquez sur Générer le rapport.
   Tous les titulaires de cartes associés au point d'accès par le biais d'une règle d'accès sont affichés dans le volet de rapport. Les résultats indiquent si l'accès du titulaire de cartes est autorisé ou non, et la règle d'accès associée.
4. Pour afficher un titulaire de cartes dans une tuile, cliquez deux fois sur le titulaire ou faites-le glisser sur le canevas.
5. Pour afficher des informations supplémentaires dans la tuile, cliquez sur .

Lorsque vous avez terminé

Le cas échéant, modifiez les droits d'accès du titulaire de cartes.

3.4.10.1 | Colonnes du volet de rapport dans la tâche Droits d'accès de titulaire de cartes

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Accès refusé par
Règles refusant l'accès à au moins une des entités sélectionnées pour le titulaire de cartes.

Prénom
Prénom du titulaire de cartes ou visiteur.

Accès autorisé par
Règles qui donnent au titulaire de cartes accès à au moins une des entités sélectionnées (secteur, porte, et ainsi de suite).

Nom
Nom du titulaire de cartes ou visiteur.

Membre de
Tous les groupes auxquels appartient le titulaire de cartes.

Photo
Photo du titulaire de cartes ou du visiteur.
Sujet parent : Identifier les personnes autorisées ou non à franchir un point d'accès

3.4.11 | Identifier les personnes ayant accès aux portes et ascenseurs

Vous pouvez vérifier quels titulaires de cartes ont accès à un côté de porte ou étage d'ascenseur particulier à un moment donné avec le rapport Diagnostic de porte.

À savoir

Ce rapport est utile, car il vous permet de consulter la configuration d'une porte ou d'un ascenseur afin de décider s'il convient de modifier ses propriétés.

Pour en savoir plus sur la modification des propriétés des portes et ascenseurs, voir le *Guide de l'administrateur Security Center*.

L'outil de diagnostic de porte n'examine pas les identifiants de chaque titulaire de cartes. Vous pouvez affiner le diagnostic de droits d'accès du titulaire avec l'outil Outil de diagnostic d'accès.

Procédure

1. Sur la page d'accueil de , ouvrez la tâche Diagnostic de porte.
2. Dans l'onglet Filtres, sélectionnez une date et une heure pour le rapport.
3. Sélectionnez la porte ou l'ascenseur que vous souhaitez examiner.
4. Dans la liste déroulante Point d'accès, sélectionnez le point d'accès (côté de porte ou étage d'ascenseur) que vous souhaitez vérifier.
5. Cliquez sur Générer le rapport.
   Tous les titulaires de cartes autorisés à passer par le point d'accès sélectionné à un moment donné sont affichés dans le volet de rapport.

Lorsque vous avez terminé

Le cas échéant, testez la configuration du contrôle d'accès.

3.4.11.1 | Colonnes du volet de rapport dans la tâche Diagnostic de porte

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Prénom
Prénom du titulaire de cartes ou visiteur.

Nom
Nom du titulaire de cartes ou visiteur.

Photo
Photo du titulaire de cartes ou du visiteur.
Sujet parent : Identifier les personnes ayant accès aux portes et ascenseurs

3.4.12 | Identifier les entités affectées par une règle d'accès

Vous pouvez identifier les entités et points d'accès affectés par une règle d'accès donnée à l'aide du rapport Configuration de règle d'accès.

À savoir

Le résultat du rapport présente les membres de la règle d'accès, comme les titulaires de cartes, les portes et l'horaire associé. Vous pouvez ainsi décider si vous devez ajouter ou supprimer des entités, ou modifier l'horaire.

Pour en savoir plus sur la modification des membres d'une règle d'accès, voir le *Guide de l'administrateur Security Center*.

Procédure

1. Ouvrez la tâche Configuration de règle d'accès.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des éléments suivants :

   Règle d'accès
   Sélectionnez la règle de contrôle d'accès à examiner.

   État du titulaire
   Sélectionnez l'état de titulaire de cartes à examiner : actif, expiré, inactif.

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

3. Dans l'option Développer les groupes de titulaires, sélectionnez Activer pour afficher les membres des groupes de titulaires de cartes affectés dans le rapport au lieu des groupes eux-mêmes.
4. Dans l'option Inclure les entités du périmètre, sélectionnez Activer pour inclure les entités de périmètre des secteurs affectés dans le rapport.
5. Cliquez sur Générer le rapport.
   Les entités et points d'accès affectés par cette règle d'accès sont affichés dans le volet de rapport.

3.4.12.1 | Colonnes du volet de rapport dans la tâche Configuration de règle d'accès

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Règles d'accès
Nom des règles d'accès.

Activation
(Règle d'accès temporaire seulement) Heure d'activation de la règle d'accès.

Expiration
(Règle d'accès temporaire uniquement) Date et heure d'expiration de la règle d'accès.

Membre
Nom de l'entité concernée.

Point d'accès
Point d'accès concerné (ne s'applique qu'aux secteurs, portes et ascenseurs).

Type
Type d'entité concerné.

État du titulaire
L'état du profil du titulaire de cartes.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.
Sujet parent : Identifier les entités affectées par une règle d'accès

3.5 | Unités de contrôle d'accès dans Security Desk

3.5.1 | Analyser les événements d'unités de contrôle d'accès

Utilisez le rapport Événements d'unité de contrôle d'accès pour analyser les événements relatifs aux unités de contrôle d'accès.

À savoir

Par exemple, vous pouvez utiliser le rapport Événements d'unité de contrôle d'accès pour savoir si des événements critiques associés aux unités de contrôle d'accès sont survenus durant la semaine écoulée, en recherchant l'événement souhaité et en spécifiant une plage horaire.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Événements d'unité de contrôle d'accès.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Unités de contrôle d'accès
   Sélectionnez les unités de contrôle d'accès à examiner.

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

   Événements
   Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

3. Cliquez sur Générer le rapport.
   Les événements d'unité de contrôle d'accès sont affichés dans le volet de rapport.
   REMARQUE : Si des rôles Gestionnaire d'accès sont hors ligne lorsque vous lancez la recherche, vous recevrez un message d'erreur pour chacun d'eux, bien qu'ils ne soient pas associés aux unités de contrôle d'accès sélectionnées. En effet, le système n'a aucun moyen de savoir si les unités sélectionnées ont été gérées par l'un d'eux dans le passé.

3.5.1.1 | Colonnes du volet de rapport dans la tâche Événements d'unité de contrôle d'accès

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Heure de l'événement
Date et heure de l'événement.

Unité
Nom de l'unité.

Événement
Nom de l'événement.

Sabotage
Nom du module d'interface qui a été altéré.

Description
Rapporte le motif de l’échec d'une mise à niveau du micrologiciel.

Période d'occurrence
Période durant laquelle l'événement est survenu.

Type de produit
Modèle de l'unité.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.
Sujet parent : Analyser les événements d'unités de contrôle d'accès

3.5.2 | Afficher la configuration des E/S des unités de contrôle d'accès

Utilisez le rapport Configuration d'E/S pour afficher les configurations d'E/S (points d'accès contrôlés, portes et ascenseurs) d'unités de contrôle d'accès.

À savoir

Par exemple, vous pouvez utiliser le rapport *Configuration d'E/S* pour rechercher une porte particulière, puis afficher la configuration des accès pour chaque côté de la porte (REX, lecteurs, modules d'E/S, et ainsi de suite).

Procédure

1. Ouvrez la tâche Configuration d'E/S.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Unités de contrôle d'accès
   Sélectionnez les unités de contrôle d'accès à examiner.

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Appareils
   Sélectionnez les caméras à examiner.

   Emplacement
   Spécifiez les secteurs qui contiennent les appareils.

3. Cliquez sur Générer le rapport.
   Les configurations des entrées et sorties des unités de contrôle d'accès sélectionnées sont affichées dans le volet de rapport.

Explorer

- Afficher les propriétés des unités

3.5.2.1 | Colonnes du volet de rapport dans la tâche Configuration d'E/S

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Point d'accès
Point d'accès concerné (ne s'applique qu'aux secteurs, portes et ascenseurs).

Gestionnaire d'accès
Gestionnaire d'accès contrôlant l'unité.

Contrôle
Porte contrôlée par le périphérique.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Appareil
Périphérique utilisé par l'unité (lecteur, entrée REX, module d'E/S, relais de pêne, et ainsi de suite).

Adresse IP
L'adresse IP de l'unité ou de l'ordinateur.

Fabricant
Fabricant de l'unité.

Nom physique
Nom du périphérique.

Unité
Nom de l'unité.

Type d'unité
Type d'unité (Contrôle d'accès, Détection d'intrusion, RAPI ou Vidéo).

Sujet parent : Afficher la configuration des E/S des unités de contrôle d'accès

3.5.3 | Activer les appareils de contrôle d'accès externes

Vous pouvez activer et désactiver les appareils de contrôle d'accès externes (lecteurs USB, tablettes de signature, lecteurs de cartes, et ainsi de suite) depuis la boîte de dialogue Options.

À savoir

Ces réglages sont enregistrés en local avec votre profil d'utilisateur Windows. Pour en savoir plus sur les appareils de contrôle d'accès disponibles, consultez la documentation de votre fabricant.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Appareils externes.
2. Réglez l'option en regard de chaque appareil externe sur Activé ou Désactivé.
3. Cliquez sur Enregistrer.
4. Redémarrez l'application.

4 | Présentation de la reconnaissance de plaques d'immatriculation dans Security Desk

4.1 | Présentation rapide de la RAPI dans Security Desk

4.1.1 | À propos de Security Center AutoVu™

Le système de reconnaissance automatique de plaques d'immatriculation (RAPI) AutoVu™ automatise la capture et l'identification de plaques de véhicules, pour permettre aux forces de l'ordre, aux municipalités et aux entreprises du privé d'identifier les véhicules recherchés et d'appliquer les règles de stationnement. Conçu pour les installations fixes et mobiles, le système AutoVu™ est idéal pour tout un éventail d'applications et d'entités, qu'il s'agisse des forces de l'ordre, des communes ou des entreprises privées.

En fonction du matériel Sharp que vous installez, vous pouvez utiliser AutoVu™ dans une configuration fixe (ex. : sur un poteau situé sur une aire de stationnement) ou dans une configuration mobile (ex. : sur un véhicule de patrouille).

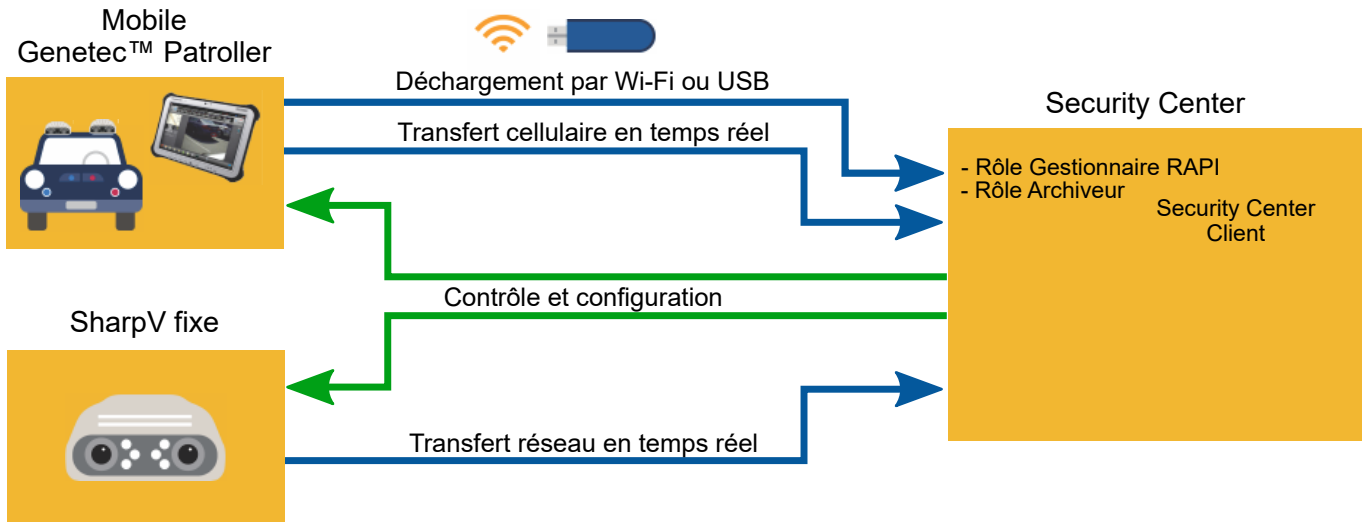
Vous pouvez utiliser AutoVu™ pour les éléments suivants :

- Scofflaw et identification du véhicule recherché
- Surveillance urbaine
- Application des règles de stationnement
- Contrôle des permis de stationnement
- Inventaire des véhicules
- Sécurité
- Contrôle d'accès

AutoVu™ Architecture système

AutoVu™ Sharp - les caméras capturent des images de plaques et transmettent les données à Genetec Patroller™ ou Security Center, qui recherche la plaque dans des listes de véhicules recherchés ou de permis.

Le diagramme suivant présente le fonctionnement d'un système AutoVu™ typique :



Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

4.2 | Événements RAPI dans Security Desk

4.2.1 | Affichage des événements de RAPI dans Security Desk

Les événements de RAPI sont des lectures et identifications de plaques d'immatriculation générées par des entités de RAPI, comme les installations Genetec Patroller™ et autres unités de RAPI. Vous pouvez suivre les événements de RAPI en temps réel avec la tâche *Surveillance*.

Lorsqu'un événement de RAPI survient, vous pouvez consulter les informations de l'événement dans la liste d'événements, dont la plaque et les images contextuelles, la position GPS du véhicule Genetec Patroller™ ou de la caméra Sharp ayant enregistré l'événement, le motif de refus d'une alerte, etc. Avec les configurations Sharp fixes avec vidéo, vous pouvez diffuser de la vidéo en direct depuis la caméra contextuelle Sharp et d'autres caméras situées à proximité de la Sharp. Vous pouvez également imprimer des événements d'alerte, puis les utiliser en tant que preuves d'infraction. Vous pouvez afficher les événements de RAPI sur le canevas en mode Tuile (tuiles individuelles) ou en mode Carte (carte routière).

Les coordonnées GPS des lectures et alertes enregistrées correspondent aux coordonnées GPS du véhicule Genetec Patroller™ ou de la caméra Sharp ayant enregistré l'événement.

ATTENTION :
Pour que les événements soient conservés dans la base de données à des fins de reporting, ils doivent être déchargés de Genetec Patroller™. Vous pouvez surveiller les événements en temps réel avec la tâche *Surveillance*, et recevoir des données en temps réel dans certains rapports sans pour autant décharger les données depuis Genetec Patroller™.

4.2.2 | Personnaliser les informations de RAPI à afficher dans Security Desk

Vous pouvez choisir les types d'informations de RAPI à afficher pour les lectures et les alertes dans les tuiles de la tâche Surveillance. Vous pouvez ainsi faire en sorte que les opérateurs Security Desk ne voient que les informations utiles dans le cadre de votre déploiement RAPI.

Avant de commencer

Fermer Security Desk.

À savoir

L'affichage de ces informations est contrôlé par l'ajout d'attributs et de paramètres XML à un fichier de configuration Security Desk spécifique situé sur le poste Security Desk client. Chaque attribut XML correspond à une information de RAPI particulière.

Procédure

1. Sur le poste Security Desk client, allez dans C:\Program Files (x86)\Genetec Security Center 5.9\ConfigurationFiles\.
2. Recherchez la balise suivante dans App.SecurityDesk.config : `<Presentation IgnoreSizeConstraints="False" EnableRatioViewbox="True" DisplayResourcesIds="False" SearchFormState="" AutoLoadHighResImages="True" WebBrowserType="InternetExplorer" DisplayFederationArrow="false" />`.
   Vous pouvez ajouter des attributs XML où vous voulez entre le crochet ouvrant et la barre oblique et le crochet fermant.
3. Pour personnaliser l'affichage d'informations sur les lectures dans une tuile, ajoutez l'attribut `"ReadDescription="`, suivi des paramètres suivants de votre choix :
   REMARQUE : Ajoutez le caractère pour forcer un retour à la ligne dans la tuile Security Desk.

   {Read.Address}
   L'adresse de la plaque lue.

   {Read.Confidence Score}
   Les données d'analyse de score de confiance accordé à la plaque lue (taux de reconnaissance). Si la caméra Sharp n'est pas configurée pour envoyer ces données d'analyse, la balise XML est affichée dans la tuile Security Desk.

   {Read.Vehicle Type}
   Les données d'analyse de Type de véhicule de la plaque lue. Si la caméra Sharp n'est pas configurée pour envoyer ces données d'analyse, la balise XML est affichée dans la tuile Security Desk.

   {Read.Relative Motion}
   Les données d'analyse de Mouvement relatif de la plaque lue. Si la caméra Sharp n'est pas configurée pour envoyer ces données d'analyse, la balise XML est affichée dans la tuile Security Desk.

   {Read.Plate}
   Les caractères de la plaque tels qu'identifiés par le module ALPR matcher.

   {Read.PlateState}
   L'État, la province ou le pays émetteur de la plaque.

   {Read.Timestamp}
   La date et l'heure de la lecture de la plaque.

   {Read.User}
   Nom de l'unité Genetec Patroller™ ayant lu la plaque.

   Voici un exemple du fichier de configuration lorsque tous les attributs de lecture sont utilisés : `<Presentation IgnoreSizeConstraints="False" EnableRatioViewbox="True" DisplayResourcesIds="False" SearchFormState="" AutoLoadHighResImages="True" WebBrowserType="InternetExplorer" DisplayFederationArrow="false" ReadDescription="{Read.Plate}, {Read.Confidence Score}%, {Read.PlateState}, {Read.Timestamp} {Read.Address}, User:{Read.User}"/>`
4. Pour personnaliser l'affichage d'informations sur les alertes dans une tuile, ajoutez l'attribut `"HitDescription="`, suivi des paramètres suivants de votre choix.
   REMARQUE : Ajoutez le caractère pour forcer un retour à la ligne dans la tuile Security Desk.

   {Hit.Category}
   L'attribut « category » de la liste de véhicules recherchés ou liste de permis.

   {Hit.Id}
   L'identifiant GUID de l'alerte.

{Hit.MatchPlate}
Le numéro de plaque trouvé par le moteur de recherche de correspondances ALPR matcher.

{Hit.Rule}
Le nom de l'entité liste de véhicules recherchés ou liste de permis dans Security Center.

{Hit.Timestamp}
La date et l'heure de l'alerte.

{Hit.Type}
Le type d'alerte (liste de véhicules recherchés, permis, dépassement horaire, IMPI).

{Hit.User}
Nom du véhicule de patrouille ayant déclenché l'alerte.

{Hit.Watermark}
La signature numérique de l'alerte.
Voici un exemple du fichier de configuration lorsque tous les attributs de lecture et d'alerte sont utilisés : `<Presentation IgnoreSizeConstraints="False" EnableRatioViewbox="True" DisplayResourcesIds="False" SearchFormState="" AutoLoadHighResImages="True" WebBrowserType="InternetExplorer" DisplayFederationArrow="false" ReadDescription="{Read.Plate}, ={Read.Confidence Score}%, {Read.PlateState}, {Read.Timestamp} {Read.Address}, User: {Read.User}" HitDescription="{Read.Plate}, {Read.ConfidenceScore}%, {Read.PlateState}, {Read.Timestamp}, {Read.Address} {Hit.Type}, {Hit.Rule} / {Hit.MatchPlate}, {Hit.Timestamp} Category: {Hit.Category}, User: {Hit.User} {Hit.Id}"/>`
REMARQUE : Vous pouvez ajouter des informations de lecture à une description d'alerte puisque toutes les alertes sont associées à au moins une lecture. Par exemple, vous voudrez parfois récupérer l'horodatage de la lecture et de l'alerte dans la description de l'alerte, puisqu'il peut y avoir un délai de traitement de l'alerte.

5. Enregistrez et fermez Bloc-notes.
6. Démarrez Security Desk.

Résultats

Les tuiles de la tâche Surveillance affichent les informations de RAPI ajoutées au fichier de configuration.

Lorsque vous avez terminé

Répétez la procédure sur tout poste Security Desk client qui nécessite des informations de RAPI particulières dans les tuiles de la tâche Surveillance.

4.2.3 | Personnaliser la qualité des images de RAPI affichées dans les colonnes du volet de rapport

Vous pouvez choisir la qualité des images de RAPI que vous souhaitez afficher dans les colonnes du volet de rapport pour les lectures et les alertes. Cela permet Security Deskaux opérateurs de scanner plusieurs images de haute qualité pour effectuer une enquête rapide.

Avant de commencer

Fermer Security Desk.

À savoir

Toute modification apportée au fichier de configuration n'est pas conservée après une Security Centermise à niveau.

Procédure

Pour personnaliser la qualité des images de RAPI affichées dans les colonnes du volet de rapport :

1. Sur le poste Security Desk client, allez dans C:\Program Files (x86)\Genetec Security Center 5.9\ConfigurationFiles\.
2. Ouvrez SecurityDesk.exe.config et trouvez la balise suivante : `<autoVuReportingConfiguration enableHighResReportImages="false" />`.
3. Modifiez la valeur **enableHighResReportImages** comme demandé.
   - Pour activer les images haute résolution, saisissez **true**.
   - Pour désactiver les images haute résolution, désactivez **false**.

   REMARQUE : La valeur par défaut de **enableHighResReportImages** est définie sur **false**.
4. Enregistrez et fermez le fichier SecurityDesk.exe.config.
5. Démarrez Security Desk.

Pour afficher des images haute résolution dans les colonnes du volet de rapport :

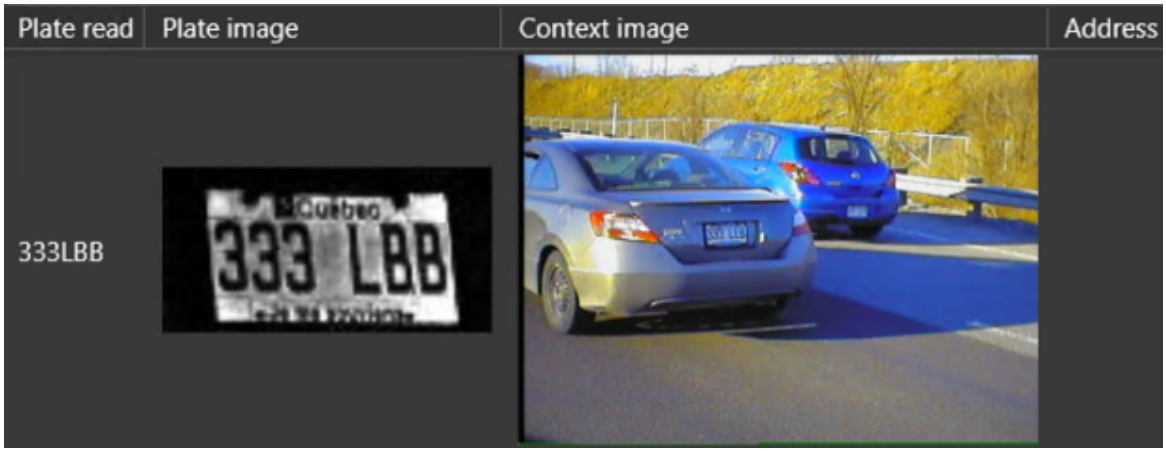
1. Sur la page d'accueil Security Desk, ouvrez la tâche Rapport désirée.
   Si vous souhaitez générer un rapport des alertes, ouvrez la tâche Alertes.
2. Configurez les filtres de requête comme demandé.
3. Cliquez sur Générer le rapport.
4. Augmentez la largeur des colonnes *Image plaque* et *Image contextuelle*, pour afficher des images haute résolution.

Exemple

Les exemples suivants illustrent la manière dont les images sont affichées dans les rapports en fonction de la valeur définie dans le fichier SecurityDesk.exe.config :

1. La valeur est définie sur false :

2. La valeur est définie sur true :



Lorsque vous avez terminé

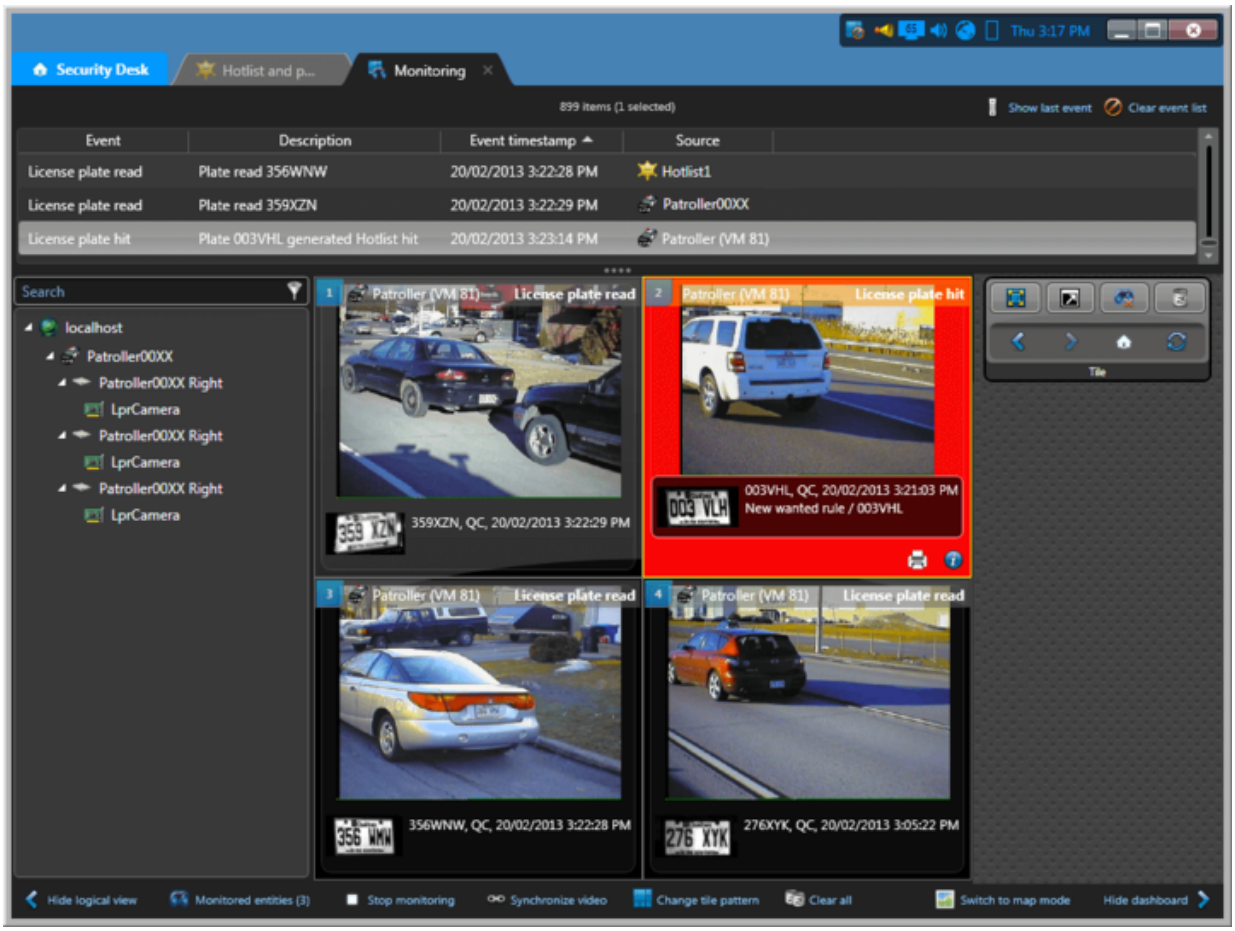
Répétez ces étapes sur tout Security Deskordinateur client qui nécessite l'affichage d'images haute résolution dans les colonnes du volet de rapport.

4.2.4 | Surveiller les événements de RAPI dans mode Tuile

Par défaut, les événements sont affichés sur le canevas en mode Tuile, ce qui vous permet d'afficher les informations sur une lecture ou alerte, d'afficher les images de plaques des événements en haute résolution, d'imprimer des alertes, etc., dans des tuiles individuelles.

Procédure

1. Dans la tâche Surveillance , sélectionnez un événement de RAPI dans une tuile, ou cliquez deux fois sur un événement dans la liste d'événements.



Par défaut, les informations suivantes sur l'événement de RAPI sont affichées dans la tuile :

Nom de l'entité
Nom de l'entité que vous surveillez, affichée dans la barre d'outils de la tuile.

Nom de l'événement de RAPI
Type d'événement (Plaque d'immatriculation lue, Identification de plaque, et ainsi de suite), affiché dans la barre d'outils de la tuile.

Couleur d'arrière-plan de la tuile :

- *Noir* (par défaut). Événement de lecture de plaque.
- *Rouge* (par défaut). Événement d'alerte de véhicule recherché.
- *Vert* (par défaut). Événement d'alerte de permis.
- *Bleu* (par défaut). Événement d'alerte de permis partagé et événement de dépassement horaire.

REMARQUE : Vous pouvez modifier les couleurs par défaut des événements de RAPI provenant des *listes de véhicules recherchés*, *règles de dépassement horaire* et *restrictions de permis* dans Config Tool.

Image contextuelle
Image grand-angle du véhicule capturée par la caméra contextuelle de l'*Unité de RAPI*.

Image de plaque
Image de la plaque capturée par la caméra de RAPI et interprétation ROC de l'événement.

Numéro de plaque
Numéro de plaque d'immatriculation.

État de la plaque
Origine de la plaque d'immatriculation.

Date et heure
Date et heure de la capture de plaque affectées à la règle d'alerte ayant identifié la plaque.

Adresse
Lieu de l'unité au moment de la capture de l'image de la plaque.
REMARQUE : L'adresse n'est affichée que si le module de *géolocalisation* est activé dans Config Tool. Si Genetec Patroller™ n'est pas équipé de cartes, l'adresse n'est affichée que si le module de géolocalisation et configuré pour interpréter la position GPS.

(Alertes seulement) Règle d'alerte
Règle d'alerte ayant déclenché l'alerte.

(Alertes de dépassement horaire seulement) Image des roues/d'aperçu
Image des roues capturées par la caméra d'*imagerie des roues* fixée à l'arrière du véhicule Genetec Patroller™. Les images des roues ne sont affichées que si l'alerte est capturée par une unité Genetec Patroller™ qui prend en charge l'imagerie des roues.

2. Pour vérifier la signature électronique de l'événement de RAPI, faites un clic droit sur la tuile, puis cliquez sur Vérifier la signature électronique.
   Une signature électronique valable confirme que l'événement de RAPI n'a pas été altéré. Security Center ajoute une signature électronique à toutes les lectures et alertes enregistrées par des unités Sharp fixes, et Genetec Patroller™ ajoute une signature électronique aux unités Sharp installées sur le véhicule. Une signature élecctronique peut avoir l'un des statuts suivants :
   - Valide ( ).
   - Non valable ( ).
   - Si aucune icône ne s'affiche, la signature électronique a été falsifiée.
3. (Alertes seulement) Pour afficher des informations complémentaires sur une alerte, comme ses attributs de liste de véhicules recherchés, cliquez sur dans la tuile (utilisateur, motif d'acception ou de rejet, État de la plaque, et ainsi de suite).
4. (Alertes seulement) Pour imprimer les données d'événement en tant que preuves d'infraction, cliquez sur dans la tuile.

Explorer

- Imprimer des rapports d'infractions

4.2.5 | Surveiller les événements de RAPI dans mode Carte

Utilisez le *mode carte* de la tâche Surveillance pour afficher tous les événements de RAPI sur une carte.

À savoir

Dans *mode Carte*, le canevas affiche une carte routière. La carte est ouverte et centrée sur la cible du zoom choisie la dernière fois que vous avez basculé en mode carte. Vous pouvez déplacer, agrandir et réduire la carte avec la souris.

REMARQUE : Le mode carte est réservé à l'affichage des événements de RAPI statiques. Pour afficher la position d'unités Genetec Patroller™ sur une carte, utilisez la tâche *Pistage de véhicule de patrouille*. Pour utiliser une carte à usage général, affichez une carte ( ) dans une tuile, ou utilisez la tâche *Cartes*.
Les symboles suivants représentent les différents types d'événements de RAPI sur la carte :

Cercle
Lectures et alertes de listes de véhicules recherchés.

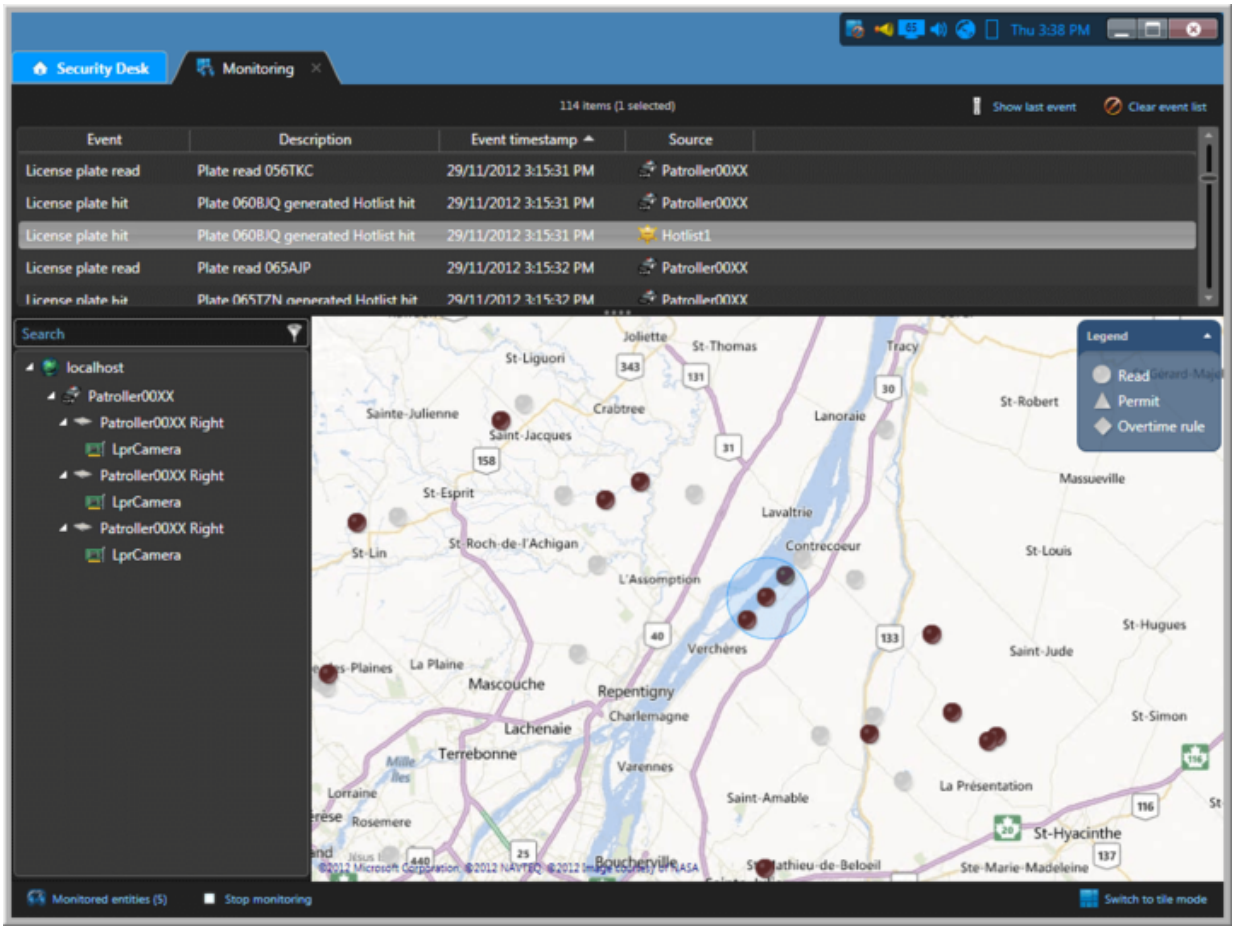
Triangle
Lectures et alertes de permis.

Losange
Lectures et alertes de dépassement horaire.

Vous pouvez modifier les couleurs par défaut des événements de RAPI provenant des *listes de véhicules recherchés*, *règles de dépassement horaire* et *restrictions de permis* dans Config Tool.

Procédure

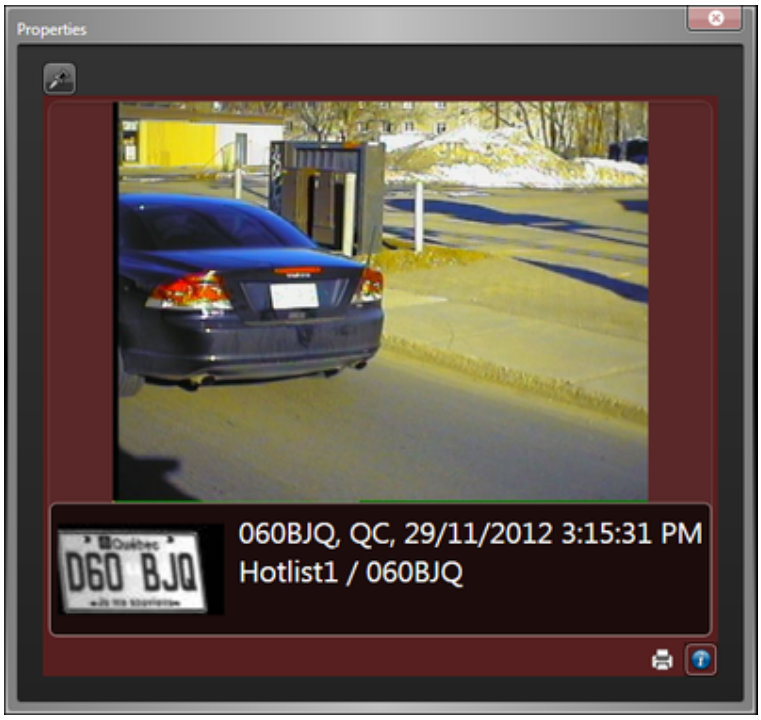
1. Dans la tâche Surveillance, cliquez sur Basculer en mode carte ( ).



2. Pour repérer un événement sur la carte, cliquez deux fois sur l'événement dans la liste d'événements.

   L'emplacement de l'événement est affiché sur la carte, et l'événement est entouré.

3. Pour afficher des informations sur l'événement, cliquez sur l'événement sur la carte.



La fenêtre Propriétés apparaît. Les propriétés et commandes affichées dans la fenêtre Propriétés sont similaires à celles qui sont présentées en *mode Tuile*.

4. Pour que la fenêtre Propriétés reste ouverte, cliquez sur Punaise ( ).

Explorer

- Relire l'itinéraire d'un véhicule de patrouille

4.3 | Lectures, alertes, listes de véhicules recherchés et permis dans Security Desk

4.3.1 | À propos des listes de véhicules recherchés

Liste de véhicules recherchés dans laquelle chaque véhicule est identifié par un numéro de plaque d'immatriculation, l'État émetteur et la raison pour laquelle le véhicule est recherché (volé, personne recherchée, alerte enlèvement, VIP, etc.). D'autres informations peuvent être utilisées, comme le modèle, la couleur et le numéro d'identification du véhicule (VIN).

Les listes de véhicules recherchés sont utilisées par les rôles AutoVu™ Genetec Patroller™ et le Gestionnaire de RAPI AutoVu™ pour comparaison avec les plaques d'immatriculation capturées par les unités de RAPI afin d'identifier les véhicules.

L'entité liste de véhicules recherchés est un type de règle d'alerte. Une règle d'alerte est une méthode utilisée par AutoVu™ pour identifier les véhicules recherchés. Les règles de *dépassement horaire*, *permis* et *restriction de permis* sont d'autres exemples de règles d'alertes. La correspondance d'une lecture de plaque avec une règle d'alerte est appelée une alerte. La correspondance d'une lecture de plaque avec une plaque répertoriée dans liste de véhicules recherchés est appelée une alerte de véhicule recherché.

4.3.2 | À propos des permis

Type d'entité qui définit une liste de détenteurs de permis de stationnement. Chaque détenteur de permis est caractérisé par une catégorie (zone de permis), un numéro de plaque d'immatriculation, l'État émetteur de la plaque, une plage de validité (date d'entrée en vigueur et date d'expiration). Les permis sont utilisés dans le cadre du stationnement urbain et universitaire.

L'entité Permis appartient à un ensemble de méthodes utilisées par AutoVu™ pour identifier les véhicules recherchés, et appelées règles d'alertes. Les règles de *liste de véhicules recherchés*, *dépassement horaire* et *restriction de permis* sont d'autres exemples de règles d'alertes. La correspondance d'une lecture de plaque avec une règle d'alerte est appelée une *alerte*. Lorsqu'une plaque ne correspond à aucun permis chargé dans Genetec Patroller™, la lecture génère une *alerte de permis*.

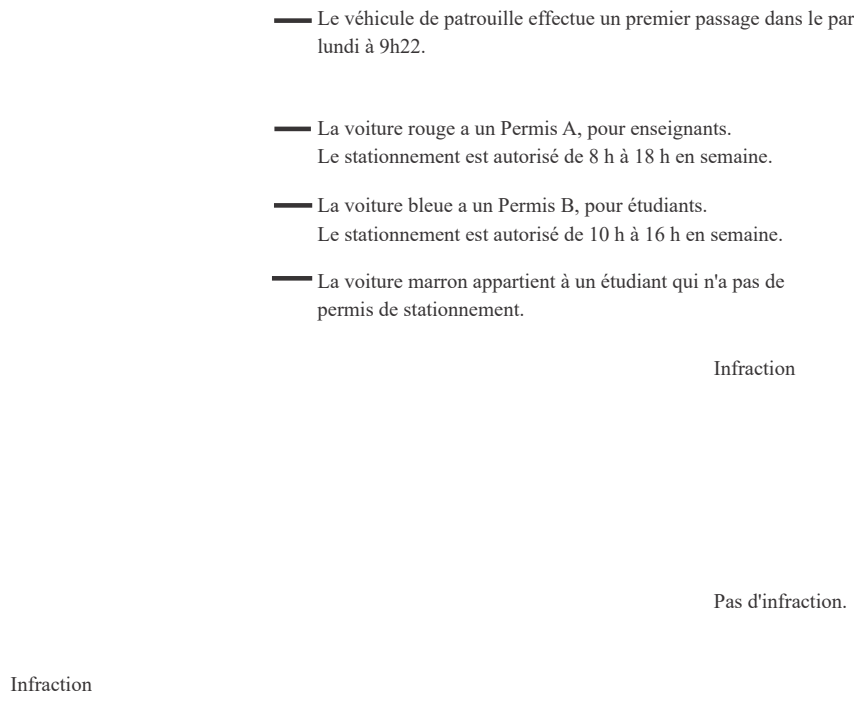
Permis en mode Stationnement urbain

Pour les installations Stationnement urbain, vous créez la liste de permis et configurez ses propriétés de base, mais il est inutile de définir une aire de stationnement ou une restriction de permis. Ce sont les autorités de la ville qui décident des lieux et horaires d'application des règles de stationnement. L'opérateur du véhicule de patrouille choisit le permis à appliquer dans Genetec Patroller™ en fonction des panneaux de règles de stationnement présents sur la voie.

Permis en mode Stationnement universitaire

Pour les installations Stationnement universitaire, vous créez et configurez une liste de permis de la même manière que pour les installations Stationnement urbain, mais vous devez également affecter des *restrictions de permis* et des aires de stationnement, afin de créer une « zone » d'application, qui est envoyée à Genetec Patroller™. Ce complément est nécessaire puisque le véhicule de patrouille surveille des aires de stationnement individuelles, et non des rues dotées de règles de stationnement existantes.

Dans cet exemple, vous utilisez une restriction de permis pour spécifier des contraintes horaires différentes pour différents détenteurs de permis.



Permis partagés

Les listes de permis ont un champ appelé *ID de permis*, qui permet à différents véhicules de partager un même permis, dès lors que les véhicules ont la même valeur *ID de permis* dans le fichier source de la liste de permis. Par exemple, en cas de covoiturage, un permis peut être partagé entre plusieurs véhicules. Chaque membre du groupe de covoiturage peut tour à tour conduire les autres membres au travail ou à l'école. Chaque membre doit alors partager le même permis pour pouvoir stationner.

Toutefois, le permis s'applique toujours à *un seul véhicule à la fois*. Par exemple, si les quatre membres du groupe de covoiturage décident d'utiliser leurs véhicules, ils ne peuvent pas tous utiliser le permis pour se garer en même temps. Genetec Patroller™ autorise le stationnement d'un des véhicules (la première plaque d'immatriculation détectée), mais génère une alerte de *permis partagé* pour tous les autres véhicules qui utilisent le même permis.

REMARQUE : Pour en savoir plus sur le fonctionnement des permis partagés avec les installations AutoVu™ Free-Flow, voir À propos des permis partagés dans AutoVu™ Free-Flow.

4.3.3 | Modifier les listes de véhicules recherchés et listes de permis

Vous pouvez modifier une *liste de véhicules recherchés* ou une *liste de permis* à l'aide de la tâche Éditeur de permis et de liste de véhicules recherchés.

Avant de commencer

La liste de véhicules recherchés ou la liste de permis doit être créée dans Config Tool, l'option *Activer la prise en charge de l'éditeur* dans l'onglet Propriétés de l'entité doit être sélectionnée, et l'utilisateur ou groupe d'utilisateurs doivent disposer des privilèges requis. Les modifications que vous pouvez apporter à une liste peuvent être limitées, selon les privilèges dont vous disposez.

À savoir

Utilisez l'Éditeur de permis et de liste de véhicules recherchés pour ajouter, modifier ou supprimer des éléments d'une liste créée dans *Config Tool*. Lorsque vous modifiez une liste de véhicules recherchés ou une liste de permis, le fichier texte est mis à jour et les véhicules de patrouille ou caméras Sharp reçoivent les nouvelles informations.
Les conditions suivantes sont à prendre en compte :

- Seules les premières 100 000 lignes d'une liste de véhicules recherchés sont chargées dans Security Desk.
- En cas d'erreur au chargement de la liste de véhicules recherchés, le chargement est interrompu et un message d'erreur est affiché. Toutefois, vous pouvez modifier les listes qui étaient déjà chargées lorsque l'erreur est survenue.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Éditeur de permis et de liste de véhicules recherchés.
   Les listes de véhicules recherchés et de permis sont affichées dans la colonne de gauche.
2. Sélectionnez la liste que vous souhaitez modifier.
3. Dans la liste déroulante, sélectionnez un Gestionnaire RAPI, puis cliquez sur Charger.
4. Pour trouver une ligne particulière de la liste, tapez le numéro de plaque d'immatriculation dans le champ Rechercher.
5. Procédez de l'une des manières suivantes :
   - Pour ajouter une ligne à votre liste, cliquez sur Ajouter ().
   - Pour supprimer une ligne, sélectionnez-la et cliquez sur Supprimer ().
   - Pour modifier une ligne, cliquez sur un élément individuel de la liste.
6. Cliquez sur Enregistrer.

Résultats

Le fichier source de la liste est actualisé.

Exemple

Imaginez qu'une liste de véhicules volés est téléchargée depuis le ministère de l'Intérieur tous les soirs à minuit. Chaque matin lorsque les agents démarrent leur ronde, ils chargent la dernière liste de véhicules recherchés dans un Genetec Patroller™. Durant la journée, certains véhicules sont retrouvés, tandis que de nouveaux véhicules sont volés. Vous pouvez supprimer les véhicules retrouvés de la liste et y ajouter les nouveaux véhicules volés, afin que tous les véhicules de patrouille disposent de la liste mise à jour.
Explorer

- Présentation de la tâche Éditeur de permis et de liste de véhicules recherchés

4.3.4 | Champs de commentaires des listes de véhicules recherchés

Les champs de commentaires contiennent des propriétés d'une alerte qui ne sont pas affichées par défaut dans Security Desk (comme le numéro d'identification ou de série du véhicule). Ils peuvent être extraits de la liste de véhicules recherchés dans laquelle la plaque a été détectée, ou il peut s'agir d'autres champs, comme le champ *UserEditedPlate*, des champs personnalisés, etc.

Les champs de commentaires ne sont disponibles que s'ils ont été créés dans Config Tool.

Voici des exemples de champs de commentaires de listes de véhicules recherchés :

{Category}
Pour les alertes de listes de véhicules recherchés, le champ *Category* correspond au motif de recherche du véhicule (*alerte enlèvement*, *personne recherchée*, *véhicule volé*, et ainsi de suite). Pour les *alertes de permis*, la valeur *Category* indique le type de permis (par exemple, *Zone 35*, *Zone 50*, et ainsi de suite).
REMARQUE : Ce champ est obligatoire pour les listes de véhicules recherchés et les *permis*. La catégorie est extraite de la liste de véhicules recherchés ou de la liste de permis dans laquelle la plaque est identifiée. Pour une plaque de *nouveau véhicule recherché*, la catégorie est définie dans les catégories *nouveau véhicule recherché* des réglages de RAPI, puis elle est téléchargée sur un Genetec Patroller™. Lorsqu'une *nouvelle plaque recherchée* est saisie manuellement dans Genetec Patroller™, l'utilisateur sélectionne la *catégorie* adaptée dans la liste téléchargée.

{MatchPlate}
Le numéro de plaque tel qu'il apparaît dans la liste de véhicules recherchés.

{PlateState}
L'État ou la province du numéro de plaque tel qu'il apparaît dans la liste de véhicules recherchés.

{EffectiveDate}
Date d'entrée en vigueur de la liste de véhicules recherchés.

{ExpiryDate}
Date d'expiration de la liste de véhicules recherchés.

{UserEditedPlate}
Indique que la plaque a été modifiée manuellement.

4.3.5 | Analyser les alertes signalées

Utilisez le rapport *Alertes* pour analyser les *alertes* signalées dans une zone géographique et durant une plage horaire particulières.

Avant de commencer

Pour afficher le résultat de la recherche sur le canevas, vous devez savoir comment surveiller les événements de RAPI dans Security Desk en mode Carte.

À savoir

Pour créer un rapport sur toutes les alertes survenues dans une région particulière sur une période donnée, sélectionnez la région et la plage horaire. Pour voir le nombre d'alertes recueillies par une unité Genetec Patroller™ pendant une ronde, recherchez cette unité Genetec Patroller™, puis définissez une plage horaire. Pour savoir si une unité Genetec Patroller™ a détecté une alerte pour une plaque particulière, vous pouvez rechercher la plaque concernée.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Alertes.
2. Pour restreindre votre recherche à des secteurs donnés, vous pouvez dessiner des régions sur la carte de la manière suivante :
    a. Dans l'onglet Filtres, cliquez sur le filtre Région.
    b. Cliquez sur Basculer en mode carte.
    c. Dans le filtre Région, cliquez sur Dessiner une région.
    d. Faites glisser le curseur de la souris pour tracer un cadre.
    Un cadre de Région numéroté est créé.
    e. Faites glisser les poignées pour redimensionner la région.

f. Pour déplacer la région, cliquez sans relâcher le bouton de la souris et faites glisser la zone à l'endroit voulu.
g. Créez d'autres régions si nécessaire.
h. Sélectionnez les régions qui vous intéressent.

Pour afficher toutes les régions que vous avez créées, cliquez sur  dans l'onglet Filtres.

3. Définissez les filtres de recherche pour votre rapport :

Motifs d'acceptation
Motif sélectionné par l'utilisateur Genetec Patroller™ pour valider une alerte. Les motifs d'acceptation sont créés et personnalisés dans Config Tool.

Action entreprise
Actions d'alerte (acceptée, rejetée, non appliquée) sélectionnées par l'utilisateur .Genetec Patroller™Genetec Patroller™ Pour les unités Sharp fixes, une alerte déclenchée par le module Hit Matcher est toujours automatiquement acceptée et appliquée.

Champs de commentaires
Commentaires d'alertes de l'utilisateur .Genetec Patroller™Genetec Patroller™

Champs personnalisés
Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Heure de l'événement
Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

Règles d'alerte
Sélectionnez les règles d'alerte à inclure dans le rapport.

Type d'alerte
Sélectionnez les types d'alertes que vous souhaitez inclure dans le rapport : *Permis*, *Permis partagé*, *Dépassement horaire* et *Liste de véhicules recherchés*.

Plaque d'immatriculation
Entrez un numéro de plaque complet ou partiel. Pour saisir plusieurs plaques d'immatriculation, voir Filtrer un rapport avec plusieurs plaques d'immatriculation

Unités de RAPI - Patroller
Limitez la recherche aux unités Genetec Patroller™ (dont les unités de RAPI associées) et/ou aux unités de RAPI représentant des caméras Sharp fixes sur l'unité Genetec Patroller™.

Décharger l'horodatage
La date et l'heure du déchargement des lectures/alertes de vers .Genetec Patroller™Security Center

État de la protection
Restreindre la recherche aux événements d'alerte protégés ou non protégés.

Motif de rejet
Motif sélectionné par l'utilisateur de pour rejeter l'alerte.Genetec Patroller™ Les motifs de rejet sont créés et personnalisés dans Config Tool. Ce filtre n'affecte que la valeur de la colonne *Alertes rejetées*.

Utilisateurs
Sélectionnez le nom d'utilisateur Patroller, ou les groupes d'utilisateurs parents du Patroller.

4. Cliquez sur Générer le rapport.
Les événements sont affichés dans le volet de rapport.
5. (Facultatif) Pour afficher les images haute résolution dans les colonnes *Image plaque* et *Image contextuelle*, augmentez la largeur de la colonne correspondante. Pour en savoir plus, voir Personnaliser la qualité des images de RAPI affichées dans les colonnes du volet de rapport

6. Vous pouvez afficher le résultat sur le canevas en exploitant l'un des modes suivants :

   mode Tuile
   Pour afficher un événement de RAPI dans une tuile, cliquez deux fois sur l'élément dans le volet de rapport, ou faites-le glisser sur le canevas.

   mode Carte
   Pour repérer un événement de RAPI sur la carte, cliquez deux fois sur l'événement dans le volet de rapport.

Lorsque vous avez terminé

Imprimer une alerte en tant que preuve d'infraction si nécessaire.
Explorer

- À propos des filtres de plaques d'immatriculation

4.3.5.1 | Colonnes du volet de rapport pour la tâche Alertes

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Motifs d'acceptation
Motif sélectionné par l'utilisateur Genetec Patroller™ pour valider une alerte. Les motifs d'acceptation sont créés et configurés dans Config Tool.

Adresse
Lieu de la lecture de RAPI.

Champs de commentaires
Tout champ de commentaires défini dans Système > Réglages de RAPI dans Config Tool. Affichés entre accolades.

Image contextuelle
Image couleur grand-angle du véhicule capturée par la caméra contextuelle.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Appareil
Périphérique utilisé par l'unité (lecteur, entrée REX, module d'E/S, relais de pêne, et ainsi de suite).

Heure de l'événement
Date et heure de l'événement.

Latitude
Les coordonnées de l'événement de RAPI.

Longitude
Les coordonnées de l'événement de RAPI.

Décharger l'horodatage
La date et l'heure de déchargement des lectures et alertes du véhicule de patrouille vers Security Center.

Entité Patroller
Nom de l'entité Patroller. Le champ de nom d'entité patroller n'est pas renseigné pour les caméras SharpV fixes.

Image de plaque
L'image de la plaque d'immatriculation capturée par la caméra de RAPI.

Origine de la plaque
L'État émetteur de la plaque d'immatriculation.

Lecture de plaque
La lecture de plaque d'immatriculation générée par l'unité .Sharp

Protégé
Indique si l'enregistrement sera protégé contre la suppression de la base de données à l'expiration de la période de rétention (pour ce type d'enregistrement).

Expiration de la protection
Indique la date d'expiration de la protection de l'alerte.

Motif de rejet
Motif sélectionné par l'utilisateur de pour rejeter l'alerte.Genetec Patroller™

Règle
Règle d'alerte qui correspond à la lecture de la plaque.

Unité de RAPI
Unité de RAPI ayant lu la plaque ; renseigné pour un véhicule de patrouille (Patroller - Gauche, Patroller - Droite, et ainsi de suite) et pour une Sharp fixe.

Utilisateur
Le nom de l'utilisateur Genetec Patroller™. Non disponible pour un hôte de fédération Security Center Federation™ pour les entités Genetec Patroller™ fédérées.

Image de la roue
Image des roues du véhicule. Sert au marquage virtuel des roues.
Sujet parent : Analyser les alertes signalées

4.3.6 | Analyser les statistiques d'alertes

Vous pouvez rapidement analyser les statistiques d'alertes pour une plage horaire et une zone géographique données avec le rapport Statistiques d'alertes.

À savoir

Pour afficher le résultat de la recherche sur le canevas, vous devez savoir comment surveiller les événements de RAPI dans Security Desk.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Alertes.
2. Pour restreindre votre recherche à des secteurs donnés, vous pouvez dessiner des régions sur la carte de la manière suivante :
    a. Dans l'onglet Filtres, cliquez sur le filtre Région.
    b. Cliquez sur Basculer en mode carte.
    c. Dans le filtre Région, cliquez sur Dessiner une région.
    d. Faites glisser le curseur de la souris pour tracer un cadre.
    Un cadre de Région numéroté est créé.
    e. Faites glisser les poignées pour redimensionner la région.
    f. Pour déplacer la région, cliquez sans relâcher le bouton de la souris et faites glisser la zone à l'endroit voulu.
    g. Créez d'autres régions si nécessaire.
    h. Sélectionnez les régions qui vous intéressent.
    Pour afficher toutes les régions que vous avez créées, cliquez sur  dans l'onglet Filtres.

3. Définissez les autres filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Motifs d'acceptation
   Motif sélectionné par l'utilisateur Genetec Patroller™ pour valider une alerte. Les motifs d'acceptation sont créés et personnalisés dans Config Tool.

   Action entreprise
   Actions d'alerte (acceptée, rejetée, non appliquée) sélectionnées par l'utilisateur .Genetec Patroller™Genetec Patroller™ Pour les unités Sharp fixes, une alerte déclenchée par le module Hit Matcher est toujours automatiquement acceptée et appliquée.

   Champs de commentaires
   Commentaires d'alertes de l'utilisateur .Genetec Patroller™Genetec Patroller™

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

   Règles d'alerte
   Sélectionnez les règles d'alerte à inclure dans le rapport.

   Type d'alerte
   Sélectionnez les types d'alertes que vous souhaitez inclure dans le rapport : *Permis*, *Permis partagé*, *Dépassement horaire* et *Liste de véhicules recherchés*.

   Plaque d'immatriculation
   Entrez un numéro de plaque complet ou partiel. Pour saisir plusieurs plaques d'immatriculation, voir Filtrer un rapport avec plusieurs plaques d'immatriculation

   Unités de RAPI - Patroller
   Limitez la recherche aux unités Genetec Patroller™ (dont les unités de RAPI associées) et/ou aux unités de RAPI représentant des caméras Sharp fixes sur l'unité Genetec Patroller™.

   Décharger l'horodatage
   La date et l'heure du déchargement des lectures/alertes de vers .Genetec Patroller™Security Center

   Motif de rejet
   Motif sélectionné par l'utilisateur de pour rejeter l'alerte.Genetec Patroller™ Les motifs de rejet sont créés et personnalisés dans Config Tool. Ce filtre n'affecte que la valeur de la colonne *Alertes rejetées*.

   Utilisateurs
   Sélectionnez le nom d'utilisateur Patroller, ou les groupes d'utilisateurs parents du Patroller.

4. Développez les options sous le bouton Créer un rapport, et sélectionnez Générer un rapport de statistiques.
   Les événements sont affichés dans le volet de rapport.

Exemple

Pour créer un rapport rapide sur toutes les alertes survenues dans une région particulière sur une période donnée, sélectionnez la région et la plage horaire.

4.3.7 | Imprimer des rapports d'infractions

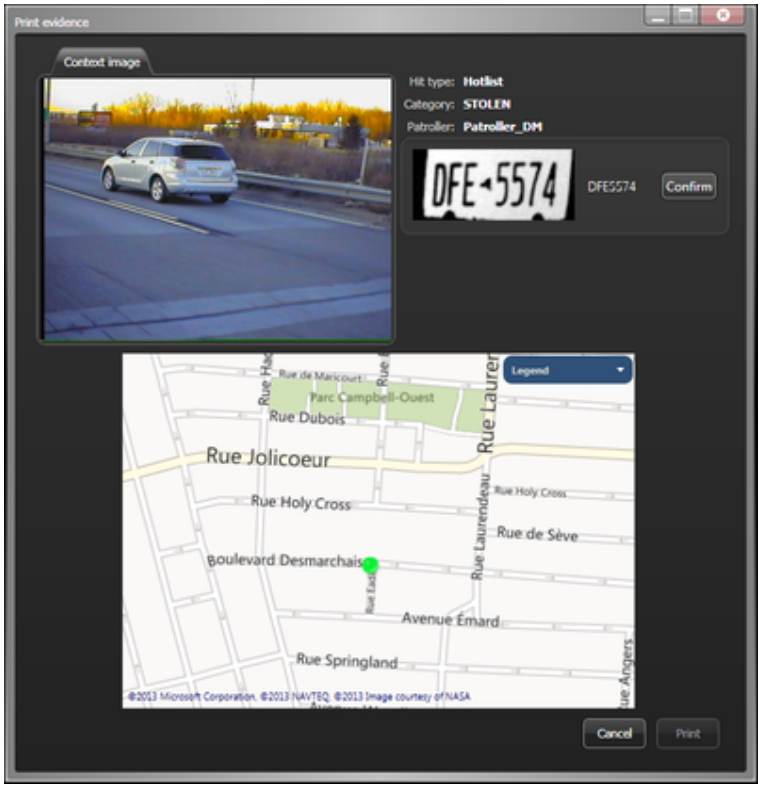
Vous pouvez imprimer un rapport d'*infractions-preuve photographique* pour les événements de Identification de plaque depuis la tâche Surveillance et d'autres tâches de RAPI.

À savoir

Le rapport imprimé contient la date du rapport, les informations d'alerte (numéro de plaque, coordonnées GPS, adresse, date de l'alerte, type d'alerte, et ainsi de suite), l'image de RAPI, l'image contextuelle, les images des roues (le cas échéant) et une représentation sur une carte.

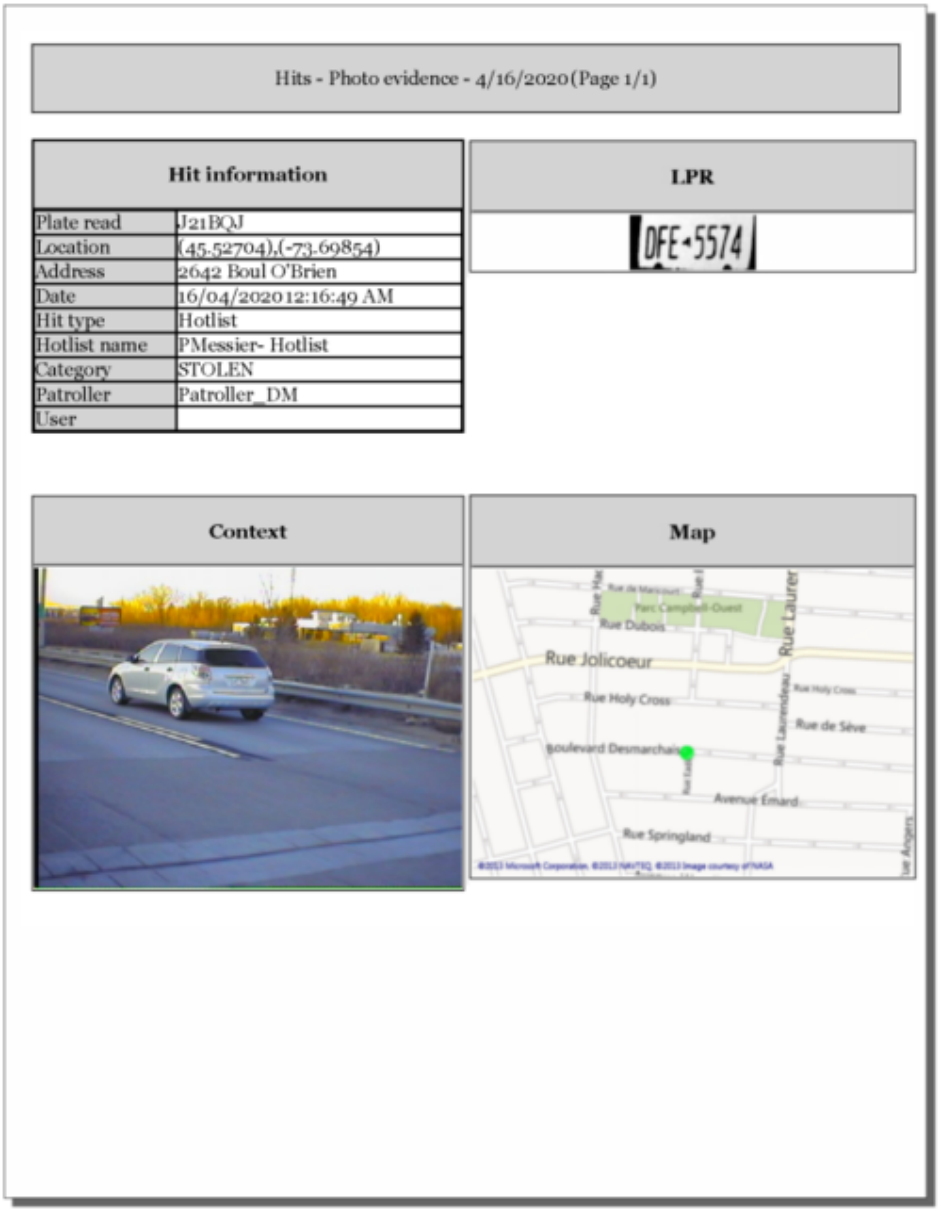
Procédure

1. Sur la page d'accueil, ouvrez la tâche Surveillance ou une tâche de RAPI.
2. Le cas échéant, créez un rapport.
3. Sélectionnez un événement d'alerte dans une tuile ou sur la carte.
4. Dans la tuile ou dans la fenêtre Propriétés, cliquez sur .
5. Dans la boîte de dialogue Imprimer les preuves, confirmez le numéro de plaque d'immatriculation pour ne pas imprimer de lecture erronée.



6. Confirmez que l'interprétation ROC correspond à l'image de RAPI.
7. Dans la zone de texte, saisissez le numéro de plaque d'immatriculation, puis cliquez sur Confirmer.
8. Cliquez sur Imprimer, sélectionnez une imprimante, puis cliquez sur Imprimer.

   Le rapport d'*infractions-preuve photographique* est imprimé.



Hits - Photo evidence - 4/16/2020 (Page 1/1)

Hit information	
Plate read	J21BQJ
Location	(45.52704),(-73.69854)
Address	2642 Boul O'Brien
Date	16/04/2020 12:16:49 AM
Hit type	Hotlist
Hotlist name	PMessier- Hotlist
Category	STOLEN
Patroller	Patroller_DM
User	

LPR

DFE•5574

Context

Map

Rue Dubois
Rue Jolicoeur
Rue Holy Cross
Rue de Sève
Boulevard Desmarchais
Avenue Émard
Rue Springland
Rue Laurier

4.3.8 | Modifier les lectures de plaques d'immatriculation

Dans certaines situations, vous voudrez parfois modifier une lecture de plaque dans Security Desk. Cela peut s'avérer nécessaire si vous remarquez que le système a capturé une lecture de plaque incorrecte, ou si le système vous invite à vérifier une lecture ambigüe (faible score de confiance).

À savoir

- Si vos privilèges utilisateur le permettent, vous pouvez modifier les lectures de plaques affichées dans les tuiles. Vous pouvez modifier les lectures de plaques dans les rapports *Lectures* et *Lectures (multi-région)*, les tuiles de surveillance et les alarmes déclenchées par les événements de lecture de plaques d'immatriculation.
- Vous ne pouvez pas modifier une lecture protégée, qui est une alerte ou qui provient d'un système fédéré ou d'un inventaire IMPI.
- Lorsque la lecture de plaque est modifiée, le score de confiance qui lui est associée passe à 100 %.
- Les détails de la modification de lecture de plaque apparaîtront dans le rapport Historiques d'activité.
- Si vous modifiez les lectures de plaques sur un système AutoVu™ Free-Flow, voir Modifier une lecture de plaque d'une zone de stationnement.

Procédure

1. Dans la tuile qui contient la lecture de plaque, cliquez sur Modifier ( ).
   REMARQUE : Si vous essayez une lecture de plaque dans un rapport *Lectures*, vous devez d'abord cliquer deux fois sur la lecture pour l'afficher dans une tuile.
2. Dans la fenêtre Modifier la lecture, modifiez manuellement les informations de Plaque et d'État.
3. Cliquez sur Enregistrer.

Résultats

La colonne Modifié des rapports *Lectures* indique si les lectures de plaques ont été modifiées. Pour en savoir plus sur l'affichage des colonnes, reportez-vous à la Présentation de l'espace de travail des tâches de rapport.

4.3.9 | Analyser les lectures NOPLATE

Si une caméra Sharp ne parvient pas à capturer une plaque lorsqu'elle est configurée pour utiliser les modes de lecture Continu avec boucle virtuelle ou Lecture unique sur déclenchement, aucune image de RAPI n'est associée à la lecture, et le numéro de plaque affiche *NOPLATE*.

À savoir

- Si la caméra ne parvient pas à capturer la plaque, aucune image de RAPI n'est associée à la lecture et le numéro de plaque *NOPLATE* est associé à la lecture. Ce mode de lecture est adapté pour obtenir un comptage plus précis du nombre de véhicules dans une aire de stationnement pour suivre l'occupation, en particulier dans les zones ou durant les saisons qui peuvent engendrer un taux plus élevé d'événements sans lecture (conditions boueuses ou neigeuses par exemple). Pour en savoir plus, voir Modifier les lectures de plaques d'immatriculation.

- Vous ne pouvez pas modifier une lecture de plaque si la lecture est protégée ou si elle provient d'un système fédéré ou d'un inventaire IMPI.
- Lorsque la lecture de plaque est modifiée, le score de confiance qui lui est associée passe à 100 %.
-
- Si le système génère trop de lectures NOPLATE (un véhicule génère plusieurs lectures NOPLATE ou un véhicule est détecté mais n'apparaît pas dans l'image) ou trop peu de lectures NOPLATE (les véhicules qui passent devant la caméra ne sont pas détectés), vous pouvez réétalonner la fonction boucle virtuelle de la caméra Sharp. Pour plus d'informations, voir Étalonner la boucle virtuelle Sharp.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Lectures.
2. Dans la liste Unités de RAPI - Patroller, sélectionnez la caméra à analyser.
3. Sélectionnez le filtre Plaque d'immatriculation et entrez `NOPLATE`.
4. Cliquez sur Générer le rapport.
   Les lectures sans numéro de plaque associé sont répertoriées dans le volet de rapport.
5. Si la plaque du véhicule est visible dans l'image de contexte, vous pouvez modifier la lecture de plaque en vue d'inclure le bon numéro de plaque.
   a. Double-cliquez sur la lecture pour l'afficher dans une mosaïque.

b. Dans la tuile qui contient la lecture de plaque, cliquez sur Modifier ( ).
c. Dans la fenêtre Modifier la lecture, modifiez manuellement les informations de Plaque.
d. Cliquez sur Enregistrer.

Explorer

- Configurer les analyses SharpV
- Étalonner la boucle virtuelle

4.3.10 | Analyser les lectures de plaques effectuées

Vous pouvez rechercher les lectures effectuées sur une période et dans une zone géographique données avec le rapport *Lectures*.

Avant de commencer

Pour afficher le résultat de la recherche sur le canevas, vous devez savoir comment surveiller les événements de RAPI dans Security Desk en mode Carte.

À savoir

Pour créer un rapport sur toutes les lectures effectuées dans une région particulière sur une période donnée, sélectionnez la région et la plage horaire. Pour voir le nombre de lectures effectuées par une unité Genetec Patroller™ pendant une ronde, recherchez cette unité Genetec Patroller™, puis définissez une plage horaire. Pour savoir si une unité Genetec Patroller™ a effectué la lecture d'une plaque particulière, vous pouvez rechercher la plaque concernée.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Lectures.
2. Pour restreindre votre recherche à des secteurs donnés, vous pouvez dessiner des régions sur la carte de la manière suivante :
   a. Dans l'onglet Filtres, cliquez sur le filtre Région.
   b. Cliquez sur Basculer en mode carte.
   c. Dans le filtre Région, cliquez sur Dessiner une région.
   d. Faites glisser le curseur de la souris pour tracer un cadre.
   Un cadre de Région numéroté est créé.
   e. Faites glisser les poignées pour redimensionner la région.
   f. Pour déplacer la région, cliquez sans relâcher le bouton de la souris et faites glisser la zone à l'endroit voulu.
   g. Créez d'autres régions si nécessaire.
   h. Sélectionnez les régions qui vous intéressent.
   Pour afficher toutes les régions que vous avez créées, cliquez sur dans l'onglet Filtres.
3. Définissez les autres filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   A généré une alerte
   Sélectionnez les lectures ayant généré une alerte dans le rapport.

   Règles d'alerte
   Sélectionnez les règles d'alerte à inclure dans le rapport.

   Plaque d'immatriculation
   Entrez un numéro de plaque complet ou partiel. Pour saisir plusieurs plaques d'immatriculation, voir Filtrer un rapport avec plusieurs plaques d'immatriculation

Unités de RAPI - Patroller
Limitez la recherche aux unités Genetec Patroller™ (dont les unités de RAPI associées) et/ou aux unités de RAPI représentant des caméras Sharp fixes sur l'unité Genetec Patroller™.

Décharger l'horodatage
La date et l'heure du déchargement des lectures/alertes de vers .Genetec Patroller™Security Center

État de la protection
Restreindre la recherche aux événements de lecture protégés ou non protégés.

Règle
Règle d'alerte qui correspond à la lecture de la plaque.

Utilisateurs
Sélectionnez le nom d'utilisateur Patroller, ou les groupes d'utilisateurs parents du Patroller.

4. Cliquez sur Générer le rapport.
   Les lectures sont affichées dans le volet de rapport.
5. (Facultatif) Pour afficher les images haute résolution dans les colonnes *Image plaque* et *Image contextuelle*, augmentez la largeur de la colonne correspondante. Pour en savoir plus, voir Personnaliser la qualité des images de RAPI affichées dans les colonnes du volet de rapport
6. Vous pouvez afficher le résultat sur le canevas en exploitant l'un des modes suivants :

mode Tuile
Pour afficher un événement de RAPI dans une tuile, cliquez deux fois sur l'élément dans le volet de rapport, ou faites-le glisser sur le canevas.

mode Carte
Pour repérer un événement de RAPI sur la carte, cliquez deux fois sur l'événement dans le volet de rapport.

Explorer

- À propos des filtres de plaques d'immatriculation

4.3.10.1 | Colonnes du volet de rapport pour la tâche Lectures

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Adresse
Lieu de la lecture de RAPI.

Image contextuelle
Image couleur grand-angle du véhicule capturée par la caméra contextuelle.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Appareil
Périphérique utilisé par l'unité (lecteur, entrée REX, module d'E/S, relais de pêne, et ainsi de suite).

Heure de l'événement
Date et heure de l'événement.

A généré une alerte
Indique que la lecture a généré une alerte avec une coche.

Latitude
Les coordonnées de l'événement de RAPI.

Longitude
Les coordonnées de l'événement de RAPI.

Aire
Zone de stationnement où une règle de stationnement donnée est en vigueur.

Capture manuelle
Affiche le numéro de plaque saisi manuellement par l'utilisateur de Genetec Patroller™.

Décharger l'horodatage
La date et l'heure de déchargement des lectures et alertes du véhicule de patrouille vers Security Center.

Entité Patroller
Nom de l'entité Patroller. Le champ de nom d'entité patroller n'est pas renseigné pour les caméras SharpV fixes.

Nom de permis
Nom de la liste de permis soumise à la restriction de permis.

Image de plaque
L'image de la plaque d'immatriculation capturée par la caméra de RAPI.

Origine de la plaque
L'État émetteur de la plaque d'immatriculation.

Lecture de plaque
La lecture de plaque d'immatriculation générée par l'unité .Sharp

Protégé
Indique si l'enregistrement sera protégé contre la suppression de la base de données à l'expiration de la période de rétention (pour ce type d'enregistrement).

Expiration de la protection
Indique la date d'expiration de la protection de la lecture.

Règle
Règle d'alerte qui correspond à la lecture de la plaque.

Unité de RAPI
Unité de RAPI ayant lu la plaque ; renseigné pour un véhicule de patrouille (Patroller - Gauche, Patroller - Droite, et ainsi de suite) et pour une Sharp fixe.

Image de la roue
Image des roues du véhicule. Sert au marquage virtuel des roues.
Sujet parent : Analyser les lectures de plaques effectuées

4.3.11 | Analyser les statistiques de lectures

Vous pouvez rapidement analyser les statistiques de lecture pour une plage horaire et une zone géographique données avec le rapport Statistiques de lecture.

À savoir

Pour afficher le résultat de la recherche sur le canevas, vous devez savoir comment surveiller les événements de RAPI dans Security Desk.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Lectures.
2. Pour restreindre votre recherche à des secteurs donnés, vous pouvez dessiner des régions sur la carte de la manière suivante :
    a. Dans l'onglet Filtres, cliquez sur le filtre Région.
    b. Cliquez sur Basculer en mode carte.
    c. Dans le filtre Région, cliquez sur Dessiner une région.
    d. Faites glisser le curseur de la souris pour tracer un cadre.
    Un cadre de Région numéroté est créé.
    e. Faites glisser les poignées pour redimensionner la région.
    f. Pour déplacer la région, cliquez sans relâcher le bouton de la souris et faites glisser la zone à l'endroit voulu.
    g. Créez d'autres régions si nécessaire.
    h. Sélectionnez les régions qui vous intéressent.
    Pour afficher toutes les régions que vous avez créées, cliquez sur  dans l'onglet Filtres.
3. Définissez les autres filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

    Champs personnalisés
    Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

    A généré une alerte
    Sélectionnez les lectures ayant généré une alerte dans le rapport.

    Règles d'alerte
    Sélectionnez les règles d'alerte à inclure dans le rapport.

    Plaque d'immatriculation
    Entrez un numéro de plaque complet ou partiel. Pour saisir plusieurs plaques d'immatriculation, voir Filtrer un rapport avec plusieurs plaques d'immatriculation

    Unités de RAPI - Patroller
    Limitez la recherche aux unités Genetec Patroller™ (dont les unités de RAPI associées) et/ou aux unités de RAPI représentant des caméras Sharp fixes sur l'unité Genetec Patroller™.

    Décharger l'horodatage
    La date et l'heure du déchargement des lectures/alertes de vers .Genetec Patroller™Security Center

    Règle
    Règle d'alerte qui correspond à la lecture de la plaque.

    Utilisateurs
    Sélectionnez le nom d'utilisateur Patroller, ou les groupes d'utilisateurs parents du Patroller.

4. Cliquez sur la petite flèche à droite du bouton Créer un rapport, et sélectionnez Générer un rapport de statistiques.
    Le nombre de lectures est affiché dans le volet de rapport.

Exemple

Pour créer un rapport rapide sur toutes les lectures effectuées dans une région particulière sur une période donnée, sélectionnez la région et la plage horaire.

4.3.12 | Analyser les lectures signalées (multi-région)

Vous pouvez consulter le nombre de lectures à l'échelle de plusieurs régions d'intérêt sur une période donnée avec le rapport *Lectures (multi-région)*.

À savoir

Pour afficher le résultat de la recherche sur le canevas, vous devez savoir comment surveiller les événements de RAPI dans Security Desk.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Lectures (multi-région).
2. Pour restreindre votre recherche à des secteurs donnés, vous pouvez dessiner des régions sur la carte de la manière suivante :
    a. Dans l'onglet Filtres, cliquez sur le filtre Région.
    b. Cliquez sur Basculer en mode carte.
    c. Dans le filtre Région, cliquez sur Dessiner une région.
    d. Faites glisser le curseur de la souris pour tracer un cadre.
    Un cadre de Région numéroté est créé.
    e. Faites glisser les poignées pour redimensionner la région.
    f. Pour déplacer la région, cliquez sans relâcher le bouton de la souris et faites glisser la zone à l'endroit voulu.
    g. Créez d'autres régions si nécessaire.
    h. Sélectionnez les régions qui vous intéressent.
    Pour afficher toutes les régions que vous avez créées, cliquez sur  dans l'onglet Filtres.
3. Définissez les autres filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

    Champs personnalisés
    Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

    Heure de l'événement
    Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

    Règles d'alerte
    Sélectionnez les règles d'alerte à inclure dans le rapport.

    Plaque d'immatriculation
    Entrez un numéro de plaque complet ou partiel. Pour saisir plusieurs plaques d'immatriculation, voir Filtrer un rapport avec plusieurs plaques d'immatriculation

    Unités de RAPI - Patroller
    Limitez la recherche aux unités Genetec Patroller™ (dont les unités de RAPI associées) et/ou aux unités de RAPI représentant des caméras Sharp fixes sur l'unité Genetec Patroller™.

    État de la protection
    Restreindre la recherche aux événements de lecture protégés ou non protégés.

4. Cliquez sur Générer le rapport.
    Les lectures associées à toutes les régions que vous avez définies sont affichées dans le volet de rapport.
5. (Facultatif) Pour afficher les images haute résolution dans les colonnes *Image plaque* et *Image contextuelle*, augmentez la largeur de la colonne correspondante. Pour en savoir plus, voir Personnaliser la qualité des images de RAPI affichées dans les colonnes du volet de rapport
6. Vous pouvez afficher le résultat sur le canevas en exploitant l'un des modes suivants :

    mode Tuile
    Pour afficher un événement de RAPI dans une tuile, cliquez deux fois sur l'élément dans le volet de rapport, ou faites-le glisser sur le canevas.

    mode Carte
    Pour repérer un événement de RAPI sur la carte, cliquez deux fois sur l'événement dans le volet de rapport.

Exemple

Pour créer un rapport sur toutes les lectures effectuées dans plusieurs régions sur une période donnée, vous pouvez créer plusieurs régions, et spécifier la plage horaire.
Explorer

- À propos des filtres de plaques d'immatriculation

4.3.12.1 | Colonnes du volet de rapport pour la tâche Lectures (multi-région)

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Adresse
Lieu de la lecture de RAPI.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Heure de l'événement
Date et heure de l'événement.

Unité de RAPI
Unité de RAPI ayant lu la plaque ; renseigné pour un véhicule de patrouille (Patroller - Gauche, Patroller - Droite, et ainsi de suite) et pour une Sharp fixe.

Capture manuelle
Affiche le numéro de plaque saisi manuellement par l'utilisateur de Genetec Patroller™.

Entité Patroller
Nom de l'entité Patroller. Le champ de nom d'entité patroller n'est pas renseigné pour les caméras SharpV fixes.

Lecture de plaque
La lecture de plaque d'immatriculation générée par l'unité .Sharp

Protégé
Indique si l'enregistrement sera protégé contre la suppression de la base de données à l'expiration de la période de rétention (pour ce type d'enregistrement).

Expiration de la protection
Indique la date d'expiration de la protection de la lecture.

Règle
Règle d'alerte qui correspond à la lecture de la plaque.

Sujet parent : Analyser les lectures signalées (multi-région)

4.3.13 | Analyser les alertes signalées (multi-région)

Vous pouvez consulter le nombre d'alertes à l'échelle de plusieurs régions d'intérêt sur une période donnée avec le rapport *Alertes (multi-région)*.

À savoir

Pour afficher le résultat de la recherche sur le canevas, vous devez savoir comment surveiller les événements de RAPI dans Security Desk.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Alertes (multi-région).
2. Pour restreindre votre recherche à des secteurs donnés, vous pouvez dessiner des régions sur la carte de la manière suivante :
    a. Dans l'onglet Filtres, cliquez sur le filtre Région.
    b. Cliquez sur Basculer en mode carte.
    c. Dans le filtre Région, cliquez sur Dessiner une région.
    d. Faites glisser le curseur de la souris pour tracer un cadre.
    Un cadre de Région numéroté est créé.
    e. Faites glisser les poignées pour redimensionner la région.
    f. Pour déplacer la région, cliquez sans relâcher le bouton de la souris et faites glisser la zone à l'endroit voulu.
    g. Créez d'autres régions si nécessaire.
    h. Sélectionnez les régions qui vous intéressent.
    Pour afficher toutes les régions que vous avez créées, cliquez sur  dans l'onglet Filtres.
3. Définissez les autres filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

    Champs personnalisés
    Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

    Heure de l'événement
    Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

    Règles d'alerte
    Sélectionnez les règles d'alerte à inclure dans le rapport.

    Plaque d'immatriculation
    Entrez un numéro de plaque complet ou partiel. Pour saisir plusieurs plaques d'immatriculation, voir Filtrer un rapport avec plusieurs plaques d'immatriculation

    Unités de RAPI - Patroller
    Limitez la recherche aux unités Genetec Patroller™ (dont les unités de RAPI associées) et/ou aux unités de RAPI représentant des caméras Sharp fixes sur l'unité Genetec Patroller™.

    État de la protection
    Restreindre la recherche aux événements d'alerte protégés ou non protégés.

4. Cliquez sur Générer le rapport.
    Les lectures associées à toutes les régions que vous avez définies sont affichées dans le volet de rapport.
5. (Facultatif) Pour afficher les images haute résolution dans les colonnes *Image plaque* et *Image contextuelle*, augmentez la largeur de la colonne correspondante. Pour en savoir plus, voir Personnaliser la qualité des images de RAPI affichées dans les colonnes du volet de rapport
6. Vous pouvez afficher le résultat sur le canevas en exploitant l'un des modes suivants :

    mode Tuile
    Pour afficher un événement de RAPI dans une tuile, cliquez deux fois sur l'élément dans le volet de rapport, ou faites-le glisser sur le canevas.

    mode Carte
    Pour repérer un événement de RAPI sur la carte, cliquez deux fois sur l'événement dans le volet de rapport.

Exemple

Pour créer un rapport sur toutes les alertes survenues dans plusieurs régions sur une période donnée, vous pouvez créer plusieurs régions, et spécifier la plage horaire.
Explorer

- À propos des filtres de plaques d'immatriculation

4.3.13.1 | Colonnes du volet de rapport pour la tâche Alertes (multi-région)

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Motifs d'acceptation
Motif sélectionné par l'utilisateur Genetec Patroller™ pour valider une alerte. Les motifs d'acceptation sont créés et configurés dans Config Tool.

Adresse
Lieu de la lecture de RAPI.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Heure de l'événement
Date et heure de l'événement.

Unité de RAPI
Unité de RAPI ayant lu la plaque ; renseigné pour un véhicule de patrouille (Patroller - Gauche, Patroller - Droite, et ainsi de suite) et pour une Sharp fixe.

Entité Patroller
Nom de l'entité Patroller. Le champ de nom d'entité patroller n'est pas renseigné pour les caméras SharpV fixes.

Lecture de plaque
La lecture de plaque d'immatriculation générée par l'unité .Sharp

Protégé
Indique si l'enregistrement sera protégé contre la suppression de la base de données à l'expiration de la période de rétention (pour ce type d'enregistrement).

Expiration de la protection
Indique la date d'expiration de la protection de l'alerte.

Règle
Règle d'alerte qui correspond à la lecture de la plaque.

Utilisateur
Le nom de l'utilisateur Genetec Patroller™. Non disponible pour un hôte de fédération Security Center Federation™ pour les entités Genetec Patroller™ fédérées.

Sujet parent : Analyser les alertes signalées (multi-région)

4.3.14 | Analyser les lectures et alertes par jour

Vous pouvez afficher le nombre de lectures et d'alertes sur une période donnée avec le rapport *Lectures/alertes par jour*.

À savoir

Ce rapport permet d'évaluer les performances des installations Genetec Patroller™ et des caméras Sharp fixes sur le terrain. Par exemple, pour mesurer l'efficacité de l'emplacement d'une Sharp fixe, vous pouvez rechercher cette Sharp, puis configurer une plage horaire d'une semaine.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Lectures/alertes par jour.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Règles d'alerte
   Sélectionnez les règles d'alerte à inclure dans le rapport.

   Type d'alerte
   Sélectionnez les types d'alertes que vous souhaitez inclure dans le rapport : *Permis*, *Permis partagé*, *Dépassement horaire* et *Liste de véhicules recherchés*.

   Unités de RAPI - Patroller
   Limitez la recherche aux unités Genetec Patroller™ (dont les unités de RAPI associées) et/ou aux unités de RAPI représentant des caméras Sharp fixes sur l'unité Genetec Patroller™.

   Motif de rejet
   Motif sélectionné par l'utilisateur de pour rejeter l'alerte.Genetec Patroller™ Les motifs de rejet sont créés et personnalisés dans Config Tool. Ce filtre n'affecte que la valeur de la colonne *Alertes rejetées*.

   Plage horaire
   La plage horaire pour le rapport.

   Utilisateurs
   Sélectionnez le nom d'utilisateur Patroller, ou les groupes d'utilisateurs parents du Patroller.

3. Cliquez sur Générer le rapport.
   Les événements de lecture et d'alerte sont affichés dans le volet de rapport.
4. Consultez les statistiques sur le nombre de lectures, d'alertes et d'actions d'alerte durant la plage horaire sélectionnée dans la section Statistiques.

4.3.14.1 | Colonnes du volet de rapport pour la tâche Lectures/alertes par jour

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Alertes appliquées
Nombre d'alertes appliquées.

Alertes
Nombre d'alertes.
REMARQUE : Si vous utilisez des critères de recherche de *Règles d'alertes* et *Type d'alerte*, cette valeur peut ne pas représenter le nombre total d'alertes de la journée.

Alertes non appliquées
Nombre d'alertes qui n'ont pas été appliquées.

Lectures
Nombre de lectures de plaques d'immatriculation.

Alertes rejetées
Nombre d'alertes qui ont été rejetées.
Sujet parent : Analyser les lectures et alertes par jour

4.3.15 | Analyser les lectures et alertes par zone de stationnement

Vous pouvez afficher le nombre de lectures et d'alertes par *zone de stationnement* sur une période donnée avec le rapport *Lectures/alertes par zone*.

À savoir

En affichant l'activité au sein d'une zone de stationnement, vous pouvez évaluer les performances des installations Genetec Patroller™ et des caméras Sharp fixes sur le terrain. Par exemple, pour mesurer l'efficacité de l'emplacement d'une Sharp fixe, vous pouvez rechercher cette Sharp, puis configurer une plage horaire d'une semaine.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Lectures/alertes par zone.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Règles d'alerte
   Sélectionnez les règles d'alerte à inclure dans le rapport.

   Type d'alerte
   Sélectionnez les types d'alertes que vous souhaitez inclure dans le rapport : *Permis*, *Permis partagé*, *Dépassement horaire* et *Liste de véhicules recherchés*.

   Unités de RAPI - Patroller
   Limitez la recherche aux unités Genetec Patroller™ (dont les unités de RAPI associées) et/ou aux unités de RAPI représentant des caméras Sharp fixes sur l'unité Genetec Patroller™.

   Motif de rejet
   Motif sélectionné par l'utilisateur de pour rejeter l'alerte.Genetec Patroller™ Les motifs de rejet sont créés et personnalisés dans Config Tool. Ce filtre n'affecte que la valeur de la colonne *Alertes rejetées*.

   Plage horaire
   La plage horaire pour le rapport.

   Utilisateurs
   Sélectionnez le nom d'utilisateur Patroller, ou les groupes d'utilisateurs parents du Patroller.

3. Cliquez sur Générer le rapport.
   Les événements de lecture et d'alerte sont affichés dans le volet de rapport.
4. Consultez les statistiques sur le nombre de lectures, d'alertes et d'actions d'alerte durant la plage horaire sélectionnée dans la section Statistiques.

4.3.15.1 | Colonnes du volet de rapport pour la tâche Lectures/alertes par zone

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Alertes appliquées
Nombre d'alertes appliquées.

Alertes
Nombre d'alertes.
REMARQUE : Si vous utilisez des critères de recherche de *Règles d'alertes* et *Type d'alerte*, cette valeur peut ne pas représenter le nombre total d'alertes de la journée.

Alertes non appliquées
Nombre d'alertes qui n'ont pas été appliquées.

Lectures
Nombre de lectures de plaques d'immatriculation.

Alertes rejetées
Nombre d'alertes qui ont été rejetées.

Fuseau horaire
Le fuseau horaire de l'unité.
Sujet parent : Analyser les lectures et alertes par zone de stationnement

4.3.16 | À propos des filtres de plaques d'immatriculation

Lorsque vous générez un rapport qui inclut des plaques d'immatriculation capturées par une caméra de RAPI, si vous ne connaissez pas le numéro de plaque complet, vous pouvez utiliser des astérisques (*) et des points d'interrogation (?) pour remplacer les caractères inconnus.

Les rapports Security Desk suivants intègrent le filtre Plaque d'immatriculation qui vous permet d'inclure des numéros de plaque complets ou partiels :

- Rapport d'infractions
- Rapport d’alertes (multi-région)
- Rapport de lectures
- Rapport de lectures (multi-région)
- Rapport d'inventaire
- Rapport de sessions de stationnement
- Rapport de zones de stationnement

Complet

Lorsque vous sélectionnez Complet, vous pouvez saisir l'intégralité de la plaque d'immatriculation. Vous pouvez également saisir les caractères génériques * et ? à la place des caractères inconnus.

- **Astérisques (*) :** Vous pouvez saisir un ou plusieurs astérisques pour représenter un caractère, plusieurs caractères ou aucun caractère. Par exemple, vous savez que la plaque commence par « A » et se termine par « 123 », mais vous n'êtes pas sûr de ce qu'il y a entre les deux. Filtrer sur **A*123** renverrait les plaques suivantes dans le rapport :

Numéro de plaque	Résultat du rapport	Motif
AB 123	Inclus	Un caractère apparaît entre « A » et « 123 ».
A**BC** 123	Inclus	Plusieurs caractères apparaissent entre « A » et « 123 ».
A 123	Inclus	Aucun caractère apparaît entre « A » et « 123 ».
AB**C** 123**4**	Exclus	Le numéro ne se termine pas par « 123 ».

- **Point d'interrogation (?) :** Vous pouvez saisir un ou plusieurs points d'interrogation pour représenter tout caractère unique. Par exemple, si vous ne vous souvenez plus du premier ou du dernier caractère d'une plaque, filtrer sur **?BC 12?** renvoie les plaques suivantes dans le rapport :

Numéro de plaque	Résultat du rapport	Motif
ABC 12**3**	Inclus	Il y a un caractère avant et après « BC 12 ».
5BC 12**L**	Inclus	Il y a un caractère avant et après « BC 12 ».
AABC 12**3**	Exclus	Chaque « ? » ne peut représenter qu'un seul caractère.

- **Combinaison :** Vous pouvez saisir une combinaison d'astérisques et de points d'interrogation. Par exemple, filtrer sur **A? C 1*** renverrait les plaques suivantes dans le rapport :

Numéro de plaque	Résultat du rapport	Motif
A**B**C 1**23**	Inclus	Le « ? » est remplacé par « B » et il y a des caractères après le « 1 ».
A**2**C 1	Inclus	Le « ? » est remplacé par « 2 » et il n'y a pas de caractère après le « 1 ».
A**BB**C 1**23**	Exclus	Chaque « ? » ne peut représenter qu'un seul caractère.

Partiel

Sélectionnez Partiel si vous ne connaissez pas le début ou la fin du numéro de plaque. Par exemple, la lecture de plaque ABC 123 ne serait renvoyée qu'avec les deux exemples de numéros de plaques ci-dessous.
REMARQUE : Vous ne pouvez pas utiliser les astérisques et les points d'interrogation avec les plaques d'immatriculation partielles.

Recherche de plaque partielle	Résultat du rapport	Motif
123	ABC 123 est inclus	Les caractères manquants viennent avant « 123 ».
C12	ABC 123 est inclus	Les caractères manquants viennent avant et après « C12 ».
ABC 23	ABC 23 n'est PAS inclus	Le caractère manquant est au milieu de « ABC23 ».

Plaques d'immatriculation multiples

Si vous souhaitez enquêter simultanément sur plusieurs plaques d'immatriculation, vous pouvez saisir les numéros de plaque souhaités à l'aide d'un délimiteur. Cette caractéristique s'applique au filtre complet et partiel des plaques d'immatriculation. Pour plus d'informations sur la manière de saisir plusieurs numéros de plaque d'immatriculation, voir Filtrer un rapport avec plusieurs plaques d'immatriculation

4.3.16.1 | Filtrer un rapport avec plusieurs plaques d'immatriculation

Pour enquêter simultanément sur plusieurs plaques d'immatriculation dans un rapport, vous pouvez entrer la liste des plaques d'immatriculation à l'aide d'un délimiteur dans le filtre des plaques d'immatriculation.

Avant de commencer

Assurez-vous de connaître les différentes combinaisons de numéros de plaque d'immatriculation complets et partiels. Pour en savoir plus, voir À propos des filtres de plaques d'immatriculation.

À savoir

Vous pouvez utiliser l'un des délimiteurs suivants pour entrer plusieurs numéros de plaque d'immatriculation dans le filtre :

- Point-virgule (;)
- Virgule (,)
- Retour à la ligne (\r\n)

Limitation : Vous pourriez connaître des vitesses de recherche lentes dans les conditions suivantes :

- Vous utilisez une combinaison de caractères génériques sur chaque numéro de plaque d'immatriculation saisi.
- Vous avez un énorme volume de documents à parcourir pour la période sélectionnée. Par exemple, vous avez sélectionné une période de six mois et la base de données contient près d'un demi-million d'enregistrements qui correspondent à cette période.

Procédure

1. Sur la page d'accueil , ouvrez la tâche Rapport désirée.
   Si vous souhaitez générer un rapport des alertes, ouvrez la tâche Alertes.
   REMARQUE : Pour la liste complète des rapports qui utilisent le filtre des plaques d'immatriculation, voir À propos des filtres de plaques d'immatriculation
2. Dans l'onglet Filtres, cliquez sur le filtre Plaque d'immatriculation.
3. Saisissez les numéros de plaque d'immatriculation souhaités, séparés par l'un des délimiteurs suivants :
   - Point-virgule (;)
   - Virgule (,)
   - Retour à la ligne (\r\n)

   REMARQUE : Ces délimiteurs peuvent être mélangés et assortis à volonté.
4. Définissez les filtres de recherche suivants pour votre rapport :

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

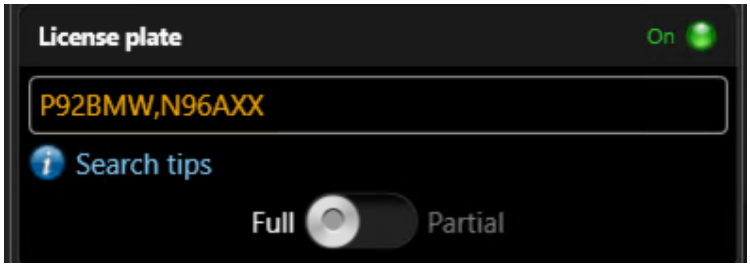
   Unités de RAPI - Patroller
   Limitez la recherche aux unités Genetec Patroller™ (dont les unités de RAPI associées) et/ou aux unités de RAPI représentant des caméras Sharp fixes sur l'unité Genetec Patroller™.

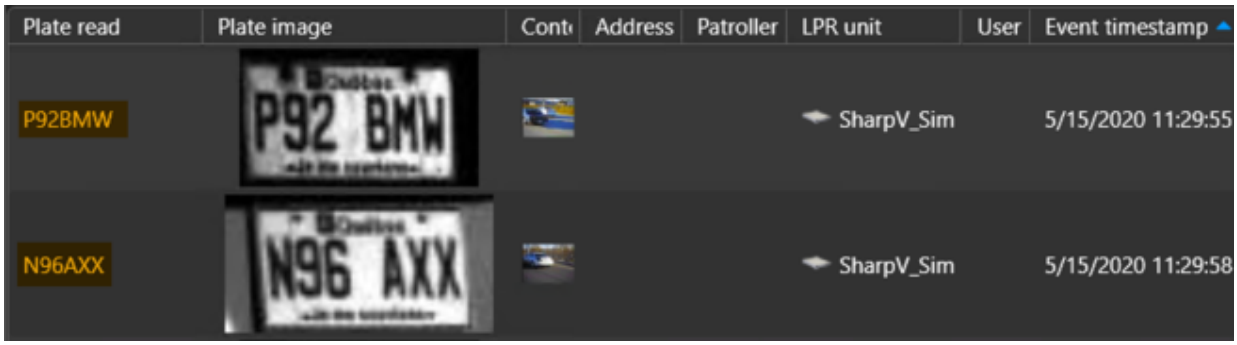
   REMARQUE : En outre, vous pouvez configurer les autres filtres de requête.
5. Cliquez sur Générer le rapport.

Exemple

Les exemples suivants illustrent les différentes façons de filtrer un rapport avec plusieurs plaques d'immatriculation :

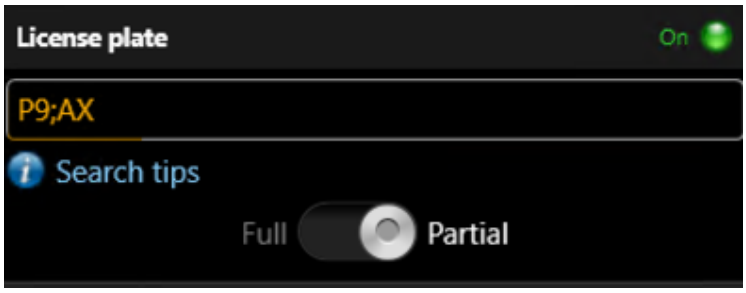
1. Plaque d'immatriculation complète : Dans cet exemple, un délimiteur à virgule sépare plusieurs numéros de plaque d'immatriculation complets.

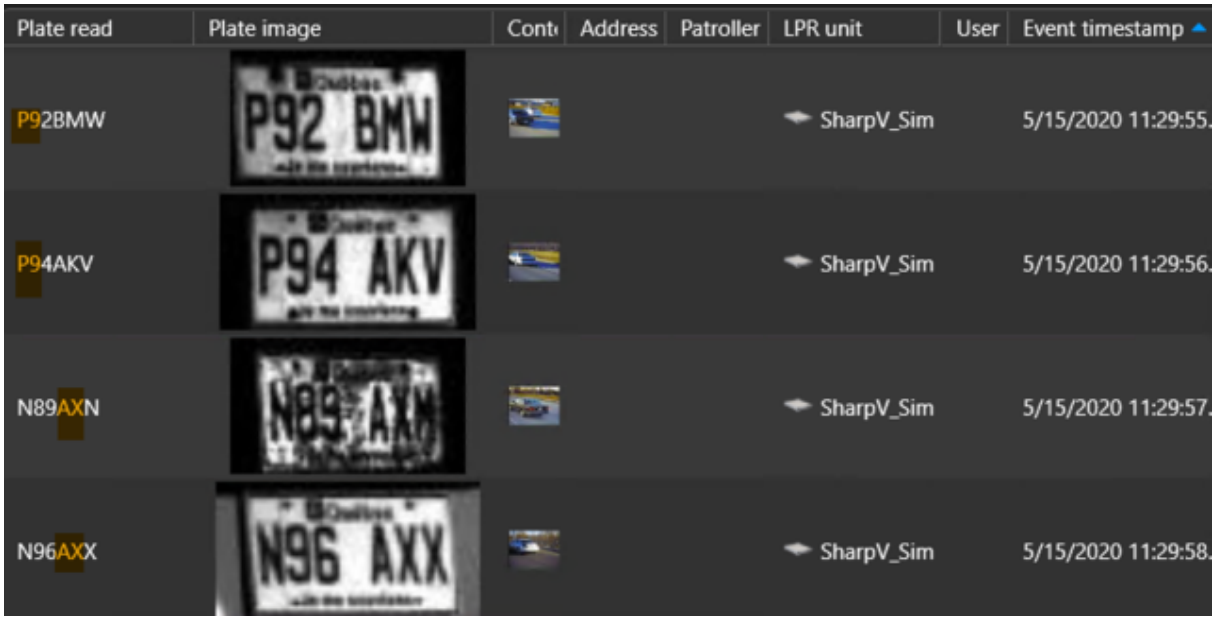




2. Plaque d'immatriculation complète avec caractère générique : Dans cet exemple, les numéros de plaque d'immatriculation comportent des caractères génériques et sont séparés par un délimiteur de retour à la ligne.

3. Plaque d'immatriculation partielle : dans cet exemple, un délimiteur à point-virgule sépare plusieurs numéros de plaque d'immatriculation partiels.





Sujet parent : À propos des filtres de plaques d'immatriculation

4.3.17 | Protéger les lectures et alertes contre la suppression

Un opérateur Security Desk peut empêcher qu'une lecture ou alerte importante soit supprimée de la base de données du Gestionnaire RAPI. La lecture ou l'alerte ne sera alors pas supprimée, même si la période de rétention est dépassée.

Avant de commencer

Pour protéger et déprotéger les lectures et les alertes, le privilège *Protéger/annuler la protection des lectures/alertes de RAPI* est nécessaire.

À savoir

- Vous pouvez protéger les lectures et alertes dans les tâches suivantes :
  - Alertes
  - Alertes (multi-région)
  - Lectures
  - Lectures (multi-région)
- Vous pouvez utiliser le filtre État de la protection pour rechercher les lectures et les alertes protégées dans les rapports.
- Vous pouvez voir quels utilisateurs ont protégé et déprotégé des lectures et alertes dans la tâche Historiques d'activité.

Procédure

1. Ouvrez une tâche Lectures ou Alertes.
2. Créez votre rapport.
   Les lectures ou alertes sont affichées dans le volet de rapport.
3. Dans le volet de rapport, sélectionnez la lecture ou l'alerte à protéger, puis cliquez sur Protéger ( ).
   Pour sélectionner plusieurs événements, appuyez sur la touche Ctrl ou Maj.
4. Dans la boîte de dialogue Protéger les résultats sélectionnés, réglez la durée de protection de la lecture ou alerte.

Indéfiniment
Pas de date de fin. Vous devez supprimer la protection manuellement en sélectionnant la lecture ou l'alerte dans le volet de rapport, puis en cliquant sur Annuler la protection ( ).
REMARQUE : Lorsque vous déprotégez une lecture ou une alerte qui a dépassé la période de rétention configurée, elle est supprimée et n'apparaît plus dans les rapports.

Pendant les x prochains jours
La lecture ou l'alerte est protégée durant le nombre de jours spécifié.

Jusqu'au
La lecture ou l'alerte est protégée jusqu'à la date spécifiée.
Exemple : Si vous protégez la lecture ou l'alerte jusqu'au 20/11/2017, elle sera supprimée de la base de données de RAPI le 21/11/2017 à minuit.

5. Cliquez sur Protéger.

Résultats

La lecture ou l'alerte est protégée.

Lorsque vous avez terminé

Ajoutez les colonnes Protégé et Expiration de la protection à votre rapport pour voir les lectures et alertes qui sont protégées, et jusqu'à quand. Voir Créer et enregistrer un rapport

4.4 | AutoVu™ Free-Flow dans Security Desk

4.4.1 | Gestion des zones de stationnement

La fonctionnalité AutoVu™ Free-Flow de Security Desk vous permet de surveiller le nombre de véhicules en infraction dans chaque zone de stationnement. Elle vous permet donc de prendre des décisions en fonction d'informations sur l'inventaire et la capacité des zones de stationnement qui sont à jour.

Sharp Les caméras Sharp peuvent détecter les plaques d'immatriculation des véhicules qui passent. Lorsque des caméras Sharp sont installées aux entrées et sorties d'une zone de stationnement, le système peut suivre la durée du séjour des véhicules dans l'aire de stationnement. Lorsque des règles sont définies pour l'aire de stationnement (par exemple, « stationnement gratuit pendant une heure »), le système peut vous montrer les véhicules qui sont en infraction et doivent être verbalisés.

4.4.1.1 | À propos des sessions de stationnement

La fonction AutoVu™ Free-Flow de Security Center utilise les sessions de stationnement pour suivre le séjour de chaque véhicule dans une zone de stationnement.

Les termes suivants sont importants lors de la configuration des zones de stationnement AutoVu™ Free-Flow :

Temps de commodité
Le temps de commodité est une période de souplesse configurable avant qu'un véhicule commence à payer une fois dans la zone de stationnement. Par exemple, si vous voulez configurer une période de « stationnement gratuit » de 2 heures avant que le stationnement devienne payant, le temps de commodité doit être réglé sur 2 heures. Pour les aires de stationnement payantes, vous devez également définir un bref laps temps de commodité pour permettre aux conducteurs de trouver une place de stationnement et de payer pour une durée de stationnement donnée.

Délai d'expiration par défaut
Le Délai d'expiration par défaut est utilisé pour les permis fournis par Pay-by-Plate Sync sans date d'expiration. Dans ce cas, AutoVu™ Free-Flow vérifie auprès du fournisseur du permis de stationnement que le permis est encore valable. L'augmentation de cette valeur diminue la fréquence des vérifications de permis. Par exemple, si l'aire de stationnement facture par périodes de 15 minutes, et que vous réglez également le délai d'expiration par défaut sur 15 minutes, le système valide le permis auprès du fournisseur de stationnement toutes les 15 minutes.

Délai de grâce
Vous pouvez ajouter un délai de grâce à une session de stationnement pour une application des règles plus souple. À l'expiration de la durée de stationnement payant ou du temps de commodité du véhicule, un délai de grâce est accordé avant de considérer que la session de stationnement soit signalée comme étant en *infraction*.

Délai de session maximal
La définition d'un délai de session maximal permet d'optimiser les statistiques d'occupation d'une aire de stationnement. Lorsqu'un véhicule dépasse ce délai, le système considère que la plaque du véhicule n'a pas été lue à la sortie et qu'il n'est plus présent dans la zone de stationnement. Le délai de session maximal apparaît dans les rapports générés par la tâche Sessions de stationnement avec le *Motif d'état : Délai de session maximal dépassé*.

Temps payé
La phase temps payé d'une session de stationnement commence à l'expiration du temps de commodité. Les propriétaires des véhicules peuvent payer leur stationnement sur une borne ou avec une app mobile, et le système de paiement peut être fourni par des fournisseurs de permis de stationnement tiers.

Règle de stationnement
Définit quand et comment une session de stationnement est considérée comme étant valable ou en infraction.

États de sessions de stationnement
La session de stationnement d'un véhicule est divisé en quatre états : *Valable* (comprend le temps de commodité, le temps payé et le délai de grâce), *Infraction*, *Appliqué* et *Terminé*. Lorsqu'un véhicule se gare dans une zone de stationnement, l'état de sa session de stationnement évolue en fonction des délais configurés pour la règle de stationnement, la validité du temps payé, et le signalement ou non d'une infraction.

Zone de stationnement
Les zones de stationnement que vous définissez dans Security Center représentent des parkings hors voirie dont les entrées et sorties sont surveillées par des caméras Sharp.

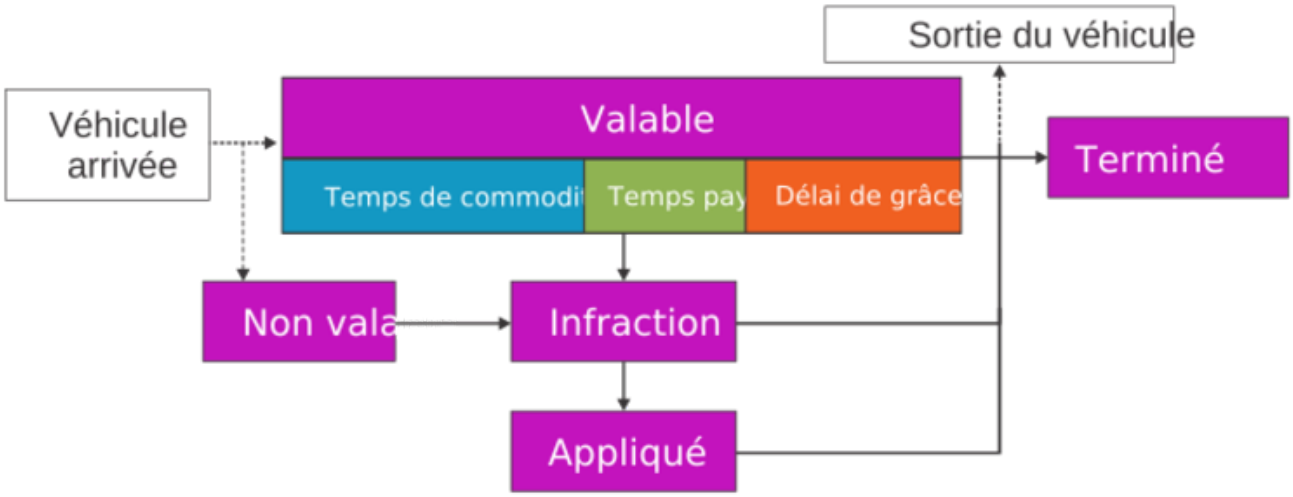
Capacité de zone de stationnement
La capacité de zone de stationnement correspond au nombre de véhicules qui peuvent s'y garer.

Seuil de capacité de zone de stationnement
Le réglage de seuil de capacité d'une zone de stationnement détermine le seuil à partir duquel un événement seuil de capacité atteint est généré. Par exemple, si vous baissez le seuil à 90 %, le système génère un événement lorsque la capacité de la zone de stationnement atteint 90 %.
Sujet parent : Gestion des zones de stationnement

4.4.1.2 | États de sessions de stationnement

La session de stationnement d'un véhicule est divisée en quatre états, qui décrivent l'évolution du séjour du visiteur. Si vous devez surveiller et analyser les zones de stationnement, ou si vous configurez des zones et des règles de stationnement, il est important de comprendre les états successifs d'une.

Lorsqu'un véhicule se gare dans une zone de stationnement, les états successifs d'une session de stationnement dépendent de la survenue ou non d'une infraction. Le diagramme suivant montre les états possibles d'une session de stationnement :



Valable
Une session de stationnement passe en état *valable* car :

- La plaque d'immatriculation du véhicule est lue à l'entrée de la zone de stationnement.
  REMARQUE : Selon la configuration de la règle de stationnement, l'état *valable* peut inclure du *temps de commodité*, du *temps payé* ainsi qu'un *délai de grâce*.

Infraction
Une session de stationnement passe en état *infraction* car :

- Le temps de validité prend fin. Celui-ci peut inclure une combinaison de *temps de commodité*, de *temps payant* et un *délai de grâce*, qui sont configurés pour la règle de stationnement.

Appliqué
Une session de stationnement passe en état *appliqué* car :

- L'infraction peut être mise à jour automatiquement par Genetec Patroller™ ou manuellement par l'opérateur Security Desk.

Terminé
Une session de stationnement passe en état *terminé* car :

- Le véhicule quitte la zone de stationnement. La session de stationnement est en état *terminé* quel que soit l'état actuel lorsque le véhicule quitte la zone de stationnement.
- L'inventaire de la zone de stationnement est actualisé.
- Le véhicule pénètre à nouveau dans la zone de stationnement. Cela peut indiquer que lors de la session de stationnement précédente du véhicule, sa plaque n'a pas été lue à la sortie de la zone de stationnement.
- Le véhicule a dépassé le *délai de session maximal* défini pour la zone de stationnement.

Sujet parent : Gestion des zones de stationnement

4.4.1.3 | Scénarios de stationnement courants avec AutoVu™ Free-Flow

La fonctionnalité AutoVu™ Free-Flow de Security Center permet de personnaliser le système afin de l'adapter à vos règles de stationnement.

Les exemples suivants montrent comment utiliser la AutoVu™ Free-Flow dans des situations courantes.

Stationnement transitoire

Dans le scénario *Stationnement transitoire*, lorsqu'un véhicule pénètre dans l'aire de stationnement, son propriétaire doit payer immédiatement.

À propos de ce scénario :

- Un bref laps de *temps de commodité* peut être ajouté pour donner au propriétaire du véhicule le temps de trouver une place et de s'acquitter du paiement.
- Si le propriétaire n'a pas réglé la durée de stationnement à l'issue des 15 minutes de commodité et des 15 minutes de grâce, la session de stationnement est indiquée comme étant En *infraction*.
- Si le propriétaire a payé mais que la durée de stationnement et de la période de grâce est dépassée, le véhicule est signalé en *infraction*.

Stationnement transitoire avec période de stationnement gratuit

Dans le scénario de stationnement transitoire, les véhicules peuvent stationner gratuitement et sans permis pendant les 2 premières heures. Si le propriétaire du véhicule compte stationner pendant plus de 2 heures, du temps de stationnement doit être acheté à l'avance.

À propos de ce scénario :

- Le temps de commodité est configuré pour 2 heures.
- Si le propriétaire n'a pas réglé la durée de stationnement à l'issue des 2 heures de commodité et des 15 minutes de grâce, la session de stationnement est indiquée comme étant en *infraction*.
- Si le propriétaire a payé mais que la durée de stationnement et de la période de grâce est dépassée, le véhicule est signalé en *infraction*.

Dépassement horaire

Dans un scénario de *dépassement horaire*, n'importe quel véhicule peut stationner pendant 2 heures maximum. Les propriétaires de véhicules ne peuvent pas acheter du temps payant.

À propos de ce scénario :

- Le temps de commodité est configuré pour deux heures.
- Si le propriétaire stationne son véhicule pendant une durée supérieure au temps de commodité de 2 heures et à la période de grâce de 15 minutes, la session de stationnement est indiquée comme étant En infraction.

Stationnement avec permis

Dans le scénario *stationnement dans le cadre d'un abonnement*, seuls les conducteurs munis de permis mensuels peuvent stationner dans la zone de stationnement. Un permis Security Center est utilisé pour accorder l'accès à la zone de stationnement aux véhicules.

À propos de ce scénario :

- Puisqu'il n'y a pas de temps payant, la règle de stationnement n'inclut que le minimum de 1 minute, et aucun délai de grâce n'est configuré.
- Avec cette configuration, vous pouvez suivre la durée de séjour de chaque véhicule dans la zone de stationnement.

Permis statique et stationnement transitoire

Dans ce scénario, un permis est utilisé pour accorder l'accès aux véhicules à la zone de stationnement, et lorsqu'un véhicule inconnu pénètre dans l'aire de stationnement, le conducteur doit immédiatement payer pour stationner.

À propos de ce scénario :

- Le stationnement transitoire est configuré comme dans l'exemple *Stationnement transitoire avec période de stationnement gratuit*.
- Pour les sessions de stationnement qui utilisent un permis statique Pay-by-Plate Sync, le permis statique est soumis au même temps de commodité et délai de grâce qui sont configurés pour la règle de stationnement permis transitoire, mais comme ils ne s'appliquent pas aux permis statiques, le permis ne passe pas en état d'infraction dès lors qu'il est valables.
- Si l'aire de stationnement est configurée pour utiliser les restrictions de permis, le système vérifie la validité des sessions de stationnement lorsque la restriction entre en vigueur.
- Si l'aire de stationnement est configurée pour utiliser des permis sans restrictions, le système valide les sessions de stationnement toutes les quinze minutes par défaut, conformément au réglage Délai d'expiration par défaut de la règle de stationnement.

Sujet parent : Gestion des zones de stationnement

4.4.1.4 | Événements de zone de stationnement

Durant la session de stationnement d'un véhicule, divers événements et sous-événements sont déclenchés en fonction des règles de stationnement appliquées à la zone de stationnement.

Événements
Les administrateurs peuvent utiliser les événements pour créer des associations événement-action pour la zone de stationnement. Vous pouvez par exemple configurer une association événement-action qui envoie un e-mail ou déclenche une alarme lorsqu'un événement *infraction détectée* est généré.

Sous-événements
Les sous-événements sont visibles dans le rapport Security Desk *Activités par zone de stationnement*. Vous pouvez filtrer le rapport pour afficher des sous-événements particuliers, mais vous ne pouvez pas les inclure dans une association événement-action.

Les événements et sous-événements suivants sont disponibles :

Événements	Sous-événements
Seuil de capacité atteint	Non applicable
Temps de commodité démarré	Non applicable
Délai de grâce démarré	• Expiration du temps de commodité • Temps payé non valide
Inventaire réinitialisé	Non applicable
Temps payé démarré	• Temps payé valide • Impossible de valider le temps payant
Session terminée	• Inventaire réinitialisé • Délai de session maximal dépassé • Véhicule inconnu sorti • Véhicule sorti • Véhicule rentré • Lecture modifiée • Règle supprimée
Session démarrée	• Véhicule inconnu sorti • Véhicule entré
Validation du temps payé	• Expiration du temps de commodité • Temps payé expiré • Lecture modifiée
Infraction détectée	• Expiration du temps de commodité • Délai de grâce expiré • Temps payé non valide • Correspondance de permis partagé
Infraction appliquée	Non applicable

Sujet parent : Gestion des zones de stationnement

4.4.2 | À propos des permis partagés dans AutoVu™ Free-Flow

Si votre système AutoVu™ Free-Flow est configuré pour autoriser les permis de stationnement partagés, un même permis de stationner peut être associé à plusieurs véhicules. Les permis partagés sont généralement utilisés lorsqu'un détenteur de permis a plusieurs véhicules ou dans le cadre du covoiturage.

Toutefois, les permis partagés ne s'appliquent toujours qu'à un seul véhicule à la fois. Par exemple, si les quatre membres du groupe de covoiturage qui partagent un permis décident d'utiliser leurs véhicules en même temps, seul le premier véhicule qui entre dans la zone de stationnement est autorisé à stationner en utilisant le permis. Les trois autres véhicules généreront une alerte de *permis partagé* s'ils entrent dans la zone de stationnement alors que le premier véhicule y stationne déjà.

Utilisation des Pay-by-Plate Sync

Tenez compte des points suivants lors de la configuration des permis partagés :

- Pour utiliser les permis partagés, les permis doivent provenir d'un fournisseur de permis de stationnement tiers via le module externe Pay-by-Plate Sync. Vous pouvez définir des permis statiques pour les véhicules dans Security Center, mais ces permis ne peuvent pas être partagés entre plusieurs véhicules.
- Pour utiliser cette fonctionnalité, le fournisseur de permis Pay-by-Plate Sync doit prendre en charge les permis partagés.
- Les véhicules partagent un permis dès lors qu'ils ont le même ID de permis. Veillez donc à ce que chaque permis ait un ID unique. Si deux permis ont le même ID de permis lorsque cette fonctionnalité est activée, ils risquent de générer des alertes de permis partagé.

Fonctionnement des permis partagés

1. Lorsqu'un véhicule pénètre dans une zone de stationnement, le système démarre une nouvelle *session de stationnement* pour le véhicule et valide le permis de stationner associé à la plaque d'immatriculation.
   REMARQUE : Si la caméra Sharp interprète mal certains caractères de la plaque d'immatriculation du véhicule, le système peut malgré tout associer la plaque du véhicule à la celle du permis de stationnement. En effet, le système utilise une technique de correspondance de RAPI qui ne nécessite que cinq caractères communs et quatre caractères contigus.
2. Le système compare l'*ID de permis* avec les véhicules déjà présents dans la zone de stationnement.
   - Si aucune autre plaque n'a le même ID de permis, le *temps payé* de la session de stationnement démarre.
   - Si une autre plaque a le même ID de permis, la session de stationnement passe en mode infraction.
   - Si la plaque n'est pas associée à un permis, le *temps de commodité* de la session de stationnement démarre.
   - Si le système ne parvient pas à communiquer avec le fournisseur de permis Pay-by-Plate Sync pour valider le permis, le temps de commodité de la session de stationnement démarre. Le système tente à nouveau de valider le permis à la fin de la session de stationnement du véhicule.

4.4.3 | Surveiller les zones de stationnement

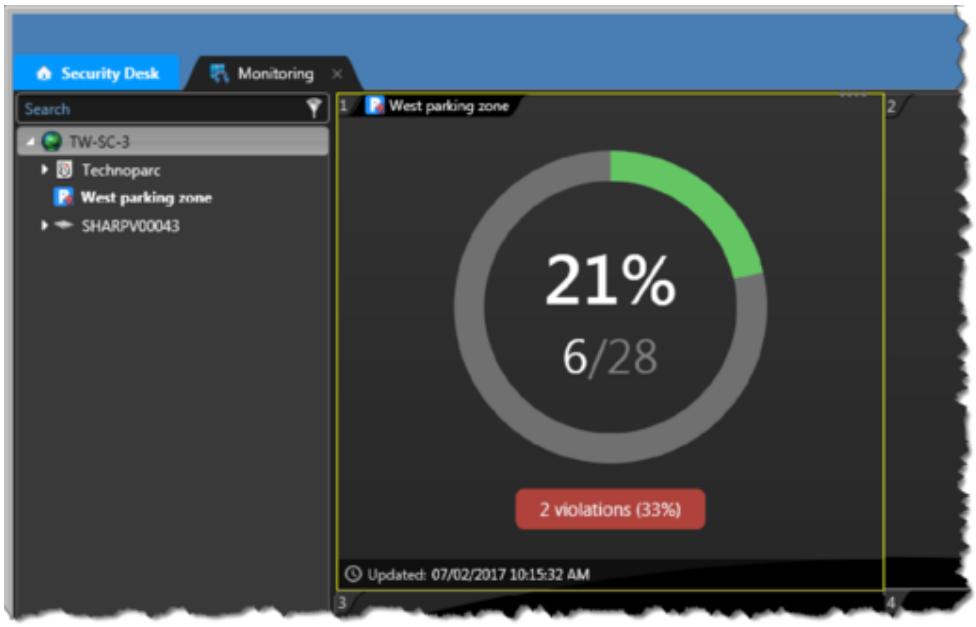
Vous pouvez surveiller les zones de stationnement depuis la tâche Surveillance. Les tuiles de la tâche Surveillance peuvent afficher l'occupation de la zone de stationnement et le nombre d'infractions. Si des caméras de surveillance supplémentaires sont associées à la zone de stationnement, les tuiles peuvent également afficher leurs flux vidéo.

Procédure

1. Ouvrez la tâche Surveillance.
2. Cliquez deux fois sur une zone de stationnement depuis la vue secteur, ou faites glisser une zone de stationnement dans une tuile de surveillance.

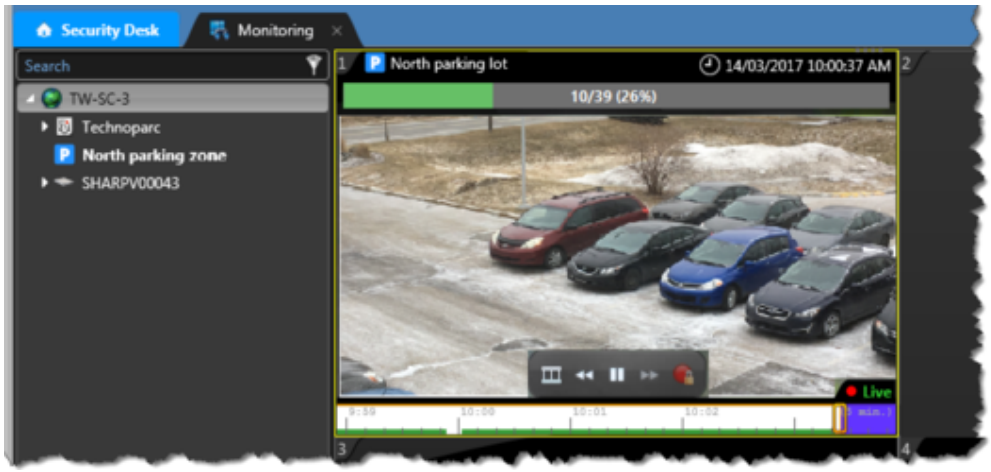
   Si des caméras de surveillance supplémentaires ne sont pas associées à la zone de stationnement, les informations suivantes sont affichées dans la tuile :

   - Nom de la zone de stationnement
   - Occupation actuelle de la zone de stationnement exprimée sous forme de proportion, de pourcentage et de graphique circulaire
     REMARQUE : Le graphique d'occupation passe du vert à l'orange lorsque la zone de stationnement atteint une occupation de 70 % Lorsque la zone de stationnement atteint une occupation de 90 %, le graphique passe de l'orange au rouge et se met à clignoter.
   - Infractions en cours, exprimées sous forme de nombre et de pourcentage des sessions de stationnement actives
   - Date et heure de mise à jour des informations de la tuile



Si des caméras de surveillance supplémentaires sont associées à la zone de stationnement, les informations suivantes sont affichées dans la tuile :

- Flux vidéo provenant des unités vidéo associées
  REMARQUE : Vous pouvez alterner les flux vidéo dans la tuile de surveillance à l'aide des commandes dans le widget de la tuile.
- Nom de la zone de stationnement
- L'occupation actuelle de la zone de stationnement exprimée sous forme de proportion, de pourcentage et de graphique à barres au-dessus du flux vidéo
- Infractions en cours, exprimées sous forme de nombre et de pourcentage des sessions de stationnement actives
  REMARQUE : Le graphique d'occupation passe du vert à l'orange lorsque la zone de stationnement atteint une occupation de 70 % Lorsque la zone de stationnement atteint une occupation de 90 %, le graphique passe de l'orange au rouge et se met à clignoter.
- Date et heure de mise à jour des informations de la tuile



3. (Facultatif) À un certain point (par exemple à la fermeture de l'aire de stationnement), vous pouvez partir du principe que toutes les sessions de stationnement ont pris fin et que tout véhicule encore présent dans la zone de stationnement ont été verbalisés ou doivent être embarqués à la fourrière. Vous pouvez utiliser l'action *Réinitialiser l'inventaire de la zone de stationnement*.

4.4.4 | AutoVu™ Free-Flow rapports

À l'aide des rapports AutoVu™ Free-Flow, vous pouvez identifier les véhicules qui sont en violation des règles de stationnement. Ces rapports peuvent être utilisés lors de l'émission manuelle de procès-verbaux, ou pour exporter les infractions vers un système tiers.

Vous pouvez générer des rapports de zones de stationnement à partir des tâches de rapport suivantes :

Sessions de stationnement
La tâche Sessions de stationnement fournit un inventaire des sessions de stationnement pour les véhicules actuellement présents dans la zone, ou qui ont déjà quitté la zone. Elle vous permet de créer un rapport d'inventaire de véhicules pour l'occupation actuelle de la zone de stationnement, ou pour une plage horaire dans le passé grâce à un filtre horaire.

Activités de zone de stationnement
La tâche Activité de zone de stationnement permet de suivre les événements associés à la zone survenus entre les heures de lecture de la plaque du véhicule à l'entrée et à la sortie de la zone de stationnement. Cette tâche sert aux enquêtes ou en cas de contestation d'un PV.

4.4.4.1 | Analyser les sessions de stationnement

Security Desk suit plusieurs états de session de stationnement associés à un véhicule en stationnement. Grâce à ces états, vous pouvez dresser la liste des véhicules actuellement en infraction, ou créer un rapport d'inventaire de véhicules pour l'occupation actuelle de la zone de stationnement, ou pour une plage horaire dans le passé grâce à un filtre horaire.

À savoir

- La tâche Sessions de stationnement peut également afficher des informations comme l'heure d'arrivée du véhicule, l'heure de son départ, la durée de son état en infraction, et si l'infraction a été verbalisée.
- Une zone de stationnement affichée dans une tuile de la tâche Surveillance présente l'occupation de la zone de stationnement ainsi que le nombre de véhicules en infraction.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Sessions de stationnement.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Sélection de plage horaire
   Il s'agit de la plage horaire pour le rapport. Le filtre de sélection horaire est utile à des fins de reporting a posteriori. Par exemple, vous pouvez générer un rapport qui inclut toutes les sessions de stationnement terminées au cours des dernières 24 heures. Vous pouvez ensuite exporter le rapport pour traitement par le système de paiement.

   Vous pouvez définir les filtres horaires suivants :

   Plage horaire
   Utilisez les filtres Au cours du dernier… et Plage spécifique pour afficher toutes les sessions de stationnement démarrées ou terminées durant la plage horaire concernée.

   Heure particulière
   Utilisez le filtre Maintenant pour générer une liste d'inventaire actuelle, ou le filtre Date spécifique pour générer une liste d'inventaire à un moment donné dans le passé.

   Zone de stationnement
   Sélectionnez une ou plusieurs zones de stationnement à inclure dans le rapport.

   Durée de séjour minimale
   Exclure du rapport les véhicules qui n'ont pas dépassé la durée de séjour maximale.

État de la session
Sélectionnez les états de véhicule suivants à inclure dans le rapport :

Terminé
La session de stationnement n’est plus active pour l’une des raisons suivantes :
- Le véhicule a quitté la zone de stationnement.
- L’inventaire de la zone de stationnement a été réinitialisé.
- La durée d’inventaire maximale a été atteinte.

REMARQUE : Pour déterminer si la session de stationnement est en infraction, reportez-vous à l’horodatage d'infraction dans le rapport Sessions de stationnement.

Appliqué
Le véhicule est dans la zone de stationnement, est en infraction et a été verbalisé.

Valable
Le véhicule est dans la zone de stationnement, et n'est pas en infraction.

Infraction
Le véhicule est dans la zone de stationnement, est en infraction et n'a pas été verbalisé.

Raison de l'état :
Sélectionnez une ou plusieurs raisons d'état à inclure dans le rapport.
CONSEIL : Dans les aires de stationnement AutoVu™ Free-Flow, étant donné qu'une infraction peut uniquement être verbalisée si le véhicule se trouve toujours sur l'aire de stationnement, il peut être utile d'exclure la raison d'état Véhicule sorti du rapport sur les sessions de stationnement.

Plaque d'immatriculation
Entrez un numéro de plaque Complet or Partiel pour créer un rapport sur un véhicule particulier.

3. Cliquez sur Générer le rapport.
   Les sessions de stationnement sont affichées dans le volet de rapport.
4. Pour afficher le résultat de la recherche dans une tuile, cliquez deux fois sur un événement, ou faites-le glisser sur une tuile du canevas.
5. Imprimez () le rapport ou exportez () le rapport dans un fichier CSV ou PDF.

Sujet parent : AutoVu™ Free-Flow rapports
Explorer

- À propos des filtres de plaques d'immatriculation

4.4.4.1.1 | Colonnes du volet de rapport pour la tâche Rapport de sessions de stationnement

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Horodatage terminé
Heure de fin de la session de stationnement du véhicule. Généralement, il s'agit de l’heure de sortie du véhicule de la zone de stationnement.

Horodatage du temps de commodité
Heure de début du temps de commodité de la session (période de stationnement gratuit avant que le stationnement payant entre en vigueur).

Durée du temps de commodité
Durée du temps de commodité du véhicule (période de stationnement gratuit avant l’application du stationnement payant entre en vigueur).

Durée appliquée
Durée durant laquelle le véhicule était signalé en état appliqué avant la fin de la session de stationnement.

Horodatage appliqué
Heure à laquelle l'infraction a été appliquée par un opérateur.

Image contextuelle d'entrée
L'image contextuelle capturée lorsque le véhicule est entré dans la zone de stationnement.

Image RAPI d'entrée
L'image de la plaque d’immatriculation capturée lorsque le véhicule est entré dans la zone de stationnement.

Numéro de plaque d'entrée
Le numéro de plaque d’immatriculation lu lorsque le véhicule est entré dans la zone de stationnement.

Image contextuelle de sortie
L'image contextuelle capturée lorsque le véhicule est sorti de la zone de stationnement.

Image RAPI de sortie
L'image de la plaque d’immatriculation capturée lorsque le véhicule est sorti de la zone de stationnement.

Numéro de plaque de sortie
Le numéro de plaque d’immatriculation lu lorsque le véhicule est sorti de la zone de stationnement.

Durée du délai de grâce
La durée du délai de grâce du véhicule. À l'issue du temps de commodité ou du temps payant du véhicule, le délai de grâce est le temps supplémentaire accordé avant que le véhicule soit signalé en infraction.

Horodatage du délai de grâce
L'heure à laquelle le délai de grâce du véhicule a démarré. À l'expiration de la durée de stationnement du véhicule, le délai supplémentaire accordé avant que le véhicule soit signalé en infraction.

Durée payée
Temps payant passé par le véhicule dans la zone de stationnement.

Horodatage payé
Heure de début du stationnement payant du véhicule.

Règle de stationnement
La règle de stationnement associée à la zone de stationnement durant une session de stationnement.

Zone de stationnement
La zone de stationnement associée à une session de stationnement.

État de la session
L’état de la session de stationnement du véhicule.

Indiquer la raison
Indique la raison de l’état de la session du véhicule.

Horodatage de début
Heure de début de la session de stationnement du véhicule. Généralement, il s'agit de l’heure d’entrée du véhicule dans la zone de stationnement.

Durée totale
Durée totale du séjour, de l'ouverture de la session du véhicule à sa clôture.

Durée de l'infraction
Durée durant laquelle le véhicule était signalé en infraction.

Horodatage d'infraction
Heure à laquelle le véhicule a été signalé en infraction.
Sujet parent : Analyser les sessions de stationnement

4.4.4.2 | Analyser les activités de zone de stationnement

La tâche Activité de zone de stationnement permet de suivre les événements associés à la zone survenus entre les heures de lecture de la plaque du véhicule à l'entrée et à la sortie de la zone de stationnement.

À savoir

Utilisez la tâche Activités de zone de stationnement pour mener un audit des activités liées à une plaque d'immatriculation ou pour analyser les situations lorsque le propriétaire conteste l'infraction.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Activités de zone de stationnement.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

   Zone de stationnement
   Sélectionnez une ou plusieurs zones de stationnement à inclure dans le rapport.

   Plaque d'immatriculation
   Entrez un numéro de plaque Complet or Partiel pour créer un rapport sur un véhicule particulier.

   Événements
   Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

   Pour en savoir plus sur les événements et sous-événements associés à AutoVu™ Free-Flow, voir Événements de zone de stationnement.
3. Cliquez sur Générer le rapport.
   Les sessions de stationnement sont affichées dans le volet de rapport.
4. Pour afficher le résultat de la recherche dans une tuile, cliquez deux fois sur un événement, ou faites-le glisser sur une tuile du canevas.
5. Imprimez () le rapport ou exportez () le rapport dans un fichier CSV ou PDF.

Sujet parent : AutoVu™ Free-Flow rapports
Explorer

- À propos des filtres de plaques d'immatriculation

4.4.4.2.1 | Colonnes du volet de rapport pour la tâche Rapport d'activité par zone de stationnement

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Image contextuelle
Image couleur grand-angle du véhicule capturée par la caméra contextuelle.

Événement
Nom de l'événement.

Heure de l'événement
Date et heure de l'événement.

Expire
Heure à laquelle l'activité actuelle expire, comme le temps de commodité ou le stationnement payant.

Zone de stationnement
La zone de stationnement associée à une session de stationnement.

Image de plaque
L'image de la plaque d'immatriculation capturée par la caméra de RAPI.

Lecture de plaque
La lecture de plaque d'immatriculation générée par l'unité .Sharp
Sujet parent : Analyser les activités de zone de stationnement

4.4.5 | Modifier une lecture de plaque d’une zone de stationnement

Si une caméra Sharp qui surveille une zone de stationnement AutoVu™ Free-Flow ne parvient pas a interpréter ou capturer une plaque, vous pouvez modifier la lecture afin que les lectures d’entrée et de sortie concordent.

À savoir

- Ces informations concernent les systèmes qui utilisent AutoVu™ Free-Flow. Si vous n’utilisez pas cette fonctionnalité, voir Modifier les lectures de plaques d'immatriculation.
- Si la caméra ne parvient pas à capturer la plaque, aucune image de RAPI n'est associée à la lecture et le numéro de plaque *NOPLATE* est associé à la lecture. Tous les objets qui traversent le champ de la caméra sont ainsi capturés pour analyse, ce qui permet d'améliorer la fiabilité de l'occupation de la zone de stationnement. Cela s'avère particulièrement utile pour les installations qui présentent un risque élevé de mauvaise lecture de plaques, comme lorsque les conditions météo sont difficiles (boue, neige, et ainsi de suite).

- Vous ne pouvez pas modifier une lecture de plaque si la lecture est protégée ou si elle a généré une alerte.
- Lorsque la lecture de plaque est modifiée, le score de confiance qui lui est associée passe à 100 %.
-
- Si le système génère trop de lectures NOPLATE (un véhicule génère plusieurs lectures NOPLATE ou un véhicule est détecté mais n'apparaît pas dans l'image) ou trop peu de lectures NOPLATE (les véhicules qui passent devant la caméra ne sont pas détectés), cela peut indiquer un problème d’installation (obstruction partielle, mauvais éclairage, mauvais positionnement), ou de configuration. Par ailleurs, vous devez peut-être réétalonner la fonction boucle virtuelle de la caméra Sharp. Pour plus d’informations, voir Étalonner la boucle virtuelle Sharp.
- Vous pouvez modifier les lectures de plaques à partir des tâches suivantes :
  - Tâche Lectures
  - surveillance, tâche
  - Tâche Sessions de stationnement (n'inclut pas les lectures NOPLATE)
  - Tâche Activités de zone de stationnement (n'inclut pas les lectures NOPLATE)
  - Tâche Surveillance d'alarmes (si des alarmes sont configurées pour les lectures NOPLATE ou celles dont le score de confiance est faible)

Effets de la modification de lectures de plaques sur les sessions de stationnement et l’occupation des zone de stationnement

- **Modifier une lecture de plaque d’entrée :**
  - Si vous modifiez une lecture de plaque d’entrée d'un véhicule associé à une session de stationnement active, la session est mise à jour avec le bon numéro de plaque. L’occupation de la zone de stationnement n’est alors pas affectée. Si le système utilise des permis de stationnement Pay-by-Plate Sync, l’état *temps payé*, *infraction* ou *délai de grâce* de la session de stationnement est réévalué avec Pay-by-Plate Sync.
  - Si la plaque d'un véhicule est mal interprétée à l’entrée d'une zone de stationnement, une session de stationnement est créée et l'occupation de la zone de stationnement augmente. Dans ce cas, vous devez modifier la lecture de plaque d’entrée avant que le véhicule ne quitte la zone de stationnement ou que la session de stationnement atteigne le *délai de session maximal*, car à ce stade, la session est fermée et la modification de la plaque n’actualise plus la session de stationnement. Toutefois, cette situation n’affecte pas l’occupation. Lorsque la plaque du véhicule est lue correctement à la sortie de la zone de stationnement, le véhicule est signalé comme étant un *véhicule inconnu* et l’occupation diminue.
  - Si la lecture d’entrée génère une lecture NOPLATE, le véhicule est pris en compte pour l’occupation de la zone de stationnement, mais une session de stationnement n’est pas créée. La modification de la lecture crée une session de stationnement pour le véhicule, et le permis est évalué en fonction de l’heure d’entrée du véhicule.
- **Modifier une lecture de plaque de sortie :**
  - Si vous modifiez une lecture de plaque de sortie qui correspond au numéro de plaque d'une session de stationnement active, le système ferme la session et l'occupation de la zone de stationnement est actualisée en conséquence.
  - Lorsqu'une lecture NOPLATE est générée à la sortie d'une zone de stationnement, l'occupation de la zone diminue. Si cet événement est modifié pour correspondre au numéro d’une session active dans la zone de stationnement, la session de stationnement est fermée, puisque la lecture NOPLATE correspond bien au même véhicule.

Procédure

Pour modifier une lecture de plaque :

1. Dans la tuile qui contient la lecture de plaque, cliquez sur Modifier ( ).
   REMARQUE : Si vous essayez une lecture de plaque dans un rapport *Lectures*, vous devez d'abord cliquer deux fois sur la lecture pour l'afficher dans une tuile.
2. Dans la fenêtre Modifier la lecture, modifiez manuellement les informations de Plaque et d'État.
3. Cliquez sur Enregistrer.

Pour analyser et modifier une lecture *NOPLATE* :

1. Sur la page d'accueil, ouvrez la tâche Lectures.
2. Dans la liste Unités de RAPI - Patroller, sélectionnez la caméra à analyser.
3. Sélectionnez le filtre Plaque d'immatriculation et entrez `NOPLATE`.
4. Cliquez sur Générer le rapport.
   Les lectures sans numéro de plaque associé sont répertoriées dans le volet de rapport.
5. Si la plaque du véhicule est visible dans l'image de contexte, vous pouvez modifier la lecture de plaque en vue d'inclure le bon numéro de plaque.
   a. Double-cliquez sur la lecture pour l'afficher dans une mosaïque.
   b. Dans la tuile qui contient la lecture de plaque, cliquez sur Modifier ( ).
   c. Dans la fenêtre Modifier la lecture, modifiez manuellement les informations de Plaque.
   d. Cliquez sur Enregistrer.

Résultats

La colonne Modifié des rapports *Lectures* indique si les lectures de plaques ont été modifiées.

4.4.6 | Appliquer les infractions de zone de stationnement

Lorsque des véhicules sont en infraction dans une zone de stationnement, les étapes requises pour appliquer l’infraction dépendent de qui émet les PV (un intervenant sur site ou un système tiers).

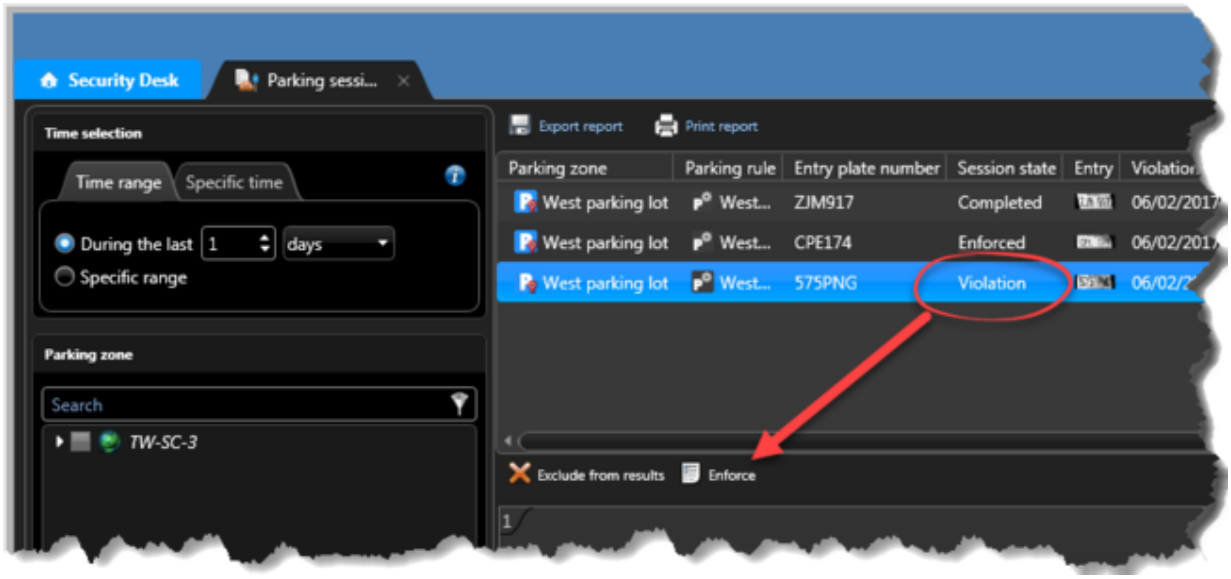
À savoir

- Cette procédure est uniquement requise si le véhicule de patrouille ne peut pas envoyer d'alertes en direct. En général, Security Desk peut surveiller les événements de RAPI depuis les véhicules de patrouille et peut automatiquement mettre à jour l'état des sessions de stationnement.
- Si les PV sont émis manuellement pendant que les véhicules sont encore présents dans la zone de stationnement, chaque fois qu'un PV est émis pour un véhicule en *infraction* (comme indiqué dans le rapport *Sessions de stationnement*) et que la session de stationnement du véhicule est marquée comme étant *appliquée*, le nombre d'infractions de la zone de stationnement est réduit en conséquence.
- Si votre système AutoVu™ Free-Flow utilise un système de verbalisation tiers pour appliquer les infractions dans la zone de stationnement, il n'est pas nécessaire de marquer les sessions comme étant *appliquées* dans le système.

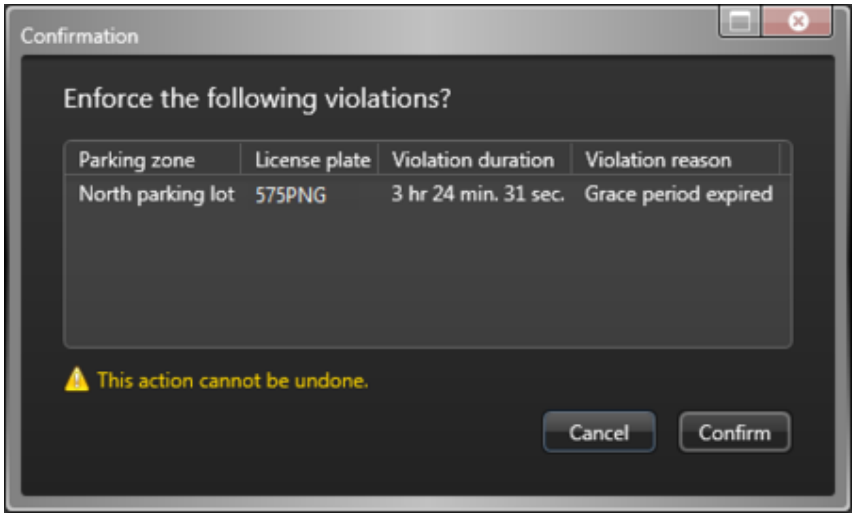
Procédure

Pour appliquer une infraction de session de stationnement lorsque les PV sont émis sur site :

1. Sur la page d'accueil, ouvrez la tâche Sessions de stationnement.
2. Créez un rapport de sessions de stationnement qui contient les véhicules en infraction.
3. Verbalisez les véhicules en infraction.
4. Dans le résultat du rapport Session de stationnement, cliquez sur chaque véhicule ayant été verbalisé, puis cliquez sur Appliquer.



5. Dans la fenêtre Confirmation, cliquez sur Confirmer.



Pour appliquer une infraction de session de stationnement lorsque les PV sont émis par un système tiers :

1. Sur la page d'accueil, ouvrez la tâche Sessions de stationnement.
2. Créez un rapport de sessions de stationnement qui contient les véhicules en infraction.

3. Exportez ( ) le rapport au format Excel, CSV ou PDF, et envoyez le fichier au système de verbalisation tiers.

4.4.7 | Réinitialiser l'inventaire d'une zone de stationnement

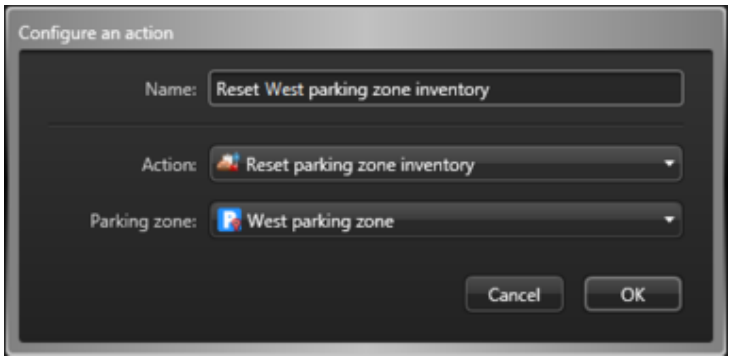
À un certain point (par exemple à la fermeture de l'aire de stationnement), vous pouvez partir du principe que toutes les sessions de stationnement ont pris fin et que tout véhicule encore présent dans la zone de stationnement a été verbalisé ou doit être embarqué à la fourrière. Vous pouvez réinitialiser l'occupation d'une zone de stationnement à l'aide d'une action éclair.

À savoir

La réinitialisation de l'inventaire met fin à toutes les sessions de stationnement et supprime toutes les infractions signalées. Pour ce faire, vous devez créer une action éclair pour la zone de stationnement en utilisant l'action *Réinitialiser l'inventaire de zone de stationnement*.

Procédure

1. Dans la zone de notification de Security Desk, cliquez sur Actions éclair ( ).
2. Dans la boîte de dialogue Actions éclair, cliquez sur Modifier.
3. Cliquez sur Ajouter ( ).
4. Entrez un Nom qui sera affiché dans la liste des actions éclair. Par exemple, *Réinitialiser l'inventaire de la zone de stationnement ouest*.
5. Dans la liste déroulante Action, sélectionnez Réinitialiser l'inventaire de zone de stationnement.
6. Dans la liste déroulante Zone de stationnement, sélectionnez la zone de stationnement que vous souhaitez réinitialiser.



7. Cliquez sur OK.
   L'action éclair est créée et la boîte de dialogue Actions éclair est fermée.
8. Pour ouvrir à nouveau la boîte de dialogue Actions éclair, cliquez sur Actions éclair ( ) dans la zone de notification.
9. (Facultatif) Cliquez sur Modifier. Si vous avez créé plusieurs actions éclair, cliquez sur ou pour déplacer l'action éclair sélectionnée dans la liste. Vous modifiez ainsi la touche de fonction affectée à l'action.
10. Cliquez sur Terminé.
    L'action éclair que vous avez créée est présentée avec sa touche de fonctions associée (F1, F2, et ainsi de suite).
11. Déclenchez l'action éclair pour réinitialiser l'inventaire de la zone de stationnement de l'une des manières suivantes :
    - Sélectionnez l'action éclair, puis cliquez sur Exécuter.
    - Appuyez sur Ctrl+F*n*.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

4.4.8 | Fermeture manuelle des sessions de stationnement dans Security Center

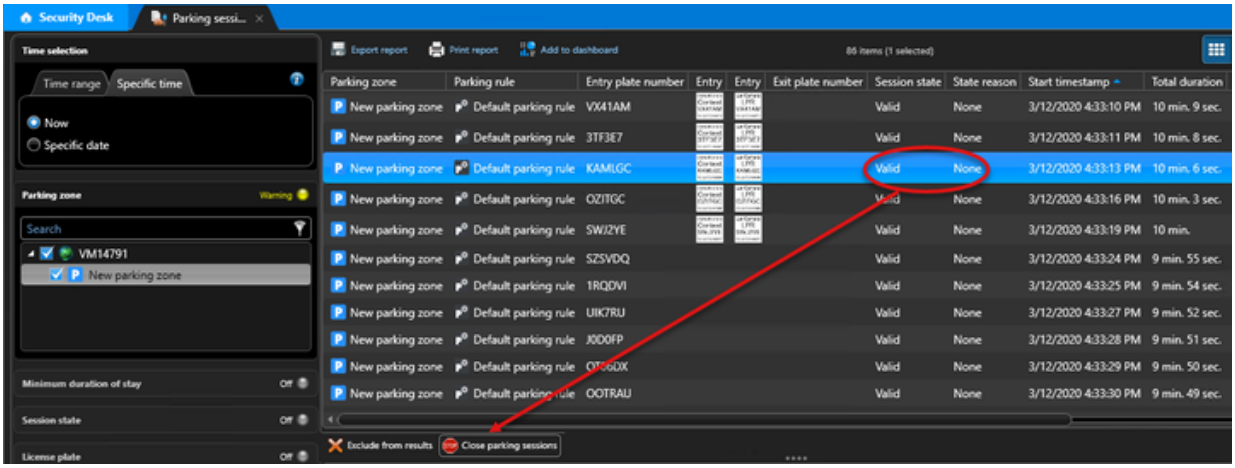
Pour les sites avec une longue durée de session maximale, plusieurs entrées non valides créées par des lectures erronées ou dupliquées dans le rapport des sessions de stationnement peuvent entraver la gestion de la zone de stationnement. Vous pouvez fermer manuellement ces entrées pour les supprimer du rapport.

Avant de commencer

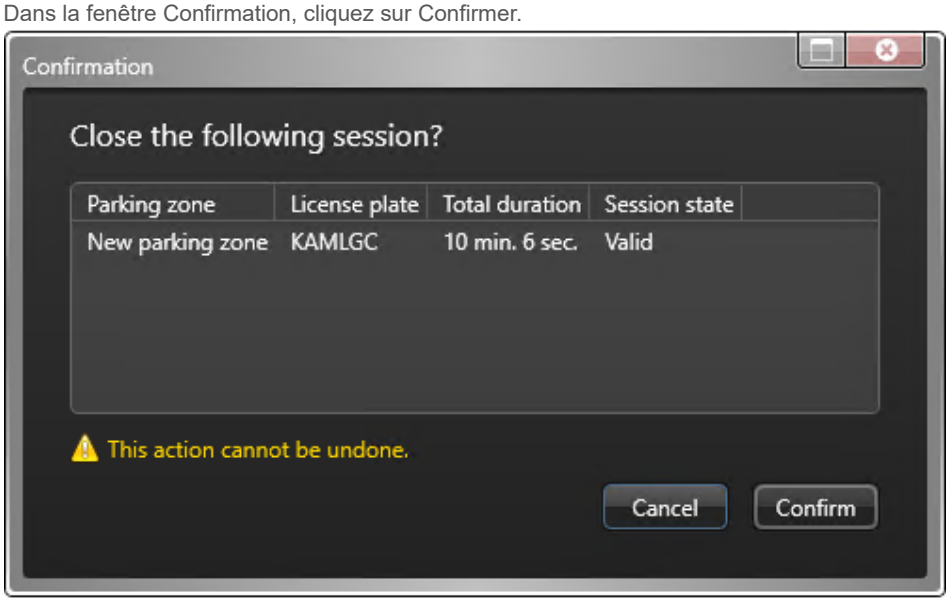
Pour fermer manuellement les sessions de stationnement, vous devez disposer du privilège *Fermer les sessions de stationnement* activé.

Procédure

1. Sur la page d'accueil Security Desk, ouvrez la tâche Sessions de stationnement.
2. Définissez les filtres de recherche suivants pour votre rapport :
   a. Dans la zone Sélection de l'heure, cliquez sur Heure spécifique, puis sélectionnez Maintenant.
   b. Cliquez sur le filtre État de la session et sélectionnez Valide.
   c. Cliquez sur le filtre Raison de l'état et sélectionnez Aucun.
3. Cliquez sur Générer le rapport.
   Les sessions de stationnement sont affichées dans le volet de rapport.
4. Dans les résultats du rapport des sessions de stationnement, sélectionnez chaque résultat sans *Numéro de plaque de sortie* et cliquez sur Fermer les sessions de stationnement.



5. Dans la fenêtre Confirmation, cliquez sur Confirmer.



6. Dans la boîte de dialogue Informations, cliquez sur Fermer.
7. Cliquez sur Générer le rapport pour afficher les résultats mis à jour.

Résultats

Les sessions terminées par cette procédure sont marquées comme **Terminé** dans la colonne *État de la session* et **Aucune** dans la colonne *Raison de l'état*.

4.4.9 | Modifier l'occupation d'une zone de stationnement

Si l'occupation indiquée pour une zone de stationnement ne correspond pas au nombre de voitures présentes dans la zone, vous pouvez corriger l'occupation au sein du système à l'aide d'une action manuelle, d'une action éclair ou d'un déclencheur d'événement.

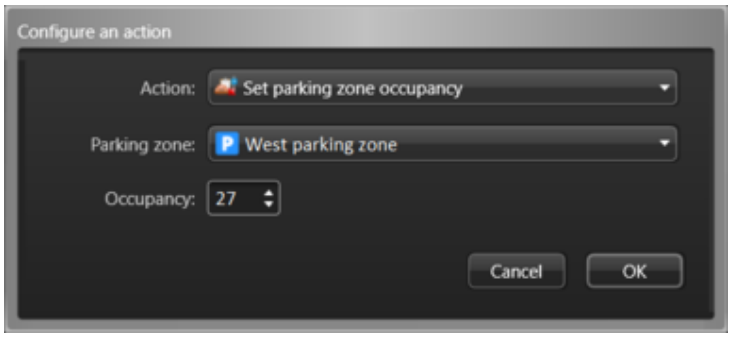
À savoir

- Une incohérence entre l'occupation signalée pour une zone de stationnement et le nombre de voitures présentes dans la zone peut survenir en cas de mauvaises lectures de plaques d'immatriculation à l'entrée ou la sortie de la zone de stationnement, entraînant des lectures erronées ou NO PLATE, selon la manière dont le système est configuré. Dans de tels cas, l'occupation augmente ou diminue en conséquence, mais des sessions de stationnement ne sont pas ouvertes ou fermées.
- Lorsque vous modifiez l'occupation d'une zone de stationnement, le système ne ferme pas de sessions de stationnement actives. En effet, si la plaque d'un véhicule n'est pas lue à la sortie de la zone de stationnement et génère une lecture NO PLATE, le système ne peut pas savoir quelle session de stationnement fermer, puisque la lecture NO PLATE ne peut pas être associée à une session. Cela diffère de ce qui se produit lorsque vous réinitialisez l'inventaire d'une zone de stationnement, auquel cas toutes les sessions de stationnement sont automatiquement fermées et les véhicules restants doivent être verbalisés ou envoyés à la fourrière.

L'exemple suivant utilise une action manuelle pour modifier l'occupation. Vous pouvez également configurer une action éclair ou un déclencheur d'événement.

Procédure

1. Dans la zone de notification de Security Desk, cliquez sur Actions éclair ( ).
2. Dans la boîte de dialogue Actions éclair, cliquez sur Action manuelle.
3. Dans la boîte de dialogue Configurer une action, sélectionnez Définir la capacité de la zone de stationnement dans la liste des actions.
4. Dans la liste déroulante Zone de stationnement, sélectionnez la zone de stationnement que vous souhaitez modifier.
5. Entrez l'Occupation de la zone de stationnement, soit le nombre de véhicules actuellement présents dans la zone.



6. Cliquez sur OK.
   L'action manuelle est déclenchée et l'occupation de la zone de stationnement est définie.

Explorer

- Déclenchement d'actions ponctuelles dans Security Center
- Déclenchement d'actions éclair dans Security Center

4.5 | Genetec Patroller™ dans Security Desk

4.5.1 | À propos de Genetec Patroller™

Une entité *Genetec Patroller™* représente le logiciel exécuté sur l'ordinateur embarqué dans le véhicule de patrouille. Le logiciel compare les lectures de plaques d'immatriculation effectuées par les caméras de RAPI fixées au véhicule à des listes de véhicules recherchés et de véhicules ayant des permis. Il recueille également des données pour l'application d'horaires de stationnement.

L'interface de *Genetec Patroller™* alerte l'utilisateur en cas de plaques répondant aux règles définies afin qu'une action immédiate puisse être entreprise.

Selon la version de votre solution AutoVu™, Genetec Patroller™ peut servir à effectuer les tâches suivantes :

- Comparer les lectures de plaques d'immatriculation effectuées par une *Caméra de RAPI* à des véhicules d'intérêt (listes de véhicules recherchés) et de véhicules ayant des permis (listes de permis).
- Vous notifier en cas d'alerte de liste de véhicules recherchés, de permis ou de dépassement horaire, afin que vous puissiez immédiatement réagir.
- Recueillir des données pour l'application d'horaires de stationnement.
- Recueillir des lectures de plaques afin de créer et gérer l'inventaire de plaques d'immatriculation d'un parc de stationnement.

4.5.2 | Relire l'itinéraire d'un véhicule de patrouille

Vous pouvez relire sur une carte l'itinéraire emprunté par un véhicule qui exécute Genetec Patroller™ un jour donné avec le rapport *Suivi de véhicule de patrouille*.

Avant de commencer

Pour afficher le résultat de la recherche sur le canevas, vous devez savoir comment surveiller les événements de RAPI dans Security Desk en mode Carte.

À savoir

Le rapport Suivi de véhicule de patrouille fournit une représentation plus visuelle que les rapports *Alertes* ou *Lectures*. Par exemple, pour afficher l'itinéraire précis d'un Genetec Patroller™ durant sa ronde, sélectionnez le Genetec Patroller™ concerné, puis la date de sa ronde.

L'itinéraire du Genetec Patroller™ est affiché sous forme d'animation en mode Carte, et une représentation graphique de l'itinéraire du Genetec Patroller™ est affichée dans la frise chronologique. Sur la carte, les 15 événements de RAPI survenus

avant et après l'emplacement actuel de Genetec Patroller™ sont affichés. Vous pouvez parcourir l'itinéraire depuis la frise chronologique, et analyser les alertes et lectures capturées par le Genetec Patroller™.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Suivi de véhicule de patrouille.
2. Dans la liste déroulante Patroller, sélectionnez une unité Genetec Patroller™.
3. Cliquez sur Date, puis sélectionnez la journée qui vous intéresse.
4. Cliquez sur Actualiser.

   Security Center reçoit les données Genetec Patroller™ de la *base de données*. L'itinéraire est représenté sur la carte et dans la frise chronologique.

5. Utilisez les commandes de la frise chronologique pour parcourir l'itinéraire du Genetec Patroller™ et repérer les événements de RAPI.
6. Pour afficher les propriétés d'un événement de RAPI, cliquez deux fois sur un élément sur la carte.

Lorsque vous avez terminé

Imprimer une alerte en tant que preuve d'infraction si nécessaire.

Explorer

- Présentation de la tâche Pistage Genetec Patroller™
- Commandes de suivi de la frise chronologique Genetec Patroller™

4.5.3 | Suivre la position actuelle d'une unité Genetec Patroller™

Utilisez le rapport Genetec Patroller™ pour suivre la position actuelle des véhicules Suivi de véhicule de patrouille sur une carte.

À savoir

Genetec Patroller™ nécessite une connexion active à Security Center pour cette fonctionnalité.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Suivi de véhicule de patrouille.
2. Cliquez sur Reprendre le suivi.
   Tout véhicule Genetec Patroller™ actif est indiqué sur la carte, où vous pouvez suivre sa position.

4.5.4 | Analyser l'utilisation de l'application Genetec Patroller™ au quotidien

Utilisez le rapport Utilisation quotidienne par l'entité Patroller pour consulter la durée *totale* quotidienne (en minutes) et le *pourcentage* de la journée pendant lesquels une application Genetec Patroller™ est ouverte, arrêtée ou éteinte. Vous pouvez également voir la durée moyenne d'ouverture, d'arrêt et d'extinction d'un Genetec Patroller™ sur une période donnée.

À savoir

Ce rapport n'est utilisé que pour les installations Genetec Patroller™ mobiles. Utilisez ces chiffres pour évaluer l'efficacité de vos véhicules Patroller. Par exemple, pour voir les statistiques d'une unité Genetec Patroller™ pendant sa dernière ronde, recherchez cette unité Genetec Patroller™, puis définissez une plage horaire.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Utilisation quotidienne par l'entité Patroller.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

Champs personnalisés
Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Patroller
Limitez la recherche aux unités Genetec Patroller™ (dont toutes les unités de RAPI associées).

Plage horaire
La plage horaire pour le rapport.

3. Cliquez sur Générer le rapport.
   Les résultats sont affichés dans le volet de rapport.
4. Consultez la section Statistiques pour analyser les statistiques d'utilisation suivantes concernant le Genetec Patroller™ sélectionné :

Durée de fonctionnement (moyenne)
Moyenne de durée de fonctionnement pendant la plage horaire sélectionnée.

Arrêt le plus long (min.) (moyenne)
Moyenne en minutes de l'arrêt le plus long durant la plage horaire sélectionnée.

Arrêt le plus long % (moyenne)
Moyenne en pourcentage de l'arrêt le plus long durant la plage horaire sélectionnée.

Total des arrêts (min.) (moyenne)
Moyenne en minutes du total des arrêts durant la plage horaire sélectionnée.

Total des arrêts % (moyenne)
Moyenne en pourcentage du total des arrêts durant la plage horaire sélectionnée.

Instances (moyenne)
Moyenne des instances d'ouverture de l'application Genetec Patroller™ durant la plage horaire sélectionnée.

Extinction la plus longue (min.) (moyenne)
Moyenne en minutes de l'extinction la plus longue durant la plage horaire sélectionnée.

Extinction la plus longue % (moyenne)
Moyenne en pourcentage de l'extinction la plus longue durant la plage horaire sélectionnée.

Total des extinctions (moyenne)
Moyenne en minutes du total des extinctions durant la plage horaire sélectionnée.

Total des extinctions % (moyenne)
Moyenne en pourcentage du total des extinctions durant la plage horaire sélectionnée.

4.5.4.1 | Colonnes du volet de rapport pour la tâche Utilisation quotidienne par l'entité Patroller

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Date
Jour de la tournée du véhicule de patrouille

Instances
Nombre total d'ouvertures de l'application Genetec Patroller™ durant la journée.

Extinction la plus longue (%)
Pourcentage de la fermeture la plus longue rapporté au nombre de minutes de la journée.

Extinction la plus longue (min.)
Fermeture la plus longue, en minutes, de l'application Genetec Patroller™ durant la journée.

Arrêt le plus long (%)
Pourcentage de l'arrêt le plus long du véhicule rapporté à la durée de fonctionnement.

Extinction la plus longue (min.)
Fermeture la plus longue, en minutes, de l'application Genetec Patroller™ durant la journée.

Heures de fonctionnement
Nombre de minutes dans la journée durant lesquelles l'application Genetec Patroller™ est lancée.

Total des extinctions (%)
Pourcentage du total des fermetures rapporté au nombre de minutes de la journée.

Total des extinctions (min.)
Nombre de minutes dans la journée durant lesquelles l'application Genetec Patroller™ est fermée. La valeur de total de l'extinction plus la valeur d'heure de fonctionnement est égale à 1440 minutes.

Total des arrêts (%)
Pourcentage du total des arrêts du véhicule rapporté à la durée de fonctionnement.

Total des arrêts (min.)
Nombre total de minutes d'arrêt du véhicule pendant les heures de fonctionnement.
Sujet parent : Analyser l'utilisation de l'application Genetec Patroller™ au quotidien

4.5.5 | Analyser les connexions/déconnexions d'une unité Patroller

Vous pouvez afficher l'historique des connexions et déconnexions d'unités Patroller sur une période donnée avec le rapport *Connexions par Genetec Patroller™*.

À savoir

Ce rapport vous permet de savoir quels véhicules de patrouille sont sur le terrain. Ce rapport n'est utilisé que pour les installations Genetec Patroller™ mobiles.

REMARQUE : Lorsque vous utilisez ce rapport avec un hôte de Security Center Federation™, la colonne Utilisateur reste vide pour les entités Genetec Patroller™ fédérées, car les entités utilisateur ne sont pas fédérées.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Connexions par Genetec Patroller™.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Patroller
   Limitez la recherche aux unités Genetec Patroller™ (dont toutes les unités de RAPI associées).

   Plage horaire
   La plage horaire pour le rapport.

Utilisateurs
Sélectionnez le nom d'utilisateur Patroller, ou les groupes d'utilisateurs parents du Patroller.

3. Cliquez sur Générer le rapport.
   Le résultat pour le Genetec Patroller™ sélectionné est affiché dans le volet de rapport.

4.5.5.1 | Colonnes du volet de rapport pour la tâche Connexions par Patroller

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Date
Jour de la tournée du véhicule de patrouille

Connexion/déconnexion
Date et heure de la connexion/déconnexion.

Utilisateur
Le nom de l'utilisateur Genetec Patroller™. Non disponible pour un hôte de fédération Security Center Federation™ pour les entités Genetec Patroller™ fédérées.

Sujet parent : Analyser les connexions/déconnexions d'une unité Patroller

4.5.6 | Analyser le nombre de véhicules dans une zone de stationnement

Vous pouvez consulter le nombre de véhicules garés dans une *zone de stationnement*, ainsi que le taux d'occupation, avec la tâche *Occupation par zone*.

À savoir

Vous pouvez également utiliser le rapport *Occupation par zone* pour rechercher les *dépassements horaires* et les *restrictions de permis* survenus dans une zone. Par exemple, sur un campus ou un aéroport, vous pouvez afficher le taux d'occupation d'un parc de stationnement à certaines heures de la journée. Si le parc est toujours saturé à certaines heures, le rapport peut vous aider à décider d'augmenter le nombre de places de stationnement.

Le taux d'occupation dans une zone de stationnement est calculé différemment selon que Genetec Patroller™ est utilisé pour l'application du *Stationnement universitaire* ou du *Stationnement urbain*.

Genetec Patroller™ configuration	Pourcentage d'occupation
Stationnement universitaire	Calculé pour la zone particulière sélectionnée dans Genetec Patroller™, qui correspond à une seule aire de stationnement définie dans une règle de dépassement horaire ou une restriction de permis.
Stationnement urbain	• Si une règle de dépassement horaire est sélectionnée :calculé pour toutes les aires de stationnement définies au sein de la règle. • Si aucune règle de dépassement horaire n'est sélectionnée :le taux d'occupation ne peut pas être calculé, car les permis ne sont pas associés à une aire de stationnement. Dans ce cas de figure, les colonnes *Places* et *Taux d'occupation* affichent 0.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Occupation par zone.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Règles d'alerte
   Sélectionnez les règles d'alerte à inclure dans le rapport.

   Dépassement horaire et restriction de permis
   Des aires de stationnement sont configurées pour les deux règles, et le nombre de places peut être défini pour chaque aire. Cela permet d'estimer le taux d'occupation lorsque ces règles sont sélectionnées dans Genetec Patroller™.

   Patroller
   Limitez la recherche aux unités Genetec Patroller™ (dont toutes les unités de RAPI associées).

   Plage horaire
   La plage horaire pour le rapport.

3. Cliquez sur Générer le rapport.
   Les résultats sont affichés dans le volet de rapport.
4. Consultez le nombre total de véhicules dans l'ensemble des zones de stationnement pris en compte dans la section Statistiques.

4.5.6.1 | Colonnes du volet de rapport pour la tâche Occupation par zone

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Du/au
Date et heure des véhicules analysés au sein de la zone.

Aire
Zone de stationnement où une règle de stationnement donnée est en vigueur.

Taux d'occupation
Pourcentage de places occupées au sein de la zone de stationnement.

Places
Nombre de places dans l'aire de stationnement.

Du/au
Date et heure des véhicules analysés au sein de la zone.

Véhicules
Nombre de véhicules ayant été lus dans la zone.

Zone
Nom de la règle de dépassement horaire ou de la restriction de permis.

Sujet parent : Analyser le nombre de véhicules dans une zone de stationnement

4.6 | Inventaire mobile des plaques d'immatriculation dans Security Desk

4.6.1 | Fonctionnement de l'IMPI AutoVu™

Inventaire mobile de plaque d'immatriculation (MLPI) est une installation logicielle Genetec Patroller™ conçue pour recueillir des numéros d'immatriculation et d'autres informations associées pour créer et actualiser un inventaire de plaques d'immatriculation dans des parcs de stationnement de taille importante.

Le processus IMPI AutoVu™ se déroule de la manière suivante :

- Un *parc de stationnement* est créé dans Config Tool. Le parc de stationnement est décrit sous forme de secteurs et de rangées.
- Genetec Patroller™ Les itinéraires sont associés à des secteurs et des rangées du parc de stationnement. Le secteur et la rangée d'une *lecture de plaque* définissent l'emplacement du véhicule dans le parc de stationnement.
- Un appareil *IMPI AutoVu* Genetec Patroller™ (ou autre appareil portable homologué par Genetec Inc.) recueille les lectures de plaques dans le parc de stationnement, puis décharge les données vers Security Center.
  REMARQUE : Les lectures d'appareils mobiles sont importées dans la base de données du Gestionnaire RAPI à l'aide du module d'importation XML. Un seul *Patroller fantôme*, appelé importation XML, apparaît alors dans la liste. Quel que soit le nombre d'appareils mobiles, toutes leurs lectures sont importées dans le même Patroller fantôme.
- Security Center interroge le dossier *Offload* à la recherche de nouvelles données IMPI.
- L'icône Inventaire ( ) dans Security Desk signale la présence de nouvelles données pouvant être ajoutées à un inventaire.

4.6.2 | Supprimer des lectures de plaques d'un fichier de déchargement

Avant d'ajouter les données d'un fichier de déchargement à un inventaire avec la tâche Gestion d'inventaire, vous pouvez supprimer des lectures de plaques d'immatriculation du fichier.

À savoir

Vous ne pouvez supprimer que les *lectures non rapprochées* d'un fichier de déchargement. Vous ne pouvez pas comparer des inventaires, puisque les lectures non rapprochées n'ont pas été ajoutées à un inventaire.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Rapport d'inventaire.
2. Dans la section Inventaire de l'onglet Filtres, cliquez sur Lecture non rapprochée.
3. Spécifiez d'autres filtres pour affiner votre recherche.
   Dans la section Plaque d'immatriculation, entrez les numéros de plaque des véhicules qui ont été emportés à la fourrière depuis la capture des lectures par Genetec Patroller™.
4. Pour n'afficher que les lectures non rapprochées et supprimées manuellement, sélectionnez l'option N'afficher que les lectures supprimées manuellement dans la section Recherche avancée.
5. Cliquez sur Générer le rapport.
6. Dans le volet de rapport, sélectionnez le véhicule que vous souhaitez supprimer.
7. En bas du volet de rapport, cliquez sur Supprimer ( ).
   La lecture de plaque est alors marquée comme *Véhicule supprimé manuellement* dans la section Statistiques.

Lorsque vous avez terminé

Une fois que vous avez supprimé les lectures de plaques non rapprochées du fichier de déchargement, créez l'inventaire pour le déchargement.

Explorer

- Analyser les lectures de plaques effectuées

4.6.3 | Supprimer des données d'un fichier de déchargement

Vous pouvez supprimer les données d'un fichier de déchargement de la base de données du Gestionnaire RAPI.

À savoir

Les unités Patroller et les appareils mobiles déchargent leurs données vers un *Gestionnaire RAPI*. Ces déchargements sont dupliqués et stockés dans la *base de données* du Gestionnaire RAPI. Dans la tâche *Gestion d'inventaire*, les lectures sont associées à un parc de stationnement, et sont signalées comme n'étant pas encore intégrées à un inventaire.

Si vous supprimez un déchargement de la liste des *Déchargements*, les lectures ne sont plus liées à un parc de stationnement. Toutefois, les données sont conservées dans la base de données Security Center sous forme de lectures de plaques ordinaires, et peuvent toujours être recherchées avec la tâche *Lectures*.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Gestion d'inventaire.
2. Dans la section Déchargements, sélectionnez une unité Genetec Patroller™ dans la liste.
   En cas d'utilisation d'un appareil mobile, sélectionnez le Genetec Patroller™ appelé XML Import.
3. Dans la section Déchargements, cliquez sur  .

4.6.4 | Créer un inventaire de parc de stationnement

Vous pouvez ajouter des lectures de plaques IMPI d'un fichier de déchargement à un inventaire de parc de stationnement, puis rapprocher les lectures avec la tâche Gestion d'inventaire.

Avant de commencer

Avant d'ajouter les données d'un fichier de déchargement à un inventaire, vous pouvez supprimer des lectures de plaques d'immatriculation non rapprochées du fichier de déchargement avec la tâche *Rapport d'inventaire*.

À savoir

Gardez les points suivants à l'esprit à propos de la création d'inventaires :

- Lorsque de nouvelles lectures de plaques IMPI sont disponibles dans la base de données, une notification apparaît sur l'icône Inventaire () dans la zone de notification. L'alerte d'inventaire est mise à jour toutes les 10 minutes. Vous pouvez également actualiser l'alerte en faisant un clic droit sur l'icône Inventaire, puis en cliquant sur Actualiser.
- Vous ne pouvez créer qu'un inventaire de parc de stationnement à la fois.
- Lorsqu'un Genetec Patroller™ décharge plusieurs fois avant la création d'un inventaire, elles sont toutes regroupées dans une même entrée.
- Vous ne pouvez pas définir l'heure de début d'un inventaire. Lorsque vous créez un inventaire pour la première fois, l'heure de début n'est pas définie. Lors de la création d'inventaire suivante, l'heure de début correspond à l'heure de fin de l'inventaire précédent.
- Le rapprochement consiste à confirmer une lecture et l'ajouter à un inventaire. En cas de conflit lors du rapprochement d'une lecture et d'un inventaire (comme deux véhicules avec le même numéro de plaque, mais provenant d'États différents), vous devrez parfois confirmer la lecture.
- Un inventaire partiel sert à effectuer une vérification ponctuelle de l'inventaire, et les lectures ne sont pas rapprochées avec l'inventaire précédent. Cette option est utile lorsque le Genetec Patroller™ n'est pas en mesure de faire une ronde complète d'un parc de stationnement. Par exemple, en cas de forte chute de neige, si le Genetec Patroller™ ne peut patrouiller que la moitié du parking, l'autre moitié n'ayant pas encore été déneigée, il peut créer un inventaire partiel afin d'enregistrer les lectures malgré tout.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Gestion d'inventaire.

REMARQUE : Le volet Déchargements ne contient des informations que si un déchargement a été dupliqué et stocké dans la base de données du Gestionnaire RAPI.
Le volet Déchargements contient les informations suivantes :

Genetec Patroller™
Nom de l'unité Genetec Patroller™ ayant déchargé le fichier.
REMARQUE : Un seul *Patroller fantôme*, appelé XML import, est affiché pour les lectures capturées par un appareil portable, car elles ont été importées dans la base de données du Gestionnaire RAPI par le module d'importation XML.

Première lecture
Horodatage de la première lecture du déchargement.

Dernière lecture
Horodatage de la dernière lecture du déchargement.

Nombre de lectures
Nombre de lectures dans le fichier de déchargement.

2. Dans la liste déroulante Parc de stationnement, sélectionnez le parc auquel vous souhaitez ajouter l'inventaire.
3. Cliquez sur Créer un inventaire.
4. Dans la boîte de dialogue Créer un inventaire, saisissez le nom de l'inventaire et l'heure de fin.
5. Pour créer un inventaire partiel, sélectionnez Partiel.
6. Cliquez sur Créer.
   Les lectures de plaques sont rapprochées, et les données de lecture de plaques sont ajoutées à l'inventaire du parc de stationnement.
7. En cas de conflit lors du rapprochement de l'inventaire (comme une plaque qui apparaît à deux endroits), la boîte de dialogue Confirmation de plaque apparaît, et vous devez vérifier que la plaque d'immatriculation dans l'image contextuelle correspond à l'image de la plaque et à la lecture par *ROC* de la manière suivante :
   CONSEIL : Comparez l'image de RAPI à la lecture ROC, sachant que la plaque dans l'image contextuelle risque d'être difficile à voir.

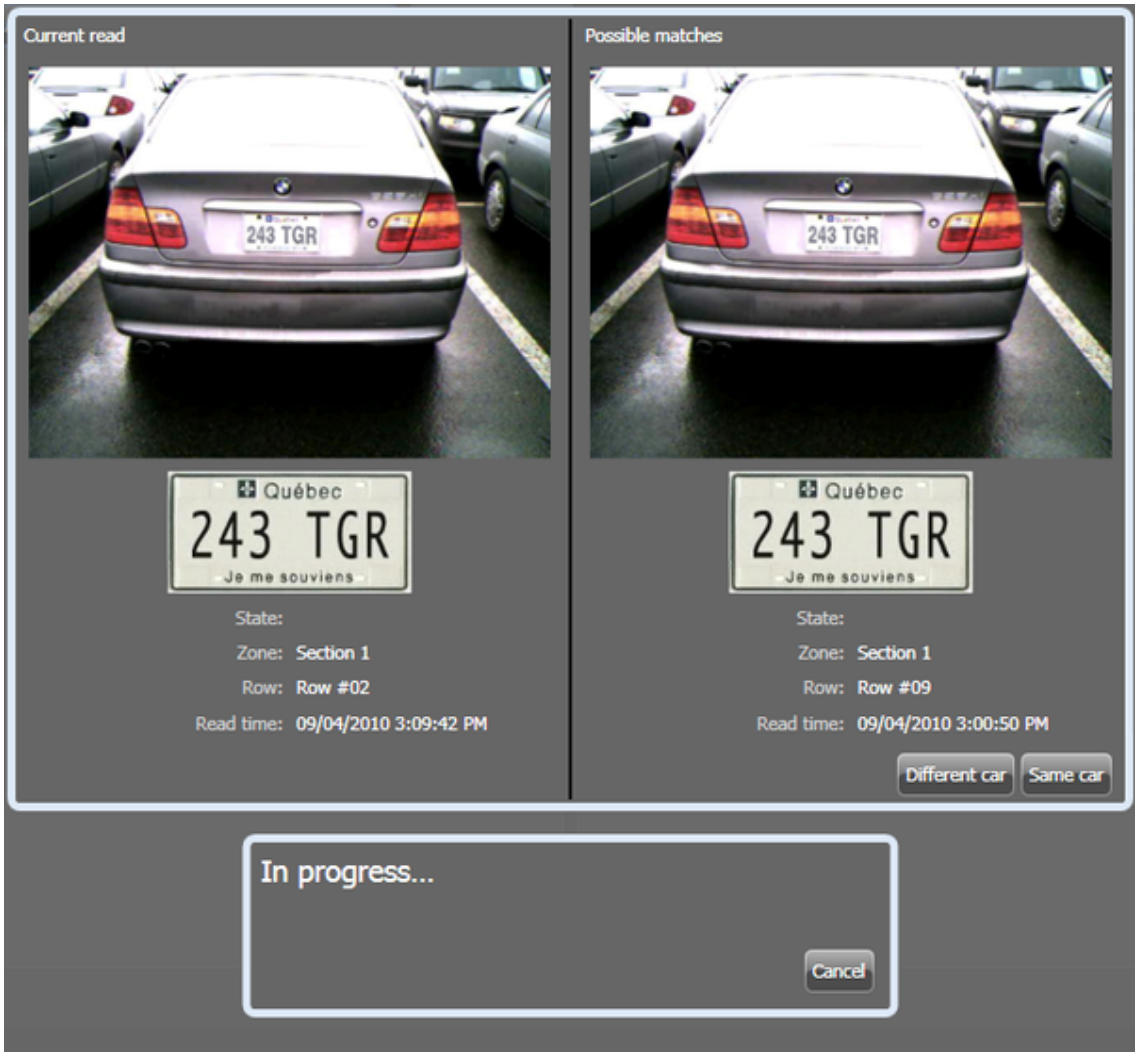
   a. En cas d'erreur dans la lecture ROC, tapez le numéro de plaque correcte dans le champ Lecture ROC.
      REMARQUE : La lecture de plaque est alors marquée comme *Modifiée* dans la tâche Rapport d'inventaire.
   b. Si la lecture par ROC est juste, mais que la plaque n'est pas du même État, entrez le nom de l'État dans le champ État.

Vous pouvez entrer l'abréviation ou le nom complet de l'état.

c. Cliquez sur Confirmer.

Les données du fichier de déchargement sont ajoutées à l'inventaire du parc de stationnement.

8. Si un conflit est détecté lors du processus d'inventaire (comme une plaque présente à deux endroits), une boîte de dialogue apparaît et présente la lecture de plaque dans l'inventaire actuel du parc de stationnement (Lecture actuelle), et une correspondance potentielle (Correspondances possibles) dans les données en cours de rapprochement avec l'inventaire.



Sélectionnez l'une des options suivantes :

Voiture différente

Sélectionnez cette option si les numéros de plaques sont identiques, mais que l'état et le véhicule diffèrent du véhicule dans l'inventaire actuel. Le véhicule affiché dans Correspondances possibles est ajouté en tant que nouveau véhicule dans l'inventaire du parc de stationnement.

Même voiture

Sélectionnez cette option si les numéros de plaque, l'état et le véhicule sont identiques, mais que le véhicule a changé d'emplacement depuis l'inventaire précédent.

Annuler

Annule le rapprochement. Si les conflits ne sont pas rapprochés, une nouvelle lecture de plaque est créée qui indique qu'un nouveau véhicule est arrivé (au lieu de l'inscrire pour une journée supplémentaire), et qu'il s'agit d'une Voiture différente.

Un message vous avertit que l'opération a été annulée. Cliquez sur OK.

L'inventaire annulé est affiché en rouge dans Inventaires existants, mais les données de déchargement restent dans le dossier Déchargement jusqu'à leur ajout ou suppression du parc de stationnement.

9. Vous devez supprimer tout inventaire annulé pour pouvoir créer un nouvel inventaire :

a. Dans le volet Inventaires existants, sélectionnez l'inventaire annulé (en rouge).

b. Dans le volet Inventaires existants, cliquez sur Supprimer ( ).

Explorer

- Fonctionnement de l'IMPI AutoVu™
- Supprimer des lectures de plaques d'un fichier de déchargement
- Présentation de la tâche Gestion d'inventaire

4.6.5 | Afficher et comparer les inventaires de parcs de stationnement

Utilisez la tâche *Rapport d'inventaire* pour afficher un inventaire ou comparer deux inventaires d'un *parc de stationnement*.

À savoir

Dans le *Rapport d'inventaire*, vous pouvez afficher et comparer les inventaires de véhicules de périodes différentes pour obtenir les informations suivantes :

- Inventaire actuel et précédent de véhicules en stationnement
- Véhicules ajoutés (arrivées) ou supprimés (départs)
- Emplacement des véhicules (secteur et rangée)
- Véhicules supprimés manuellement (fourrière)
- Durée de séjour des véhicules
- Véhicules dont les données ont été modifiées et rapprochées manuellement dans l'inventaire.

Pour éviter les problèmes de performances, les images de plaque ne sont pas affichées dans les rapports qui comptent plus de mille lignes.
BONNE PRATIQUE : Pour un résultat optimal, comparez le dernier inventaire à l'inventaire précédent. Par exemple, si le parc de stationnement est parcouru quotidiennement, comparez l'inventaire d'aujourd'hui avec celui d'hier.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Rapport d'inventaire.
2. Dans la liste déroulante Parc de stationnement de la section Source, sélectionnez le nom du parc de stationnement.
3. Dans la section Inventaire, sélectionnez l'inventaire que vous souhaitez consulter ou comparer.

   Dernier non partiel
   Le dernier inventaire.

   Spécifique
   Un inventaire particulier.

4. Pour comparer l'inventaire avec un autre inventaire du parc de stationnement, sélectionnez le deuxième inventaire dans la liste déroulante Autre inventaire.
5. Dans la liste déroulante Ajouté, sélectionnez l'état de véhicule que vous souhaitez comparer.
   Vous pouvez rechercher les véhicules *Inchangés*, *Ajoutés*, *Supprimés* ou *Déplacés*. Vous pouvez sélectionner plusieurs actions en même temps.
6. Spécifiez d'autres filtres pour affiner votre recherche. Choisissez un ou plusieurs des filtres suivants :

   Recherche avancée
   Les images de RAPI ne sont pas affichées par défaut dans le Rapport d'inventaire. Pour afficher les images, cliquez sur Obtenir des images. Pour éviter les problèmes de performances, les images de plaque ne sont pas affichées dans les rapports qui comptent plus de mille lignes.

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Plaque d'immatriculation
Entrez un numéro de plaque complet ou partiel. Pour saisir plusieurs plaques d'immatriculation, voir Filtrer un rapport avec plusieurs plaques d'immatriculation

Emplacement
Spécifiez l'emplacement dans le parc de stationnement qui vous intéresse. Vous pouvez sélectionner le parc entier ou spécifier les secteurs et rangées de votre choix.

7. Pour inclure les images de RAPI dans le rapport, sélectionnez l'option Obtenir des images dans la section Recherche avancée.
8. Cliquez sur Générer le rapport.

Les résultats sont affichés dans le volet de rapport.Les différences suivantes entre les deux inventaires sont affichées :

Véhicules ajoutés
Nombre total de véhicules ajoutés au parc de stationnement.

Véhicules supprimés
Nombre total de véhicules supprimés du parc de stationnement.

Véhicules déplacés
Nombre total de véhicules déplacés dans le parc de stationnement.

Véhicules supprimés manuellement
Nombre total de véhicules supprimés manuellement du parc de stationnement.

Nombre d'entrées manuelles
Nombre total de lectures non rapprochées supprimées du fichier de déchargement.

Explorer

- À propos des filtres de plaques d'immatriculation

4.6.5.1 | Colonnes du volet de rapport pour la tâche Rapport d'inventaire

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Action
Le changement d'état du véhicule :*ajouté*, *supprimé*, *déplacé* ou *inchangé*.

Arrivée
Heure de première lecture du véhicule. Permet de calculer le laps de temps écoulé lorsqu'un véhicule est lu une seconde fois (comme le jour suivant).

Image contextuelle
Image couleur grand-angle du véhicule capturée par la caméra contextuelle.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Modifié
Le numéro et l'état de la plaque ont été modifiés par un utilisateur dans Security Desk.

Temps passé
La différence entre l'heure d'arrivée et l'horodatage de l'événement.

Heure de l'événement
Date et heure de l'événement.

Capture manuelle
Affiche le numéro de plaque saisi manuellement par l'utilisateur de Genetec Patroller™.

Supprimé manuellement
Véhicule supprimé manuellement du parc de stationnement (fourrière).

Parking
Nom du parc de stationnement.

Entité Patroller
Entité patroller ayant lu la plaque. En cas d'utilisation d'un appareil mobile, la valeur Importation XML est affichée.

Image de plaque
L'image de la plaque d'immatriculation capturée par la caméra de RAPI.

Origine de la plaque
L'État émetteur de la plaque d'immatriculation.

Lecture de plaque
La lecture de plaque d'immatriculation générée par l'unité .Sharp

Ligne
Nom de la rangée.

Secteur
Nom du secteur.
Sujet parent : Afficher et comparer les inventaires de parcs de stationnement

5 | Alarmes et événements critiques dans Security Desk

5.1 | Alarmes Security Center dans Security Desk

5.1.1 | Affichage des alarmes sur le canevas de Security Desk

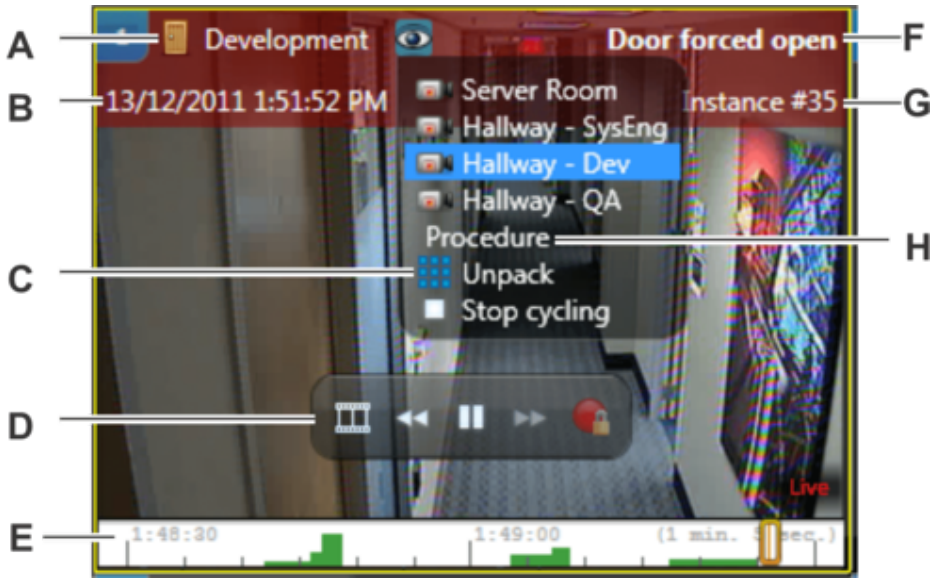
Vous pouvez afficher les alarmes actives et passées sur le canevas avec les tâches *Surveillance d'alarmes*, *Rapport d'alarmes* et *Surveillance*.

Dans les tâches *Surveillance d'alarmes* et *Surveillance*, les alarmes actives sont automatiquement affichées sur le canevas pour que vous puissiez examiner les informations et la vidéo associée. Dans la tâche *Rapport d'alarmes*, toutes les vidéos associées à l'alarme sont affichées en mode lecture. La lecture commence à l'heure à laquelle l'alarme a été déclenchée.

Les alarmes sont souvent des *entités composites*, car elles sont associées à plusieurs caméras, portes ou secteurs, et peuvent inclure des images fixes. Pour afficher toutes les entités en même temps, vous devez développer la tuile qui contient l'alarme.

REMARQUE : Si l'alarme déclenchée est liée à une entité (par exemple à une porte) qui est associée à des caméras, ces dernières sont affichées en premier sur le canevas, avant l'entité liée elle-même.

La figure suivante montre une alarme active dans une tuile du canevas dans la tâche Surveillance d'alarmes.



A	Source de l'alarme
B	Horodatage de l'alarme
C	Permet d'afficher toutes les entités en même temps
D	Commandes vidéo intégrées à la tuile
E	Frise chronologique
F	Nom de l'alarme
G	Numéro d'instance de l'alarme
H	Affiche la procédure d'alarme (si définie)

Explorer

- Commandes vidéo intégrées à la tuile
- Développer le contenu d'une tuile
- Activer la surveillance d'alarmes dans la tâche Surveillance

5.1.2 | Activer la surveillance d'alarmes dans la tâche Surveillance

Pour éviter de basculer entre les taches lorsqu'une alarme se déclenche, vous pouvez activer la surveillance d'alarmes dans la tâche Surveillance.

Avant de commencer

Créez vos alarmes.

À savoir

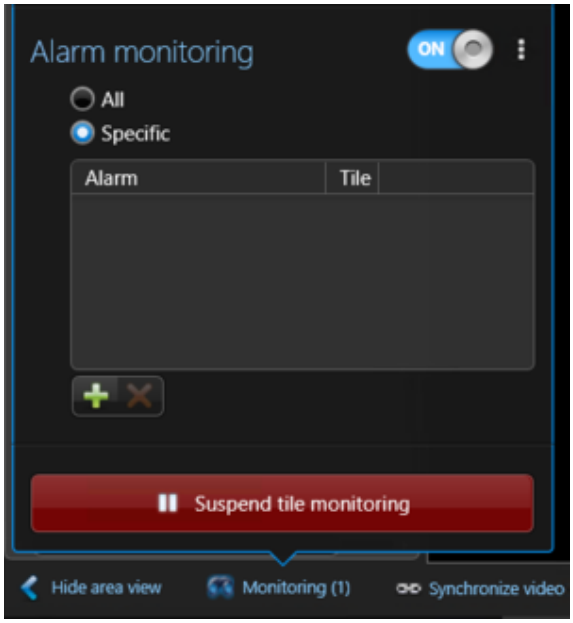
Lorsque les tuiles sont armées pour surveiller les alarmes dans la tâche Surveillance, les alarmes ne sont plus affichées en tant que fenêtres contextuelles dans la zone de notification. Vous pouvez configurer les alarmes en tant que fenêtres contextuelles.

Procédure

1. Ouvrez la tâche Surveillance.

2. En bas de la tâche Surveillance, cliquez sur Surveillance ( ).
3. ACTIVEZ l'option Surveillance d'alarmes.

   Vous pouvez armer ou désarmer les tuiles pour la surveillance d'alarmes en cliquant sur . Lorsqu'une tuile est armée pour surveiller les alarmes, l'arrière-plan de l'ID de la tuile est rouge.
4. Indiquez si vous souhaitez surveiller Toutes les alarmes ou les alarmes Spécifiques.
5. Si vous avez sélectionné Spécifique, procédez de la manière suivante :
   a. Cliquez sur et sélectionnez les alarmes que vous souhaitez surveiller.
      CONSEIL : Pour sélectionner plusieurs alarmes, appuyez sur les touches Ctrl ou Maj tout en sélectionnant les alarmes.
   b. Cliquez sur Ajouter.



Résultats

L'interrupteur Événements - Alarmes apparaît dans le coin supérieur droit de la tâche Surveillance pour que vous puissiez facilement basculer entre la surveillance des événements et des alarmes. Si vous ne voyez pas l'interrupteur Événements/Alarmes, faites glisser le canevas vers le bas pour révéler la liste d'alarmes en haut de la fenêtre.

Vous pouvez suspendre la surveillance à tout moment en cliquant sur Suspendre la surveillance de tuiles.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l’icône Sous-titres (CC) pour activer les sous-titres dans l’une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s’affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Filtrer et regrouper les alarmes dans Security Center

5.1.3 | Acquittement des alarmes

Vous pouvez afficher et acquitter les alarmes dans les tâches Surveillance d'alarmes et Surveillance.

Avant de commencer

Pour afficher et acquitter les alarmes depuis la tâche Surveillance, vous devez activer la surveillance d'alarmes pour la tâche Surveillance concernée.

À savoir

Vous ne recevez l'alarme dans Security Desk que si vous êtes un destinataire de l'alarme. Les alarmes sont affichées sur le canevas en ordre de priorité.
REMARQUE : Vous ne serez pas forcément obligé d'acquitter toutes les alarmes déclenchées. En effet, certaines alarmes sont configurées pour un acquittement automatique au bout d'un certain délai.

Procédure

1. Dans la zone de notification, double-cliquez sur l'icône Alarmes ( ).
   Toutes les nouvelles alarmes sont automatiquement affichées dans la liste d'alarmes, et la vidéo associée est affichée sur le *canevas*.
2. Pour filtrer la liste d'alarmes, cliquez sur l'icône ( ) et sélectionnez un filtre :

   Afficher tout
   Affiche toutes les alarmes (pas de filtre).

   Afficher actives
   Affiche les alarmes actives.

   Afficher les analyses en cours
   Affiche les alarmes en cours d'analyse.

Afficher les acquittements requis
Affiche les alarmes dont les conditions sources sont effacées, mais qui doivent toujours être acquittées.

Afficher les acquittés
Affiche les alarmes acquittées.

3. Pour afficher la vidéo d'une alarme, cliquez deux fois sur l'alarme ou faites-la glisser sur le canevas. Les détails de l'alarme sont incrustés dans un cadre de couleur sur la vidéo.
4. Dans le widget, cliquez sur l'un des éléments suivants :

Acquitter (par défaut) ( )
Acquitter l'alarme. L'alarme n'est plus active, et elle supprimée du canevas et de la liste d'alarmes.
REMARQUE : Certaines alarmes vous obligent à signaler un incident lors de l'acquittement.

Acquitter (secondaire) ( )
Placer l'alarme en état acquittée *secondaire*. La fonction de l'acquittement secondaire est définie par votre société. Par exemple, en cas de fausse alerte, vous pouvez acquitter l'alarme de cette façon. Cet état peut également servir à filtrer les recherches d'alarme.

Analyser ( )
Analysez l'alarme. Cette action permet aux autres utilisateurs du système de savoir que vous avez vu l'alarme sans l'acquitter, ce qui fait que l'alarme n'est pas supprimée de la liste des alarmes actives.

Acquitter de force ( )
Forcez l'acquittement de l'alarme. Cette option est utile pour effacer les alarmes en cours d'analyse et dont la condition d'acquittement n'est pas encore effacée.

Acquitter toutes les alarmes de force ( )
Forcez l'acquittement de toutes les alarmes actives. Cette option est utile pour effacer les alarmes en cours d'analyse et dont la condition d'acquittement n'est pas encore effacée.

Mettre l'alarme en rappel ( )
Placer l'alarme en veille pendant 30 secondes. Lorsqu'elle est en veille, l'alarme est temporairement retirée du canevas. Vous pouvez modifier le délai de veille par défaut dans la boîte de dialogue Options.

Afficher la procédure d'alarme ( )
Affichez la procédure particulière de l'alarme (lorsqu'une procédure est définie par l'administrateur). Les procédures d'alarme sont faciles à créer et peuvent prendre la forme de pages HTML ou d'applications Web développées par les utilisateurs.

Transférer une alarme ( )
Transférez l'alarme à un autre utilisateur. Avant de transférer une alarme, vous devez sélectionner un utilisateur, et vous pouvez ajouter un message.

Modifier le contexte ( )
Ajouter ou modifier l'annotation d'alarme.

REMARQUE : Toutes les actions relatives aux alarmes sont consignées dans l'historique d'activité.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Affichage des alarmes sur le canevas de Security Desk
- Présentation de la tâche Surveillance d'alarmes dansSecurity Center

5.1.3.1 | Informations d'alarmes disponibles durant la surveillance d'alarmes dans Security Center

Lorsqu'une alarme est déclenchée, vous pouvez consulter les informations suivantes dans les tâches Surveillance d'alarmes et Surveillance.

ID
Numéro d'instance de l'alarme. Identifie de manière unique chaque instance d'alarme.

Alarme
Nom de l'entité alarme.

Priorité
Priorité de l'alarme. Par défaut, la priorité de toutes les alarmes importées depuis Omnicast™ est réglée sur 1. Vous pouvez modifier leur priorité plus tard dans Config Tool.

Couleur de l'alarme
Couleur de l'alarme.

Source
Entité source ayant déclenché l'alarme, lorsque l'alarme est déclenchée par le mécanisme événement-action. Elle affiche un nom d'utilisateur lorsque l'alarme est déclenchée manuellement.

Événement déclencheur
Événement ayant déclenché l'alarme (en cas d'utilisation du mécanisme événement-action). Action manuelle est indiqué lorsque l'alarme a été déclenchée manuellement par un utilisateur.

Heure de déclenchement
Heure de déclenchement de l'alarme dans Security Center.

État
État actuel de l'alarme.

Actif
L'alarme n'est pas encore acquittée. La sélection d'une alarme active affiche les boutons d'acquittement dans le volet de rapport.

Acquittée (par défaut)
L'alarme a été acquittée avec le mode par défaut.

Acquittée (secondaire)
L'alarme a été acquittée avec le mode secondaire.

Acquittée (de force)
L'acquittement de l'alarme a été forcé par un administrateur.

Analyse en cours
Alarme en cours d'analyse, ce qui signifie qu'elle a été vue, mais pas forcément traitée.

Acquittement requis
Une alarme avec une condition d'acquittement effacée et prête à être acquittée.

Contexte
Annotation d'alarme.

Acquittée par
Utilisateur ayant acquitté l'alarme. Lorsque l'alarme est automatiquement acquittée par le système, la mention **Service** est indiquée.

Acquittée le
Heure d'acquittement de l'alarme.

Analysé par
L'utilisateur qui a placé l'alarme en état Analyse en cours.

Analysé le
Plage horaire durant laquelle l'alarme a été placée en état Analyse en cours.

Période d'occurrence
Période durant laquelle l'événement est survenu.

Type d'entité source
Le type d'entité source ayant déclenché l'alarme, lorsque l'alarme est déclenchée par le mécanisme événement/action. Il affiche un utilisateur lorsque l'alarme est déclenchée manuellement.

Heure source
Heure de l'événement déclenché par l'alarme. Heure source et Déclenchement ne diffèrent que lorsque l'événement est survenu alors que l'unité de contrôle d'accès était hors ligne.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.
Sujet parent : Acquittement des alarmes

5.1.4 | Filtrer et regrouper les alarmes dans Security Center

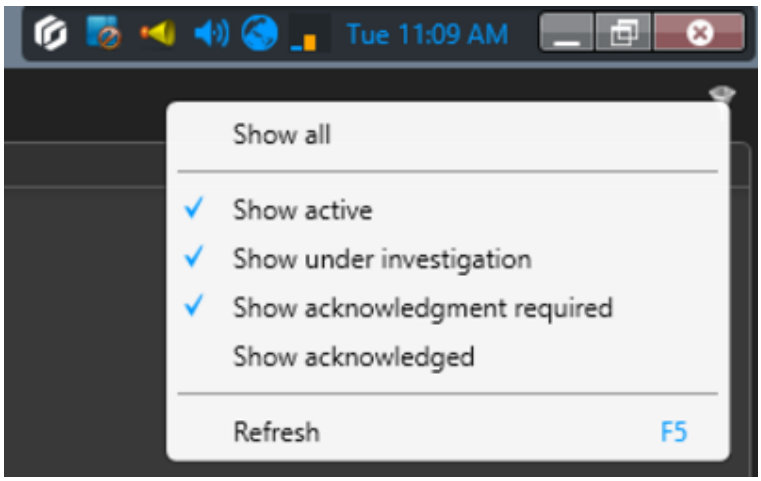
Vous pouvez filtrer et regrouper les alarmes pour contrôler leur affichage dans les tâches Surveillance d'alarmes et Surveillance.

Procédure

Pour filtrer les alarmes :

1. Dans la tâche Surveillance d'alarmes ou la tâche Surveillance, cliquez sur l'icône filtrer ( ).
   REMARQUE : Dans la tâche Surveillance, vous devez régler l'interrupteur Événements/Alarmes sur Alarmes. L'interrupteur Événements/Alarmes n'apparaît que lorsque vous activez la surveillance d'alarmes pour la tâche Surveillance.

   Si vous ne voyez pas le bouton Filtrer ( ) ou l'interrupteur Événements/Alarmes, faites glisser le canevas vers le bas pour révéler la liste d'alarmes en haut de la fenêtre.

2. Sélectionnez ou désélectionnez les filtres suivants :

   Afficher tout
   Affiche toutes les alarmes (pas de filtre).

   Afficher actives
   Affiche les alarmes actives.

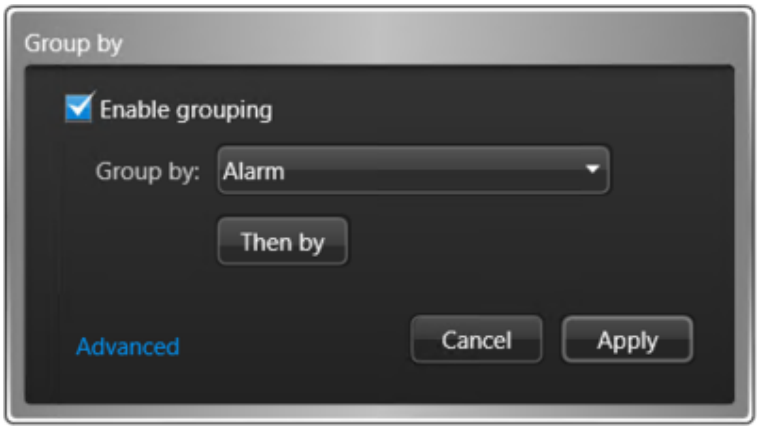
   Afficher les analyses en cours
   Affiche les alarmes en cours d'analyse.

   Afficher les acquittements requis
   Affiche les alarmes dont les conditions sources sont effacées, mais qui doivent toujours être acquittées.

   Afficher les acquittés
   Affiche les alarmes acquittées.

Pour regrouper les alarmes :

1. Dans la tâche Surveillance d'alarmes ou la tâche Surveillance, faites un clic droit sur un en-tête de colonne et sélectionnez Regrouper par.
   REMARQUE : Dans la tâche Surveillance, vous devez régler l'interrupteur Événements/Alarmes sur Alarmes. L'interrupteur Événements/Alarmes n'apparaît que lorsque vous activez la surveillance d'alarmes pour la tâche Surveillance. Si vous ne voyez pas l'interrupteur Événements/Alarmes, faites glisser le canevas vers le bas pour révéler la liste d'alarmes en haut de la fenêtre.
2. Dans la boîte de dialogue Regrouper par, sélectionnez Activer le regroupement.



3. Dans la liste déroulante, sélectionnez le niveau de regroupement le plus élevé que vous aimeriez appliquer aux alarmes. Vous pouvez regrouper les alarmes par :

Alarme
Nom de l'entité alarme.

Priorité
Priorité de l'alarme. Par défaut, la priorité de toutes les alarmes importées depuis Omnicast™ est réglée sur 1. Vous pouvez modifier leur priorité plus tard dans Config Tool.

Source
Entité source ayant déclenché l'alarme, lorsque l'alarme est déclenchée par le mécanisme événement-action. Elle affiche un nom d'utilisateur lorsque l'alarme est déclenchée manuellement.

Type d'entité source
Le type d'entité source ayant déclenché l'alarme, lorsque l'alarme est déclenchée par le mécanisme événement/action. Il affiche un utilisateur lorsque l'alarme est déclenchée manuellement.

État
État actuel de l'alarme.

Actif
L'alarme n'est pas encore acquittée. La sélection d'une alarme active affiche les boutons d'acquittement dans le volet de rapport.

Acquittée (par défaut)
L'alarme a été acquittée avec le mode par défaut.

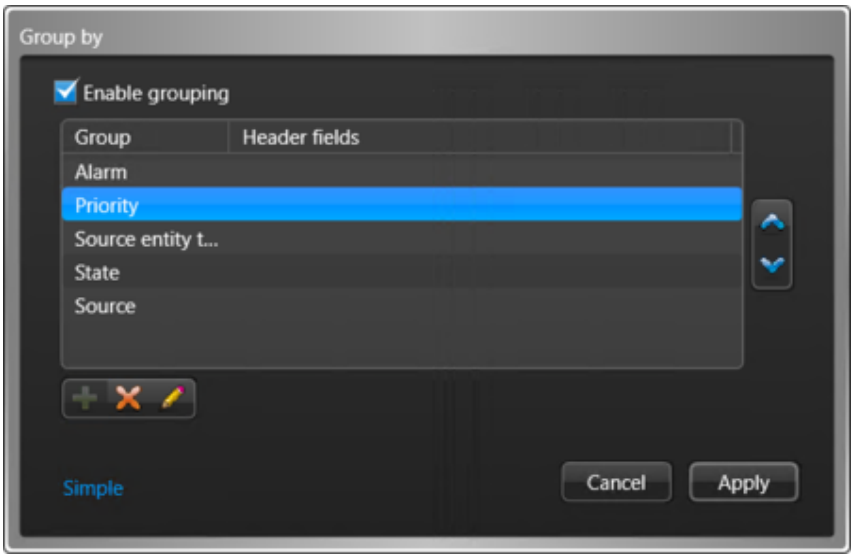
Acquittée (secondaire)
L'alarme a été acquittée avec le mode secondaire.

Acquittée (de force)
L'acquittement de l'alarme a été forcé par un administrateur.

Analyse en cours
Alarme en cours d'analyse, ce qui signifie qu'elle a été vue, mais pas forcément traitée.

Acquittement requis
Une alarme avec une condition d'acquittement effacée et prête à être acquittée.

4. Pour appliquer des niveaux de regroupement supplémentaires, sélectionnez Puis par.
5. Cliquez sur Avancé.
6. Pour modifier l'ordre de regroupement, sélectionnez un groupe, puis utilisez les flèches et .



7. Pour afficher les informations d'alarme dans l'en-tête du groupe, procédez comme suit :
    a. Sélectionnez un groupe, puis cliquez sur Modifier l'élément ( ).
    b. Sélectionnez les colonnes d'alarmes que vous souhaitez afficher.
    c. Pour modifier l'ordre d'affichage des colonnes, utilisez les flèches et .
    d. Cliquez sur OK.
8. Cliquez sur Appliquer.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Activer la surveillance d'alarmes dans la tâche Surveillance
- Informations d'alarmes disponibles durant la surveillance d'alarmes dans Security Center

5.1.5 | Couper les sons d'alarmes répétés

Si de nombreuses *alarmes actives* déclenchent des sons de manière répétée, vous pouvez couper le son en le désactivant dans la zone de notification.

À savoir

Pour éviter d'ignorer les alarmes, vous pouvez configurer Security Desk afin qu'il déclenche un son en boucle tant que des alarmes actives sont présentes dans le système. Le son s'arrête lorsque toutes les alarmes sont acquittées, ou lorsque vous décidez de le couper à titre temporaire.

Procédure

Pour désactiver le son de toutes les alarmes :

Dans la zone de notification, effectuez un clic droit sur l'icône Alarmes (), puis cliquez sur Couper toutes les alarmes.

Résultats

Tous les sons d'alarme sont désactivés. Le son est réactivé dès réception d'une nouvelle alarme et retentira tant que le système contient des alarmes actives.

Explorer

- Personnalisation du comportement des alarmes dans Security Center

5.1.6 | Transférer une alarme automatiquement

Si vous souhaitez que quelqu'un d'autre reçoive les alarmes lorsque vous devez vous absenter de votre poste, vous pouvez configurer le *transfert automatique* des alarmes.

Avant de commencer

Vérifiez que vous avez le privilège d'utilisateur *Transférer les alarmes*.

Procédure

1. Procédez de l'une des manières suivantes :
   - Dans la zone de notification, effectuez un clic droit sur l'icône Alarmes ( ou ), puis cliquez sur Démarrer le transfert automatique des alarmes.
   - Dans l'angle supérieur gauche de la tâche Surveillance d'alarmes ou Surveillance, cliquez sur Démarrer le transfert automatique des alarmes ().
2. Dans la boîte de dialogue Sélectionner les destinataires des alarmes, sélectionnez l'utilisateur ou le groupe d'utilisateurs de destination.
3. (Facultatif) Rédigez un message à envoyer avec l'alarme transférée.
4. Cliquez sur Démarrer le transfert automatique des alarmes.
   Toutes les alarmes qui vous sont envoyées sont transférées au destinataire spécifié jusqu'à ce que vous désactiviez l'option de *transfert automatique*.
5. Pour annuler le *transfert automatique*, procédez de l'une des manières suivantes :
   - Dans la zone de notification, effectuez un clic droit sur l'icône Alarmes ( ou ), puis cliquez sur Arrêter le transfert automatique des alarmes.
   - Dans l'angle supérieur gauche de la tâche Surveillance des alarmes ou Surveillance, cliquez sur Arrêter le transfert automatique des alarmes ().

5.1.7 | Transférer une alarme manuellement

Si vous recevez une alarme importante et que vous souhaitez la soumettre à quelqu'un d'autre, vous pouvez la transférer manuellement à partir des tâches *Surveillance d'alarmes, Surveillance,* et *Rapport d'alarmes*.

Avant de commencer

Vérifiez que vous avez le privilège d'utilisateur *Transférer les alarmes*.

À savoir

Le transfert d'une alarme ne la supprime pas de votre espace de travail. L'alarme est transférée à l'utilisateur sélectionné, et l'un de vous devez acquitter l'alarme.

Procédure

1. Sous la liste d'alarmes ou dans le widget Alarme, cliquez sur Transférer une alarme ( ).
2. Dans la boîte de dialogue Sélectionner les destinataires des alarmes, sélectionnez l'utilisateur ou le groupe d'utilisateurs de destination.
3. (Facultatif) Rédigez un message à envoyer avec l'alarme transférée.
4. Cliquez sur Transférer une alarme.

5.1.8 | Analyser les alarmes actuelles et passées

Vous pouvez rechercher et analyser les alarmes actuelles et passées avec la tâche Rapport d'alarmes.

À savoir

Dans Security Desk, vous pouvez examiner toutes les alarmes déclenchées durant la semaine écoulée, ou depuis votre dernière ronde. Vous pouvez également analyser les événements majeurs survenus au sein du système (en ne sélectionnant que les alarmes critiques), voir qui a acquitté une alarme particulière et pour quelle raison. Vous pouvez également examiner la vidéo associée à une alarme, qui peut être exportée et envoyée aux autorités en tant que preuve.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Rapport d'alarmes.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Alarmes

   Sélectionnez les types d'alarmes que vous souhaitez examiner. Les alarmes peuvent être définies localement ( ) ou importées depuis des systèmes fédérés ( ).

   Acquittée par
   Utilisateurs ayant acquitté l'alarme.

   Acquittée le
   Plage horaire d'acquittement de l'alarme.

Type d'acquittement
Sélectionnez l'une des options de type d'acquittement suivantes :

Secondaire
L'alarme a été acquittée par un utilisateur avec le mode secondaire.

Par défaut
Une alarme a été acquittée par un utilisateur, ou acquittée automatiquement par le système.

De force
Un administrateur a forcé l'acquittement de l'alarme.

Priorité d'alarme
Priorité de l'alarme.
REMARQUE : Par défaut, la priorité de toutes les alarmes importées depuis Omnicast est réglée sur 1. Vous pouvez modifier leur priorité plus tard dans Config Tool.

Contexte
Limitez la recherche aux alarmes dont l'annotation contient du texte particulier. Les différences de majuscules/minuscules n'influent pas sur la recherche.

Analysé par
L'utilisateur qui a placé l'alarme en état Analyse en cours.

Analysé le
Spécifiez la plage horaire durant laquelle l'alarme a été placée en état Analyse en cours.

Source
Entité source ayant déclenché l'alarme en cas de mécanisme événement/action, ou utilisateur ayant déclenché l'alarme manuellement.

État
État actuel de l'alarme.

Actif
L'alarme n'est pas encore acquittée. La sélection d'une alarme active affiche les boutons d'acquittement dans le volet de rapport.

Acquitté
Une alarme a été acquittée par un utilisateur, ou acquittée automatiquement par le système.

Analyse en cours
Alarme en cours d'analyse.

Acquittement requis
Une alarme avec une condition d'acquittement effacée est prête à être acquittée.

Déclenchée le
Plage horaire de déclenchement de l'alarme.

Événement déclencheur
Événements utilisés pour déclencher l'alarme.

Champs personnalisés
Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

3. Cliquez sur Générer le rapport.
   Les alarmes sont affichées dans le volet de rapport.

4. Pour afficher la séquence vidéo associée à une alarme dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas.
5. Pour contrôler les alarmes, utilisez le widget Alarme.

Exemple

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles. Si vous utilisez Internet Explorer, la vidéo ne s'affiche pas toujours. Pour y remédier, ouvrez les Paramètres d'affichage de compatibilité et décochez Afficher les sites intranet dans Affichage de compatibilité.

Explorer

- Affichage des alarmes sur le canevas de Security Desk
- Widget Alarme
- Présentation de la tâche Rapport d'alarmes dans Security Center

5.1.8.1 | Colonnes du volet de rapport dans la tâche Rapport d'alarmes

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

REMARQUE : Lorsque vous créez un rapport Alarmes avec Web Client, les colonnes de rapport ne sont pas toutes disponibles.

ID
Numéro d'instance de l'alarme. Identifie de manière unique chaque instance d'alarme.

Alarme
Nom de l'entité alarme.

Priorité
Priorité de l'alarme. Par défaut, la priorité de toutes les alarmes importées depuis Omnicast™ est réglée sur 1. Vous pouvez modifier leur priorité plus tard dans Config Tool.

Couleur de l'alarme
Couleur de l'alarme.

Source
Entité source ayant déclenché l'alarme, lorsque l'alarme est déclenchée par le mécanisme événement-action. Elle affiche un nom d'utilisateur lorsque l'alarme est déclenchée manuellement.

Heure source
Heure de l'événement déclenché par l'alarme. Heure source et Déclenchement ne diffèrent que lorsque l'événement est survenu alors que l'unité de contrôle d'accès était hors ligne.

Événement déclencheur
Événement ayant déclenché l'alarme (en cas d'utilisation du mécanisme événement-action). Action manuelle est indiqué lorsque l'alarme a été déclenchée manuellement par un utilisateur.

État
État actuel de l'alarme.

Actif
L'alarme n'est pas encore acquittée. La sélection d'une alarme active affiche les boutons d'acquittement dans le volet de rapport.

Acquittée (par défaut)
L'alarme a été acquittée avec le mode par défaut.

Acquittée (secondaire)
L'alarme a été acquittée avec le mode secondaire.

Acquittée (de force)
L'acquittement de l'alarme a été forcé par un administrateur.

Analyse en cours
Alarme en cours d'analyse, ce qui signifie qu'elle a été vue, mais pas forcément traitée.

Acquittement requis
Une alarme avec une condition d'acquittement effacée et prête à être acquittée.

Acquittée par
Utilisateur ayant acquitté l'alarme. Lorsque l'alarme est automatiquement acquittée par le système, la mention **Service** est indiquée.

Acquittée le
Heure d'acquittement de l'alarme.

Contexte
Annotation d'alarme.

ID externe de l'alarme
Ne concerne que les alarmes fédérées. ID de l'instance de l'alarme d'origine sur le système externe.

Analysé par
L'utilisateur qui a placé l'alarme en état Analyse en cours.

Analysé le
Plage horaire durant laquelle l'alarme a été placée en état Analyse en cours.

Période d'occurrence
Période durant laquelle l'événement est survenu.

Heure de déclenchement
Heure de déclenchement de l'alarme dans Security Center.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Sujet parent : Analyser les alarmes actuelles et passées

5.1.9 | Déclencher une alarme manuellement

Pour tester une alarme que vous venez de créer ou en cas d'événement critique, vous pouvez déclencher une alarme manuellement.

Avant de commencer

- L'alarme doit être configurée dans Config Tool.
- Si vous voulez déclencher des alarmes depuis la tâche Surveillance, vous devez activer la surveillance d'alarmes.

Procédure

1. Sur la page d'accueil, ouvrez la tâche *Surveillance d'alarmes* ou la tâche Surveillance.
2. Cliquez sur Déclencher l'alarme ().
3. Sélectionnez une alarme dans la liste, puis cliquez sur Déclencher l'alarme.

Résultats

Tous les destinataires préconfigurés reçoivent l'alarme s'ils sont connectés à Security Desk.

5.1.10 | Personnalisation du comportement des alarmes dans Security Center

Une fois que vous maîtrisez le fonctionnement des alarmes, vous pouvez personnaliser la manière dont elles sont gérées par le système dans la boîte de dialogue Options.

À savoir

L'option Afficher les noms d´entité avec le chemin d'accès complet est enregistrée avec votre profil utilisateur. Les autres réglages d'alarme sont enregistrés en local avec votre profil d'utilisateur Windows.

Procédure

1. Sur la page d'accueil, cliquez sur Options > Alarmes.
2. Configurez les options d'alarmes suivantes :

   Placer Security Desk au premier plan.
   La fenêtre de Security Desk est ramenée à l'avant-plan lorsqu'une alarme survient.

   Jouer un son
   Configurez le son qui signale l'arrivée d'une nouvelle alarme et la fréquence de ce son : *Une fois* (par défaut), *Toutes les n secondes*, ou *En continu*. Clique sur Test pour écouter le son de votre choix.

   Afficher dans

   Message contextuel
   Affiche les alarmes dans une fenêtre contextuelle dans la zone de notification de la tâche Surveillance.
   REMARQUE : Les alarmes contextuelles n'apparaissent qu'en l'absence de tuiles armées dans la tâche Surveillance.

   Tâche Surveillance des alarmes (et placer au premier plan)
   Basculer automatiquement vers la tâche Surveillance d'alarmes en cas de nouvelle alarme. Si Surveillance d'alarmes n'est pas dans la liste des tâches actives, elle y est ajoutée.

   Carte (et placer au premier plan)
   Bascule automatiquement l'affichage des alarmes dans la tâche Cartes. Si la tâche Cartes n'est pas dans la liste des tâches actives, elle y est ajoutée.

Afficher les dernières tuiles de surveillance d'alarme en premier
Lorsque cette option est activée (valeur par défaut), les alarmes sont affichées dans les tuiles armées en ordre chronologique inverse. Lorsque cette option est désactivée, les alarmes sont affichées dans les tuiles armées en ordre chronologique.
REMARQUE : Les alarmes restent affichées par ordre de priorité.

Revenir à la tâche d'origine une fois l'alarme traitée
Lorsque vous acquittez l'alarme, vous êtes automatiquement redirigé vers la tâche que vous utilisiez lorsque l'alarme est survenue.

Centrer la carte sur une alarme reçue
Lorsque les alarmes sont configurées pour être affichées dans la tâche Cartes, la carte est automatiquement centrée et zoomée sur l'objet associé.

Automatiquement afficher l'alarme en mode développé
Lorsque l'alarme est déclenchée, les entités associées sont affichées dans des tuiles séparées (et non dans une même tuile avec affichage cyclique).

Durée de mise en rappel
Configure la durée de rappel lorsque l'alarme est placée en veille avec la commande .

3. Cliquez sur l'onglet Visuel.
4. Pour afficher le chemin complet de l'entité ayant déclenché l'alarme dans la colonne Source des tâches Surveillance et Surveillance d'alarmes, sélectionnez l'option Afficher les noms d'entité avec le chemin d'accès complet.
   Le chemin d'une entité correspond à la hiérarchie de *secteurs* qui englobent l'entité dans l'arborescence de la vue secteur. Lorsque le chemin est trop long, un astérisque (*) est affiché à la place.
   Bureau de Paris/Entrée principale », ou « */*/Porte arrière ».
   REMARQUE : Cette option s'applique également aux autres entités. Quand cette option est sélectionnée, le chemin complet d'autres entités s'affiche dans les barres d'outils de la tuile.
5. Cliquez sur Enregistrer.

Explorer

- Acquittement des alarmes
- Couper les sons d'alarmes répétés
- Présentation de la tâche Surveillance d'alarmes dansSecurity Center
- Affichage des alarmes sur le canevas de Security Desk
- Inverser la priorité d'affichage des alarmes dans Security Desk

5.1.11 | Personnaliser les fenêtres image dans l'image pour les alarmes

Dans Security Desk, vous pouvez personnaliser la taille et la position de la fenêtre incrustée d'une alarme configurée pour l'affichage d'une image dans l'image. Vous pouvez également permuter le contenu affiché dans la fenêtre incrustée.

Avant de commencer

Réglez l'option d'affichage vidéo de l'alarme sur image dans l'image, voir Sélectionner les options d'affichage vidéo d'une alarme

Procédure

1. Ouvrez la tâche Surveillance ou Surveillance d'alarmes.
2. Sélectionnez une tuile qui affiche une alarme configurée pour l'affichage d'une image dans l'image.
3. Vous pouvez effectuer les tâches suivantes :
   - Cliquez dans la fenêtre incrustée pour permuter la vidéo affichée avec celle qui est affichée dans la tuile complète. Par exemple, si vous configurez l'alarme pour afficher de la vidéo en direct et enregistrée et que la vidéo en direct est affichée dans la fenêtre incrustée, un clic sur la fenêtre incrustée affiche la vidéo enregistrée.
   - Faites glisser la fenêtre incrustée pour la déplacer.
   - Faites glisser les poignées de la fenêtre incrustée pour la redimensionner.

Résultats

Les modifications sont appliquées immédiatement.

5.1.12 | Inverser la priorité d'affichage des alarmes dans Security Desk

Pour vous assurer qu'une alarme que vous surveillez reste sur le canevas lorsque de nouvelles alarmes sont déclenchées, vous pouvez configurer Security Desk pour afficher les anciennes tuiles d'alarme avant les nouvelles tuiles d'alarme.

À savoir

Security Desk suit deux règles pour afficher les alarmes dans les *tuiles armées* :

1. Alarme avec la priorité la plus élevée en premier : cette règle est prioritaire et ne peut pas être modifiée.
2. Alarme la plus récente en premier (par défaut) : cette règle peut être remplacée par *Alarme la plus ancienne en premier*.

Les alarmes sont toujours affichées par ordre de priorité décroissant. Si toutes les tuiles armées sont occupées lorsqu'une alarme est déclenchée, l'alarme avec la priorité la plus basse n'est pas affichée. Les alarmes actives sans tuile sont répertoriées dans le volet de rapport et sont affichées sur le canevas lorsque l'espace devient disponible.

Les alarmes avec la même priorité sont affichées selon les règles *Alarme la plus récente en premier* ou *Alarme la plus ancienne en premier* :

Alarme la plus récente en premier (par défaut)
Les alarmes actives de priorité égale sont affichées sur le canevas de la plus récente à la plus ancienne. Si toutes les tuiles armées sont occupées lorsqu'une alarme est déclenchée, la plus ancienne alarme est supprimée du canevas.

Alarme la plus ancienne en premier
Les alarmes actives de priorité égale sont affichées sur le canevas de la plus ancienne à la plus récente. Si toutes les tuiles armées sont occupées lorsqu'une alarme est déclenchée, cette alarme n'est pas affichée sur le canevas tant que l'espace n'est pas disponible.

Procédure

1. Sur la page d'accueil de Security Desk, cliquez sur Options > Alarmes.
2. Sous En cas de nouvelle alarme, désactivez Afficher les dernières tuiles de surveillance d'alarme en premier.
3. Cliquez sur Enregistrer.

Explorer

- Personnalisation du comportement des alarmes dans Security Center

5.2 | Incidents et niveaux de risque dans Security Desk

5.2.1 | Signaler un incident

Lorsque vous observez une situation qu'il convient de documenter, vous pouvez la signaler en tant qu'*incident*. Les événements et entités (caméras, portes, et ainsi de suite) peuvent être joints à un rapport d'incident en tant qu'information complémentaire.

À savoir

Lorsque vous signalez un incident associé à un événement ou une alarme, l'événement est joint au rapport d'incident, comme le sont les entités auxquelles l'événement fait référence. Vous pouvez également être obligé de signaler un incident lorsque vous acquittez une alarme (si l'alarme a été configurée de la sorte dans Config Tool).

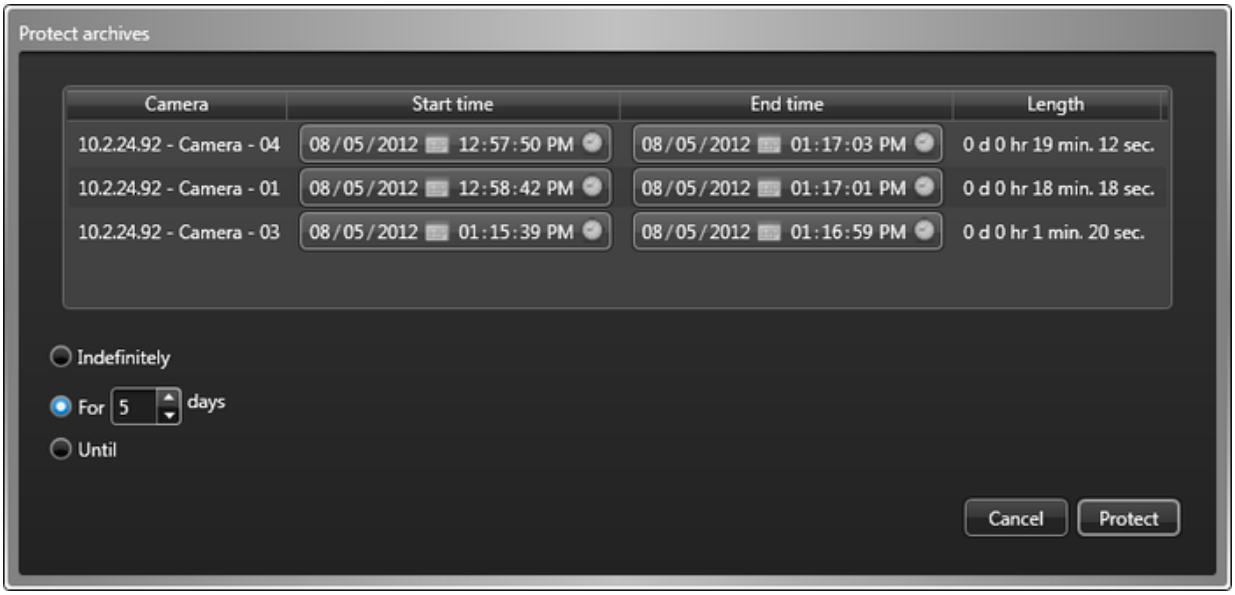
Les rapports d'incidents peuvent être analysés ultérieurement dans la tâche Incidents.

Procédure

1. Procédez de l'une des manières suivantes :
   - Pour signaler un incident qui n'est pas associé à une entité, cliquez sur l'onglet Accueil, puis sur Outils > Signaler un incident > .
   - Pour signaler un incident lié à un événement ou à une alarme, effectuez un clic droit sur l'élément dans la liste d'événements ou dans le volet de rapport, puis cliquez sur Signaler un incident.
   - Pour signaler un incident à propos de l'entité dans la tuile sélectionnée, effectuez un clic droit dans la tuile, puis cliquez sur Signaler un incident.
2. Dans la boîte de dialogue Signaler un incident, donnez un Titre à l'incident.
3. Dans la liste déroulante Catégorie, sélectionnez un des éléments suivants :
   - Sélectionnez une catégorie pour l'incident.
   - En l'absence de catégories, cliquez sur Gérer les catégories > Ajouter un élément ( ), donnez un nom à la catégorie, puis cliquez sur Ajouter > Enregistrer.
4. Dans la section Description, décrivez l'incident.
   La description fournie pourra être recherchée dans la tâche Incidents.
5. Dans la section Références, cliquez sur pour ajouter d'autres entités et informations.
   Toutes les entités associées à ce que vous surveillez dans la tuile sont ajoutées par défaut. Si vous affichez une alarme, l'alarme et sa source (l'entité l'ayant déclenchée) sont ajoutées par défaut.
6. Pour ajouter une séquence vidéo à l'incident, cliquez sur Plus, puis procédez de la manière suivante :
   a. Dans la section Séquences vidéo, cliquez sur Ajouter un élément ( ).
   b. Sélectionnez une caméra et une plage horaire, puis cliquez sur Ajouter.
   c. Pour protéger la séquence vidéo, sélectionnez l'option Protéger la vidéo contre l'effacement.
7. Créez le rapport d'incident de l'une des manières suivantes :
   - Cliquez sur Créer.
   - Pour créer le rapport d'incident et notifier d'autres utilisateurs du système, cliquez sur Créer et envoyer par e-mail, sélectionnez les utilisateurs, puis cliquez sur Créer et envoyer par e-mail.

     L'utilisateur doit avoir une adresse e-mail valable, et le serveur doit être configuré pour l'envoi d'e-mails.

   Si vous avez choisi de protéger les séquences vidéo que vous avez ajoutées à l'incident, la boîte de dialogue Protéger les archives apparaît.
8. Dans la boîte de dialogue Protéger les archives, spécifiez l'heure de début et l'heure de fin de la vidéo à protéger.



9. Sélectionnez la durée de protection du fichier vidéo avec l'une des options suivantes :

   Indéfiniment
   Pas de date de fin. Vous devez supprimer la protection manuellement en sélectionnant la vidéo dans le volet de rapport, puis en cliquant sur Annuler la protection ( ).
   REMARQUE : Lorsque la période de rétention est dépassée, les fichiers vidéo déprotégés ne sont pas supprimés immédiatement. Vous avez 24 heures pour restaurer la protection vidéo. Pour en savoir plus sur le stockage d'archives, voir le *Guide de l'administrateur Security Center*.

Pendant x jours
Le fichier vidéo est protégé durant le nombre de jours sélectionné.

Jusqu'au
Le fichier vidéo est protégé jusqu'à la date spécifiée.

10. Cliquez sur Protéger.
    L'incident est créé même si vous annulez les réglages de protection dans la boîte de dialogue Protéger les archives.

Résultats

Le rapport d'incident est enregistré dans la base de données à des fins de reporting. Si vous avez sélectionné un utilisateur, le rapport lui est envoyé.

Explorer

- Commandes du menu de tuile
- Analyser et modifier les incidents signalés
- Protéger les fichiers vidéo contre l'effacement

5.2.2 | Créer un pack d'incident

Vous pouvez ajouter de la vidéo en direct et enregistrée à une tuile, puis enregistrer le tout sous forme de pack d'incident. Cela peut s'avérer utile lorsque vous souhaitez signaler une situation et établir des preuves.

À savoir

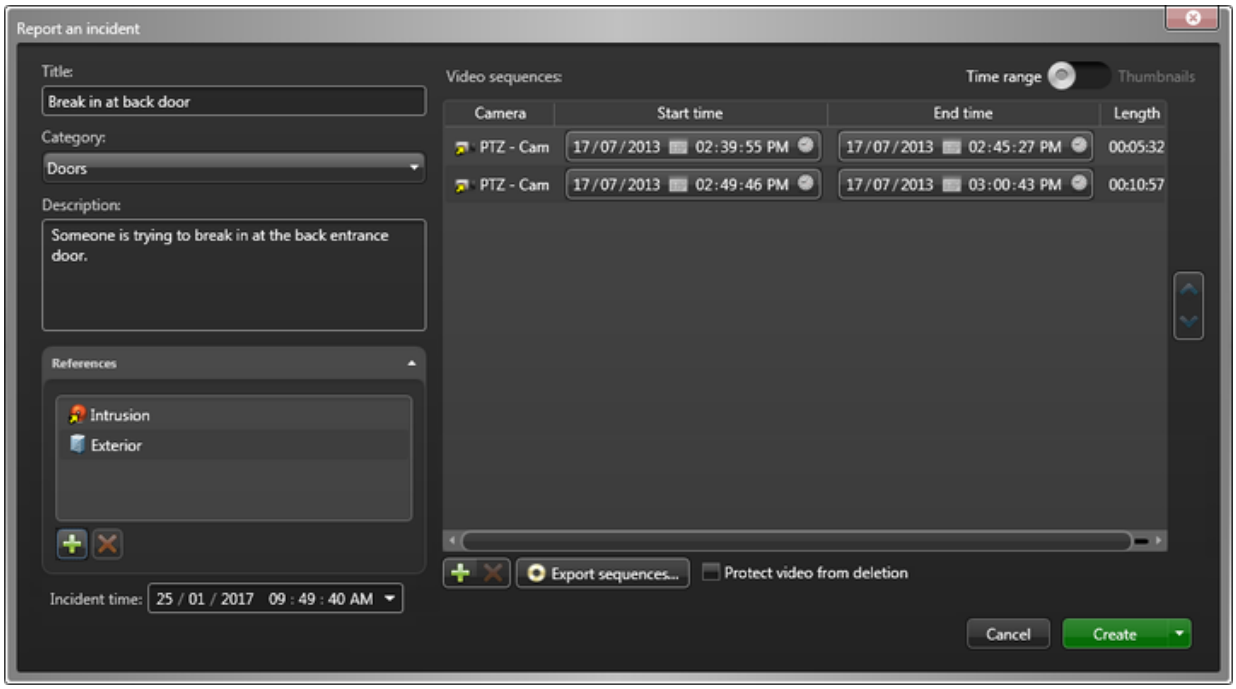
Lorsque l'enregistrement d'incidents est activé, la vidéo en direct ou enregistrée associée aux entités présentes dans la tuile (caméras, secteurs, portes, titulaires de cartes, et ainsi de suite) est enregistrée. L'affichage cyclique des entités dans la tuile est prise en charge. Les caméras placées dans la tuile se mettent à enregistrer si ce n'est pas déjà le cas.

Vous pouvez exporter les séquences vidéo associées sous forme d'un fichier G64x unique. Le fichier G64x est lisible dans Security Desk ou Genetec™ Video Player.

Vous pouvez créer plusieurs packs d'incidents en même temps.

Procédure

1. Pour vous assurer que le contenu de la tuile n'est pas remplacé lorsque de nouveaux incidents sont reçus dans Security Desk, désactivez la surveillance de la tuile de la manière suivante :
   a. Dans la tâche Surveillance, sélectionnez la tuile sur le canevas.
   b. Dans le widget tuile, cliquez sur Surveillance ( ).
   c. Cliquez sur Surveiller les alarmes et Surveiller les événements et veillez à désactiver toutes les formes de surveillance de la tuile.
      CONSEIL : Lorsque la surveillance est désactivée pour une tuile, l'arrière-plan de l'ID de tuile est affiché en noir.
2. Faites un clic droit dans la tuile qui affiche la caméra qui documente l'incident, puis cliquez sur Démarrer l'enregistrement d'incident ( ).
   Le contour de la tuile est affiché en rouge.
3. Pour documenter l'incident, ajoutez des caméras ou des entités associées à des caméras dans la tuile.
   La séquence est créée dans l'ordre de l'ajout des caméras et entités, mais peut être modifiée par la suite.
4. Faites un clic droit dans la tuile, et cliquez sur Arrêter l'enregistrement d'incident ( ).
5. Dans la boîte de dialogue Signaler un incident, donnez un Titre à l'incident.



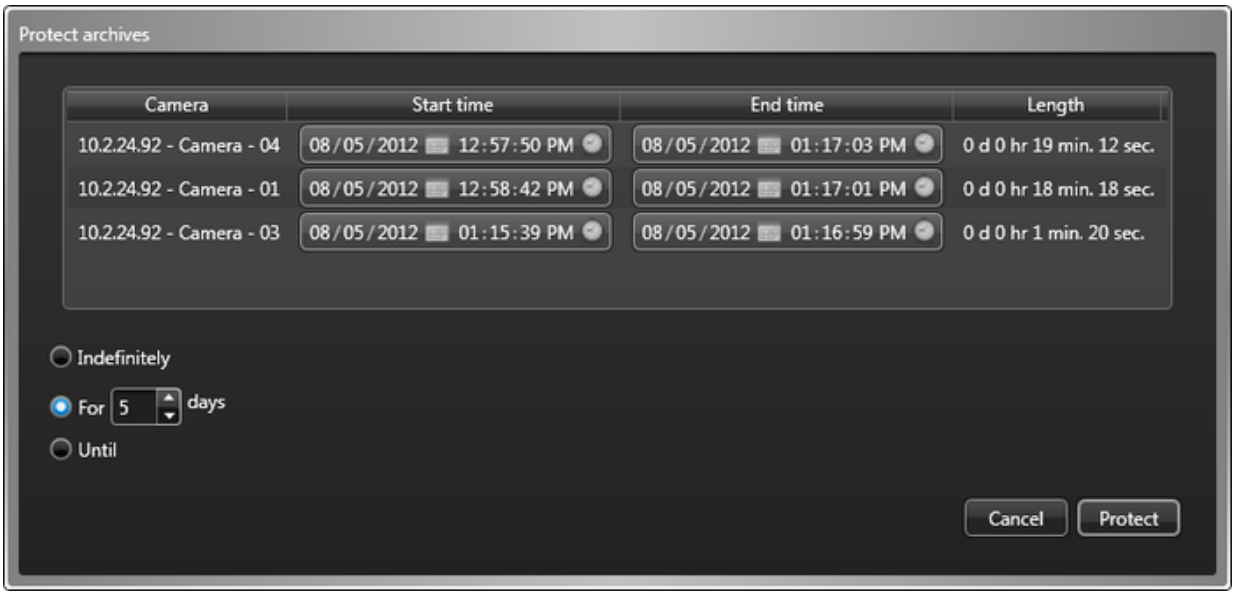
6. Dans la liste déroulante Catégorie, sélectionnez un des éléments suivants :
   - Sélectionnez une catégorie pour l'incident.
   - En l'absence de catégories, cliquez sur Gérer les catégories > Ajouter un élément ( ), donnez un nom à la catégorie, puis cliquez sur Ajouter > Enregistrer.
7. Dans la section Description, décrivez l'incident.
   La description fournie pourra être recherchée dans la tâche Incidents.
8. Dans la section Références, cliquez sur pour ajouter d'autres entités et informations.
   Toutes les entités associées à ce que vous surveillez dans la tuile sont ajoutées par défaut. Si vous affichez une alarme, l'alarme et sa source (l'entité l'ayant déclenchée) sont ajoutées par défaut.
9. Dans la section Séquences vidéo, vous pouvez effectuer les tâches suivantes :
   - Pour chaque caméra, modifiez la plage horaire de la séquence vidéo que vous souhaitez inclure dans le rapport d'incident.

     Une caméra n'aura par exemple que deux minutes de vidéo portant sur l'incident.
   - Pour ajouter une caméra au pack, cliquez sur Ajouter un élément ( ), sélectionnez une caméra et la plage horaire, puis cliquez sur Ajouter.

     L'ajout de caméras supplémentaires est utile si vous avez oublié de placer l'une des caméras dans la tuile lors de l'enregistrement de l'incident.
   - Pour protéger la séquence vidéo, sélectionnez l'option Protéger la vidéo contre l'effacement.
10. Créez le pack d'incident de l'une des manières suivantes :
    - Cliquez sur Créer.
    - Pour créer le rapport d'incident et notifier d'autres utilisateurs du système, cliquez sur Créer et envoyer par e-mail, sélectionnez les utilisateurs, puis cliquez sur Créer et envoyer par e-mail.

      L'utilisateur doit avoir une adresse e-mail valable, et le serveur doit être configuré pour l'envoi d'e-mails.
    - Pour exporter les séquences vidéo de toutes les caméras et les assembler dans un fichier G64x, cliquez sur Créer et exporter.

    Si vous avez choisi de protéger les séquences vidéo que vous avez ajoutées au pack d'incident, la boîte de dialogue Protéger les archives apparaît.
11. Dans la boîte de dialogue Protéger les archives, spécifiez l'heure de début et l'heure de fin de la vidéo à protéger.



12. Sélectionnez la durée de protection du fichier vidéo avec l'une des options suivantes :

    Indéfiniment
    Pas de date de fin. Vous devez supprimer la protection manuellement en sélectionnant la vidéo dans le volet de rapport, puis en cliquant sur Annuler la protection ( ).
    REMARQUE : Lorsque la période de rétention est dépassée, les fichiers vidéo déprotégés ne sont pas supprimés immédiatement. Vous avez 24 heures pour restaurer la protection vidéo. Pour en savoir plus sur le stockage d'archives, voir le *Guide de l'administrateur Security Center*.

    Pendant x jours
    Le fichier vidéo est protégé durant le nombre de jours sélectionné.

    Jusqu'au
    Le fichier vidéo est protégé jusqu'à la date spécifiée.

13. Cliquez sur Protéger.
    Le pack d'incident est créé même si vous annulez les réglages de protection dans la boîte de dialogue Protéger les archives.

Résultats

Le pack d'incident est enregistré dans la base de données à des fins de reporting. Si vous avez sélectionné un utilisateur, le pack lui est envoyé par e-mail.

Lorsque vous avez terminé

Une fois que vous avez créé le pack d'incident, vous pouvez l'envoyer aux forces de l'ordre ou à d'autres utilisateurs, ou l'analyser ultérieurement avec le rapport Incidents.
Explorer

- Analyser et modifier les incidents signalés
- Protéger les fichiers vidéo contre l'effacement

5.2.3 | Analyser et modifier les incidents signalés

Vous pouvez rechercher, analyser, modifier et supprimer les incidents signalés avec la tâche Incidents.

À savoir

Si vous avez signalé un incident, puis que vous devez modifier son contenu (changer la description ou ajouter une caméra au rapport par exemple), vous pouvez rechercher le nom de l'incident saisi au moment du signalement. Vous pouvez également rechercher par caméra si vous vous souvenez de la caméra associée à l'incident. Pour afficher les incidents consignés par d'autres utilisateurs durant la semaine écoulée ou depuis votre dernière ronde, vous pouvez rechercher les incidents en spécifiant une plage horaire.

Pour modifier un rapport d'incident, vous devez avoir le privilège *Modifier les incidents rapportés*. Pour supprimer un rapport d'incident, vous devez avoir le privilège *Supprimer les incidents rapportés*.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Incidents.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Titre
   Limitez la recherche aux incidents dont le titre contient du texte particulier.

   Catégorie
   Si des catégories d'incidents ont été créées, limitez votre recherche à certaines catégories.

   Heure de création
   Incidents créés ou signalés durant la plage horaire spécifiée.

   Description
   Restreindre la recherche aux entités qui contiennent cette chaîne de caractères.

   Heure de l'incident
   Incidents signalés durant la plage horaire spécifiée. L'heure de l'incident correspond à l'horodatage de l'événement ou alarme associé à l'incident. Si l'incident n'est associé à aucun événement ou alarme, l'heure de l'incident correspond à l'heure de création.

   Heure de modification
   Incidents modifiés durant la plage horaire spécifiée.

   Références
   Incidents se rapportant à toutes les entités sélectionnées.

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

3. Cliquez sur Générer le rapport.
   Les incidents signalés et packs d'incident sont affichés dans le volet de rapport.
4. Pour analyser un incident et afficher la vidéo associée dans une tuile, cliquez deux fois sur un élément dans le volet de rapport, ou faites-le glisser sur le canevas.
   En l'absence de caméra associée à l'incident, la boîte de dialogue Modifier l'incident apparaît. Si vous sélectionnez un pack d'incident, les séquences vidéo sont affichées dans une seule tuile, dans l'ordre d'enregistrement, et les entités ajoutées en tant que ressources complémentaires sont affichées dans d'autres tuiles.
5. Lorsque vous visionnez de la vidéo d'un pack d'incident, vous pouvez contrôler la lecture avec le widget *Séquences vidéo* du volet Commandes de la manière suivante :
   - Pour basculer vers une autre caméra du pack, sélectionnez une caméra dans la liste déroulante.
   - Pour basculer vers la caméra précédente ou suivante du pack, cliquez sur Séquence suivante () ou sur Séquence précédente ().
   - Pour aller à un endroit précis, déplacez le curseur dans la frise chronologique.
6. Modifiez ou supprimez l'incident de la manière suivante :
   a. Sélectionnez un incident dans le volet de rapport.

b. Au bas du volet de rapport, cliquez sur Modifier ( ) ou Supprimer ( ).
c. Dans la boîte de dialogue Modifier l'incident, modifiez la description de l'incident.
d. Dans la liste déroulante Catégorie, modifiez la catégorie d'incident.
e. Dans la section Références, cliquez sur ou pour ajouter ou supprimer les entités référencées.
f. Dans la section Séquences vidéo, vous pouvez effectuer les tâches suivantes :
- Modifiez les plages horaires des séquences vidéo incluses dans le rapport d'incident.
- Pour ajouter une caméra au pack, cliquez sur Ajouter un élément ( ), sélectionnez une caméra et la plage horaire, puis cliquez sur Ajouter.
- Pour protéger les séquences vidéo, sélectionnez l'option Protéger la vidéo contre l'effacement.

7. Pour enregistrer le rapport, procédez de l'une des manières suivantes :
- Pour enregistrer le rapport d'incident, cliquez sur Enregistrer.
- Pour enregistrer l'incident et notifier d'autres utilisateurs du système, cliquez sur Enregistrer et envoyer par e-mail, sélectionnez les utilisateurs, puis cliquez sur Enregistrer et envoyer par e-mail.
  REMARQUE : L'utilisateur doit avoir une adresse e-mail valable, et le serveur doit être configuré pour l'envoi d'e-mails.

Si vous avez choisi de protéger les séquences vidéo incluses dans le rapport, la boîte de dialogue Protéger les archives apparaît.

8. Dans la boîte de dialogue Protéger les archives, spécifiez l'heure de début et l'heure de fin de la vidéo à protéger.

9. Sélectionnez la durée de protection du fichier vidéo avec l'une des options suivantes :

Indéfiniment
Pas de date de fin. Vous devez supprimer la protection manuellement en sélectionnant la vidéo dans le volet de rapport, puis en cliquant sur Annuler la protection ( ).
REMARQUE : Lorsque la période de rétention est dépassée, les fichiers vidéo déprotégés ne sont pas supprimés immédiatement. Vous avez 24 heures pour restaurer la protection vidéo. Pour en savoir plus sur le stockage d'archives, voir le *Guide de l'administrateur Security Center*.

Pendant x jours
Le fichier vidéo est protégé durant le nombre de jours sélectionné.

Jusqu'au
Le fichier vidéo est protégé jusqu'à la date spécifiée.

10. Cliquez sur Protéger.
Le rapport d'incident est créé même si vous annulez vos modifications dans la boîte de dialogue Protéger les archives.

Résultats

Les modifications apportées à l'incident sont enregistrées dans la base de données. Si vous avez sélectionné un utilisateur, le rapport d'incident lui est envoyé par e-mail.
Explorer

- Signaler un incident
- Créer un pack d'incident

5.2.3.1 | Colonnes du volet de rapport dans la tâche Incidents

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Titre
Titre de l'incident.

Catégorie
Catégorie de l'incident.

Description
Description de l'événement, activité, entité ou incident.
IMPORTANT : Pour respecter la réglementation des États, si l'option Rapport généré est utilisée pour un rapport Historiques d'activité qui contient des données de RAPI, le motif de la recherche RAPI est inclus dans le champ Description.

Références
Liste des entités référencées par l'incident.

Heure de l'incident
L'horodatage de l'événement ou alarme référencé. Si aucun événement n'est référencé, correspond à l'heure de création de l'incident.

Créé par
Utilisateur ayant initialement signalé l'incident.

Heure de création
Heure de signalement de l'incident.

Heure de modification
Heure de la dernière modification de l'incident.

Modifié par
Dernier utilisateur à avoir modifié l'incident.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Sujet parent : Analyser et modifier les incidents signalés

5.2.4 | Réagir aux événements critiques avec les niveaux de risque

En cas d'événement critique durant la surveillance du système (incendie, fusillade, et ainsi de suite), vous pouvez réagir en modifiant l'état du système Security Center entier ou de certains secteurs par le biais des niveaux de risque.

Avant de commencer

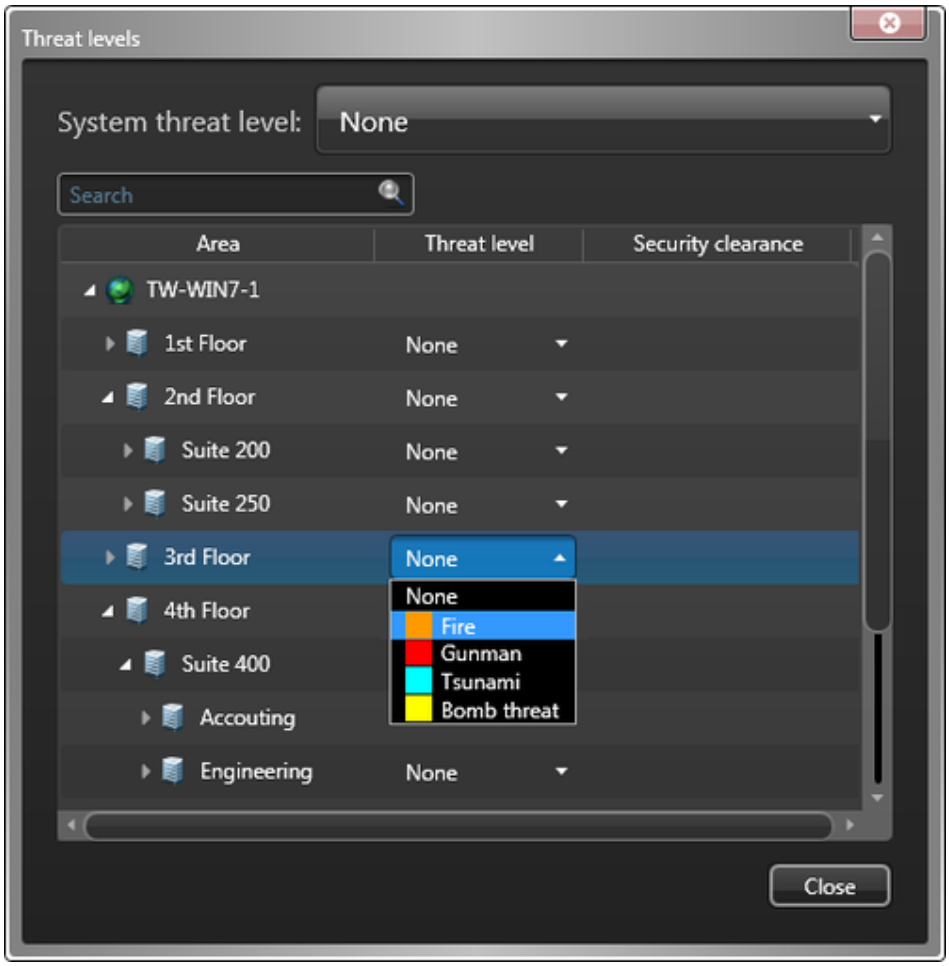
Pour définir les niveaux de risque, vous devez disposer du privilège *Activer le niveau de risque*. Si l'icône Niveaux de risque ( ) n'est pas affichée dans la zone de notification, vous pouvez l'afficher depuis la boîte de dialogue Options.

À savoir

Lorsque vous définissez un niveau de risque, vous pouvez complètement sécuriser un périmètre, ignorer les horaires de verrouillage, déclencher une alarme, refuser l'accès de certains titulaires de cartes à un secteur, etc. Les effets précis d'un niveau d'accès dépendent de sa configuration dans Config Tool.

Procédure

1. Ouvrez la boîte de dialogue Niveau de risque de l'une des manières suivantes :
   - Dans la zone de notification, double cliquez sur l'icône Niveaux de risque ( ).
   - Sur la page d'accueil, cliquez sur Outils > Niveaux de risque .
2. Procédez de l'une des manières suivantes :
   - Pour définir un niveau de risque pour tout le système, sélectionnez un niveau de risque dans la liste déroulante Niveau de risque système.
   - Pour définir un niveau de risque pour un secteur particulier, sélectionnez un niveau de risque dans la liste déroulante en regard de l'entité concernée.



3. Dans la boîte de dialogue de confirmation qui apparaît, cliquez sur Appliquer > Fermer.

Résultats

L'icône Niveaux de risque dans la zone de notification devient rouge ( ). Si vous réglez un niveau de risque pour le système en entier, l'arrière-plan de Security Desk adopte la couleur du niveau de risque. Les autres effets de la définition d'un niveau de risque dépendent de sa configuration.

CONSEIL : Vous pouvez consulter le niveau de risque actuel des secteurs dans la tâche *État du système*.

Exemple

Si vous réglez le niveau de risque sur *Incendie*, vous pouvez déclencher une alarme, déverrouiller toutes les portes, lancer l'enregistrement sur toutes les caméras, etc.

Explorer

- Configurer la zone de notification

5.2.4.1 | Effacer les niveaux de risque

Une fois que l'événement critique est passé, vous pouvez effacer le niveau de risque et rétablir l'état normal de Security Center.

Procédure

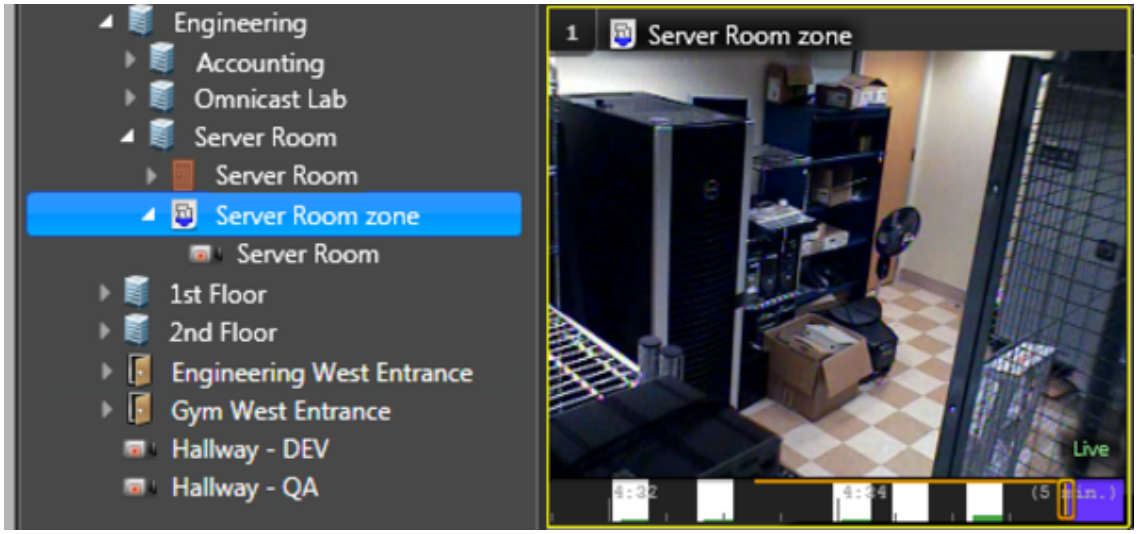
1. Dans la zone de notification, cliquez deux fois sur l'icône Niveau de risque ( ).
2. Pour rétablir le niveau d'accès sur Aucun (niveau 7) pour tous les secteurs pendant que le niveau de risque est toujours activé, cliquez sur Réinitialiser le niveau d'accès minimal.
3. Pour effacer le niveau de risque, procédez de l'une des manières suivantes :
   - Si le niveau de risque est défini pour le système tout entier, sélectionnez Aucun dans la liste déroulante Niveau de risque système.
     REMARQUE : Vous pouvez également effacer le niveau de risque pour des secteurs particuliers. Le niveau de risque est également effacé dans tous les sous-secteurs.
   - Si le niveau de risque est défini pour un secteur particulier, sélectionnez Aucun dans la liste déroulante en regard de l'entité.
4. Cliquez sur Fermer.

Sujet parent : Réagir aux événements critiques avec les niveaux de risque

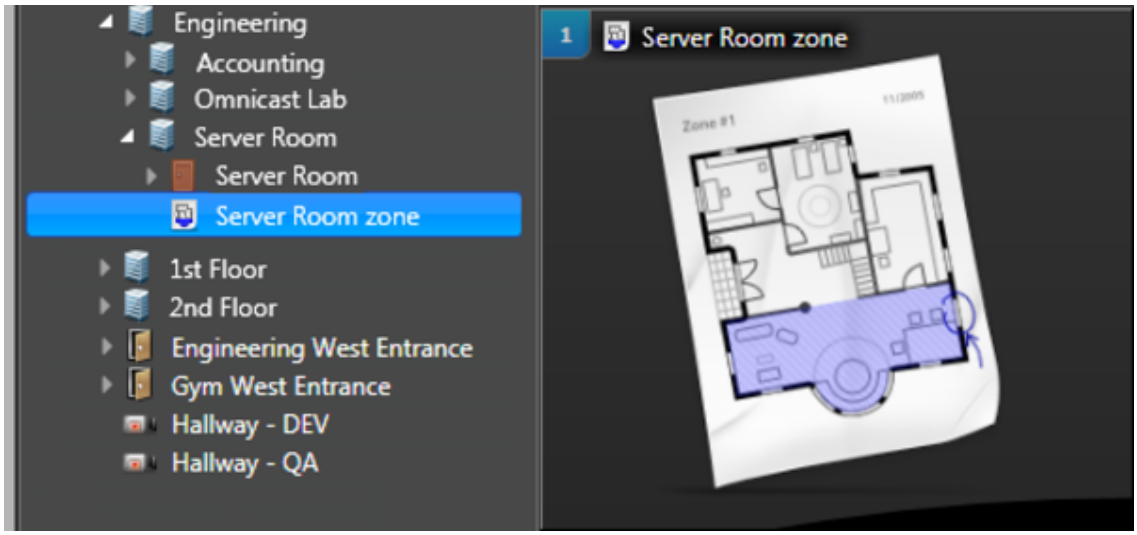
5.3 | Zones et détection des intrusions dans Security Desk

5.3.1 | Affichage des zones sur le canevas de Security Desk

Lorsque vous cliquez deux fois sur une entité zone ( ) ou que vous la faites glisser sur une tuile, et qu'une caméra est associée à la zone, le flux vidéo de la caméra est affiché.



Si aucune caméra n'est associée à une zone, seule l'icône de zone est affichée.



5.3.2 | À propos de l'aperçu de détection d'intrusion

Vous pouvez utiliser l'aperçu de détection d'intrusion pour surveiller les entités de détection d'intrusion qui nécessitent votre attention. Par exemple, une zone de détection d'intrusion dans un état d'alarme actif ou une entrée numérique dans un état d'échec. Vous pouvez épingler l'aperçu dans Security Desk pour qu'il soit visible à tout moment.

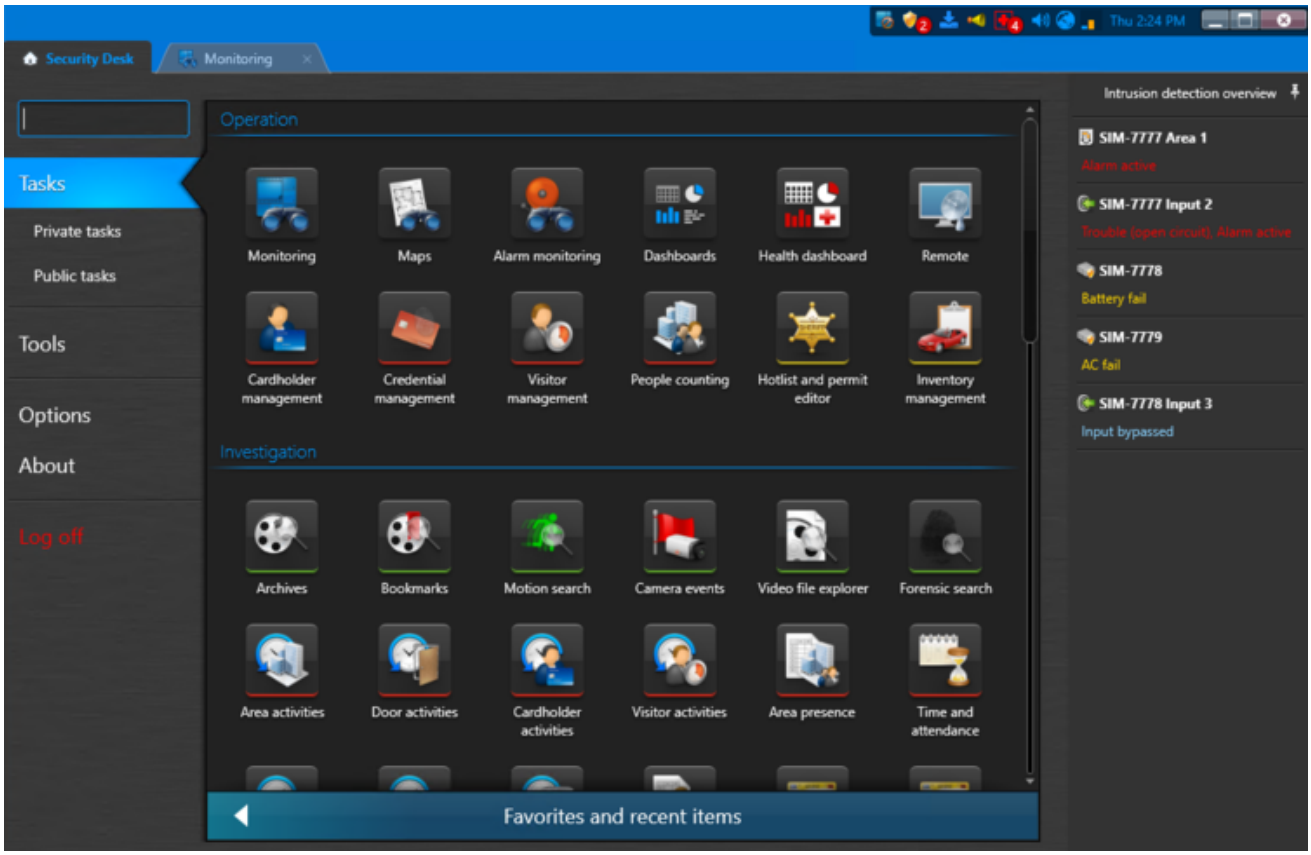
Icône de la zone de notification

L'aperçu de détection d'intrusion doit être activé dans les options Security Desk pour être accessible via la zone de notification.

Lorsque l'aperçu est activé, l'icône de détection d'intrusion ( ) s'affiche dans la barre de notification. Vous devez cliquer sur l'icône pour initialiser l'aperçu. Une fois initialisé, le nombre d'entités présentant des problèmes est indiqué sur le badge de notification, avec un code couleur par niveau d'importance : rouge pour une importance élevée et jaune pour une importance moyenne.
REMARQUE : Le badge affiche uniquement le nombre d'entités ayant le plus haut niveau d'importance dans la liste. Par exemple, s'il existe deux problèmes de haute importance et un problème d'importance moyenne, le badge affiche uniquement le nombre de problèmes de haute importance ( ).

Volet Aperçu de détection d'intrusion

Cliquer sur l'icône de la zone de notification affiche la liste des entités de détection d'intrusion du système nécessitant votre attention. Les entités que vous pouvez surveiller incluent les secteurs de détection d'intrusion, les unités et les entrées. La liste d'entités peut être épinglée pour être visible à partir de n'importe quelle tâche dans laquelle vous travaillez.



Commandes de l'aperçu

Selon le type d'entité, différentes commandes sont disponibles en cliquant avec le bouton droit sur l'entité dans la liste. Si l'entité se trouve sur une carte, vous pouvez double-cliquer dessus dans la liste pour ouvrir une boîte de dialogue affichant l'entité sur la carte.

5.3.3 | Armer et désarmer une zone

Vous pouvez armer et désarmer une zone avec la tâche État du système.

À savoir

Vous pouvez également armer et désarmer une zone avec le widget *Zone* du volet Commandes lorsque la zone est affichée dans une tuile.

Procédure

1. Sur la page d'accueil, ouvrez la tâche État du système.
2. Dans la liste déroulante Surveiller, sélectionnez Zones.
3. Dans le Sélecteur, sélectionnez un secteur.
4. Pour rechercher des zones comprises dans des sous-secteurs, sélectionnez l'option Rechercher les entités membres. Les zones sont affichées dans le volet de rapport.
5. Sélectionnez une zone, puis procédez de l'une des manières suivantes :
   - Pour armer la zone, cliquez sur Armer ( ).
   - Pour désarmer la zone, cliquez sur Désarmer ( ).

Explorer

- Widget Zone

5.3.4 | Analyser les événements de zones

Utilisez le rapport *Activités de zones* pour analyser les événements relatifs aux *zones* (zone armée, zone désarmée, serrure déverrouillée, et ainsi de suite).

À savoir

Par exemple, pour afficher l'activité d'une certaine zone sur une période donnée, sélectionnez la zone, puis une plage horaire pour le rapport. Vous pouvez restreindre la recherche aux événements critiques et sélectionnant les événements de zone qui vous intéressent (comme porte forcée).

Procédure

1. Sur la page d'accueil, ouvrez la tâche Activités de zones.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Événements
   Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

   Zones
   Sélectionnez les zones à examiner.

3. Cliquez sur Générer le rapport.
   Les événements de zone sont affichés dans le volet de rapport.
4. Pour afficher la séquence vidéo associée à un événement dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas.
   Si aucune caméra n'est associée à la zone, l'icône de zone est affichée.
5. Pour contrôler les zones, utilisez le widget Zone.

Explorer

- Widget Zone

5.3.4.1 | Colonnes du volet de rapport pour la tâche Activités de zones

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Événement
Nom de l'événement.

Heure de l'événement
Date et heure de l'événement.

Période d'occurrence
Période durant laquelle l'événement est survenu.

Zone
Nom de la zone.
Sujet parent : Analyser les événements de zones

5.3.5 | Modifier l'état d'un secteur de détection d'intrusion

Vous pouvez armer et désarmer un secteur de détection d'intrusion et déclencher une alarme d'intrusion avec la tâche État du système.

À savoir

Vous pouvez également armer, désarmer et déclencher une alarme d'intrusion avec le widget *Secteur de détection d'intrusion* dans le volet Commandes lorsqu'un secteur de détection d'intrusion est affiché dans une tuile. Pour en savoir plus sur les effets de l'armement ou désarmement d'un secteur de détection d'intrusion ou le déclenchement d'une alarme d'intrusion, voir Widget Secteur de détection d'intrusion.

Procédure

1. Sur la page d'accueil, ouvrez la tâche État du système.
2. Dans la liste déroulante Surveiller, sélectionnez Secteur de détection d'intrusion.
3. Dans le Sélecteur, sélectionnez un secteur de détection d'intrusion.
4. Pour rechercher des secteurs de détection d'intrusion compris dans des sous-secteurs, sélectionnez l'option Rechercher les entités membres.
   Les secteurs de détection d'intrusion sont affichés dans le volet de rapport.
5. Sélectionnez un secteur de détection d'intrusion, puis procédez de l'une des manières suivantes :
   - Pour armer le secteur, cliquez sur .
   - Pour désarmer le secteur, cliquez sur .
   - Pour déclencher une alarme d'intrusion, cliquez sur .

5.3.6 | Analyser les événements de secteurs de détection d'intrusion

Vous pouvez analyser les événements qui surviennent dans les secteurs de détection d'intrusion (Armement global du secteur de détection d'intrusion, Contrainte de secteur de détection d'intrusion, Problème d'entrée de secteur de détection d'intrusion, etc), à l'aide du rapport Activités de secteur de détection d'intrusion.

À savoir

Par exemple, si vous avez connaissance d'un événement de détection d'intrusion critique (ex. : *Contrainte de secteur de détection d'intrusion*) survenu lors des 5 dernières minutes, vous pouvez rechercher l'événement, analyser la vidéo associée et déclencher une alarme d'intrusion si nécessaire.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Activités de secteur de détection d'intrusion.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Secteurs de détection d'intrusion
   Sélectionnez les secteurs de détection d'intrusion que vous souhaitez examiner.

   Titulaires de cartes
   Limitez votre recherche à des titulaires de cartes ou groupes de titulaires de cartes spécifiques

Champs personnalisés
Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Heure de l'événement
Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

Événements
Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

3. Cliquez sur Générer le rapport.
   Les événements de secteurs de détection d'intrusion sont affichés dans le volet de rapport.
4. Pour afficher la séquence vidéo associée à un événement dans une tuile, cliquez deux fois sur un élément, ou faites-le glisser sur le canevas.
   Si aucune caméra n'est associée au secteur de détection d'intrusion, l'icône du secteur de détection d'intrusion s'affiche.
5. Contrôlez la tuile sélectionnée avec le widget Secteur de détection d'intrusion.

Explorer

- Widget Secteur de détection d'intrusion

5.3.6.1 | Colonnes du volet de rapport dans la tâche Activités de secteurs de détection d'intrusion

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Événement
Nom de l'événement.

Heure de l'événement
Date et heure de l'événement.

Secteur de détection d'intrusion
Nom du secteur de détection d'intrusion.

Titulaire de cartes
Nom de l'entité titulaire de cartes.

Description
Description de l'événement, activité, entité ou incident.

Appareil
Périphérique utilisé par l'unité (lecteur, entrée REX, module d'E/S, relais de pêne, et ainsi de suite).
REMARQUE : Cette colonne est vide si l'événement est un *contournement d'entrée*.

Type d’entrée
Le type d’entrée.

Unité de détection d'intrusion
Unité de détection d'intrusion impliquée.

Période d'occurrence
Période durant laquelle l'événement est survenu.

Photo
Photo du titulaire de cartes ou du visiteur.

Utilisateur
Nom de l'utilisateur ayant déclenché l'événement. Le nom d'utilisateur est vide si l'événement n'a pas été déclenché depuis Security Desk.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.
Sujet parent : Analyser les événements de secteurs de détection d'intrusion

5.3.7 | Analyser les événements d'unités de détection d'intrusion

Vous pouvez analyser les événements associés aux unités de détection d'intrusion (Panne de courant, Unité perdue, Problème d'entrée d'unité de détection d'intrusion, et ainsi de suite) à l'aide de la tâche Événements d'unités de détection d'intrusion.

Procédure

1. Sur la page d'accueil, ouvrez la tâche *Événements d'unités de détection d'intrusion*.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

   Champs personnalisés
   Limitez la recherche à un champ personnalisé prédéfini pour l'entité. Ce filtre n'apparaît que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

   Événements
   Sélectionnez les événements qui vous intéressent. Les types d'événements disponibles dépendent de la tâche que vous utilisez.

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

   Unités de détection d'intrusion
   Sélectionnez les unités de détection d'intrusion que vous souhaitez examiner.

3. Cliquez sur Générer le rapport.
   Les événements d'unités de détection d'intrusion sont affichés dans le volet de rapport.

5.3.7.1 | Colonnes du volet de rapport pour la tâche Événements d'unités de détection d'intrusion

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Appareil
Périphérique utilisé par l'unité (lecteur, entrée REX, module d'E/S, relais de pêne, et ainsi de suite).
REMARQUE : Cette colonne est vide si l'événement est un *contournement d'entrée*.

Événement
Nom de l'événement.

Heure de l'événement
Date et heure de l'événement.

Unité de détection d'intrusion
Unité de détection d'intrusion impliquée.

Période d'occurrence
Période durant laquelle l'événement est survenu.

Utilisateur
Nom de l'utilisateur ayant déclenché l'événement. Le nom d'utilisateur est vide si l'événement n'a pas été déclenché depuis Security Desk.
Sujet parent : Analyser les événements d'unités de détection d'intrusion

6 | Présentation des rubriques de dépannage dans Security Desk

6.1 | Dépannage général dans Security Desk

6.1.1 | Afficher les messages système

Si vous recevez des messages du système, vous pouvez les afficher à partir de la zone de notification, puis analyser les entités problématiques.

À savoir

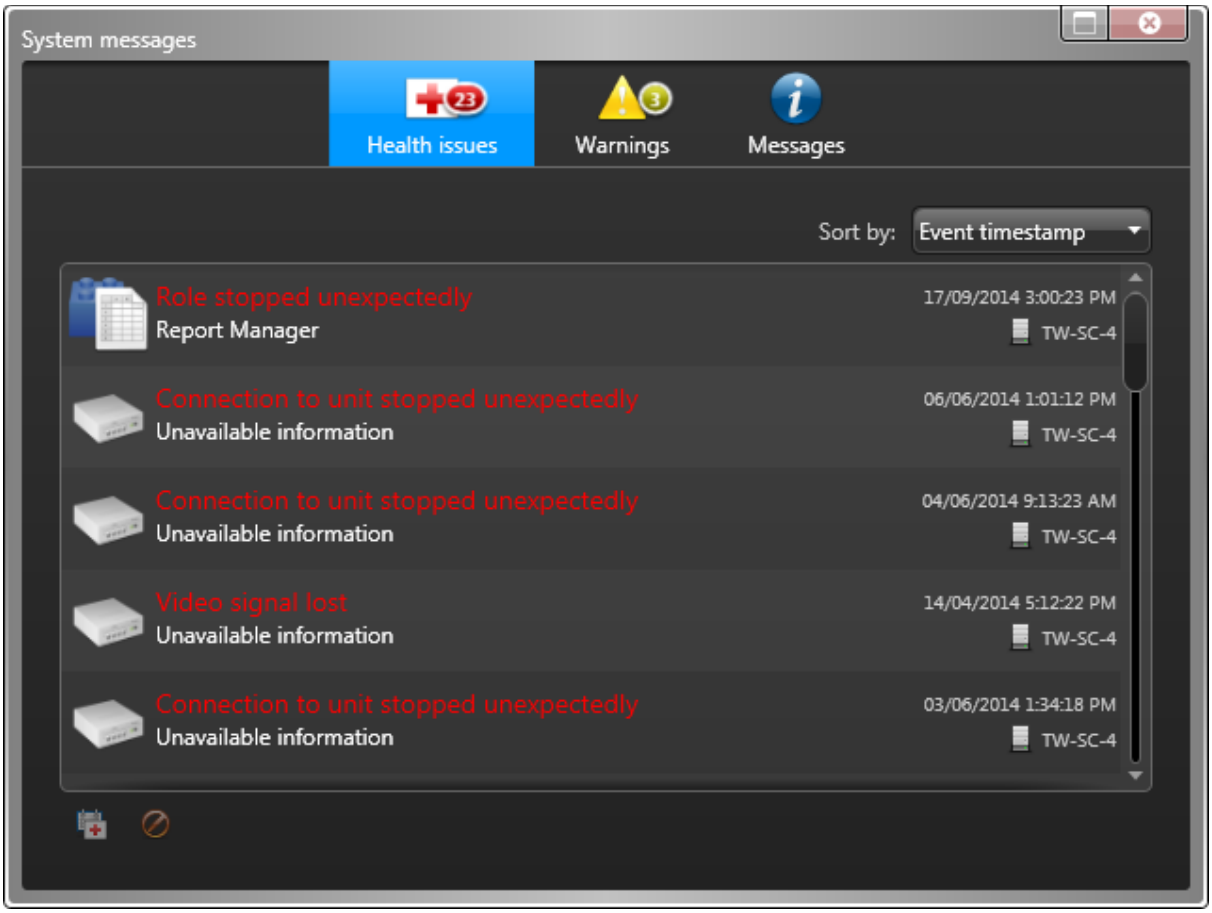
Vous pouvez recevoir trois types de messages système :

- Problèmes de fonctionnement
- Avertissements
- Messages

REMARQUE : Il ne faut pas confondre les messages système et les dysfonctionnements d'entités. Les seuls messages système qui ont des dysfonctionnements correspondants dans le Rapport d'état sont les problèmes de fonctionnement. Ces dysfonctionnements ont le niveau de gravité *Erreur*.

Procédure

1. Dans la zone de notification, cliquez deux fois sur l'icône Messages système ().
2. Sur la page Problèmes de fonctionnement () de la boîte de dialogue Messages système, procédez de l'une des manières suivantes :
   - Utilisez la liste Trier par pour choisir le mode d'affichage des dysfonctionnements. Vous pouvez les trier par ordre alphabétique et par dysfonctionnement, horodatage, ordinateur (nom) ou source (nom de l'entité).
   - Pour ouvrir la page de configuration d'une entité, cliquez sur l'entité. Vous devez avoir accès à Config Tool.
   - Pour lancer la tâche Rapport d'état et afficher les dysfonctionnements du système, sélectionnez un dysfonctionnement puis cliquez sur Rapport d'état ().
   - Pour ignorer un dysfonctionnement, sélectionnez-le, puis cliquez sur Ignorer le dysfonctionnement (). REMARQUE : Cette option n'est disponible que pour les utilisateurs dotés du privilège *Ignorer les dysfonctionnements*. Lorsqu'un dysfonctionnement est fermé, il est supprimé de la liste, et l'événement correspondant n'est plus considéré comme étant actif. Cela signifie que l'événement n'est pas affiché si vous générez un Rapport d'état et que le filtre Afficher les dysfonctionnements en cours est activé.
   - Pour mettre à jour le contenu de la page Rapport d'état, cliquez sur Actualiser.



3. Sur la page Avertissements ( ), procédez de l'une des manières suivantes :
   - Pour ouvrir la page de configuration d'une entité, cliquez sur l'entité. Vous devez avoir accès à Config Tool.
   - Pour ouvrir la fenêtre Diagnostic qui fournit des informations complémentaires sur l'avertissement, cliquez sur Détails ( ).

     Dans la fenêtre Diagnostic, vous pouvez enregistrer l'avertissement sous forme de fichier texte.
4. Sur la page Messages ( ), sélectionnez un message et procédez de l'une des manières suivantes :
   - Pour copier le message sélectionné dans le presse-papier, cliquez sur Copier dans le presse-papiers ( ).
   - Pour effacer le message sélectionné, cliquez sur Effacer ( ).
   - Pour effacer tous les messages, cliquez sur Effacer tout.
5. Fermez la boîte de dialogue Messages système.

Explorer

- Afficher les dysfonctionnements du système

6.1.2 | Afficher les dysfonctionnements du système

Vous pouvez afficher les dysfonctionnements du système associés à des entités sur une période donnée avec le Rapport d'état.

À savoir

Les dysfonctionnements peuvent avoir trois niveaux de gravité :

- Erreur
- Avertissement
- Informations

Pratiquement toutes les entités du système peuvent générer des dysfonctionnements. Vous pouvez choisir les dysfonctionnements à surveiller en configurant le rôle *Surveillance de l'état*. Pour en savoir plus sur la sélection des dysfonctionnements à surveiller dans Config Tool, voir le *Guide de l'administrateur Security Center*.

Par exemple, lorsqu'une entité rencontre des problèmes, vous pouvez rechercher les précédents dysfonctionnements associés à l'entité. Vous pouvez rechercher les erreurs critiques survenues au sein du système durant la semaine écoulée en filtrant la recherche pour n'afficher que les erreurs, et en spécifiant une plage horaire.
REMARQUE : Les dysfonctionnements sont également affichés dans la zone de notification sous forme de messages système () en temps réel.

Procédure

1. Sur la page d'accueil, ouvrez la tâche Rapport d'état.
2. Définissez les filtres de recherche pour votre rapport. Activez un ou plusieurs des filtres suivants :

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

   Dysfonctionnement
   Nom du dysfonctionnement.

   Gravité du dysfonctionnement
   Niveau de gravité du dysfonctionnement :
   - Informations
   - Avertissement
   - Erreur

   Ordinateur
   Sélectionnez un ordinateur qui présente des dysfonctionnements pour analyse.

   Afficher les dysfonctionnements en cours
   Limitez la recherche aux entités associées à des dysfonctionnements actifs. Seuls les événements actifs depuis plus longtemps que la durée spécifiée sont affichés dans le rapport.
   REMARQUE : Fermer un événement depuis la tâche Rapport d'état ou la boîte de dialogue Messages système le supprime de la liste des événements actifs.

   Entité source
   Entité source de l'événement.

   Groupe source
   Groupe d'entités sources de l'événement. En général un rôle ou une unité.

3. Cliquez sur Générer le rapport.
   Les dysfonctionnements des entités sélectionnées sont affichés dans le volet de rapport.

Lorsque vous avez terminé

Pour fermer les dysfonctionnements actifs qui ont le niveau de gravité *Erreur*, sélectionnez l'événement et cliquez sur Ignorer le dysfonctionnement. L'événement est supprimé du rapport et de la boîte de dialogue Messages système. Lorsque vous relancez le rapport, les événements ignorés sont toujours affichés si le filtre Afficher les dysfonctionnements en cours est désactivé.
Explorer

- Afficher les messages système

6.1.2.1 | Colonnes du volet de rapport pour la tâche Rapport d'état

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Numéro de dysfonctionnement
Numéro d'identification du dysfonctionnement.

Heure de l'événement
Date et heure de l'événement.

Gravité
Niveau de gravité du dysfonctionnement :

- Informations
- Avertissement
- Erreur

Dysfonctionnement
Nom du dysfonctionnement.

Entité source
Entité source associée à l'événement.

Nombre d'occurrences
Nombre d'occurrences de ce dysfonctionnement sur l'entité sélectionnée.

Description de l'entité
Description sur la page Identité de l'entité dans Config Tool.

Description
Description de l'événement.

Ordinateur
Ordinateur sur lequel le dysfonctionnement est survenu.

Adresse IP
L'adresse IP de l'unité ou de l'ordinateur.

Adresse physique
Adresse MAC de l'interface réseau de l'appareil.

Sujet parent : Afficher les dysfonctionnements du système

6.1.3 | Afficher l'état de fonctionnement et la disponibilité d'une entité

Le rapport Statistiques de fonctionnement vous permet de consulter ls statistiques de disponibilité des entités et de surveiller l'état de fonctionnement du système.

À savoir

En surveillant l'état et la disponibilité des ressources, comme les rôles, unités vidéo, contrôleurs de porte, tableaux de détection d'intrusion, etc., vous pouvez détecter les instabilités avant qu'elles n'entraînent des dysfonctionnements graves.

La disponibilité est exprimée sous forme de pourcentage dans le volet de rapport.

Procédure

1. Ouvrez la tâche Statistiques de fonctionnement.
2. Définissez les filtres de recherche pour votre rapport :

   Heure de l'événement
   Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

   Afficher les dysfonctionnements en cours
   Limitez la recherche aux entités associées à des dysfonctionnements actifs. Seules les entités avec des événements actifs depuis plus longtemps que la durée spécifiée sont affichées dans le rapport.

   Entité source
   Entité source de l'événement.

   Groupe source
   Groupe d'entités sources de l'événement. En général un rôle ou une unité.

3. Cliquez sur Générer le rapport.

Résultats

Le volet de rapport affiche les statistiques de fonctionnement pour les entités sélectionnées. Lorsqu'une statistique de fonctionnement n'a pas pu être calculée pour un rôle ou pour une entité, le motif est indiqué dans la colonne *État des calculs* :

Un ou plusieurs événements servant à calculer la disponibilité sont actuellement désactivés.
L'administrateur système doit sélectionner les dysfonctionnements à surveiller en configurant le rôle Surveillance de l'état. Pour en savoir plus sur la sélection des dysfonctionnements à surveiller dans Config Tool, voir le *Guide de l'administrateur Security Center*.

Un ou plusieurs serveurs du système sont hors ligne
Le serveur qui héberge le rôle sélectionné est hors ligne, ce qui empêche de calculer les statistiques pour le rôle.

Exemple

Un contrôleur de porte appelé *Gym* a été indisponible quatre fois durant la semaine écoulée, pour une disponibilité de 90,72 %. Dans le résultat du rapport, vous pouvez voir que ce contrôleur de porte est potentiellement problématique, et décider d'envoyer une équipe de maintenance sur place.

6.1.3.1 | Colonnes du volet de rapport dans la tâche Statistiques de fonctionnement

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Entité source
Entité source associée à l'événement ou l'alarme.

Disponibilité
Le pourcentage de disponibilité d'une entité donnée.

Temps disponible
Nombre de jours, heures et minutes de disponibilité en ligne de l'entité.

Indisponibilité prévue
Nombre de jours, heures, minutes d'indisponibilité de l'entité, prévue par l'utilisateur ou pour cause de *mode maintenance*. Par exemple, la désactivation d'un rôle ou la déconnexion d'une application client correspond à une indisponibilité prévue. L'indisponibilité prévue est toujours exclue des calculs de pourcentage de *Disponibilité*.

Indisponibilité non prévue
Nombre de jours, heures, minutes d'indisponibilité de l'entité, à l'exclusion du temps passé en *mode maintenance*. L'indisponibilité imprévue n'est pas due à un choix de l'utilisateur.

MTBF
Mean time between failures (période moyenne entre les défaillances), en heures.

MTTR
Mean time to recovery (temps de rétablissement moyen), en heures.

Défaillances
Nombre de défaillances qui sont survenues.

Perte de paquets RTP élevée
Le nombre de paquets *Real-time Transport Protocol* perdus.

État des calculs
En cas d'indisponibilité des statistiques de fonctionnement, le motif est affiché ici.

Horodatage de la dernière erreur
Horodatage de la dernière déconnexion ou indisponibilité inattendue de l'entité.
Sujet parent : Afficher l'état de fonctionnement et la disponibilité d'une entité

6.1.4 | Surveiller l'état de votre système Security Center

Utilisez la tâche État du système pour surveiller l'état actuel de différents types d'entités et analyser les dysfonctionnements éventuels.

À savoir

Utilisez le rapport État du système pour surveiller votre système. Par exemple, si une caméra ne marche pas, vous pouvez sélectionner l'entité caméra dans la tâche État du système, puis obtenir un diagnostic pour savoir pourquoi elle est hors ligne. Dans la tâche État du système, vous pouvez également lancer la tâche Rapport d'état et créer un rapport d'état pour pousser l'analyse.

Lorsque vous surveillez les *Routes*, un *Redirecteur* doit être configuré sur chaque réseau pour pouvoir détecter les capacités réseau et afficher l'état actuel.

Procédure

1. Ouvrez la tâche État du système.
2. Dans la liste déroulante Surveiller, sélectionnez un des éléments suivants :

- Unités de contrôle d'accès
- Moniteurs analogiques
- Applications (réservé aux administrateurs)
- Secteurs
- Archiveurs
- Caméras
- Caisses enregistreuses
- Portes
- Ascenseurs
- Problèmes de fonctionnement
- Secteur de détection d'intrusion
- Unités de détection d'intrusion
- Macros
- Périphériques
- Rôles
- Itinéraires
- Serveurs
- Zones

3. Le cas échéant, sélectionnez un secteur dans le Sélecteur.
4. Pour rechercher des entités comprises dans des secteurs imbriqués, sélectionnez l'option Rechercher les entités membres.
   Les entités, rôles, applications et éléments associés sont affichés dans le volet de rapport.
5. (Facultatif) Procédez de la manière suivante, selon l'entité sélectionnée :
   - Pour lancer un *Rapport d'état*, cliquez sur  .
   - Pour diagnostiquer l'entité sélectionnée, cliquez sur  .
   - Pour imprimer le rapport, cliquez sur  .
   - Pour modifier la configuration d'une entité, faites un clic droit sur l'entité dans le volet de rapport, puis cliquez sur Configurer une entité ().
   - Pour enregistrer le rapport, cliquez sur  .

Explorer

- Afficher les dysfonctionnements du système
- Dépannage : entités
- Présentation de la tâche État du système

6.1.5 | États des entités

Les entités peuvent apparaître dans différents états dans la vue secteur, représentées par différentes couleurs.

Le tableau suivant présente les trois états des entités :

État	Couleur	Description
En ligne	Blanc	Le serveur parvient à se connecter à l'entité.
Hors ligne	Rouge	Le serveur ne parvient pas à se connecter à l'entité.
Avertissement	Jaune	Le serveur peut se connecter à l'entité, mais un problème est survenu.

Les avertissements sont généralement le résultat d'une configuration non valable. Par exemple, les deux conditions suivantes peuvent faire basculer une caméra vers l'état d'avertissement (jaune) :

- Plusieurs horaires d'enregistrements conflictuels affectés à une même caméra.
- Un événement *Transmission perdue* est survenu. Cela signifie que l'Archiveur est toujours connecté à la caméra, mais n'a pas reçu de paquets vidéo depuis plus de 5 secondes.

Pour dépanner une caméra en état hors ligne ou avertissement, procédez de l'une des manières suivantes :

- Modifiez les horaires en conflit. Pour plus de détails sur les conflits horaires, voir le *Guide de l'administrateur Security Center*.
- Corriger le rôle Archiveur.

Explorer

- Afficher une entité sur le canevas
- Rechercher des entités
- Dépannage : entités

6.1.6 | Dépannage : entités

Vous pouvez dépanner les entités et les rôles avec l'outil *Diagnostic*.

À savoir

Les entités ou les rôles qui ne sont pas correctement configurés sont affichés en jaune. Les entités hors ligne sont affichées en rouge. L'outil *Diagnostic* peut vous aider à corriger un problème associé à une entité.

Procédure

1. Ouvrez la tâche État du système.
2. Dans le menu déroulant Surveiller, sélectionnez le type d'entité que vous souhaitez diagnostiquer.
3. Le cas échéant, sélectionnez un secteur dans le Sélecteur.
4. Pour inclure les entités comprises dans des secteurs imbriqués, sélectionnez l'option Rechercher les entités membres.
   Les entités sont affichées dans le volet de rapport.
5. Sélectionnez une entité problématique, et cliquez sur Diagnostiquer ().
   Une fenêtre de diagnostic apparaît et présente le résultat d'un ensemble de tests effectués sur l'entité concernée.
6. Pour enregistrer le résultat du test, cliquez sur Enregistrer > Fermer.

Explorer

- États des entités

6.1.7 | Placer les entités en mode maintenance dans Security Center

Si vous devez modifier la configuration d'une entité ou effectuer la maintenance d'un appareil comme une caméra ou une unité de contrôle d'accès, vous pouvez placer l’appareil en mode maintenance pour éviter d’affecter les statistiques de fonctionnement.

À savoir

- Lorsqu'une entité est déconnectée en mode maintenance, l'indisponibilité est considérée comme étant prévue. L'indisponibilité prévue n’est pas prise en compte dans le calcul de disponibilité de l’entité dans le rapport Statistiques de fonctionnement.
  REMARQUE : Les dysfonctionnements des entités en mode maintenance sont signalés avec la gravité *Information*.
- Vous pouvez placer les entités suivantes en mode maintenance :
  - Rôles
  - Unités vidéo
  - Caméras
  - Unités de contrôle d'accès
  - Unités de détection d'intrusion
  - Zones matérielles
  - Alarmes
  - Véhicules de patrouille
  - Unités de RAPI
- Vous pouvez déverrouiller une porte à des fins de maintenance sur la page Propriétés de la porte.
- En mode manuel, vous ne pouvez déclencher les alarmes qu’avec une action manuelle. En mode maintenance, les alarmes ne peuvent pas être déclenchées par une association événement-action.
  REMARQUE : Une alarme active placée en mode maintenance n’est pas acquittée.

Procédure

1. Ouvrez la tâche pertinente dans Security Desk
2. Faites une clic droit dans l’arborescence des entités, sélectionnez l’entité dans la liste et sélectionnez Mode maintenance ( ).
   Vous pouvez également sélectionner le mode maintenance en faisant un clic droit sur une entité dans une tuile ou sur une carte.
3. Dans la boîte de dialogue Mode maintenance, cliquez sur ACTIVER.
4. Sélectionnez la durée souhaitée du mode maintenance de l’entité.
   Sélectionnez l’une des options suivantes :

   Manuellement
   Le mode de maintenance doit être désactivé manuellement.

   Durée
   Le mode maintenance est activé pour le nombre de jours spécifié.

   Heure de fin particulière
   Le mode maintenance est activé jusqu'à la date sélectionnée.

   Vous pouvez modifier la durée pendant qu'une entité est en mode maintenance.

5. Dans le champ Motif, entrez la raison de la mise en mode maintenance de l'entité.
6. Cliquez sur Enregistrer.
   Si les icônes de rôles Federation™ ne sont pas actualisées immédiatement, appuyez sur F5 pour actualiser l'arborescence des entités.

Résultats

L'entité est placée en mode maintenance pour la durée spécifiée.

Pendant que l'entité est en mode maintenance, l'icône ( ) est affichée sur l'icône de l'entité dans la vue secteur, dans les tuiles et le cas échéant sur les cartes. Lorsque vous survolez l’icône d'une entité dans la vue secteur ou sur les cartes, le motif de la mise en mode maintenance de l’entité est affiché.

6.1.8 | Activer et désactiver les rôles

À des fins de maintenance ou de dépannage, vous pouvez désactiver un rôle sans affecter ses réglages, puis le réactiver plus tard.

À savoir

Si votre système rencontre des problèmes de fonctionnement, il peut être utile de redémarrer un rôle. Les rôles peuvent aussi être désactivés, afin de modifier leurs propriétés. Pour en savoir plus sur la configuration des rôles dans Config Tool, voir le *Security CenterGuide de l'administrateur* .

Vous devez disposer du privilège *Modifier les propriétés du rôle* pour désactiver un rôle.

Procédure

1. Sur la page d'accueil, ouvrez la tâche État du système.
2. Dans la liste déroulante Surveiller, sélectionnez Rôles.
   Les rôles de votre système sont affichés dans le volet de rapport.
3. Sélectionnez le rôle que vous souhaitez désactiver, et cliquez sur Désactiver le rôle ( ) > Continuer.
   Le rôle est affiché en gris (inactif) dans le volet de rapport.
4. Pour réactiver le rôle, sélectionnez-le et cliquez sur Activer le rôle ( ).

6.1.9 | Dépannage :filtres de recherche

Lorsque vous créez un rapport ou recherchez des entités, les filtres servent à spécifier les critères de recherche. Une icône de DEL ( ) indique qu'un filtre est activé. Toutefois, si le filtre n'est pas valable, un message d'erreur ou d'avertissement est affiché.

Avertissement ( )
Le problème vient potentiellement des informations du filtre. Le rapport ou la recherche risque de prendre plus de temps que d'ordinaire.

Erreur ( )
Problème avec les informations du filtre. Vous ne pouvez pas générer le rapport ou effectuer la recherche en cas d'erreur.

Survolez l'icône avec la souris pour consulter l'avertissement ou le message d'erreur dans une infobulle. Le tableau suivant présente des exemples de messages, et la marche à suivre pour résoudre le problème.

Message d'avertissement/d'erreur	Essayer ceci
La recherche porte sur plusieurs jours	Raccourcissez la plage horaire du rapport ou de la recherche.
Aucune entité sélectionnée	Le filtre est vide. Sélectionnez une entité ou désactivez le filtre.
Aucune sélection	Le filtre est vide. Sélectionnez une option ou désactivez le filtre.
Dates et heures non valables	La plage horaire n'est pas valable La date et heure de fin est avant la date et heure de début, ou inversement. Reconfigurez la plage horaire du rapport.

Explorer

- Générer un rapport
- Rechercher des entités
- Sélectionner la plage horaire d'un rapport

6.1.10 | Recueillir des données de diagnostic

À des fins de dépannage, l'*Outil de collecte de données de diagnostic* recueille et prépare les informations système pour que vous puissiez facilement les envoyer au Centre d'assistance technique Genetec™.

Avant de commencer

Pour exécuter l'outil Collecte de données de diagnostic :

- Vous devez disposer des droits d'administrateur Windows sur votre ordinateur.
- Vous devez avoir des droits d'administrateur dans Security Center.

À savoir

- L'outil récupère différents types d'informations système (types de collections), comme l'information système Genetec, la collection d'Archiveur et l'inventaire vidéo. Voir les étapes ci-dessous pour la liste complète de ces collections et ce qu'elles contiennent.
- L'exécution de l'Outil de collecte de données de diagnostic peut avoir un impact temporaire sur les performances de l'ordinateur.
- Si votre ordinateur est équipé de Windows XP ou 2003, les journaux des événements et les données de surveillance des performances Windows ne sont pas récupérés.

Procédure

1. Sur la page d'accueil, cliquez sur Outils > Outil de collecte de données de diagnostic.
2. Dans la boîte de dialogue, sélectionnez l'une des options suivantes :

   Collecte de données par défaut sur tous les serveurs Security Center
   N'envoie qu'un ensemble prédéfini de collections de données (valeur par défaut).

   Collections de données et serveurs particuliers
   Envoie un ensemble de données de collection et d'informations serveur que vous sélectionnez.

3. Si vous sélectionnez Collections de données et serveurs particuliers, procédez de la manière suivante :
   a. Dans le volet de gauche, sélectionnez le ou les serveurs que vous souhaitez analyser.
   b. Dans le volet de droite, sélectionnez le ou les types de collections.

   Les collections suivantes sont disponibles :

   Informations système
   (Sélectionné par défaut) Un ensemble de données recueillies pour des tests de diagnostic intégrant des journaux et des informations système non limitées aux applications Genetec. Cette collecte contient :
   - Journaux des événements de Genetec
   - Journaux des événements du système
   - Journaux des événements de l'application
   - Journaux des événements de sécurité
   - Applications installées
   - Mises à jour installées
   - Applications en cours d'exécution
   - Connexions réseau actuellement actives
   - Assemblages .NET CLR requis pour le débogage

Informations système Genetec
(Sélectionné par défaut) Un ensemble de données recueillies pour des tests de diagnostic qui inclut des informations sur les applications Genetec™. Elle contient :

- Security Center - fichiers de configuration
- Security Center - journaux de traçage
- Security Desk et journaux d'erreur Config Tool (quand les clients sont sélectionnés)
- Données de surveillance des performances
- Informations sur les processus d'exécution
- Security Center - informations sur les processus en cours d'exécution avec assemblages chargés
- Dumps mémoire
- Clés de registre (uniquement celles qui sont utilisées ou créées par Genetec Inc.)

Agent d'Archiveur
Un ensemble de données recueillies pour des tests de diagnostic qui inclut des informations sur l'Archiveur, comme le cache de l'Archiveur et les journaux de l'Archiveur.

Gestionnaire d'accès
Un ensemble de données recueillies pour des tests de diagnostic qui inclut des informations sur le Gestionnaire d'accès. Elle inclut des fichiers de configuration, les connexions réseaux actuellement actives, le cache des fichiers VertX et les fichiers temporaires VertX.

Inventaire des unités vidéo
Une collecte de données utilisée pour des essais diagnostics répertoriant les unités vidéos inscrites par le système et les caméras fédérées Security Center

4. Cliquez sur Démarrer.
   Une barre indique la progression pour chaque collection de données. Les informations sont enregistrées dans le dossier suivant sur le poste qui exécute l'outil : C:\ProgramData\Genetec Security Center 5.9\Diagnostics. Pour Windows XP et 2003, les données sont enregistrées dans : C:\Documents and Settings\All Users\Application Data\Genetec Security Center 5.9\Diagnostics.
5. Pour ouvrir le dossier, cliquez sur Ouvrir le fichier de dépôt.

Résultats

Vous pouvez maintenant envoyer les informations de diagnostic au Centre d'assistance technique Genetec™.

6.2 | Dépannage du contrôle d'accès dans Security Center

6.2.1 | Afficher les dysfonctionnements de contrôle d'accès

Utilisez la tâche Rapport d'état de contrôle d'accès pour afficher les événements relatifs aux entités de contrôle d'accès.

À savoir

Ce rapport est similaire au rapport Rapport d'état, mais la requête ne recherche que les événements ayant entraîné des avertissements et portant sur des entités de contrôle d'accès. Les entités de contrôle d'accès qui peuvent générer des avertissements sont les unités de contrôle d'accès, les portes, les secteurs, les ascenseurs et les zones.

Procédure

1. Ouvrez la tâche Rapport d'état de contrôle d'accès.
2. Définissez les filtres de recherche pour votre rapport. Choisissez un ou plusieurs des filtres suivants :

Entité source
Entité source de l'événement.

Heure de l'événement
Spécifiez la plage horaire de la requête. La plage peut être définie pour une période particulière ou pour des unités de temps prédéfinies comme la semaine ou le mois précédent.

3. Cliquez sur Générer le rapport.
   Les dysfonctionnements de contrôle d'accès sont affichés dans le volet de rapport.

6.2.1.1 | Colonnes du volet de rapport dans la tâche État de contrôle d'accès

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles pour la tâche de rapport concernée.

Entité source
Entité source associée à l'événement ou l'alarme.

Événement
Nom de l'événement.

Unité
Nom de l'unité.

Type de produit
Modèle de l'unité.

Heure de l'événement
Date et heure de l'événement.

Adresse IP
L'adresse IP de l'unité ou de l’ordinateur.

Version du micrologiciel
Version du micrologiciel installé sur l'unité.

Fuseau horaire
Le fuseau horaire de l'unité.

Appareil
Périphérique utilisé par l'unité (lecteur, entrée REX, module d'E/S, relais de pêne, et ainsi de suite).

Description
Rapporte le motif de l’échec d'une mise à niveau du micrologiciel.

Champs personnalisés
Les champs personnalisés prédéfinis pour l'entité. Les colonnes n'apparaissent que si des champs personnalisés sont définis pour l'entité, et s'ils ont été rendus visibles lors de leur création ou dernière configuration.

Sujet parent : Afficher les dysfonctionnements de contrôle d'accès

6.2.2 | Outil Diagnostic d'accès

L'outil Diagnostic d'accès vous permet de tester et dépanner un système de contrôle d'accès, et notamment les règles d'accès, ou la configuration des portes et ascenseurs.

Un système complexe peut accumuler de nombreux horaires (heures de bureau/heures de fermetures/jours fériés/week-end/événements spéciaux), secteurs et sous-secteurs, groupes de titulaires de cartes, etc. Au fur et à mesure de l'accumulation des entités, la logique d'accès de base appliquée à une porte peut devenir plus difficile à prédire.

L'outil Diagnostic d'accès permet d'obtenir les informations suivantes :

- Qui est autorisé à passer un point d'accès à un instant donné
- Quels points d'accès un titulaire de cartes est autorisé à utiliser à un instant donné
- La raison pour laquelle un titulaire de carte est autorisé ou non à utiliser un point d'accès à un instant donné

L'outil de diagnostic d'accès est plus précis lors de l'examen d'un événement qui vient de se produire. Lorsque vous utilisez l'outil pour analyser un événement passé (comme un accès refusé), sachez que la configuration a pu changer depuis la date de l'événement. L'outil ne prend pas en compte les réglages du passé. Il n'évalue la situation qu'en fonction des réglages actuels.

6.2.3 | Tester les règles d'accès aux portes et ascenseurs

Vous pouvez savoir qui a accès à un côté de porte ou un étage d'ascenseur à un moment donné avec l'outil Diagnostic de porte.

À savoir

L'outil de diagnostic de porte n'examine pas les identifiants de chaque titulaire de cartes. Vous pouvez affiner le diagnostic de droits d'accès du titulaire en cliquant sur l'onglet Diagnostic d'accès ( ).

Procédure

1. Sur la page d'accueil, cliquez sur Outils > Outil de diagnostic d'accès.
2. Dans la boîte de dialogue Outil de diagnostic d'accès, cliquez sur l'onglet Diagnostic de porte.
3. Sélectionnez la date et l'heure à évaluer avec l'outil.
   Seules les *règles d'accès* sont évaluées en fonction de la date et de l'heure spécifiées.
4. Sélectionnez le point d'accès que vous souhaitez examiner avec l'outil :
   - Si vous sélectionnez une porte, spécifiez un côté de porte.
   - Si vous sélectionnez un ascenseur, spécifiez un étage.
5. Cliquez sur Lancer.

Résultats

La liste des titulaires de cartes actifs qui disposent des droits d'utilisation du point d'accès sélectionné à l'instant spécifié, en fonction des règles d'accès en cours, est affichée.

Explorer

- Tester les droits d'accès d'un titulaire de cartes en fonction de ses identifiants

6.2.4 | Tester les droits d'accès d'un titulaire de cartes

Utilisez l'onglet *Diagnostic de titulaire de cartes* de l'Outil de diagnostic d'accès pour découvrir les points d'accès auxquels le titulaire de cartes a accès à un instant donné.

À savoir

L'outil de diagnostic de titulaire de cartes n'examine pas les identifiants de chaque titulaire de cartes. Vous pouvez affiner le diagnostic de droits d'accès du titulaire en cliquant sur l'onglet Diagnostic d'accès ( ).

Procédure

1. Sur la page d'accueil, cliquez sur Outils > Outil de diagnostic d'accès.
2. Dans la boîte de dialogue Outil de diagnostic d'accès, cliquez sur l'onglet Diagnostic de titulaire de cartes.
3. Sélectionnez la date et l'heure à évaluer avec l'outil. Seules les *règles d'accès* sont évaluées en fonction de la date et de l'heure spécifiées.
4. Sélectionnez le titulaire de cartes que vous souhaitez examiner avec l'outil. Vous pouvez également sélectionner un *identifiant* ou un visiteur au lieu d'un titulaire de cartes.
   Les entités actuellement inactives sont grisées.

5. Cliquez sur Lancer.

Résultats

La liste des points d'accès que le titulaire de cartes (ou visiteur) sélectionné est autorisé à utiliser à l'heure spécifiée, en fonction des règles d'accès en cours, est affichée.

6.2.4.1 | Tester les droits d'accès d'un titulaire de cartes en fonction de ses identifiants

Utilisez l'onglet Diagnostic d'accès de l'outil de diagnostic d'accès pour savoir pourquoi un titulaire de cartes muni d'un certain identifiant peut accéder ou non à une porte ou un ascenseur à un moment donné.

Procédure

1. Sur la page d'accueil, cliquez sur Outils > Outil de diagnostic d'accès.
2. Dans la boîte de dialogue Outil de diagnostic d'accès, cliquez sur l'onglet Diagnostic d'accès ().
3. Sélectionnez la date et l'heure à évaluer avec l'outil.
4. Sélectionnez le titulaire que vous souhaitez examiner. Vous pouvez également sélectionner un identifiant ou un visiteur au lieu d'un titulaire de cartes.
5. Si le titulaire de cartes sélectionné dispose de plusieurs identifiants, spécifiez celui que vous souhaitez examiner.
6. Sélectionnez un point d'accès à examiner.
   - Si vous sélectionnez une porte, spécifiez un côté de porte.
   - Si vous sélectionnez un ascenseur, spécifiez un étage.
7. Cliquez sur Lancer.

Résultats

L'outil crée un diagnostic basé sur la configuration actuelle du système, en prenant en compte les règles d'accès, ainsi que les dates d'activation et d'expiration du titulaire et de l'identifiant.
Sujet parent : Tester les droits d'accès d'un titulaire de cartes

6.2.5 | Dépannage : Échec de l'installation du pilote pour les lecteurs USB HID OMNIKEY

Si à chaque fois que vous essayez d'inscrire un identifiant avec un lecteur USB HID OMNIKEY, vous voyez un message d'erreur Windows indiquant que l'installation du pilote a échoué, voici une procédure que vous pouvez suivre pour résoudre le problème.

Avant de commencer

- Déconnectez le lecteur OMNIKEY de votre ordinateur.
- Fermez Security Desk et Config Tool.

À savoir

Ce problème survient généralement lorsque Windows ne trouve pas le pilote adapté pour le lecteur. Windows essaie alors de charger le pilote USB par défaut, ce qui peut donner l'impression que le lecteur fonctionne normalement, jusqu'à ce que vous observiez des comportements indésirables. Pour éviter de tels comportements, il est conseillé d'installer le pilote conçu par le fabricant pour ce type de lecteur.

Procédure

1. Vérifiez que votre lecteur OMNIKEY est compatible avec Security Center et configuré correctement.
   Pour la liste des appareils compatibles et des réglages de configuration, voir l'article KBA01374 de la Base de connaissances sur Genetec™ TechDoc Hub.
2. Installez le pilote en suivant les instructions fournies dans le manuel *OMNIKEY Smart Card Reader User Guide*.
   Vous pouvez obtenir ce guide sur le site de HID à l'adresse http://www.hidglobal.com/documents.
3. Une fois l'installation terminée, lancez Security Desk, puis vérifiez que le lecteur est activé.

4. Réessayez d'inscrire un identifiant.

Résultats

Le message d'erreur ne devrait plus apparaître.

7 | Référence de Security Desk

7.1 | Événements et actions dans Security Desk

7.1.1 | Types d'événements

Tous les événements dans Security Center sont associés à une *entité source*, qui est l'objet principal de l'événement.

Security Center prend en charge les types d'événements suivants :

Événement	Entité source	Description
La capacité à écrire sur un lecteur a été restaurée	Rôle Archiveur ou Archiveur auxiliaire	La capacité à écrire sur un lecteur a été restaurée.
Accès refusé : Violation antiretour	porte	Un titulaire de cartes a demandé l'accès à un secteur dans lequel il est déjà présent, ou a quitté un secteur qu'il n'a jamais pénétré.
Accès refusé : Deuxième titulaire de cartes obligatoire	porte	Deux titulaires de cartes doivent présenter leurs identifiants dans un délai donné et le délai a expiré. Cet événement ne s'applique qu'aux portes contrôlées par les unités Synergis™.
Accès refusé : Refusé par une règle d'accès	porte ou ascenseur	L'accès est refusé au titulaire de cartes en fonction de la règle d'accès.
Accès refusé : Capacité maximale atteinte	porte	Le titulaire de carte est refusé parce que la zone a atteint sa limite de capacité.
Accès refusé : Escorte non prise en charge par ce modèle d'unité	porte	La règle d'escorte de visiteur est appliquée à un secteur, mais l'unité contrôlant ses portes ne prend pas en charge cette fonctionnalité.
Accès refusé : Identifiant expiré	titulaire de cartes, identifiant, porte ou ascenseur	Un identifiant ayant expiré a été utilisé.
Accès refusé : Pas de superviseur de règle Premier entré	porte	La règle premier entré a été appliquée au secteur, et aucun superviseur n'est encore arrivé.
Accès refusé : Titulaire de cartes inactif	titulaire de cartes, porte ou ascenseur	Un titulaire de cartes avec un profil inactif a tenté d'accéder à une porte ou un ascenseur.
Accès refusé : Identifiant inactif	titulaire de cartes, identifiant, porte ou ascenseur	Un identifiant dont le profil est inactif a été utilisé.
Accès refusé : Privilèges insuffisants	porte ou ascenseur	L'accès est refusé au titulaire de cartes car il n'a pas le niveau d'accès requis. Cet événement ne s'applique qu'aux portes contrôlées par les unités Synergis™.

Événement	Entité source	Description
Accès refusé : Sas	porte	L'accès est refusé en raison d'une restriction de sas.
Accès refusé : Code PIN non valable	porte ou ascenseur	Le titulaire de cartes a saisi un code PIN non valable.
Accès refusé : Identifiant perdu	titulaire de cartes, identifiant, porte ou ascenseur	Un identifiant dont le vol a été déclaré a été utilisé.
Accès refusé : Aucune règle d'accès affectée	porte ou ascenseur	L'accès est refusé au titulaire de cartes car aucun droit d'accès ne lui est affecté.
Accès refusé : Hors plage horaire	porte ou ascenseur	La règle d'accès associée à ce titulaire de cartes ne s'applique pas à lors de la date ou de l'heure de l'horaire.
Accès refusé : Identifiant volé	titulaire de cartes, identifiant, porte ou ascenseur	Un identifiant volé a été utilisé.
Accès refusé : Identifiant non affecté	identifiant, porte ou ascenseur	Un identifiant qui n'a pas été affecté à un titulaire de cartes a été utilisé.
Accès refusé : Identifiant inconnu	porte ou ascenseur	Un identifiant qui n'est pas connu par le système Security Center a été utilisé.
Accès refusé : Carte valable, code PIN non valable	porte ou ascenseur	Une carte et un code PIN sont requis pour accéder au secteur, et le titulaire de cartes a saisi un code PIN non valable.
Accès refusé : L'accompagnateur du visiteur a été refusé	porte	Dans le cadre d'un visiteur accompagné, l'accès a été refusé à un visiteur ou un hôte.
Accès autorisé	titulaire de cartes, porte ou ascenseur	L'accès à une porte a été accordé à un titulaire de cartes en fonction des règles d'accès qui régissent la porte, l'ascenseur ou le secteur. Pour une porte de périmètre d'un sas : Lorsqu'un titulaire de cartes autorisé accède à la porte d'un sas, Security Center peut générer un événement *Accès autorisé* pour la porte même si la porte n'est pas déverrouillée (lorsqu'une autre porte de périmètre est déjà ouverte).
Panne de courant	unité de contrôle d'accès ou unité de détection d'intrusion	Panne de courant.
Porte de sas sur horaire d'accès libre	secteur	Une porte qui fait partie d'une configuration de sas est dotée d'un horaire de déverrouillage.
Porte de sas en mode de maintenance	secteur	Une porte qui fait partie d'une configuration de sas est en mode maintenance.
Mouvement qui s'adapte déclenché	caméra (analyse vidéo)	Du mouvement a été détecté sur une caméra dotée de fonctions d'analyse vidéo.
Alarme acquittée	alarme	Une alarme a été acquittée par un utilisateur, ou acquittée automatiquement par le système.

Événement	Entité source	Description
Alarme acquittée (secondaire)	alarme	Une alarme a été acquittée par un utilisateur avec le mode secondaire.
Alarme en cours d'analyse	alarme	Une alarme dotée d'une condition d'acquittement encore active a été placée en état *Analyse en cours*.
Condition d'alarme effacée	alarme	La condition d'acquittement de l'alarme a été effacée.
Alarme acquittée de force	alarme	Une alarme a été acquittée de force par un utilisateur doté de privilèges spéciaux.
Alarme déclenchée	alarme	Une alarme a été déclenchée.
Sas incorrectement configuré en mode antiretour physique	secteur	Sas incorrectement configuré en mode antiretour physique. Cette configuration n'est pas autorisée.
Un sas ne peut pas avoir une porte de périmètre sans capteur de porte configuré	secteur	Pour utiliser un sas, le système doit pouvoir savoir si une porte est ouverte ou non.
Un sas ne peut pas avoir qu'une seule porte de périmètre	secteur	Vous devez avoir au moins deux portes de périmètre pour créer un sas.
Antiretour désactivé : Réglages incorrects	secteur	Antiretour désactivé : Réglages incorrects.
Antiretour désactivé : Non pris en charge par les unités en mode serveur	secteur	Les unités n'ont pas été réglées en mode serveur. La disponibilité de l'antiretour dépend du mode de fonctionnement de l'unité. Pour en savoir plus sur les limitations des unités, voir Limitations dans Security Center.
Violation antiretour	secteur ou titulaire de cartes	Une demande a été reçue pour accéder à un secteur avec un identifiant de titulaire de cartes déjà présent dans le secteur, ou pour quitter un secteur avec un identifiant qui n'y est jamais entré.
Violation antiretour pardonnée	titulaire de cartes	Un opérateur de sécurité a accordé l'accès à un titulaire de cartes responsable d'une violation antiretour.
Application connectée	application ou rôle	Une application ou un rôle s'est connecté au Répertoire.
Application perdue	application ou rôle	Une application ou un rôle a perdu sa connexion au Répertoire.
Le chemin du dossier d'archivage est trop long	Rôle Archiveur ou Archiveur auxiliaire	Le chemin d'accès aux archives vidéo dépasse la longueur maximale autorisée par le système d’exploitation.
Le disque d'archivage a changé	Rôle Archiveur ou Archiveur auxiliaire	L'espace alloué sur un disque affecté au stockage d'archives par cet Archiveur est saturé, et l'Archiveur a basculé vers le disque spécifié suivant. Le nom du disque précédent et du disque actuel est indiqué dans le champ Description.
File d’attente d'archivage saturée	caméra	Une caméra (codeur vidéo) diffuse de la vidéo trop rapidement pour que l'Archiveur puisse écrire les paquets vidéo sur disque. Un problème de base de données de

Événement	Entité source	Description
		l'Archiveur peut également déclencher cet événement. Le nom de la caméra dont les paquets sont perdus est indiqué dans le champ Description.
Archivage arrêté	Rôle Archiveur ou Archiveur auxiliaire	L'archivage a été interrompu, car les disques affectés à l'archivage sont saturés. Cet événement est toujours déclenché en cas d'événement *Disque saturé*.
Actif déplacé	actif	Un actif a été déplacé.
Actif hors ligne	actif	La puce RFID d'un actif a basculé hors ligne.
Actif en ligne	actif	La puce RFID d'un actif a basculé en ligne.
Alarme sonore	caméra	Un son a été détecté par un micro associé à une caméra.
Événement d'analyse audio	caméra (analyse vidéo)	Un événement d'analyse audio a été détecté sur une caméra dotée de fonctions d'analyse audio.
Tâche d'impression de badges annulée	utilisateur	Un utilisateur a annulé une tâche d'impression de badge.
Tâche d'impression de badges terminée	utilisateur	Un utilisateur a terminé une tâche d'impression de badge.
Tâche d'impression de badges mise en file d'attente	utilisateur	Un utilisateur a mis en fille d'attente une tâche d'impression de badge.
Panne de batterie	unité de contrôle d'accès ou unité de détection d'intrusion	Défaillance de la batterie.
Blocage de caméra démarré	caméra	Un utilisateur a bloqué l'affichage d'un flux vidéo par d'autres utilisateurs du système.
Blocage de caméra arrêté	caméra	Un utilisateur a débloqué l'affichage d'un flux vidéo par d'autres utilisateurs du système.
Archivage de la caméra arrêté	caméra	La caméra est gérée par un horaire d'archivage actif, mais l'Archiveur ne reçoit pas le flux vidéo.
Sabotage de caméra	caméra (analyse vidéo)	Un problème est survenu. Il peut s'agir de l'obstruction partielle ou complète du champ de la caméra, d'un changement brutal du champ de la caméra, ou d'une perte de mise au point.
Impossible d'écrire à l'emplacement spécifié	Rôle Archiveur ou Archiveur auxiliaire	L'Archiveur ne parvient pas à écrire sur un disque particulier. Le chemin d'accès au lecteur est indiqué dans le champ Description.
Impossible d'écrire sur aucun disque	Rôle Archiveur ou Archiveur auxiliaire	L'Archiveur ne parvient à écrire sur aucun disque. Une telle situation peut survenir pour les raisons suivantes : Lorsque les droits d'accès en écriture sur un lecteur partagé ont été annulés. Lorsque les disques partagés sont inaccessibles. Lorsqu'un lecteur partagé n'existe plus. L'archivage est alors interrompu. L'Archiveur réévalue l'état des disques toutes les 30 secondes.

Événement	Entité source	Description
Seuil de capacité atteint	Zone de stationnement	La capacité de la zone de stationnement a atteint le seuil défini dans le Gestionnaire RAPI.
Temps de commodité démarré	règle de stationnement	La partie temps de commodité de la session de stationnement a démarré.
Identifiant expiré	identifiant	Un identifiant a expiré.
Foule détectée	caméra (analyse vidéo)	Une foule ou une file d'attente a été détectée sur une caméra dotée de fonctions d'analyse vidéo.
Événement personnalisé	à l'échelle du système	Un événement personnalisé est un événement ajouté après l'installation initiale du système. Les événements définis lors de l'installation du système sont appelés événements système. Les événements personnalisés peuvent être définis par l'utilisateur ou ajoutés automatiquement par l'installation de modules externes. Contrairement aux événements système, les événements personnalisés peuvent être renommés ou supprimés.
Base de données perdue	Rôle Archiveur ou Archiveur auxiliaire	La connexion à la base de données d'un rôle a été perdue. Lorsque cet événement concerne une base de données de rôle, cela peut indiquer que le serveur de bases de données est défaillant ou injoignable par le serveur de rôle. Lorsque cet événement concerne la base de données du Répertoire, la seule action disponible est *Envoyer un e-mail*, car toutes les autres actions requièrent une connexion valable à la base de données du Répertoire.
Base de données récupérée	Rôle Archiveur ou Archiveur auxiliaire	La connexion à la base de données de rôle a été rétablie.
Pêne dormant engagé	zone	Le pêne dormant d'une porte a été engagé.
Pêne dormant rétracté	zone	Le pêne dormant d'une porte a été rétracté.
Alarme de direction	caméra (analyse vidéo)	Une alarme de direction a été déclenchée sur une caméra dotée de fonctions d'analyse vidéo.
Seuil de saturation des disques dépassé	Rôle Archiveur ou Archiveur auxiliaire	L'espace disque alloué à l'archivage a dépassé le seuil de saturation (par défaut = 90%). Cela peut se produire en raison d'une sous-évaluation de l'espace disque nécessaire ou d'une autre application qui utilise plus d'espace disque que prévu. Si 100 % de l'espace affecté au lecteur est utilisé, l'Archiveur commence à supprimer les fichiers d'archive les plus anciens, afin de libérer de l'espace sur le disque pour les nouvelles archives.
Disques saturés	Rôle Archiveur ou Archiveur auxiliaire	Un disque affecté à l'archivage est saturé et l'Archiveur est incapable de libérer de l'espace sur le disque en supprimant d'autres fichiers vidéo. Cet événement peut survenir lorsqu'une autre application a consommé tout l'espace disque réservé à Security Center, ou lorsque l'option Supprimer fichiers plus anciens si disques pleins n'est pas sélectionnée dans Server Admin. L'archivage est alors interrompu. L'Archiveur réévalue l'espace disque toutes les 30 secondes.

Événement	Entité source	Description
Porte fermée	porte	La porte s'est refermée. Pour que cet événement soit généré, la porte doit être équipée d'un capteur de contact.
Porte forcée	porte	La porte est verrouillée, mais le capteur de contact indique que la porte est ouverte.
Poignée au repos	zone	La poignée est au repos et la porte est fermée.
Poignée actionnée	zone	La poignée a été actionnée.
Porte verrouillée	porte	La porte est considérée comme verrouillée dans Security Center.
Maintenance de porte terminée	porte	Le mode maintenance a été désactivé pour la porte.
Maintenance de porte démarrée	porte	La porte a été placée en mode maintenance.
Porte déverrouillée manuellement	porte	Dans Security Desk, un utilisateur a manuellement déverrouillé une porte.
Porte hors ligne : L'appareil est hors ligne	porte	Un ou plusieurs appareils associés à cette porte ont basculé hors ligne.
Porte ouverte	porte	La porte a été ouverte. Pour que cet événement soit généré, la porte doit être équipée d'un capteur de contact.
Porte entrebâillée trop longtemps	porte	La porte est restée ouverte trop longtemps. Pour activer cet événement, vous devez définir l'événement déclencheur sur ON dans la section Porte maintenue de la page Propriétés de la porte dans Config Tool.
Porte déverrouillée	porte	La porte a été déverrouillée.
Porte non sécurisée	porte	La porte a été déverrouillée, mais le verrou de porte indique que la porte est verrouillée. Pour que cet événement soit généré, la porte doit être équipée d'un capteur de porte, d'un verrou de porte et d'un capteur de verrou.
Porte sécurisée	porte	La porte a été correctement fermée et verrouillée après un événement *Porte non sécurisée*. Pour que cet événement soit généré, la porte doit être équipée d'un capteur de porte, d'un verrou de porte et d'un capteur de verrou.
Double balayage désactivé	titulaire de cartes, identifiant ou porte	La porte a été verrouillée et un événement associé a été arrêté.
Double balayage activé	titulaire de cartes, identifiant ou porte	La porte a été déverrouillée et un événement associé a été déclenché.
Défaillance du support de périphérique	caméra	Après redémarrage d'une unité, la vidéo enregistrée sur périphérique n'est plus accessible.
Ascenseur hors ligne : L'appareil est hors ligne	ascenseur	Un ou plusieurs appareils associés à cet ascenseur ont basculé hors ligne.
Fin de sabotage de caméra	caméra (analyse vidéo)	Un dysfonctionnement, potentiellement entraîné par un

Événement	Entité source	Description
		sabotage de caméra, a été résolu.
Entité expirée	identifiant	Un identifiant ou le titulaire de cartes associé a expiré (son état est passé sur *Expiré*).
Expiration imminente	titulaire de cartes ou identifiant	Security Center génère cet événement pour prévenir que la date d'expiration d'une entité est proche. Le nombre de jours avant l'échéance doit être spécifié pour cet événement.
Avertissement d'entité	toute entité	Une alerte a été émise concernant le bon fonctionnement de cette entité.
Entrée supposée	titulaire de cartes ou porte	L'accès à une porte, un ascenseur ou un secteur a été accordé à un titulaire de cartes, et l'entrée est présumée, car aucun capteur de prote n'est configuré.
Entrée détectée	titulaire de cartes ou porte	L'accès à une porte ou un secteur a été accordé à un titulaire de cartes, et l'entrée a été détectée. Pour que cet événement soit généré, vous devez configurer un capteur d'entrée du bon côté de la porte. En l'absence de capteurs d'entrée sur la porte, l'événement est généré en fonction de l'entrée du capteur de porte.
Visage détecté	caméra (analyse vidéo)	Un visage a été détecté sur une caméra dotée de fonctions d'analyse vidéo.
Visage reconnu	caméra (analyse vidéo)	Un visage d'une *liste de véhicules recherchés* a été détecté sur une caméra dotée de fonctions d'analyse vidéo.
Fichier supprimé	caméra	Un fichier vidéo associé à une caméra a été supprimé, car sa durée de conservation est dépassée ou parce que le disque de stockage est saturé.
Échec de la mise à niveau du micrologiciel	unité de contrôle d'accès	La mise à niveau du micrologiciel d'une unité de contrôle d'accès a échoué.
Mise à niveau du micrologiciel lancée	unité de contrôle d'accès	La mise à niveau du micrologiciel d'une unité de contrôle d'accès a démarré.
Succès de la mise à niveau du micrologiciel	unité de contrôle d'accès	La mise à niveau du micrologiciel d'une unité de contrôle d'accès s'est terminée avec succès.
Premier entré	secteur	Un titulaire de cartes a pénétré dans un secteur vide.
Accès à un étage	ascenseur	Un bouton d'ascenseur a été activé.
Vitre brisée	zone	Bris de glace.
Sabotage matériel	unité de contrôle d'accès, porte, ascenseur ou zone	L'entrée sabotage d'une unité a été déclenchée.
Dysfonctionnement	Rôle Surveillance de l'état	Un dysfonctionnement est survenu.
Carte des risques modifiée	caméra (analyse vidéo)	Une modification a été détectée dans une zone de carte thermique sur une caméra dotée de fonctions d'analyse

Événement	Entité source	Description
		vidéo.
Alarme d'entrée activée	entrée sur unité de détection d'intrusion	L'entrée est passée en état *alarme*.
Alarme d'entrée restaurée	entrée sur unité de détection d'intrusion	L'entrée a quitté un état *alarme*.
Entrée contournée	entrée sur unité de détection d'intrusion	L'entrée est passée en état *contourné*.
Contournement d'entrée restaurée	entrée sur unité de détection d'intrusion	L'entrée a quitté un état *contourné*.
État d'entrée modifié : Entrée active	entrée sur caméra, unité de contrôle d'accès ou unité de détection d'intrusion	L'entrée est passée en état *actif*.
État d'entrée modifié : Entrée normale	entrée sur caméra, unité de contrôle d'accès ou unité de détection d'intrusion	L'entrée est passée en état *normal*.
État d'entrée modifié : Problème d'entrée	entrée sur unité de contrôle d'accès ou unité de détection d'intrusion	L'entrée est passée en état *problème*.
État Défaillance de l’alimentation du module d'interface actif	unité de contrôle d'accès	L’alimentation CA (courant alternatif) d'un module d'interface est en panne.
État Défaillance de l’alimentation du module d'interface restauré	unité de contrôle d'accès	L’alimentation CA (courant alternatif) d'un module d'interface a été restaurée.
État Défaillance de la batterie du module d'interface actif	unité de contrôle d'accès	La batterie d'un module d'interface est en panne.
État Défaillance de la batterie du module d'interface restauré	unité de contrôle d'accès	La batterie d'un module d'interface a été restaurée.
Module d'interface hors ligne	unité de contrôle d'accès	Le module d'interface a basculé hors ligne.
Module d'interface en ligne	unité de contrôle d'accès	Le module d'interface a basculé en ligne.
État Sabotage du module d'interface actif	unité de contrôle d'accès	L'entrée sabotage d'un module d'interface a été déclenchée.
État Sabotage du module d'interface restauré	unité de contrôle d'accès	L'entrée sabotage d'un module d'interface est revenue à la normale.
Sas non pris en charge par l'unité	secteur	Un sas est activé pour un secteur, mais l'unité de contrôle d'accès qui contrôle les portes ne prend pas en charge cette fonctionnalité.
Entrée de confinement de sas active	secteur	Le confinement a été activé pour un sas.
Entrée de confinement de sas normale	secteur	Le confinement a été désactivé pour un sas.

Événement	Entité source	Description
Entrée de contournement de sas active	secteur	L'annulation de la configuration par défaut d'un sas a été activée.
Entrée de contournement de sas normale	secteur	L'annulation de la configuration par défaut d'un sas a été désactivée.
Alarme de secteur de détection d'intrusion activée	secteur de détection d'intrusion	Alarme de secteur de détection d'intrusion activée.
Armement du secteur de détection d'intrusion	secteur de détection d'intrusion	Une unité de détection d'intrusion est en cours d'armement.
Armement du secteur de détection d'intrusion reporté	secteur de détection d'intrusion	Armement du secteur de détection d'intrusion reporté.
Alarme annulée du secteur de détection d'intrusion	secteur de détection d'intrusion	L'alarme du secteur de détection d'intrusion est annulée.
Le secteur de détection d'intrusion a annulé la demande de report	secteur de détection d'intrusion	La demande de report du secteur de détection d'intrusion a été annulée.
Demande de désarmement du secteur de détection d'intrusion	secteur de détection d'intrusion	La demande de report du secteur de détection d'intrusion a été annulée.
Secteur de détection d'intrusion désarmé	secteur de détection d'intrusion	Le secteur de détection d'intrusion est désarmé.
Contrainte de secteur de détection d'intrusion	secteur de détection d'intrusion	Le secteur de détection d'intrusion est désarmé sous la contrainte.
Délai d'entrée de secteur de détection d'intrusion activé	secteur de détection d'intrusion	Délai d'entrée de secteur de détection d'intrusion activé.
Armement forcé du secteur de détection d'intrusion	secteur de détection d'intrusion	Une unité de détection d'intrusion est en cours d'armement forcé.
Contournement des entrées de secteur de détection d'intrusion activé	secteur de détection d'intrusion	Le contournement des entrées de secteur de détection d'intrusion est activé.
Contournement des entrées de secteur de détection d'intrusion désactivé	secteur de détection d'intrusion	Le contournement des entrées de secteur de détection d'intrusion est désactivé.
Problème d'entrée de secteur de détection d'intrusion	secteur de détection d'intrusion	Problème d'entrée de secteur de détection d'intrusion.
Demande d'armement global du secteur de détection d'intrusion	secteur de détection d'intrusion	Une demande d'armement global du secteur de détection d'intrusion est émise.
Armement global du secteur de détection d'intrusion	secteur de détection d'intrusion	L'armement global du secteur de détection d'intrusion est effectif.
Demande d'armement du périmètre de secteur de détection d'intrusion	secteur de détection d'intrusion	Une demande d'armement du périmètre du secteur de détection d'intrusion est émise.

Événement	Entité source	Description
Périmètre de secteur de détection d'intrusion armé	secteur de détection d'intrusion	Le périmètre de secteur de détection d'intrusion est armé.
Demande d'armement du secteur de détection d'intrusion reportée	secteur de détection d'intrusion	L'armement du secteur de détection d'intrusion est reporté.
Contournement des entrées d'unité de détection d'intrusion activé	unité de détection d'intrusion	Le contournement des entrées d'unité de détection d'intrusion est activé.
Contournement des entrées d'unité de détection d'intrusion désactivé	unité de détection d'intrusion	Le contournement des entrées d'unité de détection d'intrusion est désactivé.
Problème d'entrée d'unité de détection d'intrusion	unité de détection d'intrusion	Problème d'entrée d'unité de détection d'intrusion.
Altération d'unité de détection d'intrusion	unité de détection d'intrusion	L'unité de détection d'intrusion a été altérée.
Configuration non valable dans l'unité	unité vidéo	La configuration de l'unité est non valable.
Valeurs de chiffrement personnalisées incorrectes	Rôle Archiveur ou Archiveur auxiliaire	L'Archiveur émet cet avertissement au démarrage et toutes les 5 minutes si l'une des valeurs de chiffrement personnalisées (valeur de départ ou clé de chiffrement) fournies dans Server Admin est incorrecte.
Inventaire réinitialisé	zone de stationnement	L'inventaire d'une zone de stationnement à été remise à zéro afin de pouvoir réinitialiser l'occupation de la zone.
Dernier sorti	secteur	Le dernier titulaire de cartes a quitté un secteur.
Identification de plaque	Toute règle d'alerte	Une lecture de plaque d'immatriculation a été trouvée dans une liste de véhicules recherchés, une règle de dépassement horaire ou une restriction de permis.
Plaque d'immatriculation lue	Unité de RAPI ou Genetec Patroller™	Une plaque d'immatriculation a été lue.
Signet en direct ajouté	caméra	Un utilisateur a ajouté un signet à de la vidéo en direct.
Serrure déverrouillée	zone	Événement associé à une entité zone.
Serrure verrouillée	zone	Événement associé à une entité zone.
Présence prolongée	caméra (analyse vidéo)	Une présence trop prolongée a été détectée dans l'enregistrement vidéo.
Batterie faible	actif	La batterie de la puce RFID d'un actif est presque épuisée.
Macro interrompue	macro	L'exécution d'une macro a échoué.
Macro lancée	macro	L'exécution d'une macro a démarré.
Station manuelle activée	porte	Quelqu'un a activé le système d'ouverture d'urgence de la

Événement	Entité source	Description
		porte (station manuelle activée).
État normal de la station manuelle rétabli	porte	L'ouverture d'urgence de la porte (station manuelle activée) a été ramenée à sa position de fonctionnement normal.
Macro terminée	macro	L'exécution d'une macro s'est déroulée normalement.
Hôte de queue manquant	porte	L'hôte de queue d'une délégation de visiteurs à deux hôtes n'a pas badgé.
Mouvement	caméra	Mouvement détecté.
Mouvement absent	caméra	Cet événement se produit suite à un événement *Mouvement présent* lorsque le mouvement (mesuré en terme de nombre de blocs de mouvement) tombe en dessous du « seuil de mouvement absent » pendant au moins 5 secondes.
Mouvement présent	caméra	Cet événement se produit lorsqu'un mouvement a été confirmé.
Unités multiples configurées pour le sas	secteur	Toutes les portes qui appartiennent à un même sas doivent être contrôlées par la même unité.
Aucune entrée détectée	titulaire de cartes ou porte	L'accès à une porte ou un secteur a été accordé à un titulaire de cartes, mais aucune entrée n'a été détectée. Pour que cet événement soit généré, vous devez configurer un capteur de porte du bon côté de la porte.
Aucune correspondance	liste de véhicules recherchés	Un véhicule n'a pas été détecté dans la liste de véhicules recherchés associée à l'unité Sharp.
Aucun paquet RTP perdu durant la dernière minute	caméra	L'Archiveur a reçu tous les paquets RTP durant la minute écoulée.
Changement de condition d'objet	caméra (analyse vidéo)	Un objet a subitement changé de direction ou de vitesse (comme lorsqu'une personne se met à courir ou tombe).
Compte objet modifié	caméra (analyse vidéo)	Un changement a été détecté dans le compte d'objets sur une caméra dotée de fonctions d'analyse vidéo.
Compte objet atteint	caméra (analyse vidéo)	Une limite de nombre d'objets a été atteinte sur une caméra dotée de fonctions d'analyse vidéo.
Objet a franchi la ligne	caméra (analyse vidéo)	Un objet a franchi une ligne prédéfinie.
Objet détecté	caméra (analyse vidéo)	Un objet est présent dans le champ de la caméra.
Objet détecté dans le champ	caméra (analyse vidéo)	Un objet a été détecté dans une zone surveillée pour les intrusions sur une caméra dotée de fonctions d'analyse vidéo.
Direction objet modifiée	caméra (analyse vidéo)	Un objet a été détecté en train de changer de direction sur une caméra dotée de fonctions d'analyse vidéo.
Objet entré	caméra (analyse vidéo)	Un objet est entré dans le champ de la caméra.
Objet sorti	caméra (analyse vidéo)	Un objet est sorti du champ de la caméra.

Événement	Entité source	Description
Objet suit l'itinéraire	caméra (analyse vidéo)	Un objet suit un itinéraire prédéfini, dans une direction particulière.
Objet parti	caméra (analyse vidéo)	Un objet est entré et sorti du champ de la caméra.
Objet fusionné	caméra (analyse vidéo)	Deux objets distincts ont fusionné dans le champ de la caméra.
Objet enlevé	caméra (analyse vidéo)	Un objet a été retiré du champ de la caméra.
Objet séparé	caméra (analyse vidéo)	Un objet présent dans le champ de la caméra s'est scindé en deux objets.
Objet arrêté	caméra (analyse vidéo)	Un objet en mouvement s'est arrêté.
Vélocité objet modifiée	caméra (analyse vidéo)	Un objet a été détecté en train de changer de vitesse sur une caméra dotée de fonctions d'analyse vidéo.
Échec du déchargement	Genetec Patroller™	Un déchargement du Genetec Patroller™ vers Security Center a échoué.
Déchargement réussi	Genetec Patroller™	Un déchargement du Genetec Patroller™ vers Security Center a réussi.
Temps payé démarré	règle de stationnement	La durée de stationnement a été payée sur une borne de paiement ou via une app mobile.
Nombre d'individus remis à zéro	secteur	Le nombre d'individus comptés dans un secteur a été remis à 0.
Chute d'une personne	caméra (analyse vidéo)	La chute d'une personne a été détectée par la caméra.
Personne qui court	caméra (analyse vidéo)	Une personne qui court a été détectée par la caméra.
Personne qui glisse	caméra (analyse vidéo)	Une personne qui glisse a été détectée par la caméra.
Signet de lecture ajouté	caméra	Un utilisateur a ajouté un signet à de la vidéo enregistrée.
Seuil de protection dépassé	Rôle Archiveur ou Archiveur auxiliaire	Le Seuil limite de vidéo protégé configuré sur l'Archiveur a été dépassé. Vous pouvez surveiller le pourcentage d'espace disque occupé par les fichiers vidéo protégés sur la page Statistiques de l'onglet Ressources de l'Config Tool.
PTZ activé	caméra (PTZ)	Un utilisateur a commencé à utiliser le PTZ qui était inactif. Le champ spécifie l'utilisateur ayant activé le PTZ. Cet événement est créé à chaque fois qu'un utilisateur différent prend le contrôle du PTZ, même si le PTZ est encore actif.
PTZ verrouillé	caméra (PTZ)	Un utilisateur essaie d'actionner le PTZ alors qu'il est verrouillé par un autre utilisateur ayant une priorité sur PTZ supérieure. Le champ indique l'ordinateur, le type d'application et l'utilisateur qui détient actuellement le verrou de PTZ.
PTZ arrêté	caméra (PTZ)	Le PTZ n'a pas été manipulé depuis un laps de temps prédéfini. Le champ indique le dernier utilisateur à avoir

Événement	Entité source	Description
		utilisé le PTZ.
Zoom PTZ par utilisateur	caméra (PTZ)	Un utilisateur a actionné le zoom de PTZ. Le champ Description indique l'utilisateur ayant effectué le zoom. Les événements *Zoom PTZ par utilisateur* suivants sont générés si un autre utilisateur active le zoom de PTZ, ou si le premier utilisateur active le zoom après l'expiration du délai d'inactivité.
Zoom PTZ par utilisateur arrêté	caméra (PTZ)	Aucun zoom de PTZ n'a pas été effectué depuis un laps de temps prédéfini. Le champ indique le dernier utilisateur à avoir utilisé le zoom de PTZ.
Réception de paquets RTP depuis plusieurs sources	caméra	L'Archiveur reçoit plusieurs flux d'une même caméra. IMPORTANT : Lorsque cette situation rare survient, l'Archiveur ne peut pas reconnaître le bon flux en examinant l'adresse IP source à cause des NAT (Network Address Translators ou traducteurs d'adresses réseau) et choisit alors un flux au hasard. Cela peut donc entraîner l'archivage du mauvais flux vidéo. Toutefois, l'adresse IP et le numéro de port des deux flux sont indiqués dans le champ, et les deux sources sont indiquées. Vous pouvez identifier l'unité défectueuse à l'origine du conflit.
Problème d'enregistrement	caméra	Problème d'enregistrement de la caméra. Il peut s'agir d'une erreur d'écriture sur disque, d'écriture dans la base de données de l'Archiveur, ou d'un problème de diffusion vidéo en continu. Si vous rencontrez cette erreur, contactez votre administrateur système pour résoudre le problème.
Enregistrement démarré (alarme)	caméra	L'enregistrement d'une caméra a démarré suite au déclenchement d'une alarme.
Enregistrement démarré (continu)	caméra	L'enregistrement d'une caméra a été lancé par un horaire d'archivage continu.
Enregistrement démarré (source externe)	caméra	L'enregistrement d'une caméra a démarré suite à l'action *Démarrer l'enregistrement*. Cette action peut avoir été déclenchée par un autre événement ou exécutée par une macro.
Enregistrement démarré (mouvement)	caméra	L'enregistrement d'une caméra a démarré en raison d'une détection de mouvement.
Enregistrement démarré (utilisateur)	caméra	L'enregistrement d'une caméra a été lancé manuellement par un utilisateur.
Enregistrement arrêté (alarme)	caméra	L'enregistrement d'une caméra a été arrêté car la durée d'enregistrement après alarme est écoulée.
Enregistrement arrêté (continu)	caméra	L'enregistrement d'une caméra a été arrêté car elle n'est plus couverte par un horaire d'archivage continu.
Enregistrement arrêté (source externe)	caméra	L'enregistrement d'une caméra a été arrêté suite à l'action Arrêter l'enregistrement. Cette action peut avoir été déclenchée par un autre événement ou exécutée par une macro.

Événement	Entité source	Description
Enregistrement arrêté (mouvement)	caméra	L'enregistrement d'une caméra a été arrêté car le mouvement a cessé.
Enregistrement arrêté (utilisateur)	caméra	L'enregistrement d'une caméra a été arrêté manuellement par un utilisateur.
Demande de passage	porte	Quelqu'un a appuyé sur le bouton de déverrouillage de porte ou a déclenché une demande de sortie sur détection de mouvement. L'événement *Demande de passage* est doté de filtres particuliers pour assurer la compatibilité avec les appareils de demande de sortie sur détection de mouvement. Réglez ces propriétés dans l'onglet Config Tool > Porte > Propriétés.
Demande de passage (état normal)	porte	Aucune demande de sortie en cours.
Paquets RTP perdus	caméra	Des paquets RTP n'ont jamais été reçus par l'Archiveur. Ceci peut se produire lorsque les paquets sont perdus sur le réseau ou si l'Archiveur n'a pas le temps de traiter tous les paquets qu'il reçoit de sa carte réseau. Le champ indique alors le nombre de paquets perdus depuis la dernière génération de l'événement (pas plus qu'une fois par minute).
Accès contrôlé sur horaire	ascenseur	L'horaire d'accès contrôlé aux étages d'ascenseurs est entré en vigueur.
Libre accès sur horaire	ascenseur	L'horaire d'accès libre aux étages d'ascenseurs est entré en vigueur.
Verrouillage sur horaire	porte	L'horaire de déverrouillage de la porte a expiré, le verrou est appliqué (la porte est verrouillée).
Déverrouillage sur horaire	porte	Le verrou de la porte est déverrouillé en raison d'un horaire de déverrouillage.
Déverrouillage sur horaire ignoré :pas de superviseur de règle Premier entré	porte	L'horaire de déverrouillage de porte est ignoré, car la condition imposée par la règle premier entré n'a pas encore été satisfaite.
Session terminée	règle de stationnement	Le véhicule a quitté la zone de stationnement.
Session démarrée	règle de stationnement	Le véhicule a pénétré la zone de stationnement.
Signal perdu	caméra	Le signal de la caméra a été perdu.
Signal retrouvé	caméra	Le signal de la caméra a été récupéré.
Synchronisation terminée : Système externe	Rôle Active Directory	La synchronisation d'un système externe est terminée.
Erreur de synchronisation : Système externe	Rôle Active Directory	La synchronisation d'un système externe a entraîné une erreur.
Synchronisation lancée : Système externe	Rôle Active Directory	La synchronisation d'un système externe a démarré.

Événement	Entité source	Description
Talonnage	caméra (analyse vidéo)	Deux personnes ont pénétré un secteur sécurisé en rapide succession.
Alarme de température	unité vidéo	La température de l'unité vidéo a dépassé le seuil de sécurité.
Niveau de risque effacé	niveau de risque	Un niveau de risque a été effacé.
Niveau de risque défini	niveau de risque	Un niveau de risque a été défini.
Transmission perdue	caméra	L'Archiveur est toujours connecté à la caméra, mais n'a pas reçu de paquets vidéo depuis plus de 5 secondes.
Transmission rétablie	caméra	L'Archiveur reçoit à nouveau des paquets vidéo de la caméra.
Événement d'analyse vidéo non identifié	caméra (analyse vidéo)	Un événement d'analyse vidéo générique a été émis, mais il n'a pas encore été associé à un événement Security Center. CONSEIL : Vous pouvez vérifier les informations de sous-type dans les métadonnées d'analyse.
Unité connectée	unité	La connexion à une unité a été établie ou restaurée.
L'unité n'a pas répondu à la demande de vidéo sur périphérique	caméra	Événement associé à une caméra qui enregistre directement sur l'unité.
Unité perdue	unité	La connexion à une unité a été perdue.
Échec de la synchronisation de l'unité	unité de contrôle d'accès	La synchronisation de l'unité avec le Gestionnaire d'accès a échoué.
La synchronisation de l'unité a démarré	unité de contrôle d'accès	La synchronisation de l'unité avec le Gestionnaire d'accès a démarré.
La synchronisation de l'unité a réussi	unité de contrôle d'accès	La synchronisation de l'unité avec le Gestionnaire d'accès s'est terminée avec succès.
Mise à jour publiée	Genetec Patroller™, Sharp mobile	Une mise à jour a été traitée, et elle est prête à être déployée sur Genetec Patroller™.
Échec de la mise à jour	Genetec Patroller™, Sharp mobile	Une mise à jour sur une unité Genetec Patroller™ ou Sharp mobile a échoué, ou le fichier n'a pas pu être synchronisé sur un ordinateur Genetec Patroller™.
Installation de la mise à jour terminée	Genetec Patroller™, Sharp mobile	Une mise à jour a été effectuée sur une unité Genetec Patroller™ ou Sharp mobile, et aucun redémarrage n'est nécessaire.
Installation de la mise à jour lancée	Genetec Patroller™, Sharp mobile	Un utilisateur a lancé une mise à jour sur un Genetec Patroller™ en cliquant sur l'icône « Mettre à jour ».
Désinstallation de la mise à jour terminée	Genetec Patroller™, Sharp mobile	Une désinstallation sur une unité Genetec Patroller™ ou Sharp mobile est terminée.
Désinstallation de la mise à jour lancée	Genetec Patroller™, Sharp mobile	Un utilisateur a lancé une désinstallation sur un Genetec Patroller™ en cliquant sur l'icône « Rétablir ».

Événement	Entité source	Description
Déconnexion d'un utilisateur	utilisateur	Un utilisateur s'est déconnecté d'une application Security Center.
Connexion d'un utilisateur	utilisateur	Un utilisateur s'est connecté à une application Security Center.
Validation du temps payé	règle de stationnement	Le temps de commodité ou le délai de stationnement payant a expiré pour la session de stationnement.
Infraction détectée	règle de stationnement	Le temps de commodité, le délai de grâce ou le délai de stationnement payant a expiré pour la session de stationnement.
Infraction appliquée	règle de stationnement	Le véhicule en infraction a été verbalisé.
Visiteur égaré	porte	Un visiteur n’a pas badgé dans les délais impartis, après un hôte de la délégation ou le visiteur précédent.
Tentative de connexion VRM	Rôle Archiveur	L'Archiveur a essayé de se connecter à une unité VRM.
Échec de connexion VRM	Rôle Archiveur	L'Archiveur n'a pas réussi à se connecter à une unité VRM.
Fenêtre fermée	zone	Une fenêtre physique a été fermée.
Fenêtre ouverte	zone	Une fenêtre physique a été ouverte.
Zone armée	zone	Une zone a été armée.
Zone désarmée	zone	Une zone a été désarmée.
Maintenance de zone terminée	Zone d'E/S	Une zone d'E/S est sortie de mode maintenance.
Maintenance de zone lancée	Zone d'E/S	Une zone d'E/S est passée en mode maintenance.
Zone hors ligne	Zone d'E/S	Une zone d’E/S est hors ligne.

Pour obtenir la liste des événements pouvant être utilisés avec l'analyse vidéo KiwiVision™, voir Événements à surveiller dans Security Desk.

7.1.2 | Types d'actions

Toutes les actions dans Security Center sont associées à une entité cible, affectée par l'action. Des paramètres supplémentaires sont indiqués dans la colonne *Description*. Tous les paramètres doivent être configurés pour que l'action soit valable.

Action	Description
Ajouter un signet	Ajoute un *signet* à l'enregistrement d'une *caméra*. **Caméra** Sélectionnez la caméra. **Message** Texte du signet.

Action	Description
Armer un secteur de détection d'intrusion	Arme un *secteur de détection d'intrusion*. **Secteur de détection d'intrusion** Sélectionnez un secteur de détection d'intrusion. **Global** Arme tous les capteurs au sein du secteur de détection d'intrusion sélectionné. Tout capteur peut déclencher l'alarme en cas d'activation. **Périmètre** Arme uniquement les capteurs désignés en tant que capteurs de périmètre. L'activité sur les capteurs à l'intérieur du secteur, comme les capteurs de mouvement, est ignorée. **Instantané** Arme le secteur immédiatement. **Délai** Arme le secteur au bout d'un délai. Si vous ne spécifiez pas la durée, la valeur par défaut du tableau est utilisée. **Mode d'armement** **Normal** Arme le secteur de détection d'intrusion normalement. Les secteurs avec des capteurs actifs ou en mode problème restent désarmés. **Forcer** Si le secteur n’est pas prêt pour l’armement normal, cette option force l'armement du secteur. Cette option ignore à titre temporaire les capteurs actifs ou en mode problème pendant la séquence d'armement. Si un capteur ignoré retrouve un état normal pendant l’armement, l’activité peut déclencher l'alarme. **Contourner** Si le secteur n’est pas prêt pour l’armement normal, cette option contourne automatiquement les capteurs actifs ou en mode problème avant l'armement du secteur. Les capteurs restent contournés pendant que le secteur est armé. Désarmer le secteur supprime le contournement.
Armer la zone	Arme une *zone virtuelle*. **Zone** Sélectionnez une zone virtuelle.
Bloquer et débloquer la vidéo	Bloque ou débloque une caméra pour les autres utilisateurs du système. **Bloquer/Débloquer** Spécifiez si l'action doit bloquer ou débloquera la caméra. **Caméra** Sélectionnez la caméra.

Action	Description
	Fin Sélectionnez la durée de blocage de la caméra : **Pour** La vidéo est bloquée pour la durée spécifiée. **Indéfiniment** La vidéo est bloquée jusqu'à ce que vous la déverrouilliez manuellement. **Niveau utilisateur** Sélectionnez le niveau utilisateur minimum. L'affichage de la vidéo est bloqué pour tous les utilisateurs dont le niveau est inférieur au niveau sélectionné.
Annuler le report de l'armement du secteur de détection d'intrusion	Annule le report de l'armement d'un *secteur de détection d'intrusion*. **Secteur de détection d'intrusion** Sélectionnez le secteur de détection d'intrusion.
Effacer les tâches	Efface la liste des tâches des moniteurs Security Desk spécifiés. **Destination** Sélectionnez l'une des options suivantes : **Utilisateur** Tous les moniteurs de toutes les applications Security Desk connectées avec le nom d'utilisateur spécifié. **Surveiller** Moniteur Security Desk particulier identifié par un nom de machine et un ID de moniteur.
Désarmer le secteur de détection d'intrusion	Désarme le *secteur de détection d'intrusion* sélectionné. **Secteur de détection d'intrusion** Sélectionnez le secteur de détection d'intrusion.
Désarmer la zone	Désarme une *zone virtuelle*. **Zone** Sélectionnez une zone virtuelle.
Afficher une caméra sur un moniteur analogique	Affiche une caméra sur un moniteur analogique dans une tuile du canevas. **Caméra** Sélectionnez la caméra à afficher sur le moniteur analogique. La caméra doit être prise en charge par le moniteur analogique, et utiliser le même format vidéo. **Moniteur analogique** Sélectionnez le moniteur analogique qui affichera la caméra.

Action	Description
Afficher une entité dans Security Desk	Affiche une liste d'entités sur le *canevas* Security Desk des *utilisateurs* sélectionnés, sous forme d'une entité par tuile. Cette action est ignorée si l'utilisateur n'a pas ouvert de tâche de *Surveillance* dans Security Desk. **Destinataires** Sélectionnez les utilisateurs. **Entités** Liste des entités à afficher. Chaque entité est affichée dans une tuile distincte. **Options d'affichage** Sélectionnez l'une des options suivantes : **Visualiser dans une tuile libre** N'utiliser que des tuiles libres. **Forcer l'affichage dans les tuiles** Afficher d'abord dans une tuile libre. Lorsqu'il n'y a plus de tuiles libres, utiliser les tuiles occupées en suivant la séquence d'ID de tuile.
Envoyer un rapport par e-mail	Envoie un rapport (basé sur une tâche de rapport enregistrée) sous forme de pièce jointe d'email à une liste d'*utilisateurs*. **Rapport** Sélectionnez une tâche publique enregistrée. **Destinataires** Sélectionnez les utilisateurs qui doivent recevoir le rapport. **Format d'exportation** Format de rapport : *PDF* ou *Excel*.
Envoyer un instantané par e-mail	Envoie une série d'instantanés d'un flux vidéo sous forme de pièce jointe d'e-mail à une liste d'utilisateurs. **Caméra** Sélectionnez la caméra. **Instantanés** Sélectionnez le nombre de secondes avant (maximum -300 secondes) ou après (maximum 5 secondes) le *Délai de récurrence* pour l'envoi de l'instantané par e-mail. **Destinataires** Sélectionnez les destinataires de l'instantané. Une adresse e-mail doit être définie dans les réglages des utilisateurs. **Format d'exportation** Formats d'image disponibles : PNG, GIF, JPEG ou Bitmap. REMARQUE : Pour envoyer des instantanés, l'option Activer les demandes de vignettes doit être activée dans l'onglet Ressources de l'Archiveur ou de l'Archiveur auxiliaire qui gère la caméra.
Exporter un rapport	Génère et enregistre un rapport spécifié par une tâche publique.

Action	Description
	Rapport Sélectionnez une tâche publique. **Éléments à exporter** **Data** Exportez les données et sélectionnez le format d'exportation (Excel, CSV, PDF). **Graphiques** Exportez les graphiques associés et sélectionnez le format d'exportation (PNG, JPEG). **Orientation** (PDF seulement) Sélectionnez l'orientation en mode portrait ou paysage du fichier PDF. **Remplacement du fichier existant** Indiquez si vous souhaitez remplacer un rapport précédemment enregistré dans le dossier de destination.
Pardonner une violation antiretour	Pardonne une violation *antiretour* d'un *titulaire de cartes* ou d'un *groupe de titulaires de cartes*. **Entité** Sélectionnez un titulaire de cartes ou un groupe de titulaires de cartes.
Aller à l'origine	Indique à la caméra PTZ de revenir à sa position d'origine. Cette fonctionnalité n'est pas prise en charge par toutes les caméras PTZ. **Caméra** Sélectionnez une caméra PTZ.
Aller au préréglage	Indique à la caméra PTZ d'aller à une position prédéfinie. **Caméra** Sélectionnez une caméra PTZ. **Préréglage** Position prédéfinie (numéro) cible.
Importer à partir d'un fichier	Importe un fichier et envoie le résultat de l'importation à un *utilisateur*. **Destinataire** Sélectionnez un utilisateur. **Nom de fichier** Ouvre la fenêtre de l'Outil d'importation, où vous pouvez sélectionner le fichier qui servira à importer les données. REMARQUE : Si l'importation se termine sans erreur, le fichier source est supprimé. Sans quoi il est renommé. Cela vous permet d'exécuter cette action avec une tâche planifiée sans jamais importer deux fois le même fichier. Le même comportement est utilisé pour les événements-actions.
Qualité d'enregistrement selon la configuration sur événement	Règle l'option Accroître la qualité en cas d'enregistrement sur événement de la caméra sélectionnée sur MARCHE, et applique les réglages personnalisés d'amélioration de la qualité d'enregistrement. Cette option prime sur les paramètres généraux

Action	Description
	d'enregistrement sur événement. L'effet de cette action persiste tant qu'il n'est pas modifié par une autre action comme *Qualité d'enregistrement selon la configuration standard*, ou jusqu'au redémarrage de l'Archiveur. **Caméra** Sélectionnez une caméra.
Qualité d'enregistrement selon la configuration manuelle	Règle l'option Accroître la qualité en cas d'enregistrement manuel de la caméra sélectionnée sur MARCHE, et applique les réglages personnalisés d'amélioration de la qualité d'enregistrement. Cette option prime sur les paramètres généraux d'enregistrement sur événement. L'effet de cette action persiste tant qu'il n'est pas modifié par une autre action comme *Qualité d'enregistrement selon la configuration standard*, ou jusqu'au redémarrage de l'Archiveur. **Caméra** Sélectionnez une caméra.
Jouer un son	Déclenche un son dans Security Desk. Cette action est ignorée si l'utilisateur n'a pas lancé Security Desk. **Utilisateur, groupe d'utilisateurs** Sélectionnez un utilisateur ou groupe d'utilisateurs. **Son à jouer** Fichier son (.wav) à déclencher. Pour que les utilisateurs entendent l'alarme sonore correctement, les mêmes fichiers son doivent être installés sur les ordinateurs qui exécutent Security Desk. Les fichiers son standard installés par défaut sont situés dans C:\Program files\Genetec Security Center 5.9\Audio.
Reporter l'armement du secteur de détection d'intrusion	Reporte l'armement du secteur de détection d'intrusion. **Mode d'armement** *Armement global* ou *Armement du périmètre*. **Secteur de détection d'intrusion** Sélectionnez le secteur de détection d'intrusion. **Reporter de** Spécifiez la durée du report de l'armement, en secondes. **Délai d'armement** Spécifiez le délai d'armement en secondes.
Redémarrer l'unité	Redémarre une unité. **Entité** Sélectionnez l'unité vidéo ou l'unité de contrôle d'accès à redémarrer.

Action	Description
Qualité d’enregistrement selon la configuration standard	Annule l'effet des actions *Qualité d’enregistrement selon la configuration manuelle* et *Qualité d’enregistrement selon la configuration sur événement*, et rétablit la configuration d'enregistrement standard. **Caméra** Sélectionnez une caméra.
Réinitialiser le comptage d'individus.	Réinitialise le comptage d'individus dans un *secteur*. **Secteur** Sélectionnez un secteur.
Réinitialiser le système externe	Force le rôle Omnicast™ Federation™ à se reconnecter au système Omnicast™ distant. **Rôle** Sélectionnez un rôle Omnicast™ Federation™.
Réinitialiser l'inventaire de zone de stationnement	Remet l’inventaire de zone de stationnement à zéro afin de pouvoir réinitialiser l'occupation de la zone.
Exécuter une macro	Lance l'exécution d'une *macro*. **Macro** Sélectionnez une macro. **Contexte** valeurs particulières pour les variables contextuelles.
Exécuter un parcours	Indique à la caméra PTZ d'exécuter le parcours spécifié. **Caméra** Sélectionnez une caméra PTZ. **Parcours** Numéro de parcours à exécuter.
Envoyer un message	Affiche un message contextuel dans Security Desk. Cette action est ignorée si l'utilisateur n'a pas lancé Security Desk. **Destinataires** Sélectionnez un utilisateur ou groupe d'utilisateurs. **Message** Le texte à afficher dans le message contextuel. **Avec délai d'expiration** Sélectionnez la durée d'affichage du message.

Action	Description
Envoyer un e-mail	Envoie un e-mail à des utilisateurs ou titulaires de cartes. L'utilisateur sélectionné doit avoir une adresse e-mail configurée, et le serveur de messagerie doit être configuré correctement pour Security Center, sans quoi l'action est ignorée. **Destinataires** Sélectionnez un utilisateur, groupe d'utilisateurs ou groupe de titulaires de cartes. **Message** Le texte de l'e-mail à envoyer au destinataire.
Envoyer une tâche	Envoie et ajoute une tâche publique à une application Security Desk. **Tâche** Sélectionnez une tâche publique enregistrée à envoyer. **Destination** Sélectionnez l'une des options suivantes : **Utilisateur** Toute application Security Desk connectée avec l'utilisateur concerné. **Surveiller** Moniteur Security Desk particulier identifié par un nom de machine et un ID de moniteur.
Définir le mode de lecteur	Définit le mode du lecteur pour l'accès aux portes. **Emplacement** Sélectionnez un secteur, une porte ou un ascenseur. **Mode de lecteur** Réglez l'autorisation d'accès sur *Carte et code PIN* ou *Carte ou code PIN* pour le secteur, la porte ou l'ascenseur sélectionné. Cette action ne fonctionne qu'avec les lecteurs et contrôleurs de porte compatibles.
Définir le mode de maintenance de la porte	Active ou désactive l'état Déverrouillé pour maintenance d'une *porte*. **Porte** Sélectionnez une porte. **Maintenance** Mode maintenance souhaité : activé ou désactivé.
Activer le niveau de risque	Définit un niveau de risque à l'échelle du système Security Center ou de certains secteurs. **Secteur** Sélectionnez les secteurs soumis au niveau de risque. Il peut s'agir de l'intégralité du système ou de secteurs particuliers. **Niveau de risque** Sélectionnez le niveau de risque à appliquer.

Action	Description
Désactiver l'avertisseur sonore	Réinitialise la sortie de l'alarme sonore associée à une porte. Cette action règle l'option Avertisseur sonore sur Aucun dans l'onglet Matériel d'une porte dans Config Tool. **Porte** Sélectionnez une porte.
Activer l'avertisseur sonore	Définit la sortie de l'alarme sonore associée à une porte. Le son à utiliser est spécifié dans l'option Avertisseur sonore de l'onglet Matériel d'une porte dans Config Tool. **Porte** Sélectionnez une porte.
Démarrer la protection vidéo	Démarre la protection contre la suppression pour les prochains enregistrements vidéo. La protection est appliquée à tous les *fichiers vidéo* nécessaires au stockage de la *séquence vidéo* protégée. Puisqu'un fichier vidéo doit être protégé en entier, la longueur réelle de la séquence vidéo protégée dépend de la granularité des fichiers vidéo. Lorsque plusieurs actions *Démarrer la protection vidéo* sont appliquées à un même fichier vidéo, la période de protection la plus longue est prise en compte. **Caméra** Sélectionnez une caméra. **Protéger pendant** Durée de la protection vidéo. **Spécifique** Spécifiez le nombre de jours de protection vidéo. **Infini** La protection ne pourra être désactivée que manuellement depuis la tâche Détails de stockage d'archive. **Protéger la vidéo pour les prochains** Durée de la vidéo à protéger. **Spécifique** Définit la durée sous forme de minutes et d'heures. **Infini** Tous les enregistrements à venir seront protégés jusqu'à ce que l'action *Arrêter la protection vidéo* soit exécutée.
Démarrer l'enregistrement	Active l'enregistrement sur la caméra spécifiée. Cette action est ignorée si la caméra n'est pas gérée par un horaire d'enregistrement actif. L'enregistrement démarré par cette action ne peut pas être arrêté manuellement par l'utilisateur. **Caméra** Sélectionnez une caméra.

Action	Description
	Durée d'enregistrement Règle la durée de l'enregistrement vidéo. **Par défaut** Règle la durée sur la valeur de *Durée par défaut de l'enregistrement manuel* configurée pour la caméra. **Infini** L'enregistrement ne peut être arrêté que par l'action *Arrêter l'enregistrement*. **Spécifique** Règle la durée d'enregistrement sous forme de secondes, de minutes et d'heures.
Démarrer le transfert	Démarre un transfert d'archive. **Groupe de transfert** Sélectionnez un groupe de transfert pour lequel lancer le transfert. Le transfert peut impliquer la récupération des enregistrements des unités vidéo, la duplication des archives entre Archiveurs, ou la sauvegarde des archives vers un emplacement particulier.
Arrêter la protection vidéo	Arrête la protection contre la suppression pour les prochains enregistrements vidéo. Cette action n'affecte pas les *archives vidéo* déjà protégées. **Caméra** Sélectionnez une caméra. **Arrêter dans** Règle l'arrêt de la protection vidéo sur Maintenant ou passé un délai Spécifique en minutes et en heures.
Arrêter l'enregistrement	Arrête l'enregistrement sur la caméra spécifiée. L'action n'est exécutée que si l'enregistrement a été déclenché par l'action *Démarrer l'enregistrement*. **Caméra** Sélectionnez une caméra. **Arrêter dans** Règle l'arrêt de l'enregistrement sur Maintenant ou passé un délai Spécifique en minutes et en heures.
Arrêter le transfert	Arrête un transfert d'archive. **Groupe de transfert** Sélectionnez un groupe de transfert concerné par l'arrêt du transfert.

Action	Description
Synchroniser le rôle	Lance un processus de synchronisation sur le rôle spécifié : *Active Directory* ou *Synchroniseur de titulaires de cartes globaux*. **Rôle** Sélectionnez un rôle à synchroniser. **Obtenir une image** (rôle Active Directory seulement) Activez cette option si les attributs des images doivent également être synchronisés.
Annuler temporairement les horaires de déverrouillage	Verrouille ou déverrouille temporairement la porte pour une durée déterminée. **Porte** Sélectionnez une porte. **Mode de verrouillage** Sélectionnez *Déverrouillé* ou *Verrouillé*. **Pour** Durée en minutes ou en heures. **Du/au** Plage de dates et d'heures de déverrouillage de la porte.
Déclencher l'alarme	Déclenche une alarme. Cette action peut déclencher des événements supplémentaires, selon la configuration de l'alarme. **Alarme** Sélectionnez une alarme. **Condition d'acquittement** Type d'événement à déclencher avant de pouvoir acquitter l'alarme. **Acquittement par un utilisateur requis** Spécifiez si l'alarme doit être acquittée manuellement, ou si elle sera automatiquement acquittée par le système lorsque les conditions d'acquittement seront effacées.
Déclencher une alarme d'intrusion	Déclenche une alarme physique sur un secteur de détection d'intrusion. **Type de destinataire :** Type de déclencheur d'alarme : secteur de détection d'intrusion ou entrée d'alarme spécifique. **Secteur de détection d'intrusion** Sélectionnez un secteur de détection d'intrusion.

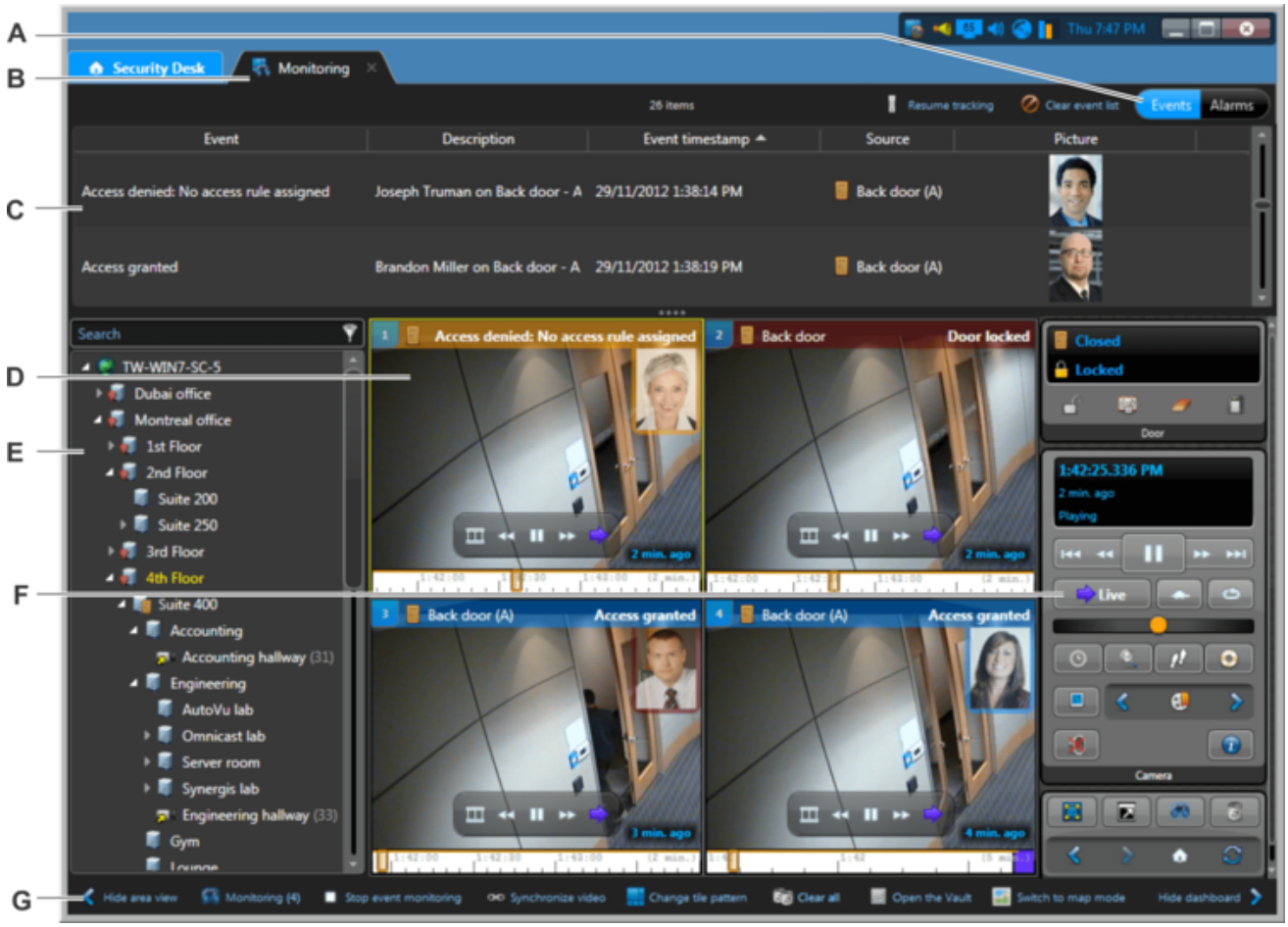
Action	Description
Déclencher un signal de sortie	Déclenche un *signal de sortie* ou une sortie numérique d'une *unité*. Par exemple, une action peut déclencher la sortie numérique d'une unité (contrôleur ou module d'entrée/sortie). **Relais de sortie** Sélectionnez une sortie numérique (unité). **Signal de sortie** Sélectionnez le signal de sortie à déclencher.
Déclencher la recherche d'anciennes lectures	Indique au rôle Gestionnaire RAPI de comparer une liste de véhicules recherchés nouvelle ou mise à jour aux lectures de plaques déjà recueillies.
Déverrouiller expressément la porte	Déverrouille temporairement une porte pendant cinq secondes, ou durant le *Délai d'accès normal* configuré pour la porte. **Porte** Sélectionnez une porte.
Déverrouiller expressément les portes du périmètre	Déverrouille temporairement les portes du périmètre d'un secteur pendant cinq secondes, ou durant le *Délai d'accès normal* configuré pour les portes. **Secteur** Sélectionnez un secteur.
Mettre à jour le mot de passe de l'unité	Envoie des requêtes de mise à jour de mot de passe aux unités sélectionnées via leurs rôles. Les mots de passe sont automatiquement générés par le système. **Entités** Ajoutez une ou plusieurs unités vidéo. REMARQUE : Le système ne vérifie pas si les unités sélectionnées prennent en charge la mise à jour des mots de passe.

7.2 | Présentation graphique des tâches de Security Desk

7.2.1 | Présentation de la tâche Surveillance

Utilisez la tâche Surveillance pour surveiller les événements, comme les événements de contrôle d'accès associés aux portes et titulaires de cartes, les lectures et alertes de plaques d'immatriculation provenant d'unités de RAPI fixes et mobiles, et les événements associés aux caméras, le tout en temps réel.

L'image suivante montre une tâche Surveillance d'un système de contrôle d'accès et de vidéosurveillance.



A	**Événements** Affichez les événements dans le volet de rapport. **Reprendre le suivi** Affichez les événements dans la liste dès qu'ils se produisent. **Effacer la liste d'événements** Supprimez tous les événements de la liste d'événements. **Alarmes** Affichez les alarmes dans le volet de rapport. Les mêmes commandes sont disponibles dans la tâche Surveillance d'alarmes. REMARQUE : Les boutons Événements et Alarmes n'apparaissent que lorsque vous activez la surveillance d'alarmes pour la tâche Surveillance.
B	Les nouvelles alertes d'événements apparaissent dans l'onglet Surveillance lorsque la tâche n'est pas au premier plan.
C	Le volet de rapport affiche les événements ou les alarmes en temps réel, selon la sélection effectuée.
D	Une tuile peut servir à surveiller les événements (ID de tuile bleu), les alarmes (ID de tuile rouge), les deux ou aucun des deux (ID de tuile gris).
E	Sélectionner des entités dans la vue secteur pour les afficher sur le canevas. Vous pouvez sélectionner plusieurs entités et les faire glisser vers le canevas en même temps.
F	Widgets servant à contrôler les entités surveillées.

G	**Masquer la vue secteur** Permet de masquer la vue secteur. **Surveillance** Sélectionnez les entités à surveiller. **Synchroniser la vidéo** Synchronisez la vidéo affichée sur le canevas. **Effacer tout** Effacer toutes les tuiles configurées dans la tâche Surveillance. **Modifier la mosaïque** Changer la mosaïque sur le canevas. **Ouvrir le Coffre-fort** Ouvrez l'outil Coffre-fort pour afficher les instantanés précédemment enregistrés et les fichiers vidéo exportés. **Basculer en mode carte** Basculez entre le *mode Tuile* et le *mode Carte*. REMARQUE : Pour basculer entre le mode tuile et le mode carte, vous devez avoir le privilège *Basculer en mode carte*. **Masquer les commandes** Masquez les commandes.

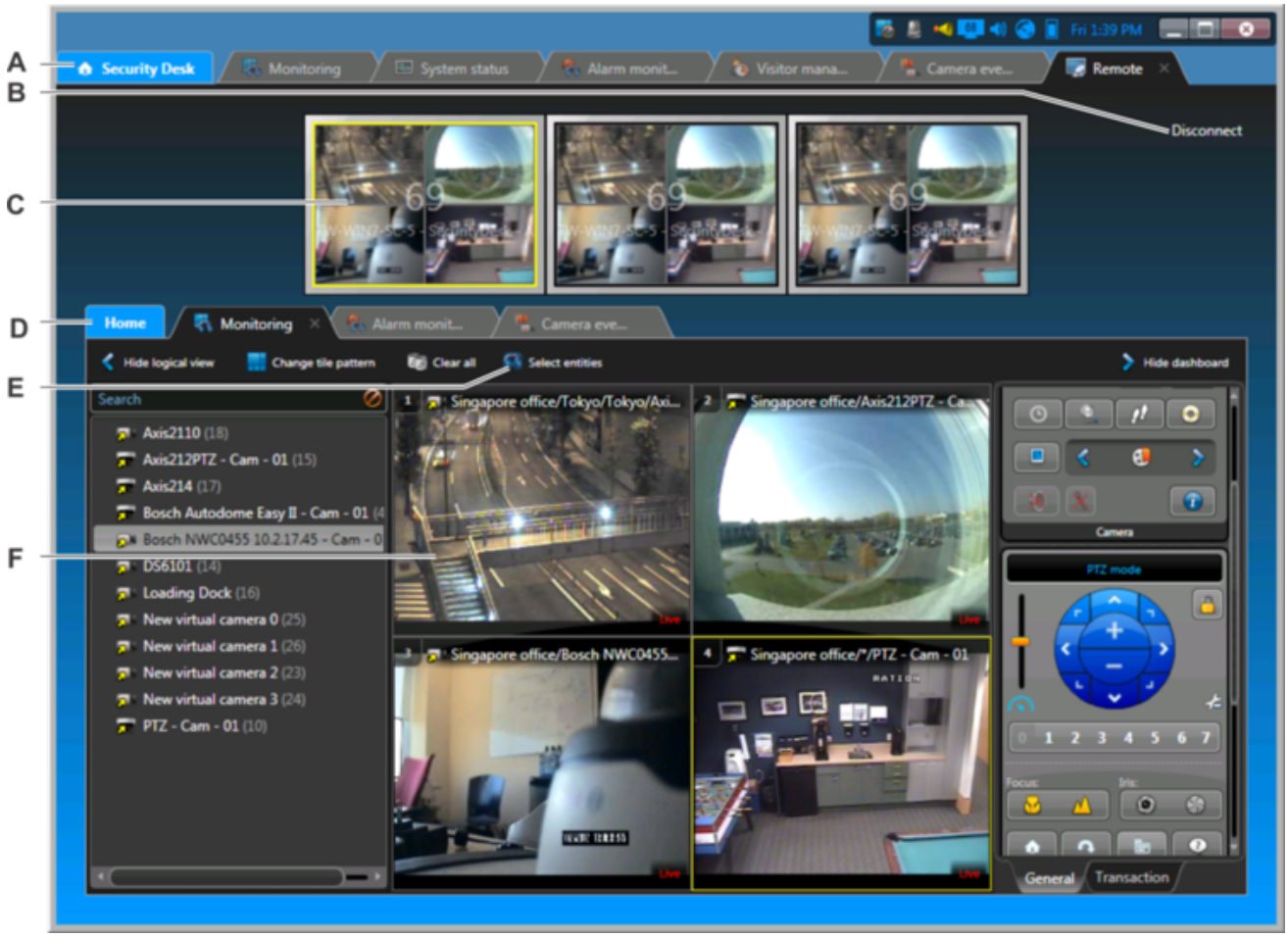
Explorer

- Surveiller les événements
- Sélectionner des entités à surveiller
- Synchroniser la vidéo dans les tuiles
- Modifier la mosaïque des tuiles
- Capturer des instantanés vidéo
- Afficher les fichiers vidéo exportés
- Surveiller les événements de RAPI dans mode Tuile

7.2.2 | Présentation de la tâche Distant

Utilisez la tâche Distant pour surveiller et contrôler à distance d'autres instances de Security Desk qui font partie de votre système.

La figure suivante montre une tâche Distant.



A	Tâches Security Desk locales en cours. Cliquez sur un onglet pour basculer vers la tâche correspondante.
B	Se déconnecter du Security Desk distant.
C	Basculer entre les moniteurs Security Desk auxquels vous êtes connectés en mode Mur d'images.
D	Tâches Security Desk distantes ouvertes. Lorsque vous êtes connecté à distance, vous ne pouvez utiliser que les tâches *Surveillance* et *Surveillance d'alarmes*.
E	Sélectionnez les entités à surveiller.
F	Surveiller les entités sur le canevas. Ce que vous affichez sur le canevas est également affiché sur le canevas du Security Desk distant.

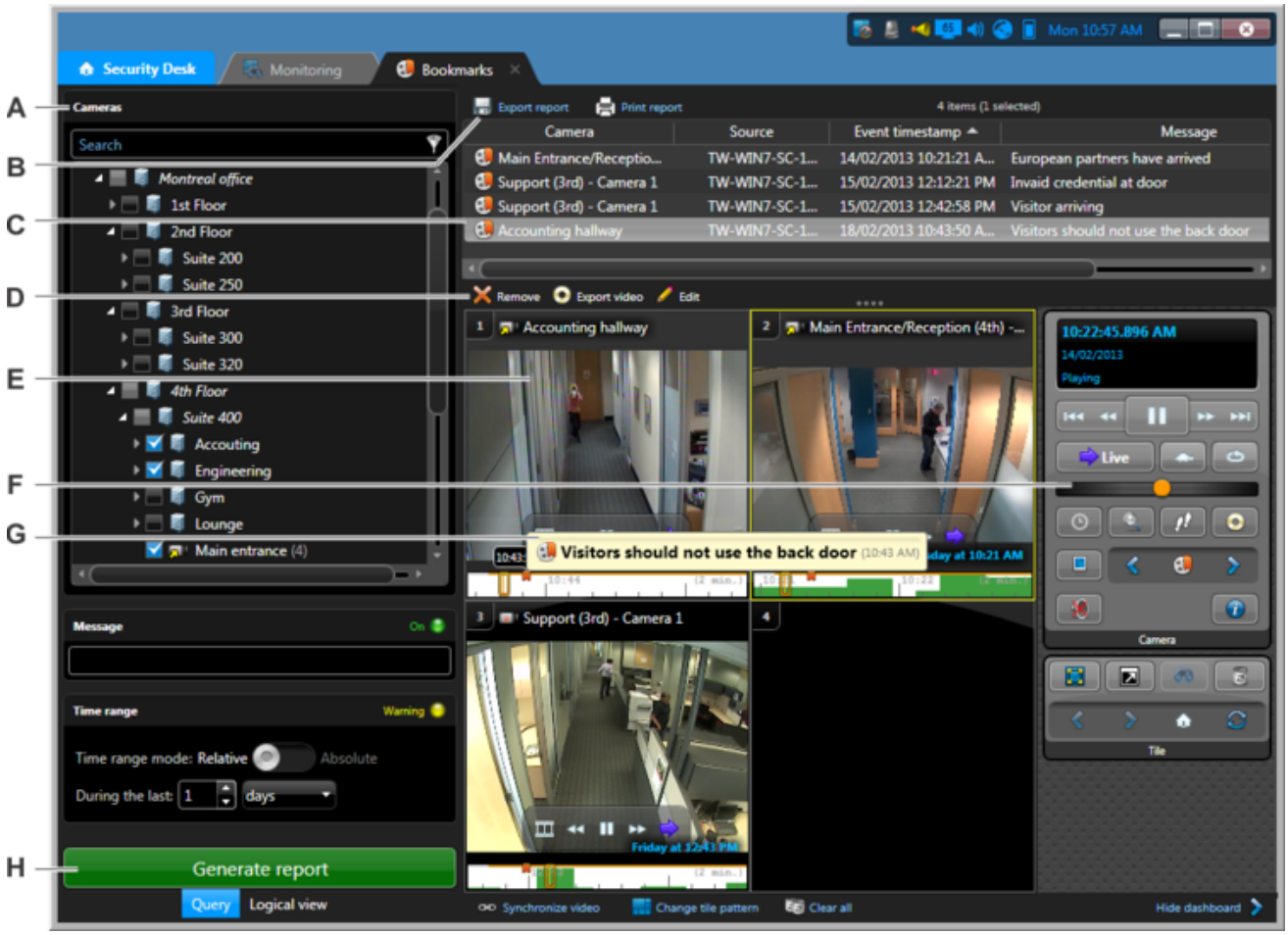
Explorer

- Surveillance à distance
- Se connecter aux applications Security Desk distantes

7.2.3 | Présentation de la tâche Signets

Utilisez la tâche Signets pour rechercher, afficher et créer des rapports sur les signets .

La figure suivante montre la tâche Signets.



A	Filtres de recherche.
B	Cliquez sur pour exporter ou sur pour imprimer le rapport.
C	Les événements de signet sont affichés dans le volet de rapport.
D	Options disponibles lorsqu'un signet est sélectionné dans le volet de rapport : • - Supprimer les signets sélectionnés de la base de données. • - Exporter la vidéo associée aux signets sélectionnés. • - Modifier les signets sélectionnés.
E	Vidéo du signet dans une tuile.
F	Widget Caméra.
G	Survolez un signet dans une tuile avec la souris pour afficher le message associé, si disponible.
H	Générer le rapport.

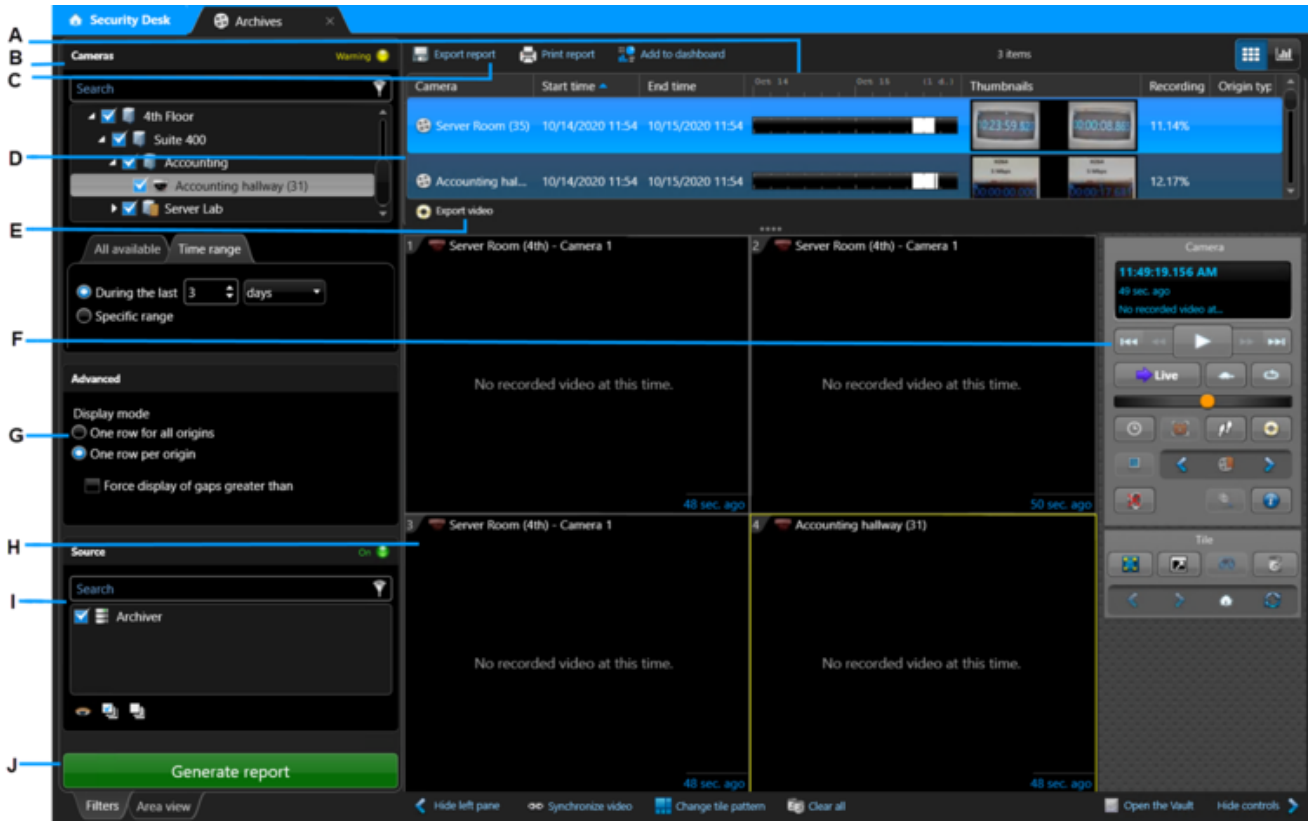
Explorer

- Ajouter des signets à une séquence vidéo
- Afficher de la vidéo associée à un signet
- Exporter un rapport
- Imprimer les rapports générés

7.2.4 | Présentation de la tâche Archives

Utilisez la tâche Archives pour rechercher et consulter les *archives vidéo* disponibles de votre système par caméra et plage horaire.

La figure suivante montre la tâche Archives.



A	Colonnes du volet de rapport.
B	Filtres de recherche.
C	Exportez ou imprimez le rapport.
D	La liste des enregistrements vidéo correspondants est affichée dans le volet de rapport.
E	Exporter la vidéo de l'archive sélectionnée.
F	Widget Caméra.
G	Séquence vidéo d'une alarme dans une tuile.
H	Générer le rapport.

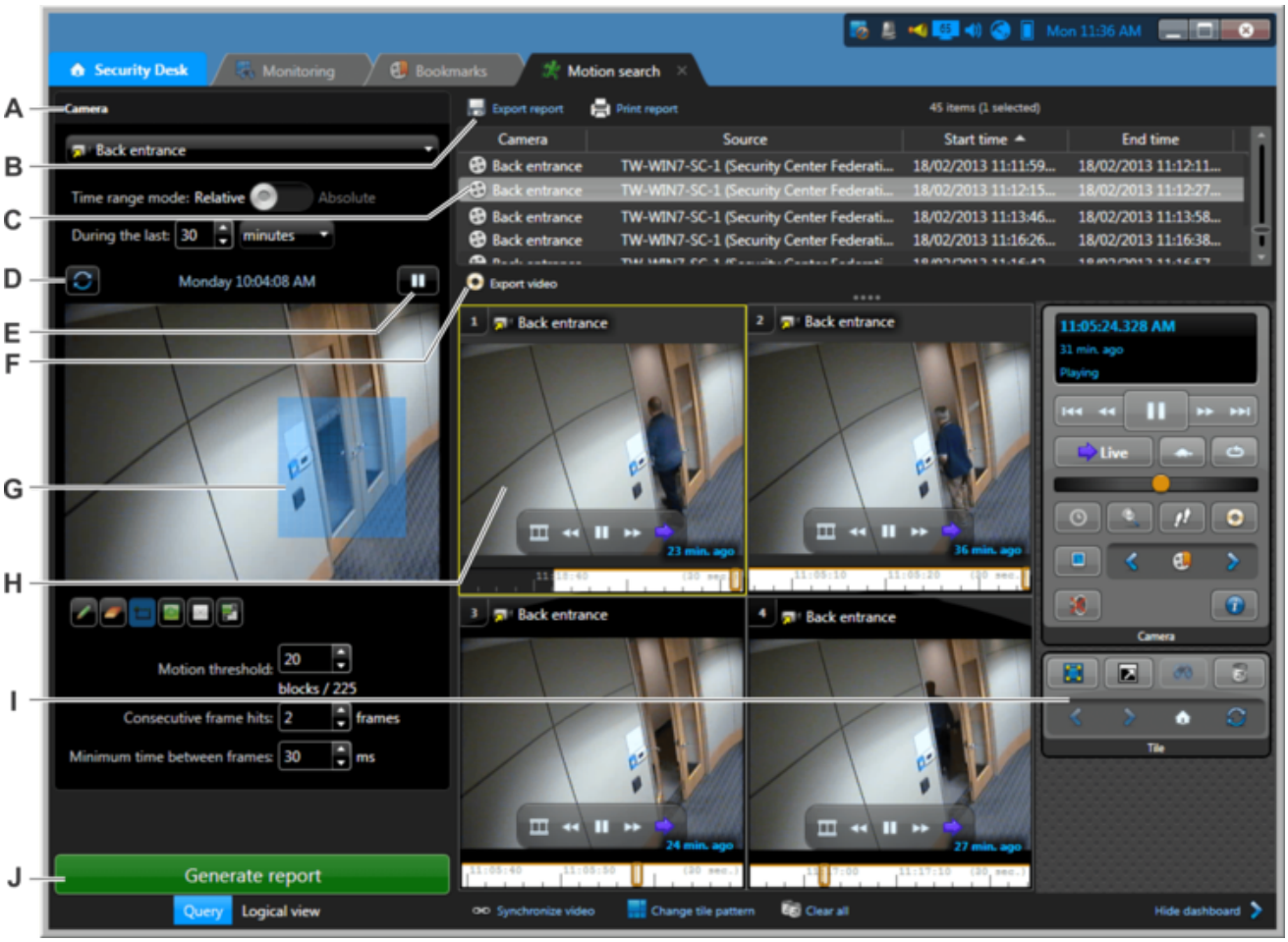
Explorer

- Afficher des archives vidéo
- Exporter de la vidéo

7.2.5 | Présentation de la tâche Recherche de mouvement

Utilisez la tâche Recherche de mouvement pour rechercher des *séquences vidéo* dans les archives vidéo qui contiennent du mouvement dans certaines zones du champ d'une caméra.

La figure suivante montre la tâche Recherche de mouvement.



A	Filtres de recherche.
B	Exportez ou imprimez le rapport.
C	Les événements de mouvement sont affichés dans le volet de rapport.
D	Actualiser l'image d'aperçu.
E	Lancer la lecture de la vidéo dans l'image d'aperçu.
F	Exporter la vidéo associée aux signets sélectionnés.
G	Zone de détection de mouvement pour la recherche.
H	Séquence vidéo d'un événement de mouvement dans une tuile.
I	Widgets du volet Commandes.
J	Générer le rapport.

Explorer

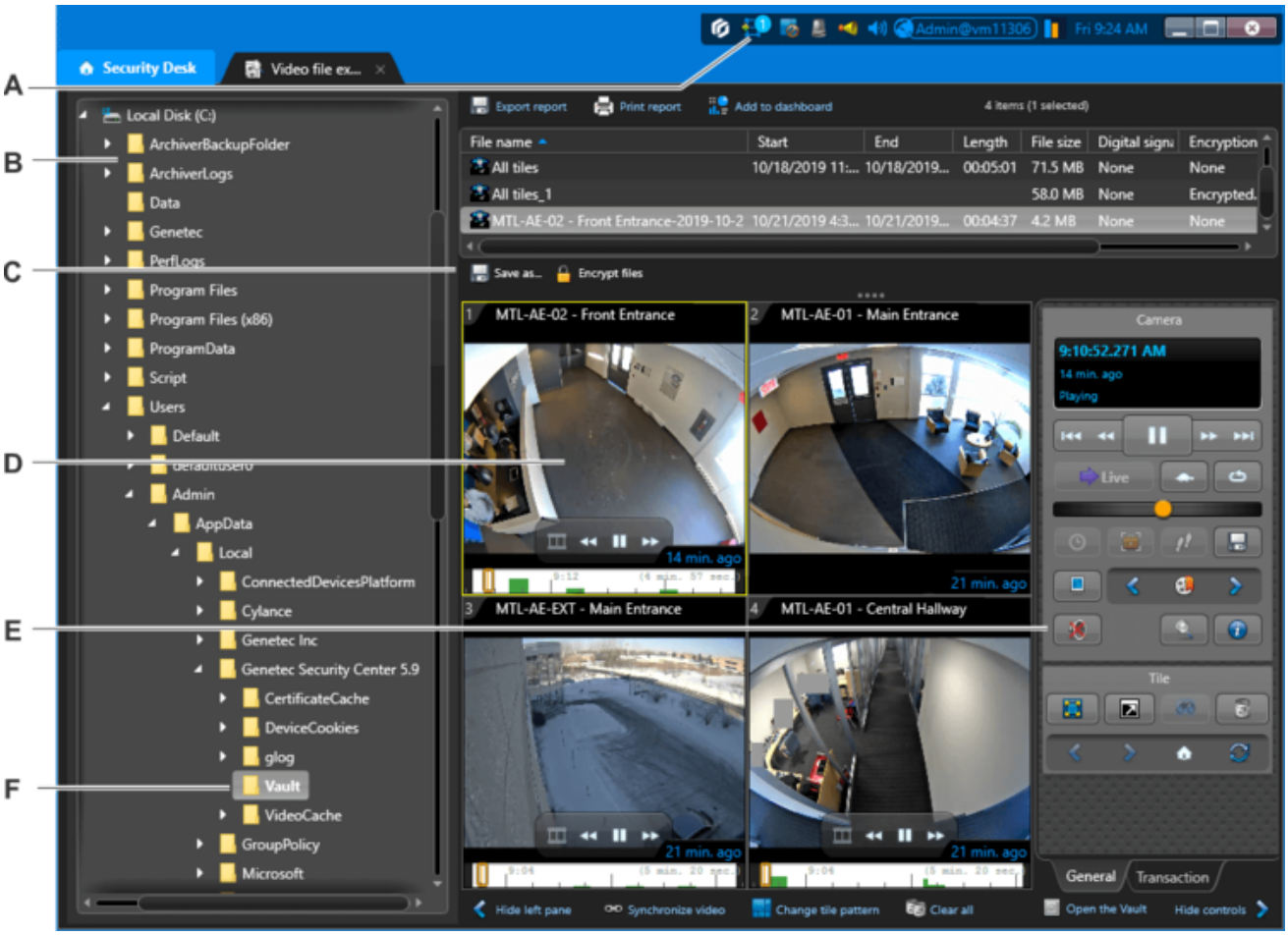
- Rechercher des événements de mouvement dans les archives vidéo
- Exporter de la vidéo

7.2.6 | Présentation de la tâche Explorateur de fichiers vidéo

Utilisez la tâche Explorateur de fichiers vidéo pour rechercher et visionner les fichiers vidéo G64x exportés.

Lors de la lecture d'un fichier vidéo, la frise chronologique n'indique aucun marqueur d'événement si :

- Le fichier vidéo a été créé avant Omnicast™ 4 .x. Les fichiers vidéo créés avec la fonction *Exporter* de Omnicast™ 4.x ou ultérieur peuvent contenir des signets ou des marqueurs d'événements de mouvement.
- Le fichier vidéo est toujours géré par un Archiveur ou Archiveur auxiliaire (généralement dans \VideoArchives).
- Le fichier vidéo fait partie d'un jeu de sauvegarde (généralement dans \Tables\VideoFile).



A	Ouvrez la boîte de dialogue Conversion. Cette icône s'affiche uniquement si vous convertissez des fichiers G64 au format ASF.
B	Rechercher des fichiers vidéo dans les dossiers sur votre réseau.
C	Options disponibles lorsqu'un fichier vidéo est sélectionné dans le volet de rapport : • - Convertir les fichiers vidéo sélectionnés au format ASF. • - Chiffrer les fichiers vidéo sélectionnés. L'icône indique que le fichier vidéo est déjà chiffré. • - Si le fichier vidéo est signé numériquement, vérifiez la signature numérique. REMARQUE : Les signatures numériques sont signées à l'aide d'EdDSA. Les fichiers vidéo qui ont été signés avec RSA peuvent toujours réussir la validation, mais ils sont signalés comme étant authentifiés avec un algorithme obsolète.
D	Fichier vidéo exporté dans une tuile.
E	Widgets du volet Commandes.
F	Dossier sélectionné. Les fichiers vidéo présents dans le dossier sont affichés dans le volet de rapport.

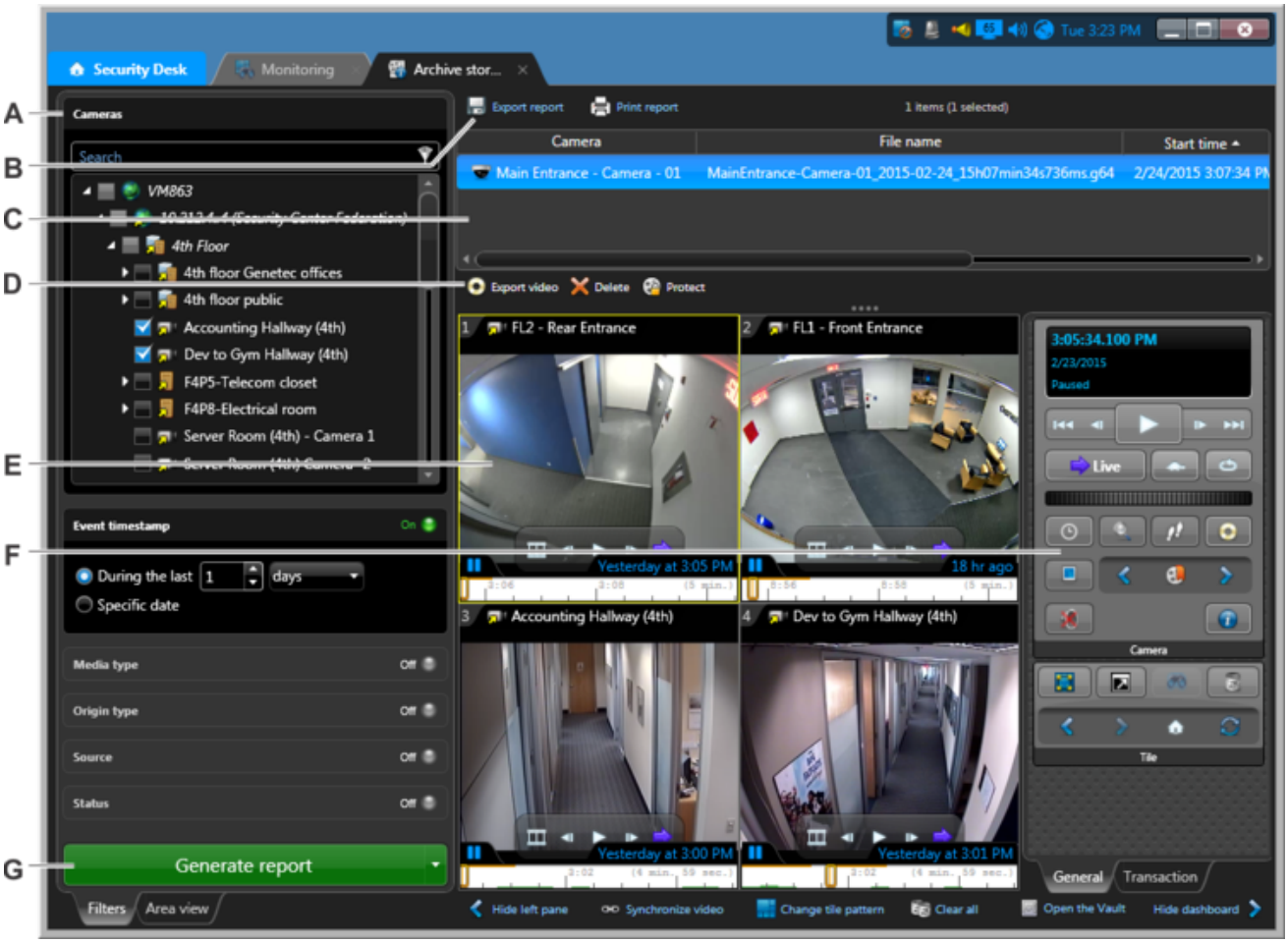
Explorer

- Visionner les fichiers vidéo exportés avec l'Explorateur de fichiers vidéo

7.2.7 | Présentation de la tâche Détails de stockage d'archive

Utilisez la tâche Détails de stockage d'archive pour rechercher les *fichiers vidéo* utilisés pour stocker les *archives vidéo* des caméras et afficher les propriétés des fichiers vidéo.

La figure suivante montre la tâche Détails de stockage d'archive.



A	Filtres de recherche.
B	Exportez ou imprimez le rapport.
C	La liste des fichiers vidéo est affichée dans le volet de rapport.
D	Options disponibles lorsqu'un fichier vidéo est sélectionné dans le volet de rapport : • - Exporter la vidéo associée aux fichiers vidéo sélectionnés. • - Supprimer le fichier vidéo sélectionné de la base de données. • - Protéger les fichiers vidéo sélectionnés. • - Supprimer la protection des fichiers vidéo sélectionnés contre la suppression automatique.
E	Fichier vidéo affiché dans une tuile.
F	Widgets du volet Commandes.
G	Générer le rapport.

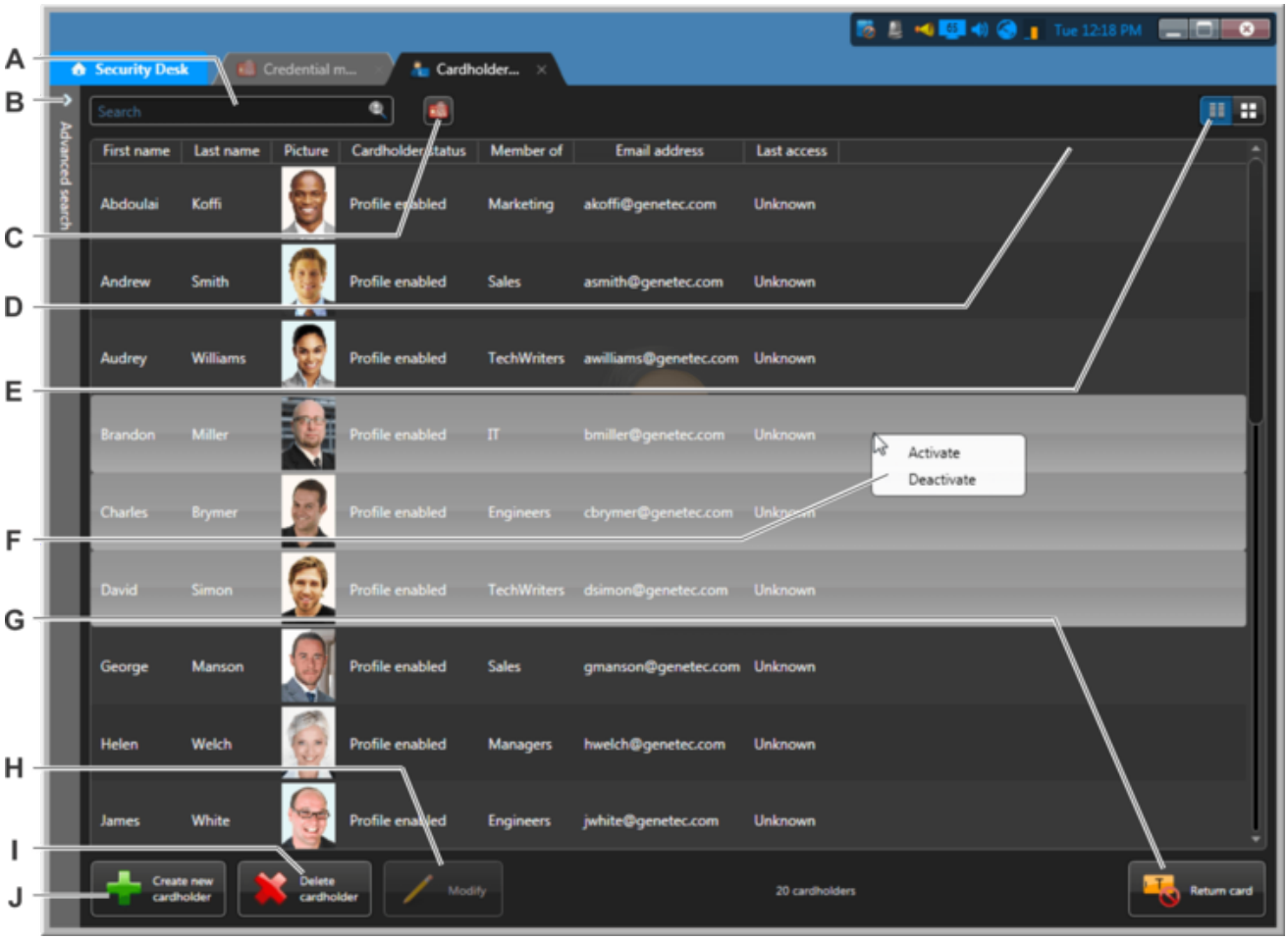
Explorer

- Afficher les propriétés des fichiers vidéo

7.2.8 | Présentation de la tâche Gestion des titulaires de cartes

Utilisez la tâche Gestion des titulaires de cartes pour créer des *titulaires de cartes*, modifier des titulaires de cartes existants, et affecter des identifiants aux titulaires de cartes.

La figure suivante montre la tâche Gestion des titulaires de cartes. Il n'est possible d'exécuter qu'une seule instance de cette tâche dans Security Desk.



A	Rechercher un titulaire de cartes par nom.
B	Options de recherche avancées.
C	Rechercher un titulaire de cartes par son identifiant.
D	Sélectionnez les colonnes à afficher en faisant un clic droit sur les en-têtes de colonne, ou en tapant Ctrl+Maj+C.
E	Basculez entre les vues *Tuiles* et *Liste*. **Tuiles** Afficher les images grand format. Les images peuvent être redimensionnées. **Liste** Afficher toutes les informations concernant l'entité : prénom, nom, photo, date d'activation, date d'expiration, ainsi que tout champ personnalisé défini.
F	Activer ou désactiver plusieurs titulaires de cartes à la fois. Pour modifier plusieurs titulaires de cartes à la fois, utilisez la vue *Liste*.

G	Retourner une carte temporaire.
H	Afficher ou modifier le titulaire de cartes sélectionné.
I	Supprimer le titulaire de cartes sélectionné.
J	Créer un titulaire de cartes.

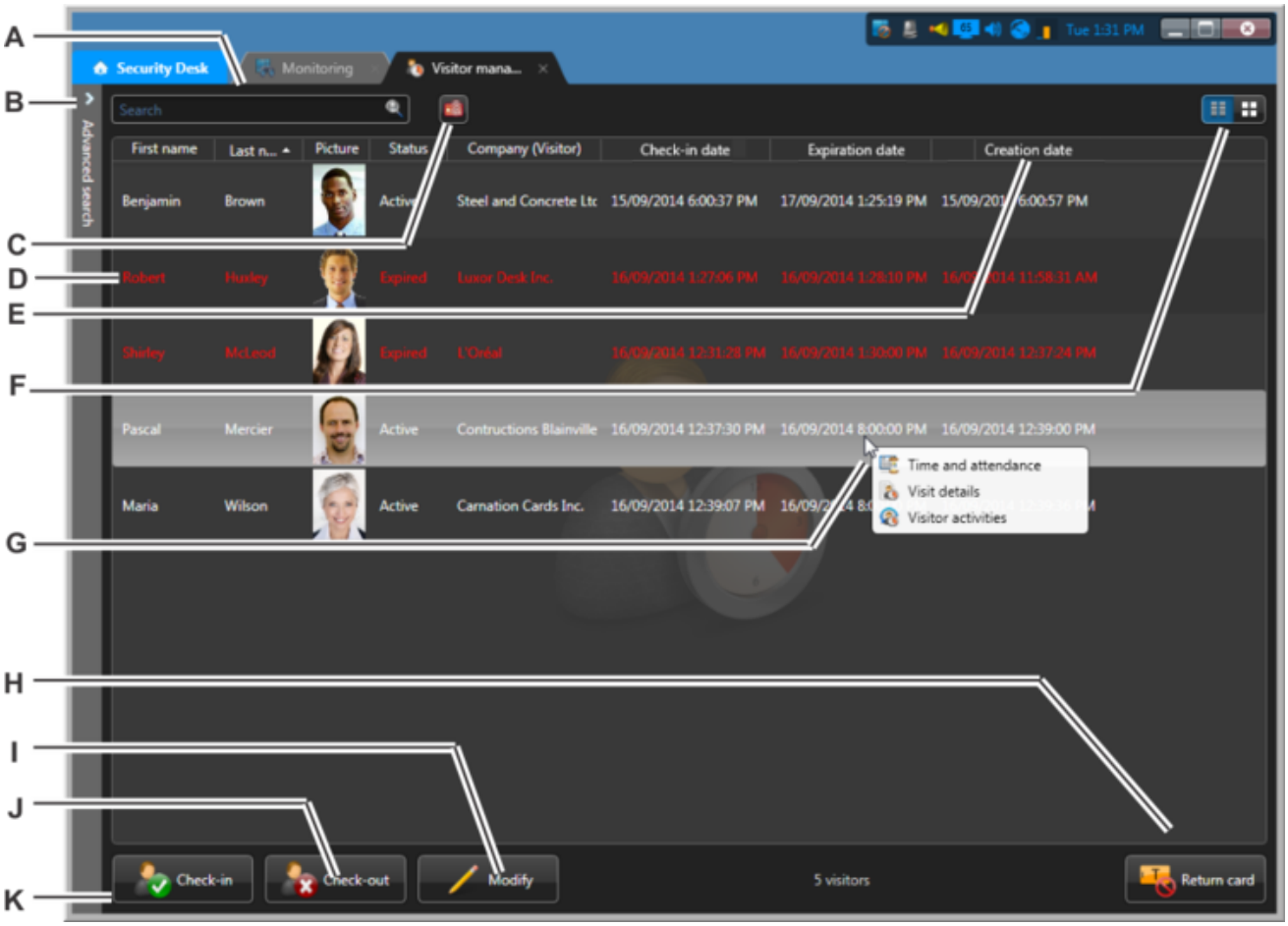
Explorer

- Créer des titulaires de cartes
- Affecter des identifiants
- Affecter une carte temporaire

7.2.9 | Présentation de la tâche Gestion des visiteurs

Utilisez la tâche Gestion des visiteurs pour inscrire les nouveaux visiteurs, modifier les visiteurs existants et affecter des identifiants aux visiteurs.

La figure suivante montre la tâche Gestion des visiteurs. Il n'est possible d'exécuter qu'une seule instance de cette tâche dans Security Desk.



A	Rechercher un visiteur par son identifiant.
B	Rechercher un visiteur par nom.
C	Options de recherche avancées.
D	Les visiteurs dont le profil est désactivé ou a expiré sont affichés en rouge.

E	Sélectionnez les colonnes à afficher en faisant un clic droit sur les en-têtes de colonne, ou en tapant Ctrl+Maj+C.
F	Basculez entre les vues *Tuiles* et *Liste*. **Tuiles** Afficher les images grand format. Les images peuvent être redimensionnées. **Liste** Afficher toutes les informations concernant l'entité : prénom, nom, photo, date d'enregistrement, date d'expiration, date de création, ainsi que tout champ personnalisé défini.
G	Générez les rapports de visiteur en faisant un clic droit sur le visiteur sélectionné. •) Présence. •) Détails de visite. •) Activités de visiteurs.
H	Retourner une carte temporaire.
I	Inscrire un nouveau visiteur ou un visiteur connu. Une fois qu'un visiteur est inscrit, le bouton indique Radier.
J	Supprimer le visiteur sélectionné.
K	Afficher ou modifier le visiteur sélectionné.
L	Ajouter un visiteur.

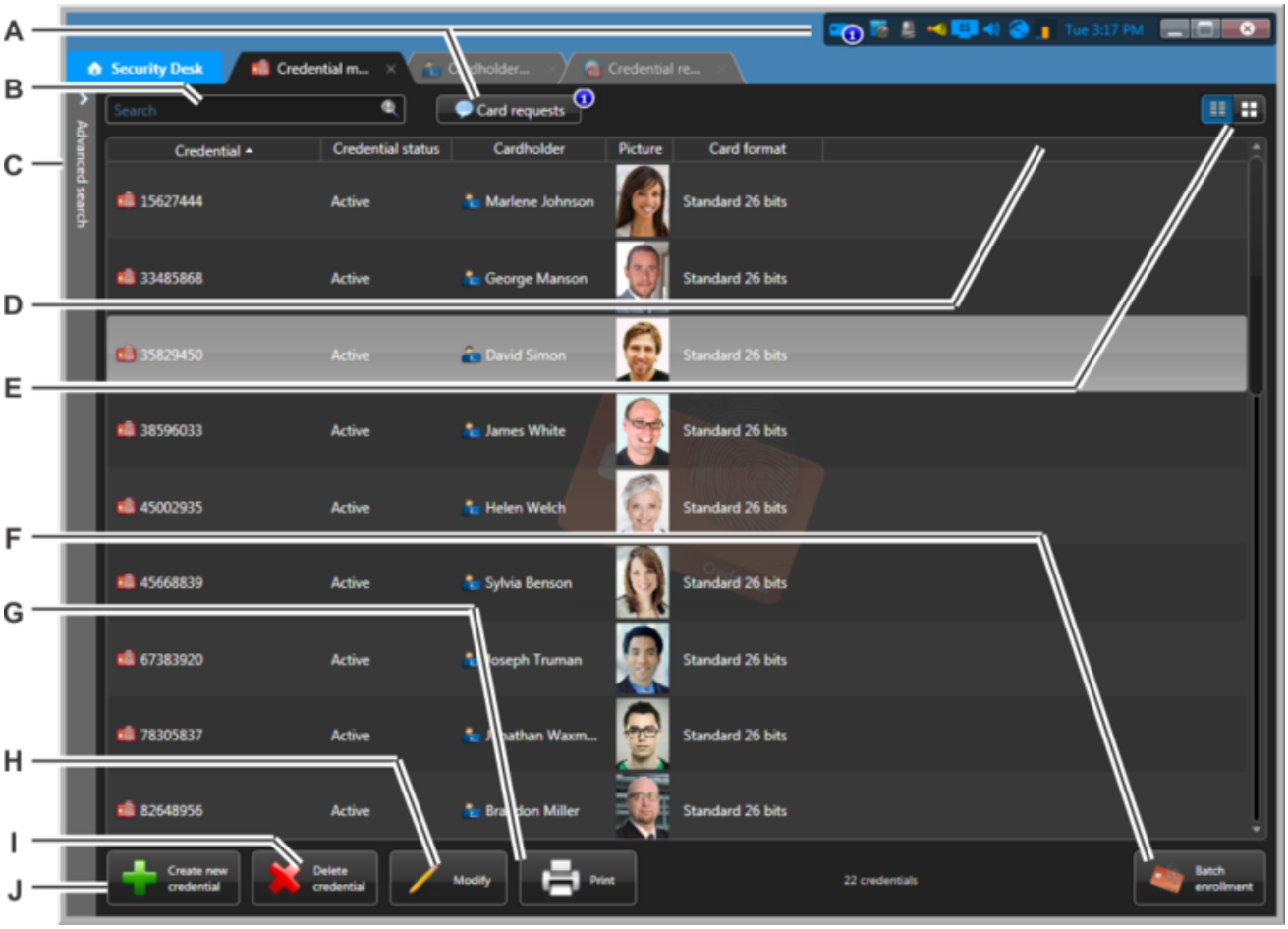
Explorer

- Inscrire de nouveaux visiteurs
- Radier les visiteurs
- Suivre la présence dans un secteur
- Afficher la durée de séjour d'un visiteur
- Analyser les événements de visiteurs
- Rétablir la carte d'origine d'un titulaire de cartes ou visiteur
- Inscrire un visiteur connu

7.2.10 | Présentation de la tâche Gestion des identifiants

Utilisez la tâche Gestion des identifiants pour créer, modifier et supprimer les identifiants, et pour imprimer des badges.

La figure suivante montre la tâche *Gestion des identifiants*. Il n'est possible d'exécuter qu'une seule instance de cette tâche dans Security Desk.



A	Afficher, modifier ou répondre à une demande de carte d'identification en attente.
B	Rechercher un identifiant par nom.
C	Options de recherche avancées.
D	Sélectionnez les colonnes à afficher en faisant un clic droit sur les en-têtes de colonne, ou en tapant Ctrl+Maj+C.
E	Basculez entre les vues *Tuiles* et *Liste*. **Tuiles** Afficher les images grand format. Les images peuvent être redimensionnées. **Liste** Afficher toutes les informations concernant l'entité : prénom, nom, photo, date d'activation, date d'expiration, ainsi que tout champ personnalisé défini.
F	Inscrire plusieurs identifiants au sein du système en même temps.
G	Imprimer les cartes d'identification sélectionnées.
H	Afficher ou modifier l'identifiant sélectionné.
I	Supprimer les identifiants sélectionnés.
J	Créer un identifiant.

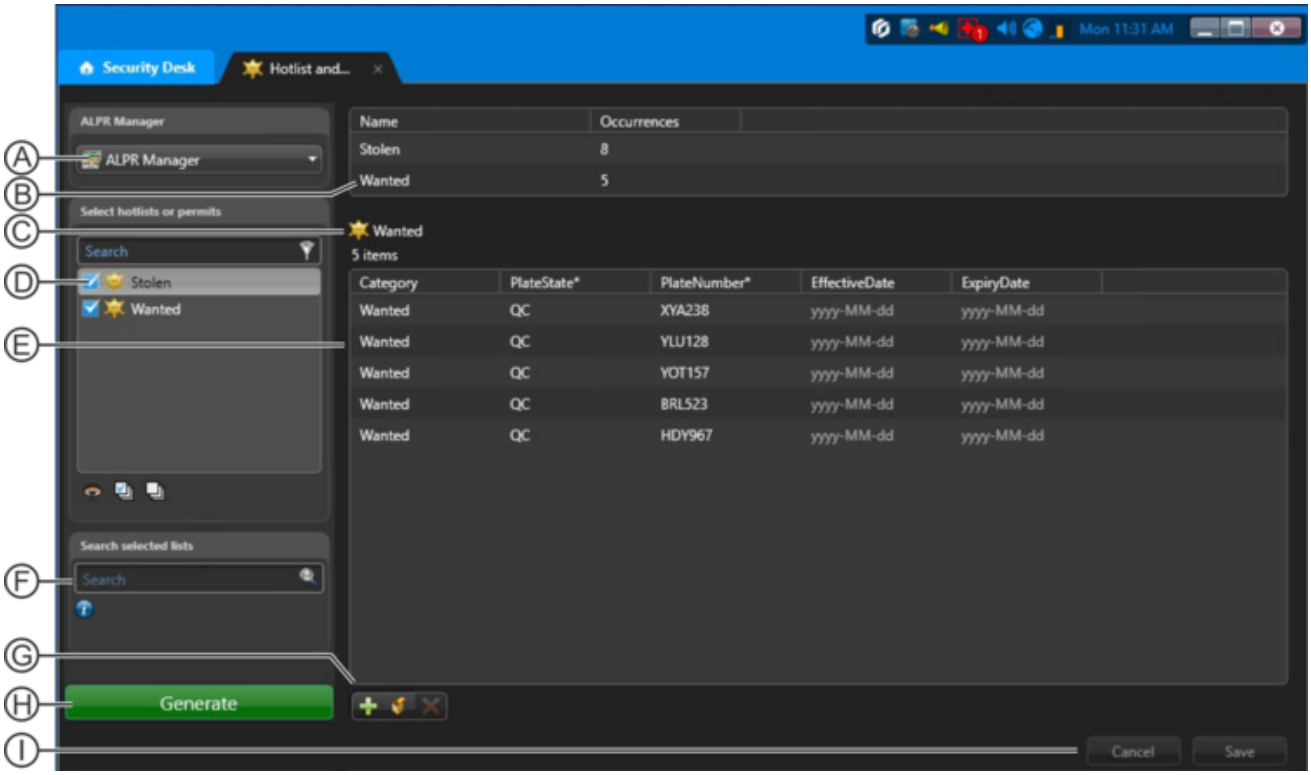
Explorer

- Créer un identifiant
- Inscrire plusieurs identifiants automatiquement
- Inscrire plusieurs identifiants manuellement
- Rechercher un identifiant

7.2.11 | Présentation de la tâche Éditeur de permis et de liste de véhicules recherchés

Utilisez la tâche Éditeur de permis et de liste de véhicules recherchés pour modifier une *liste de véhicules recherchés* ou une liste de *permis* de stationnement pour tous les véhicules de patrouille en même temps.

La figure suivante montre la tâche Éditeur de permis et de liste de véhicules recherchés.



A	Rechercher des lignes particulières dans la liste.
B	Listes de véhicules recherchés et de permis disponibles.
C	Ligne sélectionnée, prête à la modification.
D	Liste des rôles Gestionnaire RAPI.
E	Charger la liste de véhicules recherchés ou de permis sélectionnée.
F	Ajouter ou supprimer la ligne sélectionnée de la liste.
G	Enregistrer ou annuler les modifications.

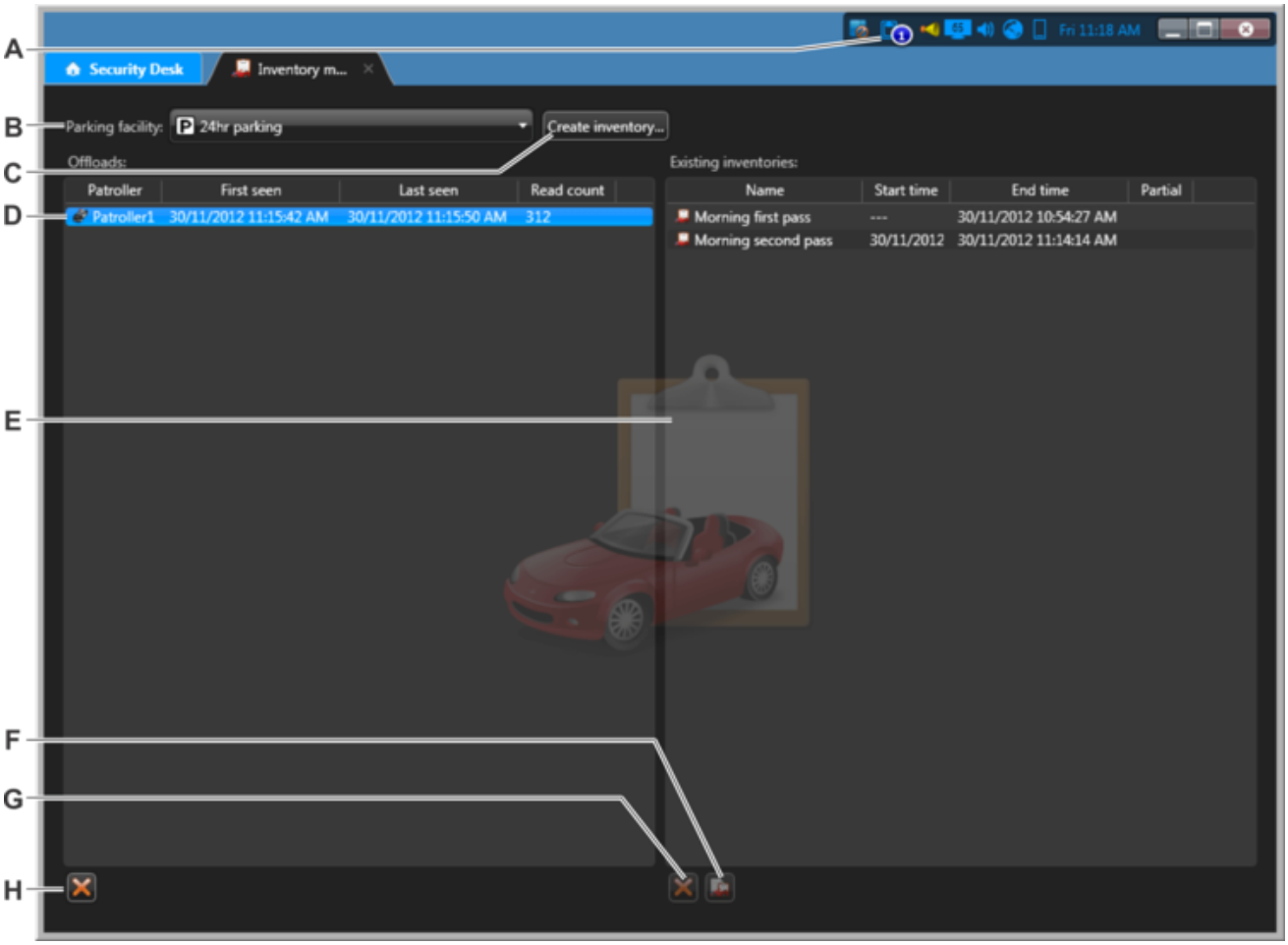
Explorer

- Modifier les listes de véhicules recherchés et listes de permis

7.2.12 | Présentation de la tâche Gestion d'inventaire

Utilisez la tâche Gestion d'inventaire pour ajouter et rapprocher les lectures de plaques IMPI à un inventaire de parc de stationnement.

La figure suivante montre la tâche Gestion d'inventaire.



A	L'icône Inventaire indique le nombre de fichiers de déchargement IMPI en attente de rapprochement
B	Parc de stationnement sélectionné pour l'ajout d'inventaire.
C	Créer un inventaire
D	La section Déchargements affiche des informations sur le déchargement IMPI. Le fichier reste dans la section Déchargements jusqu'à sa suppression ou son ajout au parc de stationnement.
E	La section Inventaires existants affiche les inventaires que vous avez créés.
F	Ouvrez la tâche Rapport d'inventaire pour afficher et comparer vos parcs de stationnement.
G	Supprimer l'inventaire sélectionné.
H	Supprimer un fichier de déchargement.

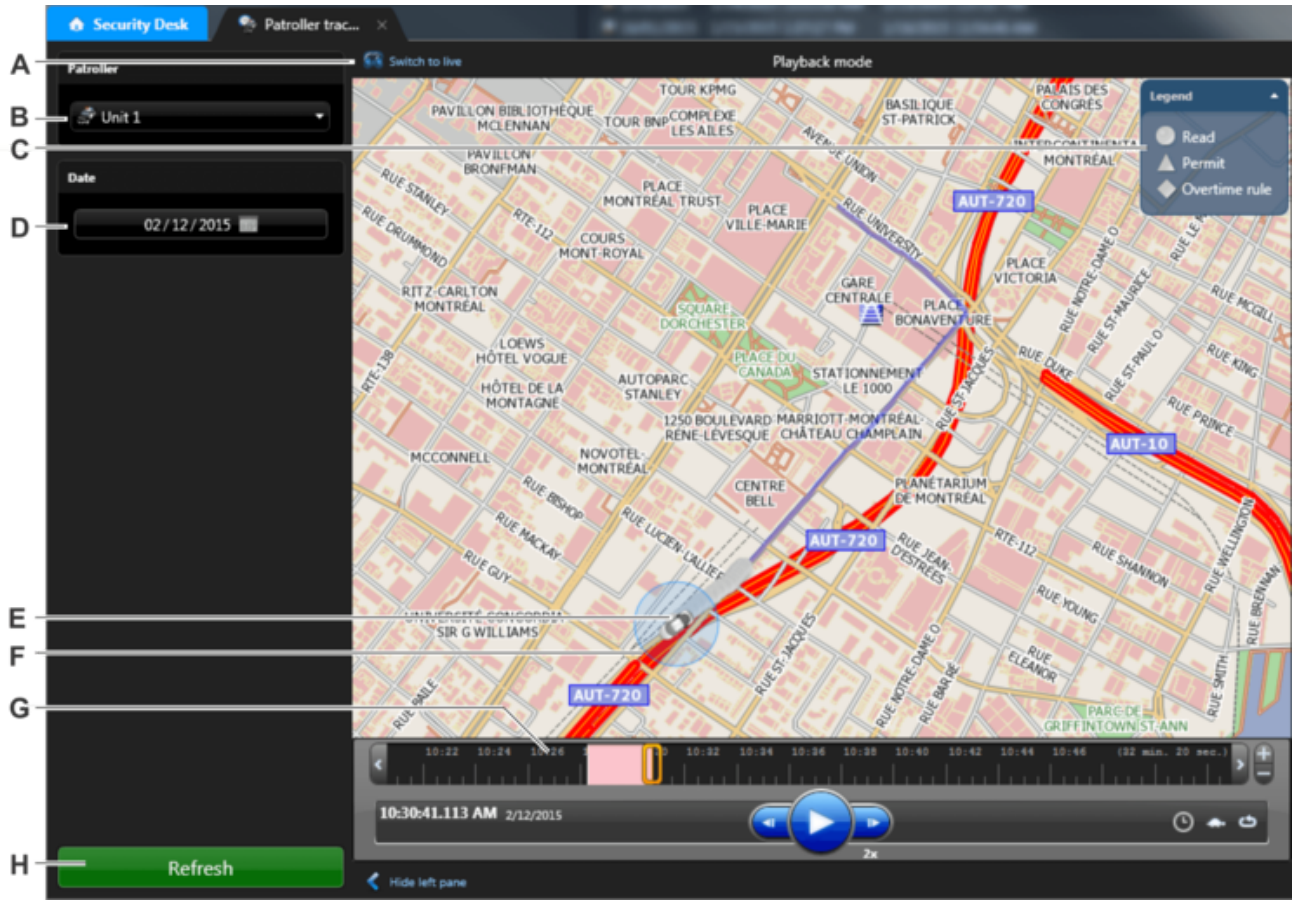
Explorer

- Créer un inventaire de parc de stationnement

7.2.13 | Présentation de la tâche Pistage Genetec Patroller™

Utilisez la tâche Suivi de véhicule de patrouille pour relire un itinéraire emprunté par un Genetec Patroller™ sur une carte, ou pour suivre le véhicule de patrouille sur la carte en temps réel.

La figure suivante montre la tâche Suivi de véhicule de patrouille.



A	Mode de pistage. Sélectionnez le mode souhaité. Le Mode lecture est ouvert par défaut, mais vous pouvez cliquer sur Basculer vers le direct pour suivre la position actuelle du véhicule de patrouille sur la carte.
B	Le véhicule de patrouille que vous examinez
C	Légende de la carte.
D	Date de la ronde du Genetec Patroller™.
E	L'icône de voiture indique la position actuelle du Genetec Patroller™ ainsi que la direction de l'unité Genetec Patroller™ le long de son itinéraire.
F	Le cercle bleu indique la dernière lecture ou alerte de RAPI visionnée dans la frise chronologique.
G	L'itinéraire du Genetec Patroller™ et les événements de RAPI sont représentés sur la frise chronologique
H	Actualisez l'écran et créez un rapport de lecture d'itinéraire Genetec Patroller™.

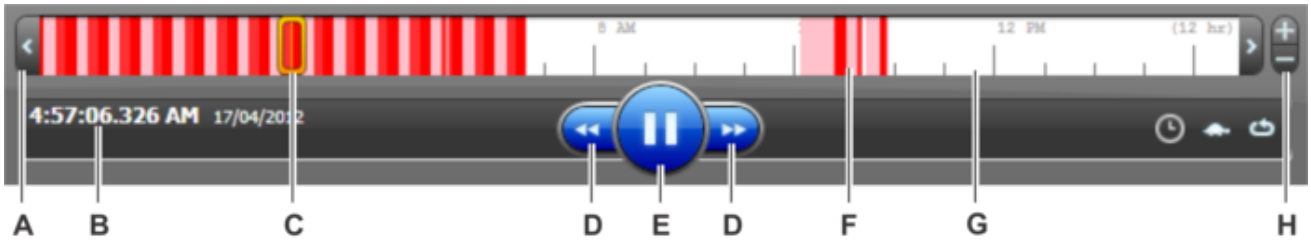
Explorer

- Relire l'itinéraire d'un véhicule de patrouille
- Surveiller les événements de RAPI dans mode Carte
- Suivre la position actuelle d'une unité Genetec Patroller™

7.2.13.1 | Commandes de suivi de la frise chronologique Genetec Patroller™

Utilisez la tâche Pistage de véhicule de patrouille pour relire l'itinéraire emprunté par un véhicule de patrouille un jour donné sur une carte.

La tâche Pistage de Genetec Patroller™ propose les commandes de frise chronologique suivantes pour vous aider à retracer l'itinéraire du véhicule de patrouille et localiser les événements de RAPI.



A	Boutons de défilement	Permet de se déplacer dans la frise sans déplacer la tête de lecture.
B	Marque d'horodatage	Indique la date et l'heure correspondant à la position du curseur de lecture dans la frise chronologique.
C	Curseur de lecture	Indique l'endroit actuel au sein de l'itinéraire du Genetec Patroller™. Pour changer d'image de lecture, faites glisser le curseur vers un autre emplacement ou cliquez dans la frise.
D	Boutons Rembobiner/Avance rapide	Pendant la lecture, les boutons Rembobiner et Avance rapide apparaissent de part et d'autre du bouton Lecture. Lorsque vous cliquez sur Rembobiner ou Avance rapide, un curseur de vitesse apparaît. Faites glisser le curseur vers la droite pour une lecture rapide (1x, 2x, 4x, 6x, 8x, 10x, 20x, 40x et 100x) ou vers la gauche pour un rembobinage (-1x, -4x, -10x, -20x, -40x ou -100x). Lorsque la vitesse souhaitée est définie, relâchez le bouton de la souris. Pour revenir à la vitesse normale (1x), cliquez sur le bouton Lecture/Pause. REMARQUE : La carte n'est pas automatiquement centrée lorsque la lecture n'est pas effectuée à vitesse normale.
E	Lecture/Pause	Basculez entre la lecture et la suspension de la lecture d'itinéraire. Vous pouvez également appuyer sur la barre d'espace.
F	Marqueurs d'événements	Les lignes verticales rouge clair sur la frise indiquent les événements de lecture. Les lignes verticales rouge foncé sur la frise indiquent les événements d'alerte. Cliquez sur un marqueur d'événement pour centrer la carte sur l'endroit de l'événement.
G	Zones blanches	Les zones blanches de la frise représentent une séquence d'itinéraire de Genetec Patroller™. Les zones noires indiquent l'absence de patrouilles à l'heure correspondante. Les zones violettes indiquent « le futur ».
H	Commandes de zoom	Permet de contrôler la partie de la séquence de lecture affichée dans la frise chronologique. Faites un zoom avant dans la frise pour voir l'emplacement précis d'un événement de RAPI.
	Aller à l'heure spécifique	Ouvrez une fenêtre de navigateur pour aller à un endroit précis de l'enregistrement (date et heure).
	Ralenti	Lire l'itinéraire du Genetec Patroller™ au ralenti. Un curseur de contrôle de la vitesse apparaît à droite du bouton de Lecture/Pause. Faites glisser la double flèche du curseur pour modifier la vitesse. Les vitesses de lecture au ralenti disponibles sont : 1/8x, 1/4x, 1/3x, 1/2x et 1x. La vitesse de lecture par défaut est 1/8x. REMARQUE : Le rembobinage au ralenti n'est pas pris en charge.

	Lecture en boucle	Reprendre automatiquement la lecture de la séquence d'itinéraire lorsque la fin de la séquence est atteinte.

Sujet parent : Présentation de la tâche Pistage Genetec Patroller™

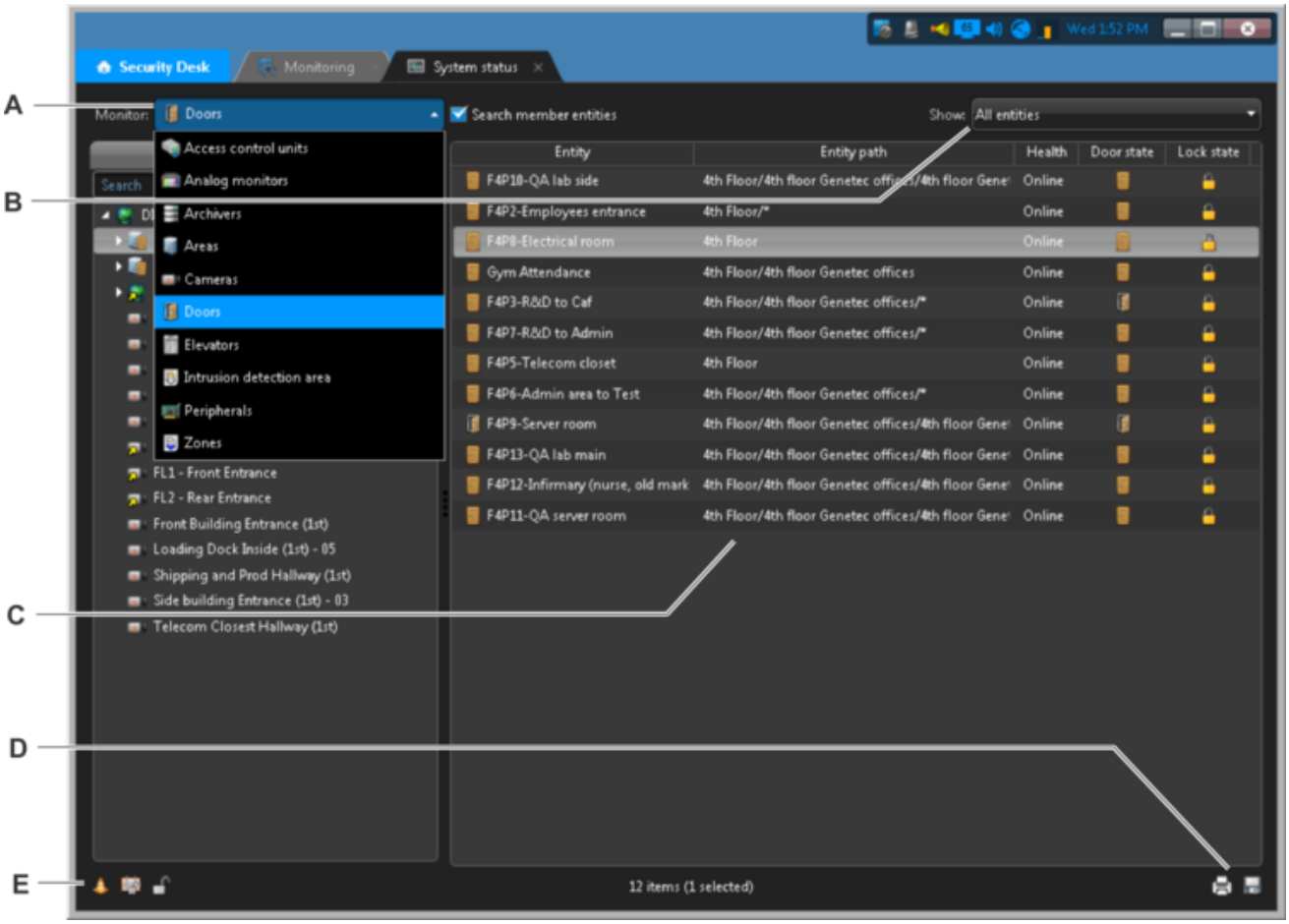
Explorer

- Relire l'itinéraire d'un véhicule de patrouille
- Suivre la position actuelle d'une unité Genetec Patroller™

7.2.14 | Présentation de la tâche État du système

Utilisez la tâche État du système pour surveiller l'état actuel de différents types d'entités et analyser les dysfonctionnements éventuels.

La figure suivante montre la tâche État du système.



A	Types d'entités que vous pouvez surveiller.
B	Types de problèmes que vous pouvez surveiller.
C	L'état des entités est affiché dans le volet de rapport.
D	Cliquez sur pour exporter ou sur pour imprimer le rapport.
E	Commandes propres aux entités.

Explorer

- Surveiller l'état de votre système Security Center
- Exporter un rapport
- Imprimer les rapports générés

7.2.14.1 | Colonnes de la tâche État du système

La tâche État du système vous permet de surveiller l'état actuel de différents types d'entités et analyser les dysfonctionnements éventuels.

Le tableau suivant présente les colonnes affichées pour chaque type d'entité dans la liste déroulante Surveiller.

Entité	Colonne	Description
Unités de contrôle d'accès	Entité	Nom de l'unité
	État	En ligne, hors ligne ou avertissement
	Adresse IP	L'adresse IP de l'unité
	Synchro	État de la synchronisation
	Panne de courant	Oui (✓) ou Non (vide)
	Panne de batterie	Oui (✓) ou Non (vide)
	Micrologiciel	Version du micrologiciel de l'unité
	Altéré	Indique si l'unité a été altérée Oui (✓) ou Non (vide)
	Maintenance	Indique si l'entité est en *mode Maintenance* et la durée du *mode Maitenance*
	Parent	Le parent direct du module d'interface ou des panneaux en aval. Si le parent direct est l'unité de contrôle d'accès, seule la colonne Unité parent est renseignée.
	Unité parent	L'unité de contrôle d'accès parent.
Moniteurs analogiques	Entité	Nom du moniteur analogique
	Chemin de l'entité	Liste de tous les secteurs parents, en partant de l'entité système. Lorsqu'un moniteur analogique a plusieurs secteurs parents, le chemin est représenté par « *\ ».
	État	En ligne, hors ligne ou avertissement
	Entité connectée	Nom des caméras affichées sur le moniteur analogique
Applications	Entité	Type d'application (Config Tool ou Security Desk)
	Source	Ordinateur qui l'héberge
	Nom d'utilisateur	Nom de l'utilisateur connecté
	Version	Version logicielle de l'application client
Archiveurs	Entité	Nom du rôle Archiveur
	Serveurs	Liste des serveurs affectés à ce rôle

Entité	Colonne	Description
	Caméras actives	Nombre de caméras détectées par l'Archiveur
	Caméras d'archivage	Nombre de caméras sur lesquelles l'archivage est activé (En continu, Sur mouvement ou Manuel) et qui ne présentent pas de problèmes d'archivage
	Nombre total de caméras	Nombre de caméras affectées à ce rôle.
	Espace utilisé	Quantité d'espace utilisé par les archives vidéo.
	Utilisation de l'espace disque d'archivage	Pourcentage d'espace utilisé sur le disque comparé à l'espace alloué.
	Débit de réception de l'Archiveur	Débit de réception des données par l'Archiveur
	Débit d'écriture de l'Archiveur	Débit d'écriture sur le disque par l'Archiveur
	Maintenance	Indique si l'entité est en *mode Maintenance* et la durée du *mode Maitenance*
	Dernière mise à jour	Heure de la dernière mise à jour de l'état
Secteurs	Entité	Nom du secteur
	Chemin de l'entité	Liste de tous les secteurs parents, en partant de l'entité système
	État	En ligne, hors ligne ou avertissement
	Niveau de risque	Indique si un niveau de risque est activé pour le secteur sélectionné, ainsi que le nom du niveau de risque. Si aucun niveau de risque n'est activé, la colonne est vide
	Niveau d'accès	(Réservé aux administrateurs) Définit le niveau d'accès minimal des titulaires de cartes nécessaire pour accéder au secteur, en sus des restrictions imposées par les règles d'accès.
	Comptage d'individus	Activé (✓) ou non activé (vide)
	Antiretour	Strict, souple ou aucun (pas d'antiretour)
	Sas	Activé (✓) ou non activé (vide)
	Priorité	Priorité d'entrée de sas : Confinement ou Dérogation
Caméras	Entité	Nom de la caméra
	Chemin de l'entité	Liste de tous les secteurs parents, en partant de l'entité système. Lorsqu'une caméra a plusieurs secteurs parents, le chemin est représenté par « *\ ».
	État	En ligne, hors ligne ou avertissement
	Enregistrement	État de l'enregistrement
	Signal analogique	Perdu, disponible ou inconnu (caméras IP).

Entité	Colonne	Description
	Bloqué	Indique si l'affichage de la caméra est bloqué pour certains utilisateurs. Bloqué (✓) ou non bloqué (vide)
	Maintenance	Indique si l'entité est en *mode Maintenance* et la durée du *mode Maitenance*
Portes	Entité	Nom de la porte
	Chemin de l'entité	Liste de tous les secteurs parents, en partant de l'entité système
	État	En ligne, hors ligne ou avertissement
	État de la porte	Ouvert () ou fermé ()
	État du verrou	Verrouillé () ou déverrouillé ()
Ascenseurs	Entité	Nom de l'ascenseur
	Chemin de l'entité	Liste de tous les secteurs parents, en partant de l'entité système
	État	En ligne, hors ligne ou avertissement
Problèmes de fonctionnement	Type d'entité	Icône représentant le type d'entité
	Entité	Nom de l'entité
	Source	Pour une entité locale, indique le serveur qui l'héberge. Pour une entité fédérée, indique le nom du rôle de Federation™
	Chemin de l'entité	Liste de tous les secteurs parents, en partant de l'entité système
	État	En ligne, hors ligne ou avertissement
	Maintenance	Indique si l'entité est en *mode Maintenance* et la durée du *mode Maitenance*
Secteurs de détection d'intrusion	Entité	Nom du secteur de détection d'intrusion
	Chemin de l'entité	Liste de tous les secteurs parents, en partant de l'entité système
	État	En ligne, hors ligne ou avertissement
	État d'alarme	Alarme active, Alarme coupée, Délai d'entrée ou Normal
	État d'armement	Armement, Désarmé (non prêt), Désarmé (prêt à armer), *Armement global* ou *Périmètre armé*
	Contourner	Actif ou inactif (représenté par une icône)
	Problème	Oui (✓) ou Non (vide)
Unités de détection d'intrusion	Entité	Nom de l'unité de détection d'intrusion
	État	En ligne, hors ligne ou avertissement
	Panne de courant	Oui (✓) ou Non (vide)
	Panne de batterie	Oui (✓) ou Non (vide)

Entité	Colonne	Description
	Sabotage	Oui (✓) ou Non (vide)
	Maintenance	Indique si l'entité est en *mode Maintenance* et la durée du *mode Maitenance*
Macros	Entité	Nom de la macro
	Heure de début	Heure de lancement de la macro
	Instigateur	Nom de l'utilisateur ayant déclenché la macro
Applications mobiles	Entité	Nom de l'appareil mobile
	Source	Modèle de l'appareil mobile
	Nom d'utilisateur	Nom de l'utilisateur connecté via cet appareil
	Version	Genetec™ Mobile Version de
	Sur liste noire	Indique si l'appareil est sur liste noire (✓) ou non (vide)
	SE	Système d'exploitation installé sur l'appareil
	Rôle actuel	Nom du rôle Mobile Server auquel l'appareil est connecté
Périphériques	Nom	Nom du périphérique
	Type	Entrée, sortie, lecteur
	État	Normal, actif ou désactivé (entrées et lecteurs)
	Infos supplémentaires	Réglages propres au type de périphérique
	Contrôle	Entité contrôlée par le périphérique.
	État	En ligne, hors ligne ou avertissement
	ID logique	ID logique affecté au périphérique
	Nom physique	Nom affecté par le système au périphérique
Rôles	Entité	Nom du rôle
	État	En ligne, hors ligne ou avertissement
	Serveur actuel	Nom du serveur qui héberge ce rôle
	Serveurs	Liste des serveurs affectés à ce rôle
	Version	Version logicielle du rôle
	État	Activé () ou désactivé ()
	Maintenance	Indique si l'entité est en *mode Maintenance* et la durée du *mode Maitenance*
Itinéraires	Route	Nom de la route, et indication des deux réseaux qu'elle relie

Entité	Colonne	Description
	Configuration actuelle	Diffusion individuelle TCP, diffusion individuelle UDP ou multidiffusion
	Capacités détectées	Diffusion individuelle TCP, diffusion individuelle UDP ou multidiffusion REMARQUE : Un *Redirecteur* est nécessaire sur chaque réseau pour pouvoir détecter les capacités.
	État	OK, ou message d'avertissement décrivant la source du problème REMARQUE : Un *Redirecteur* est nécessaire sur chaque réseau pour pouvoir afficher l'état
Serveurs	Entité	Nom du serveur
	État	En ligne, hors ligne ou avertissement
	Rôles	Rôles affectés à ce serveur
	Certificat	*certificat d'identité* actuel et sa durée de validité
	Maintenance	Indique si l'entité est en *mode Maintenance* et la durée du *mode Maitenance*
Modules vidéo	Serveur	Serveur qui héberge le module d'analyse vidéo
	Entité	Type de module d'analyse vidéo
	Nombre total de caméras	Nombre de flux vidéo en cours de traitement rapporté au nombre total de caméras configurées pour être analysées par ce module
	Utilisation du processeur	Utilisation du processeur sur le serveur
	Utilisation de la mémoire	Utilisation de la mémoire sur le serveur
	Taux de réception de l'agent d'analyse	Bande passante entrante sur le serveur
	Taux de transmission de l'agent d'analyse	Bande passante sortante sur le serveur
	Modèle de processeur graphique	Carte graphique Nvidia détectée sur le serveur
	Pilote graphique	Version du pilote Nvidia installé sur le serveur
	Utilisation du processeur graphique	Utilisation du processeur graphique sur la carte vidéo
	Charge du moteur vidéo	Pourcentage de la puce dédiée au décodage vidéo utilisé dans le processeur graphique
	Utilisation de la mémoire vidéo	Utilisation de la mémoire sur la carte vidéo

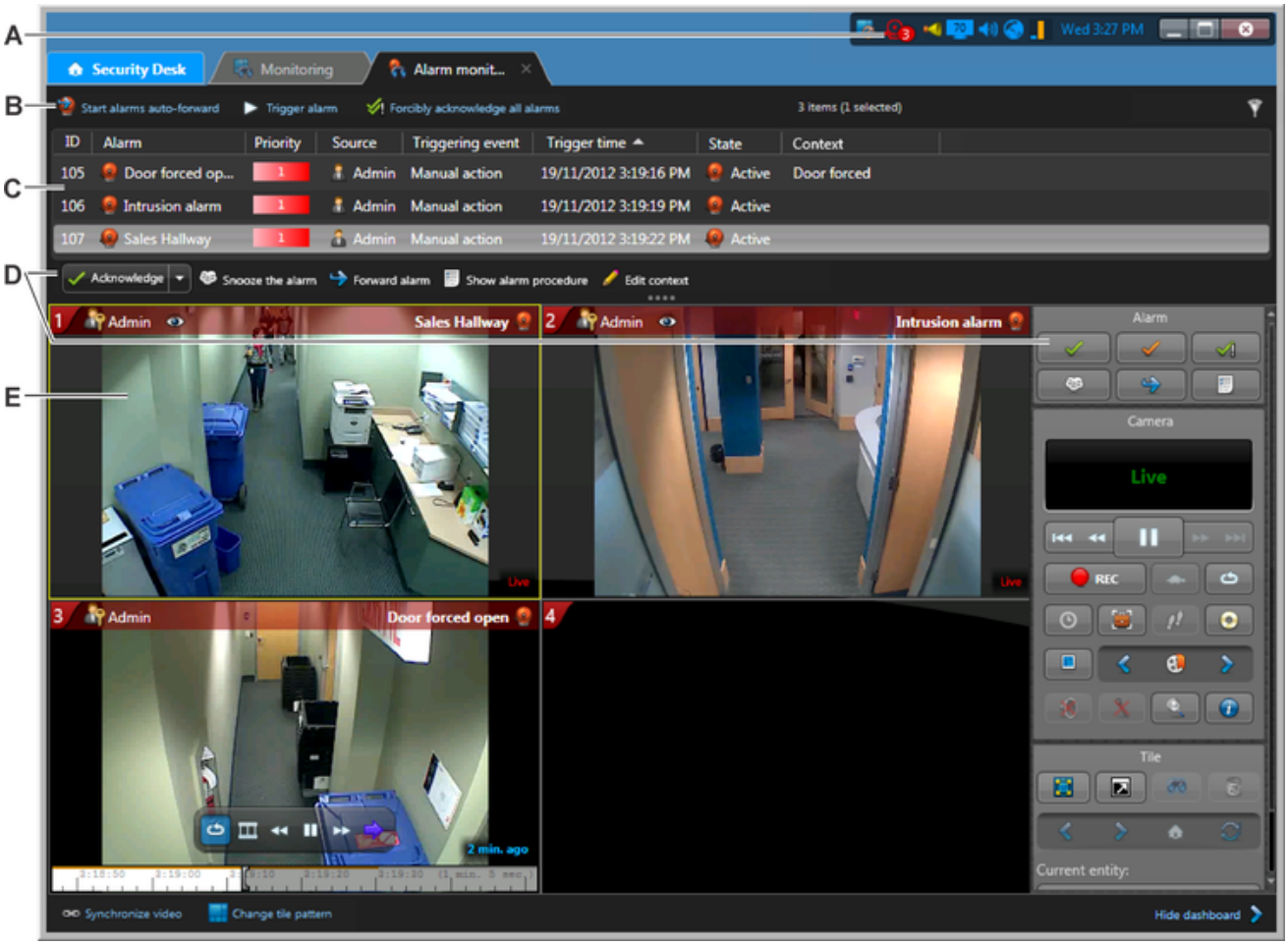
Entité	Colonne	Description
	Charge du contrôleur mémoire	Utilisation actuelle de la bande passante mémoire sur la carte graphique (transfert de la mémoire entre l'UC et le processeur graphique)
	Dernière mise à jour	Dernière mise à jour des statistiques
Zones	Entité	Nom de la zone
	Chemin de l'entité	Liste de tous les secteurs parents, en partant de l'entité système
	État	En ligne, hors ligne ou avertissement
	État	Normal, actif ou problème
	Armé	Indique si la zone est armée ou non
	Maintenance	Indique si l'entité est en *mode Maintenance* et la durée du *mode Maitenance*

Sujet parent : Présentation de la tâche État du système

7.2.15 | Présentation de la tâche Surveillance d'alarmes dansSecurity Center

Utilisez la tâche Surveillance d'alarmes pour surveiller les alarmes, répondre aux *alarmes actives* en temps réel, et consulter les anciennes alarmes.

La figure suivante montre la tâche Surveillance d'alarmes.



A	L'icône de surveillance d'alarmes devient rouge lorsqu'une alarme est active. Cliquez deux fois pour ouvrir la tâche Surveillance d'alarmes.
B	Autres commandes d'alarmes. • Démarrer le transfert automatique des alarmes. • Déclenchez l'alarme. • Forcer l'acquittement de toutes les alarmes. • Réglez les options de filtre d'alarmes.
C	Les alarmes actuelles sont affichées dans la liste d'alarmes. Pour modifier les colonnes affichées, effectuez un clic droit sur un en-tête de colonne, puis cliquez sur Sélectionner les colonnes. Cliquez avec le bouton droit sur une alarme pour accéder à la page de configuration de l'alarme ou son entité source.
D	Commandes pour contrôler les alarmes actives. Cliquez sur la liste déroulante Acquitter pour voir toutes les commandes disponibles.
E	Vidéo d'une alarme dans une tuile. Les détails de l'alarme sont incrustés dans un cadre de couleur sur la vidéo.

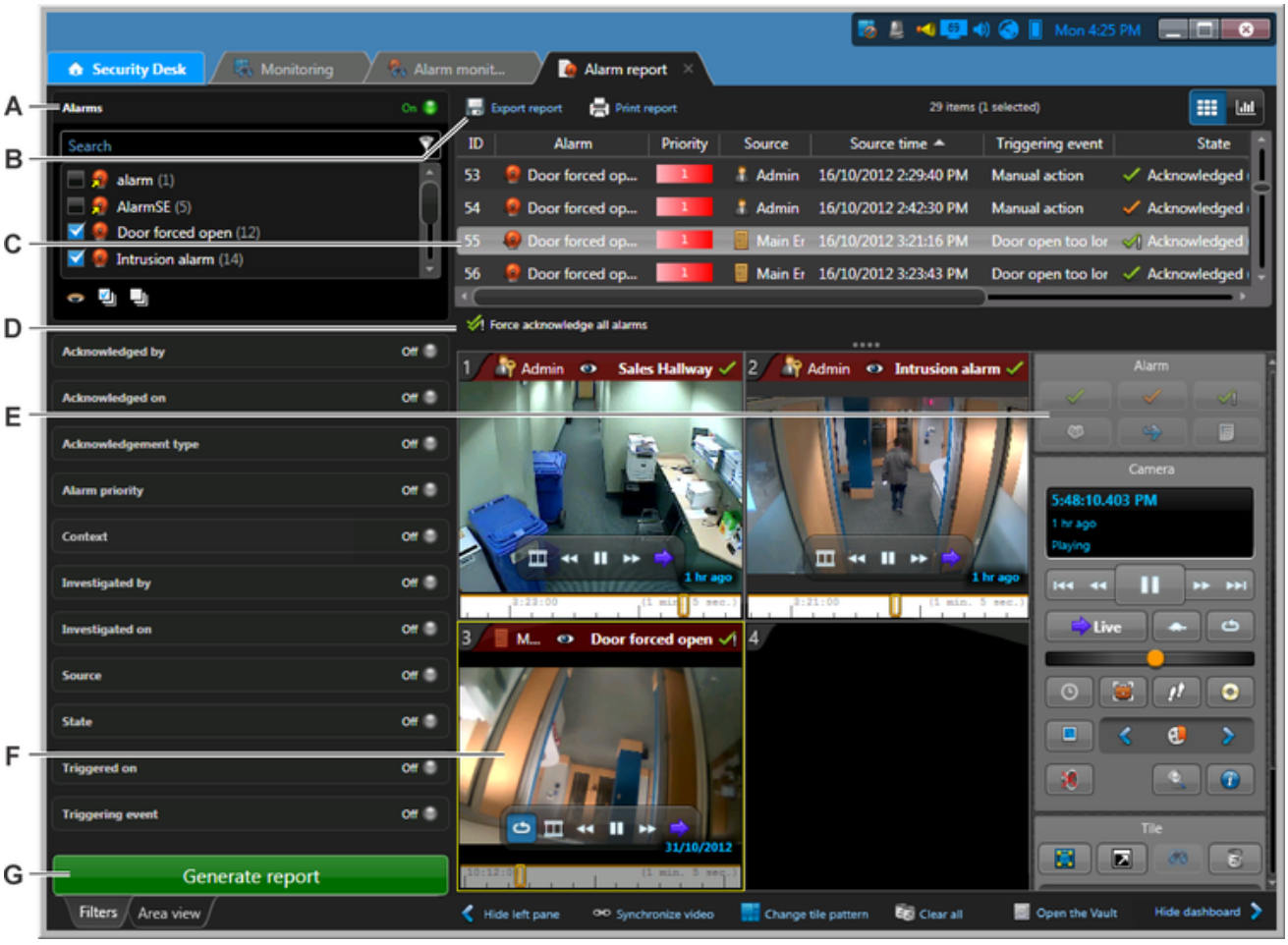
Explorer

- Acquittement des alarmes

7.2.16 | Présentation de la tâche Rapport d'alarmes dans Security Center

Utilisez la tâche Rapport d'alarmes pour rechercher et analyser les alarmes actuelles et passées.

La figure suivante montre la tâche Rapport d'alarmes.



A	Filtres de recherche.
B	Cliquez sur pour exporter ou sur pour imprimer le rapport.
C	Le résultat du rapport d'alarme est affiché dans le volet de rapport. Cliquez avec le bouton droit sur une alarme pour accéder à la page de configuration de l'alarme ou son entité source.
D	Acquitter de force toutes les alarmes actives.
E	Widget Alarme.
F	Vidéo d'une alarme dans une tuile.
G	Générer le rapport.

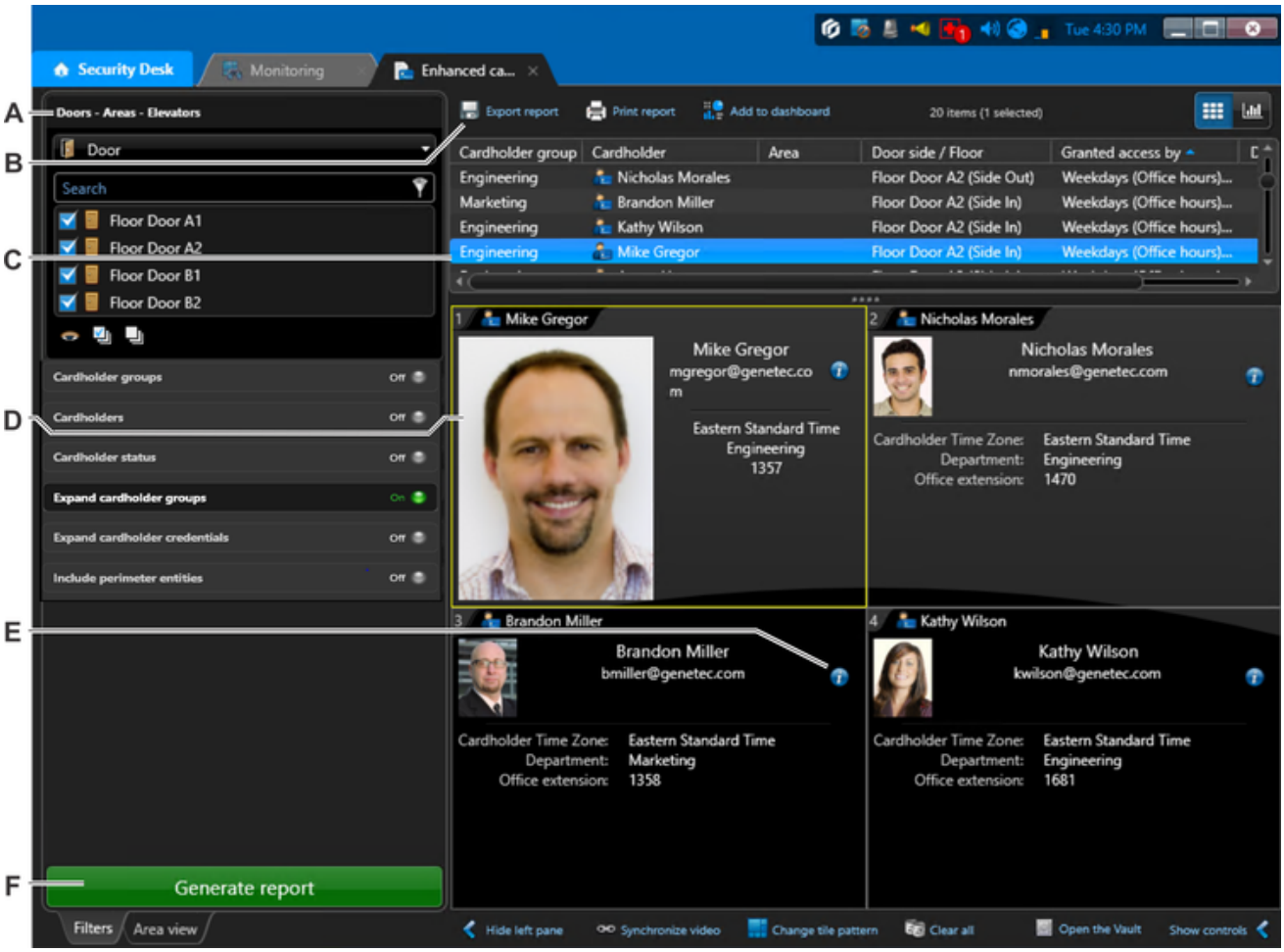
Explorer

- Widget Alarme
- Exporter un rapport
- Imprimer les rapports générés
- Analyser les alarmes actuelles et passées
- Affichage des alarmes sur le canevas de Security Desk

7.2.17 | Présentation de la tâche Droits d'accès avancés de titulaires de cartes

Utilisez le rapport *Droits d'accès avancés de titulaire de cartes* pour savoir quels titulaires de cartes et groupes de titulaires de cartes ont accès ou non à certains secteurs, portes et ascenseurs.

Ce rapport est utile, car il vous permet de voir où un titulaire peut aller, et quand il peut y aller, et ainsi de savoir si vous devez modifier ses propriétés de règles d'accès. Vous pouvez également utiliser ce rapport pour rechercher les membres d'un groupe de titulaires de cartes.
CONSEIL : Recherchez un titulaire de cartes ou groupe de titulaires de cartes à la fois pour obtenir un rapport plus précis.



A	Filtres de recherche. **Groupes de titulaires de cartes** Limitez votre recherche à des groupes de titulaires de cartes particuliers. **Titulaires de cartes** Limitez la recherche à certains titulaires de cartes. **Développer les groupes de titulaires** Affichez les membres des groupes de titulaires de cartes sélectionnés dans le rapport, au lieu des groupes eux-mêmes. **Inclure les entités du périmètre** Intégrez les entités situées sur le périmètre des secteurs inclus dans le rapport. **Champs personnalisés de titulaires de cartes** Si des champs personnalisés sont configurés pour les titulaires de cartes que vous examinez, ils peuvent tous être inclus dans ce rapport.
B	Exportez ou imprimez le rapport.
C	Tous les titulaires de cartes ou groupes de titulaires de cartes dont l'accès aux secteurs et points d'accès sélectionnés a été accordé ou refusé sont affichés dans le volet de rapport.
D	Afficher les propriétés de titulaires de cartes dans une tuile.
E	- Afficher des informations complémentaires sur les titulaires de cartes.

D	Générer le rapport.

Explorer

- Affichage des titulaires de cartes sur le canevas de Security Desk

7.2.17.1 | Activer la tâche Droits d'accès avancés de titulaires de cartes

Pour utiliser le rapport *Droits d'accès avancés de titulaires de cartes*, vous devez activer le rapport dans Security Desk à partir du fichier SecurityDesk.plugins.xml.

Procédure

1. Ouvrez le fichier SecurityDesk.Modules.xml, situé sous C:\Program files (x86)\Genetec Security Center 5.x\ sur un ordinateur 64 bits, et sous C:\Program files\Genetec Security Center 5.x\ sur un ordinateur 32 bits.
2. Réglez l'attribut Genetec.AccessControl.Reporting.Casinos.dll sur true.
   ```
   <Report Assembly="Genetec.AccessControl.Reporting.Casinos.dll" Enabled="true" />
   ```
3. Enregistrez le fichier XML, puis redémarrez Security Desk.

Résultats

À l'ouverture suivante de Security Desk, la tâche *Droits d'accès avancés de titulaires de cartes* sera disponible.

Sujet parent : Présentation de la tâche Droits d'accès avancés de titulaires de cartes