Guide de l'utilisateur de Sipelia

2.0 GA

Cliquez ici pour la plus récente version de ce document.

Avis de copyright

Informations sur le document

Titre du document : Guide de l'utilisateur de Sipelia

Numéro de document : FR.704.004-V2.0B(3)

Date de mise à jour du document : February 26, 2015

Envoyez vos commentaires, corrections et suggestions concernant ce guide à documentation@genetec.com.

À propos de ce guide

Ce guide s'adresse aux administrateurs de Sipelia. Il décrit comment installer, configurer et gérer le module Sipelia dans le cadre d'un système Security Center.

Notes et avertissements

Les avis et avertissements suivants peuvent être utilisés dans ce guide :

- **Conseil**. Suggère une manière d'appliquer les informations d'un thème ou d'une étape.
- **Remarque**. Décrit un cas particulier, ou développe un point important.
- **Important**. Souligne une information critique concernant un thème ou une étape.
- **Attention**. Indique qu'une action ou étape peut entraîner la perte de données, des problèmes de sécurité ou des problèmes de performances.
- **Avertissement**. Indique qu'une action ou une étape peut entraîner des dommages physiques, ou endommager le matériel.

IMPORTANT : Les sujets abordés dans ce guide peuvent faire référence à des informations publiées sur des sites web de tiers qui étaient correctes au moment de leur publication, mais qui peuvent changer sans que Genetec n'en soit notifié au préalable.

Sommaire

1

Prise en main

Cette section aborde les sujets suivants:

Présentation de Sipelia

Sipelia est un module principal de Security Center qui permet aux utilisateurs de passer, recevoir et gérer les appels audio et vidéo basés sur la norme SIP sur le réseau. Exploitant le protocole open source SIP (Session Initiation Protocol), Sipelia gère aussi l'intégration de plates-formes de vidéosurveillance et de contrôle d'accès comprenant des systèmes d'interphone, et permet aux utilisateurs de consigner les activités d'appel.

Fonctionnalités principales

Lorsque Sipelia est installé au sein de Security Center, vous pouvez effectuer les tâches suivantes :

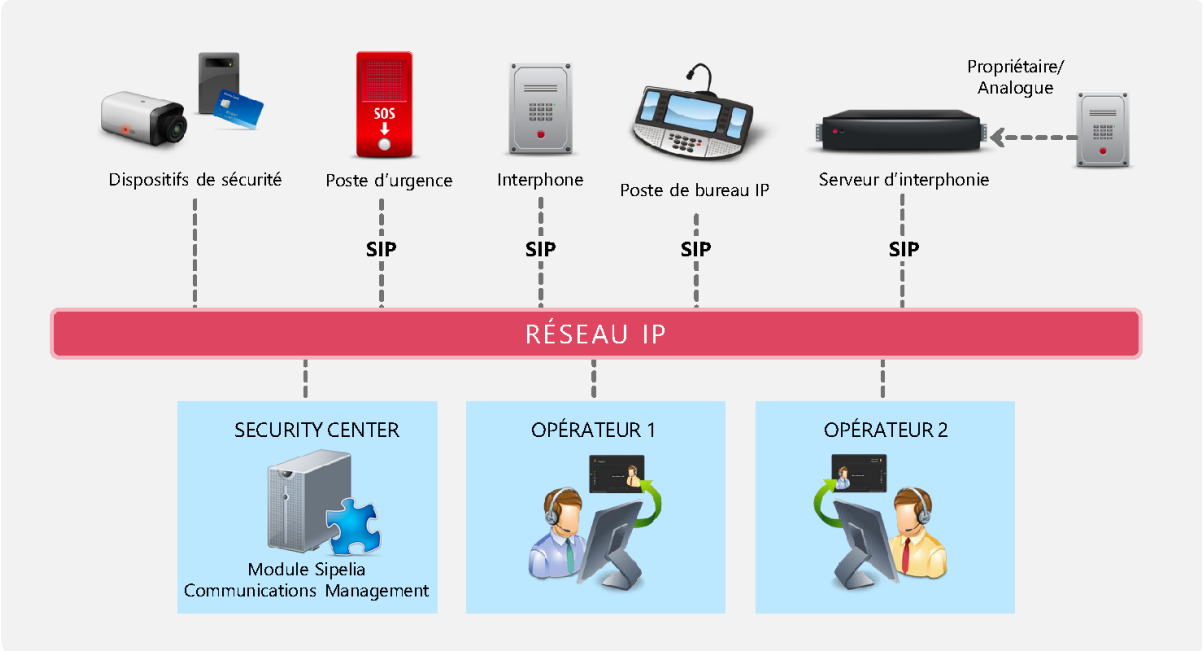
- Connecter les webcams et casques USB standard aux postes Security Desk, afin de pouvoir passer des appels voix et vidéo par le biais de Security Center.
- Recevoir des notifications d'appels entrants dans la zone de notification de Security Desk.
- Passer, prendre, transférer, mettre en attente ou annuler des appels dans une boîte de dialogue dédiée.
- Créer des rapports sur les activités au sein de sessions d'appel particulières.
- Regarder toutes les sessions d'appel associées à de la vidéo.
- Contrôler des caméras, portes, zones et sorties durant un appel.
- Déployer une solution basée sur la technologie SIP pour simplifier l'exploitation de votre infrastructure de communication existante.
- Se connecter à des interphones SIP, des centraux d'interphones et des apps mobiles via la norme SIP.
- Créer une liste personnalisée de contacts, afin que les utilisateurs puissent appeler rapidement leurs correspondants. Les listes de contacts peuvent inclure d'autres utilisateurs Security Center ainsi que des appareils SIP.
- Créer des groupes d'appel afin que plusieurs utilisateurs et *entités SIP* Security Center puissent recevoir les appels entrants en même temps ou en séquence, jusqu'à ce que quelqu'un réponde à l'appel.

Applications typiques

Une intégration Sipelia au sein de Security Center est adaptée aux applications suivantes :

- Répondre à une urgence et l'analyser
- Répondre aux employés ayant perdu leurs cartes
- Accorder l'accès à des espaces hautement sécurisés
- Surveiller et gérer qui pénètre et quitte une aire de stationnement
- Appels vidéo entre utilisateurs, pour des communications plus efficaces

Présentation de Sipelia Communications Management



Fonctionnement des licences dans Sipelia

Sipelia requiert un ensemble de licences pour permettre l'installation et l'utilisation du module externe dans Security Center et pour activer des fonctionnalités plus avancées.

Sipelia exige les licences suivantes :

- **GSC-Sipelia-Base:** La licence du système de base est requise pour installer le module externe Sipelia dans Security Center et pour autoriser les opérateurs à passer et recevoir des appels.
- **GSC-Sipelia-1SIP-STD:** La licence standard permet d'utiliser un appareil SIP (comme un interphone SIP) dans Security Center, qu'il soit inscrit sur Sipelia Server ou disponible par l'intermédiaire d'un Jonction SIP. Vous devez disposer d'une licence standard par appareil SIP que vous ajoutez à votre système.
- **GSC-Sipelia-1SIP-ADV:** La licence avancée permet l'enregistrement des sessions d'appel et le basculement du rôle Module externe Sipelia vers un serveur de secours en cas de besoin. Vous devez disposer d'une licence avancée par licence standard que vous ajoutez à votre système.

  REMARQUE : Si les nombres de licences avancées et standard ne correspondent pas, le système prend en compte le nombre inférieur pour les deux types de licences, comme illustré ci-dessous.
- **GSC-Sipelia-1Trunk:** La licence trunk (jonction) permet d'ajouter et configurer une Jonction SIP. Vous devez disposer d'une licence pour chaque Jonction SIP que vous ajoutez à votre système.

Exemple

L'exemple de licence ci-dessous illustre la manière dont le système comptabilise les licences en cas de différence :

Type de licence	Nombre de licences installées	Nombre de licences appliquées
GSC-Sipelia-Base	1	1
GSC-Sipelia-1SIP-STD	100	50
GSC-Sipelia-1SIP-ADV	50	50
GSC-Sipelia-1Trunk	4	4

Déployer Sipelia

Pour intégrer les communications SIP à Security Center, afin que les utilisateurs puissent communiquer par VoIP, vous pouvez déployer Sipelia au sein de votre système Security Center.

Avant de commencer

- Lisez les *Notes de version Sipelia 2.0 GA* .
- Prenez connaissance des ports par défaut de Sipelia Server.
- Prenez connaissance du vocabulaire VoIP courant et des termes du glossaire Sipelia utilisés dans ce guide.

Pour déployer Sipelia :

1 Installez Sipelia Server.
2 Configurez le service de communication système.
3 Configurez le port SIP de Sipelia Server.
4 Définissez les plages de numéros de postes SIP.
5 Configurez l'enregistrement des sessions d'appel audio et vidéo.
6 Configurez des comptes SIP pour les utilisateurs.
7 Créez un groupe d'appel de base.
8 Créez des groupes d'appel personnalisés.
9 Ajoutez vos interphones SIP.
10 Inscrivez vos interphones SIP sur Sipelia Server.
11 Installez Sipelia Client sur chaque poste Security Desk qui exécutera Sipelia.
12 Configurez vos appareils pour les appels audio et vidéo dans Security Desk.
13 Configurez la communication bidirectionnelle entre Sipelia Server et d'autres serveurs SIP.

Utilisation de Sipelia dans Security Desk

Dans Security Desk, vous pouvez passer et recevoir des appels, gérer votre liste de contacts et créer des rapports sur les appels effectués.

Pour en savoir plus sur l'utilisation de Sipelia dans Security Desk, consultez les vidéos suivantes :

- Sipelia - présentation de l'interface.
- Sipelia - gestion des appels.
- Sipelia - présentation de la tâche Rapport d'appels.

2

Installation

Cette section aborde les sujets suivants:

À propos Sipelia Server

Sipelia Server est le composant serveur SIP de Sipelia. Il reçoit et gère les informations sur les diverses extrémités SIP, puis permet les échanges entre extrémités communiquant en environnement SIP. Sipelia Server recueille et stocke également des informations importantes, comme les données de listes de contact, les réglages de serveur SIP et les enregistrements de sessions d'appel.

Sipelia Server est un module externe de serveur (🧩) qui doit être hébergé par un rôle Module externe Security Center. Par conséquent, Sipelia Server doit être installé sur chaque serveur Security Center sur lequel vous comptez héberger le rôle Module externe.

Sipelia Server stocke les données suivantes :

- Options utilisateur
- Liste de contacts
- Informations de session (par exemple : utilisateurs, heure et durée des appels et entités associées)
- Fichiers audio et vidéo associés aux sessions d'appel
- Configurations de numéros de postes pour les utilisateurs et appareils
- Réglages de serveurs SIP
- Configuration de groupes d'appel
- Configuration de jonctions SIP
- Configuration de plans de numérotation
- Réglages d'enregistrement des utilisateurs et appareils
- Les événements Security Center associés à l'entité interphone SIP

Ports par défaut pour Sipelia Server

Pour assurer le bon fonctionnement de Sipelia, les ports utilisés par les modules Sipelia Server doivent être ouverts et redirigés pour traverser les pare-feu.

IMPORTANT : Lorsque vous configurez les ports, vérifiez qu'ils sont ouverts et qu'ils ne sont pas utilisés par une autre application sur le même ordinateur. Par exemple, si Sipelia Server est installé sur le même ordinateur que le module Genetec Server, vous ne pouvez pas utiliser le même port que Security Center ou que d'une autre application.

Sipelia Server composant	Numéro de port par défaut	Protocole	Description
Port de communication système	5672	TCP	Le port utilisé par Sipelia pour communiquer avec le service de communication système RabbitMQ. La valeur par défaut est **5672**, qui correspond à la valeur d'une configuration standard du service RabbitMQ.
Port du service de configuration	8201	TCP	Le port utilisé par Config Tool pour échanger des réglages de configuration avec Sipelia Server. La valeur par défaut est **8201**. En cas de problème avec ce numéro de port, vous pouvez saisir un autre numéro valable.
Port de transfert de session	8202	TCP	Le port utilisé par Sipelia Server pour transférer les enregistrements vers la tâche *Rapport d'appels* dans Security Desk. La valeur par défaut est **8202**. En cas de problème avec ce numéro de port, vous pouvez saisir un autre numéro valable.
Sipelia Server : Port SIP	5060	TCP (SIP)	Le port utilisé pour activer le protocole SIP sur Sipelia Server. Par conséquent, il s'agit de la base de toutes les communications SIP dans Sipelia. La valeur par défaut est **5060**. Chaque extrémité SIP, comme les téléphones logiciels et les interphones SIP, qui doit se connecter à Sipelia Server doit être configurée avec ce numéro de port.
Jonctions SIP : Port SIP	5060	TCP (SIP)	Le port utilisé par la jonction SIP pour communiquer avec Sipelia Server. Puisque les jonctions SIP sont des serveurs, la valeur par défaut est **5060**. Les jonctions SIP sont nécessaires si vous avez un appareil connecté à un PBX externe, et que vous souhaitez le connecter à Sipelia. Dans ce cas, le PBX sera en mode jonction avec Sipelia Server.
Plage de ports UDP de Sipelia Server	20000-20500	UDP (SIP)	La plage de ports pour le protocole UDP (User Diagram Protocol). Les ports UDP sont utilisés par les différents clients SIP pour émettre et recevoir des

Sipelia Server composant	Numéro de port par défaut	Protocole	Description
			données de communication. La plage par défaut va de **20000** à **20500**. Il est recommandé de conserver les réglages par défaut et de ne les modifier que si Sipelia signale des problèmes de communication avec Security Desk liés aux ports. La plage de ports UDP utilisée par Sipelia Server est définie par les propriétés *MinimumPortRange* et *MaximumPortRange* dans *C:\ProgramData\Genetec Sipelia 2.0\SipServer\SipServer.config*.

Sipelia Client

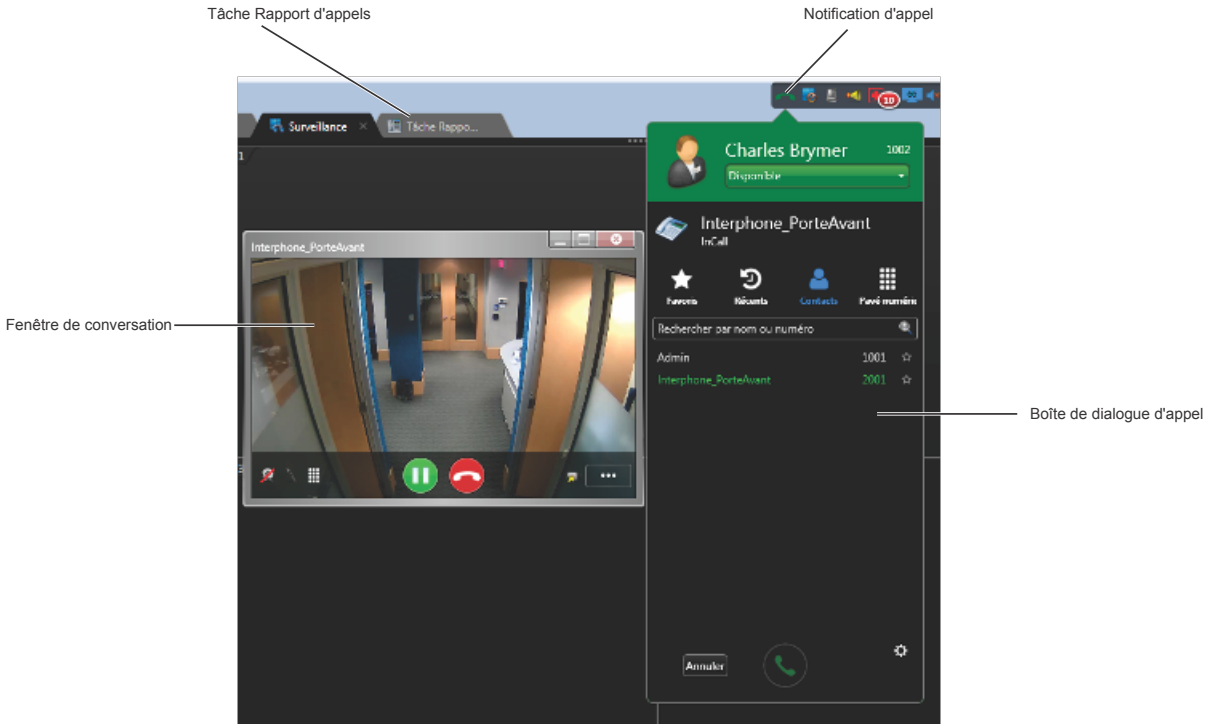
Sipelia Client est le composant téléphone logiciel de Sipelia. Par conséquent, il installe les éléments d'interface utilisateur du module Sipelia, comme la boîte de dialogue d'appel et la fenêtre de conversation.

Sipelia Client installe les éléments suivants :

- Zone de notification
- Boîte de dialogue d'appel
- Fenêtre de conversation
- *Rapport d'appels* tâche

Bien que ce ne soit pas obligatoire, il est conseillé d'installer Sipelia Client après avoir installé et déployé Sipelia Server. Si Sipelia Client est installé avant Sipelia Server, l'interface utilisateur de Sipelia ne sera pas opérationnelle.

Sipelia Client doit être installé sur chaque poste Security Desk exécutant Sipelia, et transforme ainsi Security Desk en client SIP (ou téléphone logiciel). L'image suivante présente certains composants de Sipelia Client.



Ports par défaut pour Sipelia Client

Pour assurer le bon fonctionnement de Sipelia, les ports utilisés par Sipelia Client doivent être correctement configurés dans Security Desk.

IMPORTANT : Lorsque vous configurez les ports, vérifiez qu'ils sont ouverts et qu'ils ne sont pas utilisés par une autre application sur le même ordinateur.

Sipelia Client composant	Numéro de port par défaut	Protocole	Description
Avancé : Plage de ports UDP	20000-20500	UDP (SIP)	La plage de ports pour le protocole UDP (User Diagram Protocol). Les ports UDP sont utilisés par les différents clients SIP pour émettre et recevoir des données de communication. La plage par défaut va de **20000** à **20500**. Il est recommandé de conserver les réglages par défaut et de ne les modifier que si Sipelia signale des problèmes de communication avec Security Desk liés aux ports. Vous pouvez modifier la plage de ports UDP en cliquant sur **Options** > **Sipelia** > **Avancé** dans Security Desk.

Installation Sipelia Server

Pour intégrer les fonctions SIP à Security Center et permettre au système de stocker des données comme les contacts téléphoniques et les enregistrements de sessions d'appel, vous devez installer *Sipelia Server* avant de configurer le module Sipelia dans Config Tool.

Avant de commencer

Les conditions suivantes sont requises :

- Les serveurs doivent répondre à la configuration matérielle décrite dans les *Notes de version Sipelia*.
- Config Tool est installé sur le système sur lequel vous comptez installer Sipelia Server.

IMPORTANT : Il est conseillé d'installer Sipelia Server sur un serveur d'extension Security Center dédié. Reportez-vous au *Guide de l'administrateur Security Center* pour en savoir plus sur l'ajout d'un serveur d'extension à votre système Security Center.

À savoir

Sipelia Server est un module externe de serveur () qui doit être hébergé par un rôle Module externe Security Center. Par conséquent, Sipelia Server doit être installé sur chaque serveur Security Center sur lequel vous comptez héberger le rôle Module externe.

Bien que ce ne soit pas obligatoire, il est conseillé d'installer Sipelia Client après avoir installé et déployé Sipelia Server. Si Sipelia Client est installé avant Sipelia Server, l'interface utilisateur de Sipelia ne sera pas opérationnelle.

Pour installer Sipelia Server :

1 Téléchargez le produit sur (https://gtap.genetec.com). Vous devez disposer d'un nom d'utilisateur et d'un mot de passe pour vous connecter à GTAP.

2 Cliquez deux fois sur **setup.exe** pour lancer le programme d'installation du produit.

La fenêtre *Assistant InstallShield* du produit apparaît.

3 Sélectionnez la langue d'installation, puis cliquez sur **OK**.

Ce choix de langue ne limite pas les langues disponibles dans le logiciel installé. L'interface de Sipelia adopte la langue sélectionnée pour Security Center.

4 Cliquez sur **Suivant**.

5 Lisez le contrat de licence, acceptez-le, puis cliquez sur **Suivant**.

6 Sélectionnez un dossier pour l'installation du produit, puis cliquez sur **Suivant**.

7 Dans la boîte de dialogue *Installation personnalisée*, sélectionnez **Serveur**, puis cliquez sur **Suivant**.

8 Cliquez sur **Installer**.

L'installation peut prendre quelques minutes.

9 Lorsqu'elle est terminée, sélectionnez **Redémarrer Genetec Server**, puis cliquez sur **Terminer**.

IMPORTANT : Vous devez redémarrer *Genetec Server* pour que le système détecte l'installation d'un nouveau module externe.

Le redémarrage de Genetec Server entraîne une brève interruption du service sur le serveur. Si vous ne pouvez pas vous permettre d'interrompre le service pour l'instant, vous pouvez repousser le redémarrage de Genetec Server à plus tard, dès lors que vous le faites avant de configurer Sipelia

dans Config Tool. Pour éviter les interruptions, il est conseillé d'installer Sipelia Server sur un serveur d'extension Security Center dédié.

En plus de Sipelia Server, le service de communication système RabbitMQ inclus dans le programme d'installation de Sipelia Server est installé automatiquement. RabbitMQ est le canal de communication entre Security Desk et Sipelia Server. Il s'agit d'un service indispensable au bon fonctionnement de Sipelia.

Lorsque vous avez terminé

Dans Config Tool, créez le rôle Module externeSipelia.

Installation Sipelia Client

Pour transformer Security Desk en *client SIP* et utiliser les différentes fonctionnalités du module Sipelia, vous devez installer Sipelia Client sur chaque poste Security Desk qui utilise Sipelia.

Avant de commencer

Les conditions suivantes sont requises :

- Sipelia Server est installé sur votre système Security Center.
- Security Center Client est installé sur l'ordinateur sur lequel vous voulez installer Sipelia Client.
- Sur des postes Security Desk qui possèdent plusieurs interfaces (cartes) réseau, l'interface réseau à être utilisée par Sipelia Client doit être configurée avec la plus haute priorité.

À savoir

Bien que ce ne soit pas obligatoire, il est conseillé d'installer Sipelia Client après avoir installé et déployé Sipelia Server. Si Sipelia Client est installé avant Sipelia Server, l'interface utilisateur de Sipelia ne sera pas opérationnelle.

Pour installer Sipelia Client :

1 Téléchargez le produit sur (https://gtap.genetec.com). Vous devez disposer d'un nom d'utilisateur et d'un mot de passe pour vous connecter à GTAP.

2 Cliquez deux fois sur **setup.exe** pour lancer le programme d'installation du produit.

La fenêtre *Assistant InstallShield* du produit apparaît.

3 Sélectionnez la langue d'installation, puis cliquez sur **OK**.

Ce choix de langue ne limite pas les langues disponibles dans le logiciel installé. L'interface de Sipelia adopte la langue sélectionnée pour Security Center.

4 Cliquez sur **Suivant**.

5 Lisez le contrat de licence, acceptez-le, puis cliquez sur **Suivant**.

6 Sélectionnez un dossier pour l'installation du produit, puis cliquez sur **Suivant**.

7 Dans la boîte de dialogue *Installation personnalisée*, développez le nœud **Client**.

8 Si Plan Manager est installé et si vous souhaitez ajouter des interphones SIP sur les cartes, sélectionnez **Objet interphone Plan Manager**, puis cliquez sur **Suivant**.

9 Cliquez sur **Installer**.

L'installation peut prendre quelques minutes.

10 Lorsque vous avez terminé, cliquez sur **Terminer**.

Lorsque vous avez terminé

Configurez vos appareils pour les appels audio et vidéo dans Security Desk.

3

Configuration

Cette section aborde les sujets suivants:

Créer le rôle Module externe Sipelia

Une fois que vous avez installé Sipelia Server sur un serveur Security Center, vous pouvez créer le rôle Module externe Sipelia dans Config Tool.

Avant de commencer

Vérifiez que Sipelia Server est bien installé.

Pour créer le rôle Module externe Sipelia :

1 Connectez-vous à Security Center avec Config Tool.

2 Ouvrez la tâche *Modules externes*, puis cliquez sur **Module externe** ( )

L'Assistant *Créer un rôle : Module externe* apparaît.

3 Dans la liste déroulante **Serveur**, sélectionnez le serveur qui hébergera le rôle Sipelia Server.

4 Dans la section **Sélectionner le type de module externe**, sélectionnez **Sipelia**.

5 Renseignez les valeurs **Serveur de base de données** et **Base de données** pour la base de données Sipelia, ou utilisez les valeurs proposées par défaut.

6 Cliquez sur **Suivant**, donnez un nom et une description à l'entité, puis sélectionnez la partition souhaitée pour ce rôle.

7 Cliquez sur **Suivant** et vérifiez que les informations fournies sont justes.

8 Cliquez sur **Créer**, puis sur **Fermer**.

Sipelia apparaît dans la liste des rôles Module externe ( ). La création de la base de données du rôle peut prendre quelques minutes.

Lorsque vous avez terminé

Si vous déployez Sipelia, configurez le service de communication système.

Configurer le service de communication système

Pour assurer le bon fonctionnement des communications entre Security Desk et Sipelia Server, vous devez configurer le service de communication système sur l'ordinateur qui héberge Sipelia Server.

À savoir

Sipelia utilise le service de communication système RabbitMQ. RabbitMQ est un service Windows externe open source qui permet aux applications hébergées sur différents serveurs à différents moments de communiquer entre réseaux et ordinateurs différents, qu'ils soient en ligne ou non. Sipelia Server requiert ce service pour communiquer avec Security Desk. Par conséquent, il s'agit d'une exigence pour toute installation de Sipelia.

L'adresse IP de Sipelia Server doit être la première adresse indiquée dans les propriétés du serveur de Security Center.

Pour configurer le service de communication système :

1 Connectez-vous à Security Center avec Config Tool, et ouvrez la tâche Modules externes.

2 Sélectionnez le rôle Module externe Sipelia, puis cliquez sur **Général**

3 Configurez les réglages suivants :

- **Adresse de service de communication:** Le nom d'hôte ou l'adresse IP de l'ordinateur qui héberge le service de communication système, RabbitMQ. Le service RabbitMQ est nécessaire au fonctionnement deSipelia Server, et il est automatiquement installé sur l'ordinateur qui héberge Sipelia Server. La valeur par défaut est **localhost**. Ne modifiez la valeur par défaut que si vous souhaitez référencer un service RabbitMQ exécuté sur un autre serveur.

  En cas de problèmes de DNS associés au réglage par défaut de **localhost**, vous pouvez entrer l'adresse IP de l'ordinateur qui héberge le service RabbitMQ.

- **Port de service de communication:** Le port utilisé par Sipelia pour communiquer avec le service de communication système RabbitMQ. La valeur par défaut est **5672**, qui correspond à la valeur d'une configuration standard du service RabbitMQ.

4 Ouvrez la tâche *Réseau*, puis sélectionnez le serveur qui héberge le rôle Module externe Sipelia.

5 Cliquez sur **Propriétés**, et vérifiez que la première adresse IP indiquée dans **Adresses privées** (la première de la liste), est celle qui est censée être utilisée par le serveur.

Le service de communication système est configuré. Les problèmes éventuels de connexion RabbitMQ sont décrits dans la fenêtre *Diagnostic de module externe*.

Pour une description des autres ports affichés sur la page Général, voir Ports par défaut pour Sipelia Server à la page 9.

Lorsque vous avez terminé

Si vous déployez Sipelia, configurez le port SIP de Sipelia Server.

Configurer le port SIP de Sipelia Server

Pour activer le protocole SIP sur Sipelia Server, vous devez configurer le port SIP de Sipelia Server, et vérifier que toutes les *extrémités SIP* connectées utilisent le même numéro de port.

Avant de commencer

Si vous déployez Sipelia, configurez le service de communication système.

À savoir

Lorsque vous configurez les ports, vérifiez qu'ils sont ouverts et qu'ils ne sont pas utilisés par une autre application sur le même ordinateur. Par exemple, si Sipelia Server est installé sur le même ordinateur que le module Genetec Server, vous ne pouvez pas utiliser le même port que Security Center ou que d'une autre application.

Connectez-vous à Security Center avec Config Tool, et ouvrez la tâche Modules externes.

Sélectionnez le rôle Module externe Sipelia, puis cliquez sur **Serveurs**

Configurez les réglages suivants :

- **Port SIP:** Le port utilisé pour activer le protocole SIP sur Sipelia Server. Par conséquent, il s'agit de la base de toutes les communications SIP dans Sipelia. La valeur par défaut est **5060**. Chaque extrémité SIP, comme les téléphones logiciels et les interphones SIP, qui doit se connecter à Sipelia Server doit être configurée avec ce numéro de port.

Si vous avez modifié la valeur par défaut du port SIP, vérifiez que tous les clients SIP connectés à Sipelia Server utilisent la nouvelle valeur.

Lorsque vous avez terminé

Si vous déployez Sipelia, spécifiez les plages de numéros de postes SIP.

Définir les plages de numéros de postes SIP

Avant d'affecter un numéro de poste à un utilisateur, un *groupe d'appel* ou un interphone SIP, vous pouvez spécifier plusieurs plages de numéros de postes, puis affecter une plage différente à chaque *entité SIP*.

Avant de commencer

Si vous déployez Sipelia, configurez le port SIP de Sipelia Server.

À savoir

Les plages de postes téléphoniques sont des groupes de postes SIP que vous pouvez affecter à chacune de vos entités SIP. Chaque plage de postes doit avoir un mot de passe par défaut, vous ne pouvez pas dépasser 1000 postes par plage, et vous devez avoir au moins une plage de postes définie pour pouvoir connecter une entité SIP à Sipelia. Par défaut, Sipelia fournit cinq plages de postes (Plage 1 à Plage 5), dotées du mot de passe par défaut 1234.

Pour définir une plage de numéros de postes SIP :

1 Connectez-vous à Security Center avec Config Tool, et ouvrez la tâche Modules externes.

2 Sélectionnez le rôle Module externe Sipelia, puis cliquez sur **Serveurs**

3 Notez les plages déjà définies, et décidez comment les affecter aux différentes entités SIP.

4 Pour ajouter une plage de postes, cliquez sur **Ajouter une plage** ( ).

5 Entrez les informations suivantes :

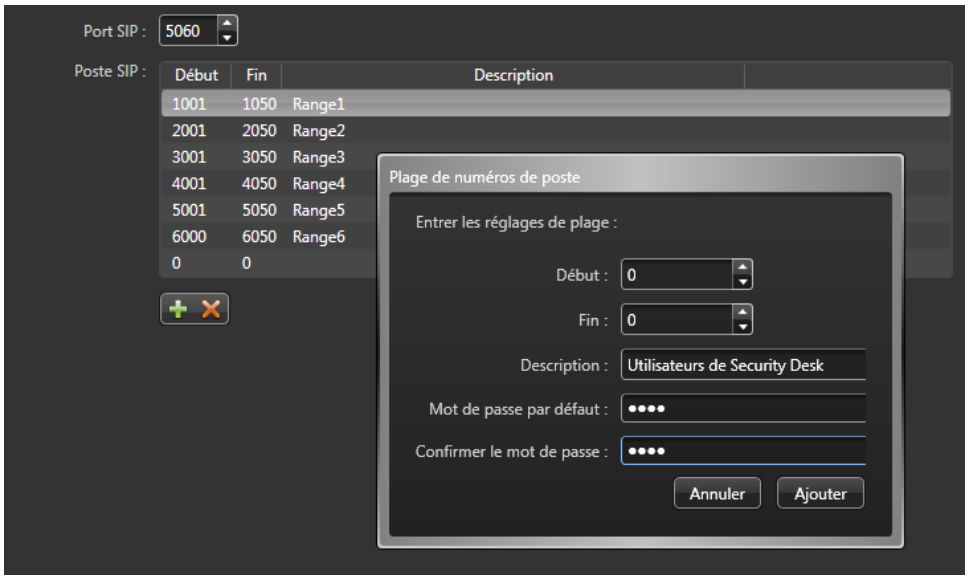
- **Début:** La valeur de début de la plage de postes SIP. La valeur de début doit être unique et ne peut pas être supérieure à la valeur de fin.
- **Fin:** La valeur de fin de la plage de postes SIP. La valeur de fin doit être unique et ne peut pas être inférieure à la valeur de début.
- **Description:** Une phrase qui décrit la plage, par exemple l'entité SIP pour laquelle la plage est réservée.
- **Mot de passe par défaut:** Le mot de passe pour tous les postes SIP de la plage. Toutes les entités SIP dont les postes appartiennent à cette plage doivent connaître ce mot de passe. Chaque extrémité SIP, comme les téléphones logiciels et les interphones SIP, qui doit se connecter à Sipelia Server doit être configurée avec cette valeur de mot de passe (associée au numéro de poste).
- **Confirmer le mot de passe:** La confirmation du mot de passe par défaut. Les valeurs des deux champs de mot de passe doivent concorder.

REMARQUE : Les valeurs de début et de fin des plages de postes sont incluses dans la plage.

6 Cliquez sur **Ajouter**, puis sur **Appliquer**.

Exemple

Comme illustré ci-dessous, imaginons que vous souhaitez définir une plage de postes réservée aux utilisateurs Security Center, et que vous voulez limiter la plage à 50 postes. Ajoutez une plage de postes unique qui couvre 50 numéros, puis entrez un mot de passe par défaut qui s'appliquera à chaque poste de la plage. Lorsque vous configurez des comptes SIP pour vos utilisateurs Security Center, vous pouvez affecter un numéro de poste de la plage à chaque utilisateur, mais vous ne pouvez affecter qu'un maximum de 50 utilisateurs à la plage.



Lorsque vous avez terminé

Si vous déployez Sipelia, configurez l'enregistrement des sessions d'appel audio et vidéo.

Enregistrer les données audio et vidéo des sessions d'appel

Pour enregistrer les données audio et vidéo des sessions d'appel impliquant les utilisateurs et interphones SIP, vous devez configurer les réglages d'enregistrement sur la page Enregistrement du rôle Module externe Sipelia.

Avant de commencer

Vérifiez que vous disposez de licences avancées installées sur votre système.

À savoir

Les options **Utilisateur qui enregistre :** et **Appareil qui enregistre :** s'appliquent à toutes les entités utilisateur et interphone SIP, sauf si un entité est configurée différemment, auquel cas elle n'héritera plus des valeurs par défaut du rôle Module externe Sipelia.

Pour enregistrer les données audio et vidéo des sessions d'appel :

1 Connectez-vous à Security Center avec Config Tool, et ouvrez la tâche Modules externes.

2 Sélectionnez le rôle Module externe Sipelia, puis cliquez sur Enregistrement.

3 Entrez les informations suivantes :

- **Utilisateur qui enregistre :** Permet l'enregistrement de sessions d'appels auxquelles participent les entités utilisateur (en tant qu'émetteur ou destinataire de l'appel). Une fois enregistrées, les sessions d'appel peuvent être écoutées et exportées dans la tâche *Rapport d'appels* de Security Desk. La valeur par défaut est définie au niveau du rôle, puis héritée par toutes les entités utilisateur. Vous pouvez activer ou désactiver l'enregistrement pour un utilisateur particulier par l'intermédiaire du réglage **Enregistrement audio et vidéo** disponible sur la page VoIP de l'entité utilisateur, sans affecter les autres utilisateurs.
- **Appareil qui enregistre :** Permet l'enregistrement de sessions d'appels auxquelles participent les entités interphone SIP (en tant qu'émetteur ou destinataire de l'appel). Une fois enregistrées, les sessions d'appel peuvent être écoutées et exportées dans la tâche *Rapport d'appels*. La valeur par défaut est définie au niveau du rôle, puis héritée par toutes les entités interphone SIP. Vous pouvez activer ou désactiver l'enregistrement pour un interphone SIP particulier par l'intermédiaire du réglage **Enregistrement audio et vidéo** disponible sur la page VoIP de l'entité interphone SIP, sans affecter les autres interphones.
- **Dossier d'enregistrement :** Le répertoire utilisé pour stocker les fichiers d'enregistrement. Il peut s'agir d'un répertoire local ou réseau. Le rôle de module externe Sipelia affiche une erreur si le format du chemin n'est pas valable, si le chemin est inaccessible, ou si le chemin réseau n'existe pas ou est inaccessible. Si le répertoire spécifié par un chemin en local n'existe pas, il est automatiquement créé. Si le chemin devient non valable, l'enregistrement de la session d'appels est interrompu et les fichiers enregistrés sont perdus.
- **Nettoyage automatique:** Permet la suppression automatique des fichiers enregistrés. Cette option est activée par défaut avec une période de rétention de 30 jours.

4 Cliquez sur **Appliquer**.

Lorsque vous avez terminé

Si vous déployez Sipelia, configurez des comptes SIP pour les utilisateurs de Security Desk.

Configurer des comptes SIP pour les utilisateurs Security Center.

Pour permettre aux utilisateurs Security Center de communiquer entre eux à l'aide des commandes SIP de Security Desk, vous devez configurer un compte SIP pour chacun d'entre eux avec les privilèges appropriés.

Avant de commencer

- Créez les utilisateurs pour lesquels vous souhaitez configurer un compte SIP (voir le *Guide de l'administrateur Security Center* pour en savoir plus).
- Si vous ne souhaitez pas utiliser les plages de numéros de postes configurées par défaut, spécifiez vos propres plages de postes téléphoniques SIP.

À savoir

Une fois qu'un compte SIP a été configuré pour un utilisateur Security Center, l'utilisateur devient une entité SIP. Une entité SIP est une entité Security Center dotée de fonctionnalités SIP. Dans Security Center, il peut s'agir d'utilisateurs, de groupes d'appel ou d'appareils SIP comme des interphones SIP.

Pour configurer un compte SIP pour un utilisateur Security Center :

1 Connectez-vous à Security Center avec Config Tool, puis ouvrez la tâche Sécurité.

2 Cliquez sur **Utilisateurs**, puis sélectionnez un utilisateur dans la liste.

3 Cliquez sur l'onglet **VoIP** pour configurer cette entité SIP en tant qu'extrémité SIP.

4 Affectez un numéro de poste à votre entité SIP de l'une des manières suivantes :

- Cliquez sur **Affectation automatique**. Cette option affecte automatiquement l'entité SIP au premier poste disponible d'une plage donnée. Par conséquent, il s'agit de la méthode conseillée pour affecter les postes aux utilisateurs, groupes d'appel et interphones SIP. Cliquez sur ce bouton, sélectionnez une plage existante, puis cliquez sur **Appliquer.**
- Entrez les informations suivantes :
  - **Poste SIP:** Le numéro de poste de l'entité SIP. Pour pouvoir communiquer avec d'autres extrémités SIP, chaque entité SIP (utilisateur, groupe d'appel ou interphone) dans Security Center doit avoir un numéro de poste attitré. Entrez le numéro de poste manuellement, ou cliquez sur **Affectation automatique** (méthode recommandée).
  - **Mot de passe:** Le mot de passe du poste. Ce mot de passe est spécifié lors de la création de la plage de postes. Chaque poste d'une plage donnée est configuré automatiquement pour recevoir un mot de passe qui correspond au mot de passe par défaut de la plage. Lorsque vous cliquez sur **Affectation automatique**, ce champ est renseigné avec le bon mot de passe pour la plage, et nous recommandons donc cette méthode.

  IMPORTANT : Bien que vous puissiez modifier le mot de passe d'un poste en en saisissant un, il est déconseillé de le faire ici. Il est recommandé de ne modifier les mots de passe des postes téléphoniques que dans l'onglet Serveurs du rôle Module externe Sipelia.

5 Configurez les réglages suivants :

- **Enregistrer le son et la vidéo:** Permet l'enregistrement des sessions d'appels auxquelles participe l'entité SIP (en tant qu'émetteur ou destinataire de l'appel). Une fois enregistrées, les sessions d'appel peuvent être écoutées et exportées dans la tâche *Rapport d'appels*. La valeur par défaut est héritée des réglages d'enregistrement globaux configurés sur la page Enregistrement

du rôle de module externe Sipelia. Lorsque vous modifiez ce réglage au niveau de l'entité, celle-ci n'hérite plus la valeur du réglage global, ce qui vous permet d'activer ou désactiver l'enregistrement pour une entité sans affecter les autres.

- **Profil d'itinérance:** Lorsque cette option est activée (valeur par défaut), elle stocke les options Security Desk de l'utilisateur dans la base de données. Les utilisateurs peuvent alors se connecter à Security Desk depuis un autre ordinateur du même réseau en conservant leurs réglages. Par exemple, si un utilisateur a configuré l'affichage des appels entrants dans une tuile, il verra le même comportement s'il utilise un autre poste Security Desk du même réseau.

6 Cliquez sur l'onglet *Privilèges* pour configurer les privilèges Sipelia de l'utilisateur.

7 Sous **Tous les privilèges** > **Privilèges d'applications** > **Sipelia**, sélectionnez les privilèges qui correspondent aux actions que l'utilisateur est autorisé à exécuter.

IMPORTANT : Les privilèges sont configurés à *Non défini* par défaut. Ils doivent être explicitement autorisés afin que les utilisateurs puisse faire et recevoir des appels.

8 Cliquez sur **Appliquer**.

Lorsque vous avez terminé

- Associez une caméra Security Center à l'utilisateur.
- Autorisez l'utilisateur à voir les photos des autres utilisateurs.
- Ajoutez vos interphones SIP.

Autoriser les utilisateurs à voir les photos des autres utilisateurs

Pour que les utilisateurs de Security Center puissent voir les photos des autres utilisateurs dans Sipelia, vous devez manuellement les ajouter dans la configuration de sécurité du champ personnalisé correspondant.

Avant de commencer

- Créez le rôle Module externe Sipelia.

À savoir

Lorsque créé, le rôle Module externe Sipelia ajoute automatiquement le champ personnalisé *Photo* dans Security Center. La photo de chaque utilisateur, affichée dans la liste de contacts par exemple, est fournie par ce champ personnalisé. Afin de voir les photos, les utilisateurs doivent être ajoutés à la propriété *Sécurité* de ce champ personnalisé.

Pour autoriser un utilisateur à voir les photos:

1 Connectez-vous à Security Center avec Config Tool, puis ouvrez la tâche *Système*.

2 Cliquez sur Champs personnalisés, sélectionnez *Photo* dans la liste, puis cliquez sur **Modifier l'élément** ( ).

3 Sous *Sécurité*, cliquez sur **Ajouter un élément** ( ), puis sélectionnez l'utilisateur.

BONNE PRATIQUE : Vous pouvez ajouter tous vos utilisateurs Sipelia dans un seul groupe d'utilisateurs, puis ajouter ce groupe au champ personnalisé. De cette façon, à chaque fois que des utilisateurs sont ajoutés au groupe, ils auront automatiquement accès aux photos.

4 Cliquez sur **OK** > **Enregistrer et fermer** > **Appliquer**.

Associer des caméras Security Center aux utilisateurs

Pour étendre votre capacité de surveillance avec Security Desk, vous pouvez associer des caméras Security Center à vos utilisateurs, pour que le flux vidéo en temps réel provenant des caméras Security Center soit affiché durant les appels entre eux.

Avant de commencer

- Ajoutez les utilisateurs Security Center (voir le *Guide de l'administrateur Security Center* pour en savoir plus).
- Configurez des comptes SIP pour les utilisateurs Security Center.

À savoir

Les flux vidéo provenant d'une caméra Security Center n'exigent pas de connexion SIP, et ne sont donc pas considérés comme des appels vidéo. Pour configurer les appels vidéo entre entités SIP, vous devez configurer les appareils audio et vidéo requis dans Security Desk.

Contrairement aux interphones SIP auxquels vous pouvez associer des caméras, portes, zones et sorties, vous ne pouvez associer qu'une caméra à un utilisateur Security Center.

Pour associer une caméra Security Center à un utilisateur :

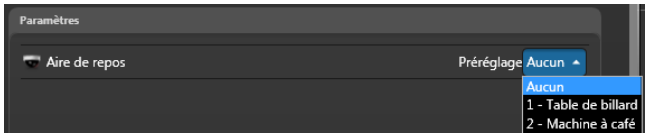
1 Connectez-vous à Security Center avec Config Tool, puis ouvrez la tâche Sécurité.

2 Cliquez sur **Utilisateurs**, puis sélectionnez un utilisateur dans la liste.

3 Cliquez sur l'onglet **VoIP** pour configurer cette entité SIP en tant qu'extrémité SIP.

4 Dans la section *Entités associées*, cliquez sur **Ajouter une entité** ( ).

5 Dans l'*Assistant d'association d'entités*, recherchez et sélectionnez l'entité caméra que vous souhaitez associer à l'utilisateur, puis cliquez sur **Suivant**. Si vous sélectionnez une caméra PTZ, vous pouvez sélectionner le préréglage PTZ dont vous souhaitez afficher le flux durant un appel.



6 Confirmez la sélection en cliquant sur **Suivant**, puis sur **Appliquer**.

7 Lorsque l'*Assistant d'association d'entités* est fermé, cliquez sur **Appliquer** pour enregistrer les modifications.

L'entité que vous avez sélectionnée apparaît dans la liste des entités associées.

8 (Facultatif) Pour configurer l'entité associée que vous avez ajoutée, cliquez sur .

9 (Facultatif) Activez **Afficher les événements** pour l'utilisateur. Afficher les événements permet d'activer les événements pour les utilisateurs et les interphones SIP, afin de pouvoir créer des événements personnalisés au sein du système (par exemple, pour déclencher une alarme si un appel reste sans réponse). Pour chaque utilisateur ou interphone SIP, vous pouvez sélectionner un événement personnalisé pour chacun des états d'appel suivants : Sonnerie en cours ; Appel déjà en cours ; Occupé ; Sans réponse ; Erreur ; Raccrocher. Pour en savoir plus sur les événements personnalisés, voir le *Guide de l'administrateur Security Center.*

10 Associez d'autres caméras à l'utilisateur en répétant les étapes ci-dessus.

La caméra sélectionnée est associée à l'utilisateur. Durant un appel, le flux en temps réel de la caméra apparaît dans la fenêtre de conversation ou la tuile Security Desk des interlocuteurs de l'utilisateur. Si vous avez associé plusieurs caméras, les utilisateurs peuvent basculer entre les différents flux vidéo.

Exemple

Imaginons que vous avez associé les deux caméras suivantes à l'utilisateur Charles : *Front Building Entrance* et *Emergency Exit*. Comme le montre l'image suivante, lorsque Charles est en conversation avec des utilisateurs Security Center, ses interlocuteurs peuvent basculer entre les flux vidéo en temps réel des deux caméras.

Ajouter des interphones SIP

Pour renforcer la sécurité de vos installations et accorder l'accès aux personnes après vérification de leur identité, vous pouvez ajouter un interphone SIP, puis l'associer à diverses entités Security Center, comme une caméra ou une porte.

Avant de commencer

- Installez l'interphone SIP en suivant les recommandations du fabricant de l'appareil.
- Si vous souhaitez connecter un interphone SIP à une *Jonction SIP* plutôt qu'à Sipelia Server, ajoutez une jonction SIP, puis définissez les règles de plan de numérotation associées.
- Spécifiez une plage de numéros de postes pour vos interphones SIP. Il est conseillé de dédier des plages de postes pour chaque entité SIP particulière, surtout les interphones qui communiquent avec Sipelia Server par l'intermédiaire d'une *Jonction SIP*.

À savoir

Un interphone SIP est une extrémité SIP intelligente qui offre une connectivité bidirectionnelle en environnement SIP. Dans Security Center, un interphone SIP est une entité SIP reconnue, et la seule à correspondre à un appareil réel. Les autres entités SIP dans Security Center sont les utilisateurs et les groupes d'appel.

Pour ajouter un interphone SIP :

1 Connectez-vous à Security Center avec Config Tool, et ouvrez la tâche Modules externes.

2 Sélectionnez le rôle Module externe **Sipelia**.

3 Au bas de la page, cliquez sur **Ajouter un interphone** ( ).

4 Donnez un nom descriptif à l'interphone SIP, puis cliquez sur **Ajouter**.

La tâche Vue logique apparaît, et l'interphone ajouté apparaît dans la liste des entités.

5 Cliquez sur l'onglet **VoIP** pour configurer cette entité SIP en tant qu'extrémité SIP.

6 Affectez un numéro de poste à votre entité SIP de l'une des manières suivantes :

- Cliquez sur **Affectation automatique**. Cette option affecte automatiquement l'entité SIP au premier poste disponible d'une plage donnée. Par conséquent, il s'agit de la méthode conseillée pour affecter les postes aux utilisateurs, groupes d'appel et interphones SIP. Cliquez sur ce bouton, sélectionnez une plage existante, puis cliquez sur **Appliquer.**
- Entrez les informations suivantes :
  - **Poste SIP:** Le numéro de poste de l'entité SIP. Pour pouvoir communiquer avec d'autres extrémités SIP, chaque entité SIP (utilisateur, groupe d'appel ou interphone) dans Security Center doit avoir un numéro de poste attitré. Entrez le numéro de poste manuellement, ou cliquez sur **Affectation automatique** (méthode recommandée).
  - **Mot de passe:** Le mot de passe du poste. Ce mot de passe est spécifié lors de la création de la plage de postes. Chaque poste d'une plage donnée est configuré automatiquement pour recevoir un mot de passe qui correspond au mot de passe par défaut de la plage. Lorsque vous cliquez sur **Affectation automatique**, ce champ est renseigné avec le bon mot de passe pour la plage, et nous recommandons donc cette méthode.

  IMPORTANT : Bien que vous puissiez modifier le mot de passe d'un poste en en saisissant un, il est déconseillé de le faire ici. Il est recommandé de ne modifier les mots de passe des postes téléphoniques que dans l'onglet Serveurs du rôle Module externe Sipelia.

7 Configurez les réglages suivants :

- **Enregistrer le son et la vidéo:** Permet l'enregistrement des sessions d'appels auxquelles participe l'entité SIP (en tant qu'émetteur ou destinataire de l'appel). Une fois enregistrées, les sessions d'appel peuvent être écoutées et exportées dans la tâche *Rapport d'appels*. La valeur par défaut est héritée des réglages d'enregistrement globaux configurés sur la page Enregistrement du rôle de module externe Sipelia. Lorsque vous modifiez ce réglage au niveau de l'entité, celle-ci n'hérite plus la valeur du réglage global, ce qui vous permet d'activer ou désactiver l'enregistrement pour une entité sans affecter les autres.

8 Cliquez sur **Appliquer**.

9 Ajoutez des interphones SIP supplémentaires en répétant les étapes ci-dessus.

Lorsque vous avez terminé

- Associez une entité Security Center à l'interphone SIP.
- Inscrivez l'interphone SIP.

Associer des entités Security Center à des interphones SIP

Pour confirmer l'identification des appelants par une image vidéo en temps réel et pour accorder l'accès aux installations par les portes contrôlées, vous pouvez associer diverses entités Security Center à un interphone SIP, puis contrôler le tout via Security Desk.

Avant de commencer

Ajoutez et configurez l'interphone SIP dans Config Tool.

À savoir

Avec les interphones SIP, vous pouvez associer des caméras, portes, zones et sorties avec leurs signaux de sortie respectifs.

Pour associer une entité Security Center à un interphone SIP :

1 Connectez-vous à Security Center avec Config Tool, et ouvrez la tâche Vue logique.

2 Dans la Vue logique, sélectionnez l'interphone SIP et cliquez sur l'onglet **VoIP**.

3 Dans la section *Entités associées*, cliquez sur **Ajouter une entité** ().

4 Dans l'*Assistant d'association d'entités*, sélectionnez l'une des entités suivantes, puis cliquez sur **Suivant**. Suivez les instructions à l'écran pour terminer l'association de l'entité.

- **Caméra:** La caméra que vous souhaitez associer à l'entité SIP. Vous pouvez associer une caméra afin que le flux vidéo en temps réel de la caméra Security Center concernée soit affiché pendant les appels en cours entre entités SIP.
- **Porte:** La porte que vous souhaitez associer à l'interphone SIP. Vous pouvez associer une porte pour pouvoir la déverrouiller et laisser passer les personnes qui utilisent l'interphone, et la verrouiller une fois qu'elles sont entrées.
- **Zone:** La zone que vous souhaitez associer à l'interphone SIP. Vous pouvez associer une zone que vous pouvez armer et désarmer en fonction des personnes qui utilisent l'interphone. Vous pouvez ainsi leur accorder ou refuser l'accès à une section particulière de vos installations. Une fois configuré, cliquez sur  dans la fenêtre ou la tuile de conversation Security Desk pour désarmer la zone.
- **Appareil:** La sortie d'un appareil que vous souhaitez associer à l'interphone SIP. Chaque sortie doit être associée à un signal de sortie, par exemple pour actionner un avertisseur sonore (via un relais de sortie) lorsqu'une fenêtre équipée d'un capteur de bris de glace (connecté à une entrée) est brisée. Une fois configuré, vous pouvez déclencher le signal de sortie sélectionné pendant un appel.

5 Si vous sélectionnez un appareil de sortie, procédez de l'une des manières suivantes pour définir le signal de sortie :

a) Dans le champ **Alias**, entrez un nom court et descriptif vous permettant d'identifier rapidement le signal de sortie.

b) Sélectionnez le type de sortie applicable (*Normal*, *Actif* ou personnalisé). Vous pouvez créer plusieurs types de sortie personnalisés basés sur les types *État*, *Impulsion* et *Périodique*. Pour en savoir plus sur les signaux de sortie, voir le *Guide de l'administrateur Security Center*.

6 Lorsque l'*Assistant d'association d'entités* est fermé, cliquez sur **Appliquer** pour enregistrer les modifications.

L'entité que vous avez sélectionnée apparaît dans la liste des entités associées.

7 (Facultatif) Si votre interphone SIP est équipé d'une caméra intégrée et que vous souhaitez que le flux vidéo de cette caméra soit affiché lors des conversations passant par l'interphone, vous pouvez associer la caméra intégrée en cliquant sur .

8 (Facultatif) Pour configurer l'entité associée que vous avez ajoutée, cliquez sur .

9 (Facultatif) Activez **Afficher les événements** pour l'interphone SIP. Afficher les événements permet d'activer les événements pour les utilisateurs et les interphones SIP, afin de pouvoir créer des événements personnalisés au sein du système (par exemple, pour déclencher une alarme si un appel reste sans réponse). Pour chaque utilisateur ou interphone SIP, vous pouvez sélectionner un événement personnalisé pour chacun des états d'appel suivants : Sonnerie en cours ; Appel déjà en cours ; Occupé ; Sans réponse ; Erreur ; Raccrocher. Pour en savoir plus sur les événements personnalisés, voir le *Guide de l'administrateur Security Center.*

10 Répétez les étapes ci-dessus pour associer d'autres entités à l'interphone SIP.

11 Pour plusieurs entités du même type, utilisez les boutons fléchés du volet *Associations* pour définir l'ordre d'apparition des entités dans la fenêtre de conversation ou une tuile dans Security Desk. Par exemple, si vous avez associé plusieurs caméras, le flux en temps réel de la première caméra de la liste est le flux par défaut. Les utilisateurs peuvent basculer vers les flux des autres caméras en cliquant sur , puis en sélectionnant une autre caméra.

Si vous associez toutes les entités possibles à un interphone SIP, toutes les entités apparaissent dans la fenêtre de conversation ou une tuile dans Security Desk. Chaque entité peut être contrôlée pendant un appel, comme l'illustre l'image suivante.

- **A:** Déclencher le signal de sortie d'un appareil
- **B:** Armer et désarmer une zone
- **C:** Ouvrir et fermer une porte
- **D:** Afficher le flux vidéo de la caméra sélectionnée

Exemple

Imaginons que vous voulez simplifier la manière de répondre aux demandes de cartes perdues. Avec un interphone SIP installé à l'entrée principale du bâtiment, vous pouvez associer les deux entités suivantes à l'interphone : la caméra de l'entrée principale et la porte de l'entrée principale. Lorsque Charles appelle avec cet interphone SIP pour dire qu'il a perdu sa carte et ne peut pas pénétrer dans

le bâtiment, vous pouvez confirmer son identité en comparant la vidéo en temps réel à son profil de titulaire de cartes, puis lui accorder ou refuser l'accès en conséquence.

Inscrire un interphone SIP sur Sipelia Server

Pour passer des appels depuis votre interphone SIP vers des utilisateurs Security Center, vous devez inscrire l'interphone surSipelia Server.

Avant de commencer

- Installez l'interphone SIP en suivant les recommandations du fabricant de l'appareil.
- Ajoutez et configurez l'interphone SIP dans Config Tool.

À savoir

En raison de l'éventail d'interphones SIP que vous pouvez installer, la manière de les configurer et de les inscrire sur Sipelia Server peut varier. La procédure ci-dessous offre un aperçu d'ordre général des réglages qui doivent être configurés. Reportez-vous toujours à la documentation fournie par le fabricant de l'interphone SIP pour des détails sur comment le configurer et l'inscrire.

Pour inscrire un interphone SIP sur Sipelia Server :

- Créez un compte SIP sur l'interphone.
- Donnez un nom pertinent au compte SIP. Il peut s'agir du nom donné à l'interphone lors de son ajout à Security Center, mais ce n'est pas obligatoire. Le nom de compte SIP n'est pas utilisé dans le cadre des communications SIP.
- Entrez le nom de domaine ou l'adresse IP de Sipelia Server.

  Vous trouverez l'adresse IP de Sipelia Server dans **Config Tool** > **Vue réseau** > **Propriétés**.
- Pour le port SIP, entrez la valeur que vous avez configurée. La valeur par défaut utilisée par *Session Initiation Protocol (SIP)* est **5060**.
- Entrez le numéro de poste qui a été affecté à l'interphone dans Security Center. Certains clients SIP utilisent le numéro de poste en tant que nom d'utilisateur.
- Entrez le mot de passe du numéro de poste qui a été affecté à l'interphone.
- Inscrivez l'interphone afin qu'il puisse communiquer avec Sipelia Server.

L'interphone SIP est prêt à passer et recevoir des appels.

Lorsque vous avez terminé

Si vous déployez Sipelia, créez des groupes d'appel de base.

Groupes d'appel

Un groupe d'appel est un ensemble d'entités SIP qui dispose de son propre numéro de poste. Toutes les entités (ou membres) d'un groupe d'appel font partie d'une liste d'appel, et les membres reçoivent tous les appels reçus par le groupe d'appel. Les membres d'un groupe d'appel peuvent être appelés tous en même temps, ou successivement selon un intervalle prédéfini. L'appel cesse de sonner lorsqu'un membre du groupe d'appel répond à l'appel.

Dans Security Center, il existe deux types de groupes d'appel : de base et personnalisé.

Groupes d'appel de base

Un groupe d'appel de base est un groupe d'utilisateurs Security Center ayant reçu leur propre numéro de poste. Dans un groupe d'appel de base, vous ne pouvez inclure que des utilisateurs Security Center et d'autres groupes d'utilisateurs Security Center.

Un groupe d'appel de base a les caractéristiques suivantes :

- Il s'agit d'un groupe d'utilisateurs Security Center.
- Il ne peut inclure que des utilisateurs Security Center et d'autres groupes d'utilisateurs Security Center.
- Il peut recevoir son propre numéro de poste SIP.
- Lorsque le numéro du poste est composé, tous les membres du groupe doté d'un poste SIP reçoivent l'appel.
- Pour pouvoir recevoir un appel, les utilisateurs qui appartiennent au groupe d'appel de base doivent avoir leur propre poste SIP.
- Si les utilisateurs n'ont pas de poste SIP, ils sont ignorées lorsque le groupe d'appel auquel ils appartiennent est appelé.

Groupes d'appel personnalisés

Un groupe d'appel personnalisé est un groupe d'appel qui peut contenir toute combinaison des entités suivantes : utilisateurs, groupes d'utilisateurs et appareils SIP. Alors que les groupes d'appel de base sont limités aux utilisateurs et groupes, les groupes d'appel personnalisés peuvent inclure des appareils SIP.

Un groupe d'appel personnalisé a les caractéristiques suivantes :

- Il peut inclure toute combinaison des entités suivantes : utilisateurs, groupes d'utilisateurs et appareils SIP.
- Il peut recevoir son propre numéro de poste SIP.
- Pour pouvoir recevoir un appel, les utilisateurs et les appareils SIP qui appartiennent au groupe d'appel personnalisé doivent avoir leur propre poste SIP.
- Si les utilisateurs et appareils SIP n'ont pas de poste SIP, ils sont ignorés lorsque le groupe d'appel personnalisé auquel ils appartiennent est appelé.
- Les groupes d'utilisateurs Security Center qui appartiennent à un groupe d'appel personnalisé n'ont pas besoin d'avoir leur propre poste, mais chaque utilisateur membre du groupe d'appel personnalisé doit en avoir un. Les entités utilisateur qui n'ont pas de poste SIP sont ignorés lorsque le groupe reçoit un appel.

Créer un groupe d'appel de base

Pour appeler plusieurs utilisateurs Security Center en même temps, vous pouvez créer un *groupe d'appel* de base en affectant tout simplement un numéro de poste à un groupe d'utilisateurs Security Center.

Avant de commencer

Configurez des comptes SIP pour les utilisateurs.

À savoir

Un groupe d'appel de base est un groupe d'utilisateurs Security Center ayant reçu leur propre numéro de poste. Dans un groupe d'appel de base, vous ne pouvez inclure que des utilisateurs Security Center et d'autres groupes d'utilisateurs Security Center.

Pour créer un groupe d'appel de base :

1 Connectez-vous à Security Center avec Config Tool, puis ouvrez la tâche Sécurité.

2 Cliquez sur **Groupes d'utilisateurs**, puis sélectionnez un groupe dans la liste.

3 Créez un groupe d'utilisateurs Security Center qui contient tous les utilisateurs que vous souhaitez inclure dans le groupe d'appel. Pour en savoir plus sur la création des groupes d'utilisateurs dans Config Tool, voir le *Guide de l'administrateur Security Center*.

4 Cliquez sur l'onglet **VoIP**.

Les membres du groupe d'utilisateurs apparaissent dans le champ **Liste d'appels**.

5 Affectez un numéro de poste au groupe d'appel de l'une des manières suivantes :

- Cliquez sur **Affectation automatique**. Cette option affecte automatiquement l'entité SIP au premier poste disponible d'une plage donnée. Par conséquent, il s'agit de la méthode conseillée pour affecter les postes aux utilisateurs, groupes d'appel et interphones SIP. Cliquez sur ce bouton, sélectionnez une plage existante, puis cliquez sur **Appliquer.**
- Entrez les informations suivantes :
  - **Poste SIP:** Le numéro de poste de l'entité SIP. Pour pouvoir communiquer avec d'autres extrémités SIP, chaque entité SIP (utilisateur, groupe d'appel ou interphone) dans Security Center doit avoir un numéro de poste attitré. Entrez le numéro de poste manuellement, ou cliquez sur **Affectation automatique** (méthode recommandée).

6 Dans le champ **Destinataires d'appels**, procédez de l'une des manières suivantes :

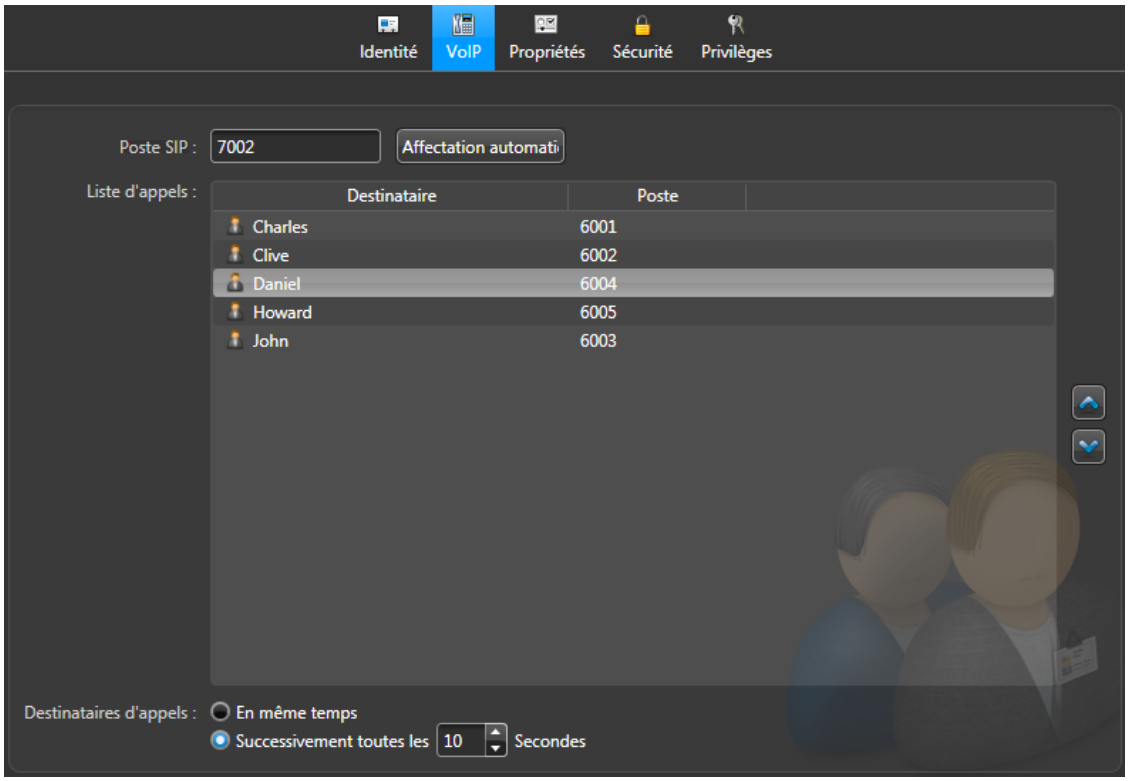
- **En même temps:** Tous les membres d'une liste d'appels sont appelés en même temps. L'appel cesse de sonner lorsqu'un membre du groupe d'appel répond à l'appel.
- **Successivement toutes les:** Les membres sont appelés les uns après les autres, avec un délai prédéfini entre chaque appel. L'ordre d'appel des membres correspond à leur position dans la liste d'appels. Cette séquence d'appels est répétée jusqu'à ce qu'un membre de la liste réponde à l'appel. Si un membre refuse l'appel, le numéro suivant de la liste est immédiatement appelé, sans prendre en compte le délai prédéfini entre les appels. Le délai minimum est de 10 secondes. Sachant cela peut affecter la durée durant laquelle un appel à un groupe d'appel reste sans réponse, il est conseillé de ne pas configurer un délai trop long.

7 (Facultatif) Pour modifier l'ordre d'appel de membres du groupe d'appel, utilisez les boutons fléchés pour déplacer les membres dans la liste. Cette option n'est disponible que si **Successivement toutes les** est sélectionné.

8 Cliquez sur **Appliquer**.

Exemple

Comme illustré ci-dessous, ce groupe d'appel de base comprend cinq utilisateurs Security Center, chacun disposant de son propre numéro de poste. La séquence d'appels pour ce groupe d'appel est réglée sur *Successivement toutes les 10 secondes*. Par conséquent, lorsque le poste du groupe d'appel (7002) est appelé, le poste de Charles (6001) sonne en premier. Si Charles ne répond pas ou ne refuse pas l'appel sous 10 secondes, le poste de Clive (6002) est appelé. La séquence continue ainsi jusqu'à ce qu'un membre de la liste prend l'appel.



Lorsque vous avez terminé

Pour créer un groupe d'appel qui contient d'autres groupes d'appel et interphones SIP, créez un groupe d'appel personnalisé.

Créer un groupe d'appel personnalisé

Pour appeler plusieurs entités SIP en même temps, vous pouvez créer un *groupe d'appel* personnalisé dans Config Tool.

Avant de commencer

En fonction des entités que vous souhaitez inclure dans votre groupe d'appel personnalisé, procédez de la manière suivante :

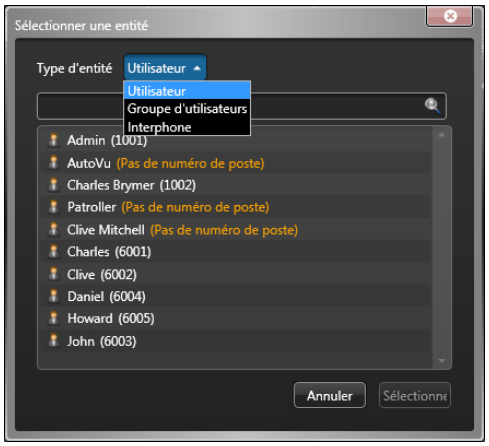
- Configurez des comptes SIP pour les utilisateurs.
- Créez un groupe d'appel de base.
- Ajoutez vos interphones SIP.

À savoir

Un groupe d'appel personnalisé est un groupe d'appel qui peut contenir toute combinaison des entités suivantes : utilisateurs, groupes d'utilisateurs et appareils SIP. Alors que les groupes d'appel de base sont limités aux utilisateurs et groupes, les groupes d'appel personnalisés peuvent inclure des appareils SIP.

Pour créer un groupe d'appel personnalisé :

1. Connectez-vous à Security Center avec Config Tool, et ouvrez la tâche Modules externes.
2. Sélectionnez le rôle Module externe **Sipelia**, puis cliquez sur **Groupes d'appel**
3. Cliquez sur **Ajouter un groupe d'appel** ( ).
4. Donnez un nom descriptif au groupe d'appel personnalisé, et cliquez sur **Ajouter**.
5. Affectez un numéro de poste au groupe d'appel de l'une des manières suivantes :
   - Cliquez sur **Affectation automatique**. Cette option affecte automatiquement l'entité SIP au premier poste disponible d'une plage donnée. Par conséquent, il s'agit de la méthode conseillée pour affecter les postes aux utilisateurs, groupes d'appel et interphones SIP. Cliquez sur ce bouton, sélectionnez une plage existante, puis cliquez sur **Appliquer.**
   - Entrez les informations suivantes :
     - **Poste SIP:** Le numéro de poste de l'entité SIP. Pour pouvoir communiquer avec d'autres extrémités SIP, chaque entité SIP (utilisateur, groupe d'appel ou interphone) dans Security Center doit avoir un numéro de poste attitré. Entrez le numéro de poste manuellement, ou cliquez sur **Affectation automatique** (méthode recommandée).
6. Dans le champ **Liste d'appels**, cliquez sur **Ajouter une entité** ( ).
7. Dans la boîte de dialogue *Sélectionner une entité*, sélectionnez les différentes entités que vous souhaitez inclure dans votre groupe d'appel personnalisé. Comme illustré ci-dessous, vous pouvez utiliser la liste déroulante **Type d'entité** pour filtrer les entités par type, puis rechercher les entités par nom.



8 Une fois que vous avez sélectionné toutes les entités, cliquez sur **Sélectionner**.

9 (Facultatif) Pour configurer l'entité associée que vous avez ajoutée, cliquez sur .

10 Dans le champ **Destinataires d'appels**, procédez de l'une des manières suivantes :

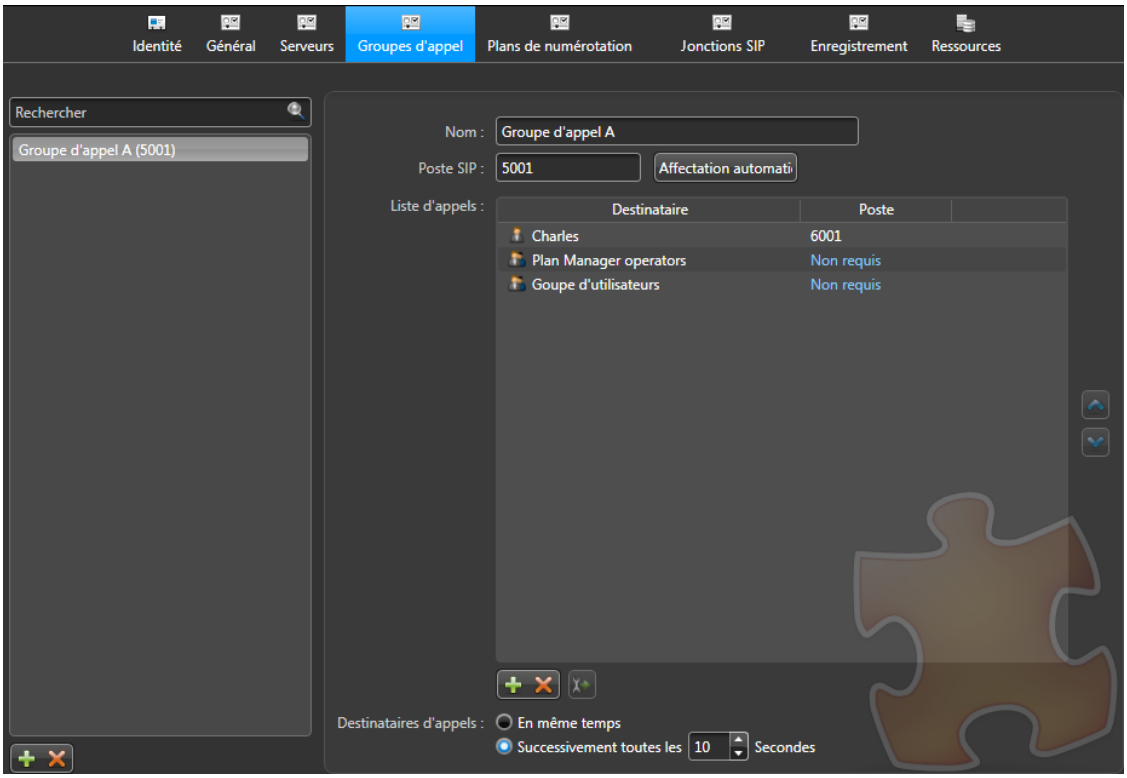
- **En même temps:** Tous les membres d'une liste d'appels sont appelés en même temps. L'appel cesse de sonner lorsqu'un membre du groupe d'appel répond à l'appel.
- **Successivement toutes les:** Les membres sont appelés les uns après les autres, avec un délai prédéfini entre chaque appel. L'ordre d'appel des membres correspond à leur position dans la liste d'appels. Cette séquence d'appels est répétée jusqu'à ce qu'un membre de la liste réponde à l'appel. Si un membre refuse l'appel, le numéro suivant de la liste est immédiatement appelé, sans prendre en compte le délai prédéfini entre les appels. Le délai minimum est de 10 secondes. Sachant cela peut affecter la durée durant laquelle un appel à un groupe d'appel reste sans réponse, il est conseillé de ne pas configurer un délai trop long.

11 (Facultatif) Pour modifier l'ordre d'appel de membres du groupe d'appel, utilisez les boutons fléchés pour déplacer les membres dans la liste. Cette option n'est disponible que si **Successivement toutes les** est sélectionné.

12 Cliquez sur **Appliquer**.

Exemple

Comme illustré ci-dessous, ce groupe d'appel contient trois entités : un utilisateur, un groupe d'utilisateurs et un groupe d'appel de base. La séquence d'appels pour ce groupe d'appel personnalisé est réglée sur *Successivement toutes les 10 secondes*. Par conséquent, lorsque le poste du groupe d'appel (5001) est appelé, le poste de Charles (6001) sonne en premier. Si Charles n'accepte ou ne refuse pas l'appel sous 10 secondes, les membres du groupe d'utilisateurs *Plan Manager operators* qui disposent d'un poste attitré sont tous appelés. La séquence continue ainsi jusqu'à ce qu'un membre de la liste prend l'appel.



Lorsque vous avez terminé

Si vous déployez Sipelia, configurez vos appareils audio et vidéo afin que les utilisateurs Security Center puissent passer et prendre des appels audio et vidéo.

Configurer les appareils pour les appels audio et vidéo

Pour participer à des appels audio et vidéo, vous pouvez connecter les équipements audio et vidéo nécessaires aux postes Security Desk sur lesquels Sipelia Client est installé, puis configurer les réglages adaptés pour chaque utilisateur Security Center.

Avant de commencer

- Configurez des comptes SIP pour les utilisateurs Security Center.
- Installez Sipelia Client sur chaque poste Security Desk qui exécute Sipelia.
- Installez les casques et webcams requis. Pour une qualité audio optimale, il est conseillé d'utiliser des casques plutôt que des micros et haut-parleurs.

Pour configurer les appareils pour les appels audio et vidéo :

1 Connectez-vous à Security Center avec Security Desk.

2 Cliquez sur **Options** > **Sipelia**.

3 Dans la section *Audio et vidéo*, sélectionnez les appareils audio et vidéo physiques utilisés pour les appels.

IMPORTANT : Vérifiez que les appareils sont correctement connectés aux postes Security Desk qui exécutent Sipelia.

4 Cliquez pour développer la section *Avancé*, et configurez les réglages suivants, selon vos besoins :

- **Codecs vidéo:** Les codecs vidéo pris en charge par Security Desk pour les communications vidéo. Par défaut, les codecs H.264 et H.263 sont activés et devraient convenir dans la plupart des cas. Par conséquent, il est recommandé de conserver les réglages par défaut, sachant que changer les codecs vidéo peut perturber la vidéo diffusée durant les appels vidéo. Pour pouvoir afficher la vidéo durant un appel vidéo SIP, les clients SIP impliqués doivent tous prendre en charge au moins un codec vidéo en commun. Par exemple, si le Client SIP A ne prend en charge que le codec H.264 et le Client SIP B ne prend en charge que le codec H.263, aucune vidéo ne sera diffusée durant une session d'appel entre ces deux clients SIP.
- **Plage de ports UDP:** La plage de ports pour le protocole UDP (User Diagram Protocol). Les ports UDP sont utilisés par les différents clients SIP pour émettre et recevoir des données de communication. La plage par défaut va de **20000** à **20500**. Il est recommandé de conserver les réglages par défaut et de ne les modifier que si Sipelia signale des problèmes de communication avec Security Desk liés aux ports.

5 Configurez les options d'appel suivantes, selon vos besoins :

- **Ouvrir les nouveaux appels dans:** Indiquez si vous souhaitez que tous les appels entrants soient automatiquement ouverts dans la fenêtre de conversation ou dans une tuile de la tâche *Surveillance* de Security Desk.
- **Alerte sonore en cas d'appel:** Cochez cette case si vous souhaitez entendre une sonnerie en cas d'appel entrant.

6 Répétez ces étapes sur chaque poste Security Desk équipé de Sipelia.

Lorsque vous avez terminé

- Testez les appareils audio et vidéo en passant des appels voix et vidéo entre les clients SIP.
- Si vous déployez Sipelia, configurez la communication bidirectionnelle entre Sipelia Server et les autres serveurs SIP.

Configurer la communication bidirectionnelle entre Sipelia Server et d'autres serveurs SIP

Pour étendre vos capacités SIP, vous pouvez configurer la communication bidirectionnelle entre Sipelia Server et d'autres serveurs SIP, afin que les postes SIP des deux serveurs puissent se joindre.

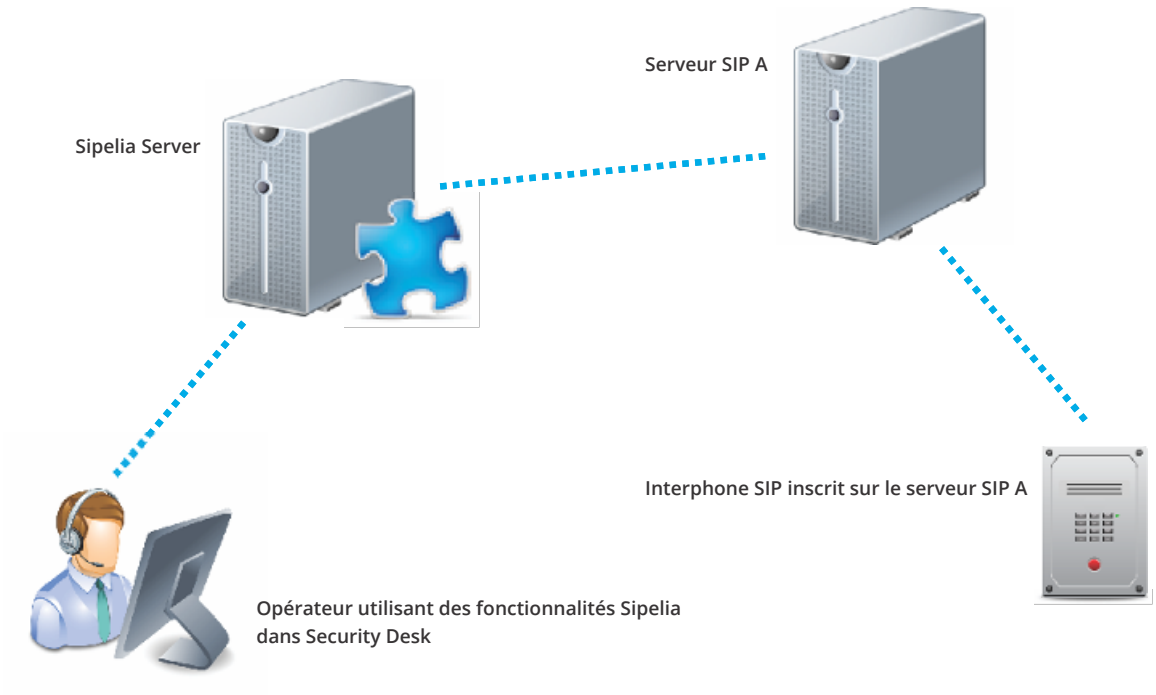
Avant de commencer

- Consultez la documentation fournie par le fabricant du serveur SIP que vous souhaitez relier à Sipelia Server.

  REMARQUE : Dans le cadre de cette rubrique, nous appellerons le serveur SIP auquel vous voulez vous connecter *SIP Server A*.
- Vérifiez que *SIP Server A* prend en charge les jonctions SIP et peut se connecter à d'autres serveurs SIP (dans notre cas, Sipelia Server). Certains serveurs SIP ne prennent pas en charge les jonctions SIP et ne peuvent donc pas appeler les postes inscrits sur d'autres serveurs SIP.
- Vérifiez que *SIP Server A* a été certifié par Genetec en tant que composant matériel compatible, et qu'il est présent dans la liste des serveurs et interphones SIP pris en charge par Sipelia.

À savoir

Pour obtenir un environnement SIP tel que celui qui est présenté dans l'image suivante, vous devez configurer correctement la communication bidirectionnelle entre les deux serveurs SIP (Sipelia Server et *SIP Server A*, qui est par exemple intégré dans un serveur d'interphone). Dans cette illustration, Sipelia Server doit ajouter *SIP Server A* en tant que jonction SIP, et *SIP Server A* doit également ajouter et configurer Sipelia Server en tant que jonction SIP. En outre, chaque serveur SIP doit définir des plans de numérotation adaptés pour pouvoir contacter l'autre serveur SIP.



Comme il existe de nombreux serveurs SIP sur le marché, chacun pouvant être configuré de nombreuses manières, la méthode à utiliser pour configurer une jonction SIP et un plan de

numérotation diffère pour chaque serveur SIP. Par conséquent, la procédure présentée ci-dessous ne fournit que des instructions d'ordre général pour configurer la communication bidirectionnelle entre Sipelia Server et *SIP Server A*. Toutefois, dans cette rubrique comme dans celles sur les jonctions SIP et les plans de numérotation, des instructions détaillées sont fournies pour configurer la communication unidirectionnelle entre Sipelia Server et la jonction SIP pour *SIP Server A*. Cela permet aux postes sur Sipelia Server d'appeler ceux sur *Serveur SIP A*.

Pour connecter Sipelia Server à *SIP Server A* :

1 Ajoutez *SIP Server A* en tant que jonction SIP.

2 Définissez des règles de plan de numérotation qui permettent aux postes SIP inscrits sur Sipelia Server à appeler les postes SIP inscrits sur *SIP Server A*.

3 Importez les règles de plan de numérotation dans Config Tool.

Pour connecter *SIP Server A* à Sipelia Server :

1 Ajoutez Sipelia Server en tant que jonction SIP. Reportez-vous à la documentation de *SIP Server A* pour savoir comment ajouter des jonctions SIP.

2 Définissez et mettez en œuvre des règles de plan de numérotation qui permettent aux postes SIP inscrits sur *SIP Server A* d'appeler les postes SIP inscrits sur Sipelia Server. Reportez-vous à la documentation de *SIP Server A* pour savoir comment définir et mettre en œuvre des jonctions SIP.

Configurer un interphone SIP pour appeler un poste particulier

Si votre interphone SIP ne peut être configuré que pour appeler un poste particulier lorsque l'utilisateur actionne un bouton, il est conseillé de configurer l'interphone SIP pour qu'il appelle un groupe d'appel, pour que vous puissiez ensuite gérer la liste d'utilisateurs qui recevront l'appel.

Avant de commencer

- Installez l'interphone SIP en suivant les recommandations du fabricant de l'appareil.
- Ajoutez et configurez l'interphone SIP dans Config Tool.

À savoir

Si votre interphone SIP ne permet que l'appel d'un seul poste SIP, il est conseillé d'utiliser le poste d'un groupe d'appel. Avec un groupe d'appel, vous pouvez ensuite décider qui sera appelé lorsque quelqu'un actionne le bouton sur l'interphone SIP et appelle le numéro de poste. Le groupe d'appel vous confère également la liberté de modifier la liste des destinataires en fonction de vos besoins.

En raison de l'éventail d'interphones SIP que vous pouvez installer, la manière de les configurer et de les inscrire sur Sipelia Server peut varier. La procédure ci-dessous offre un aperçu d'ordre général des réglages qui doivent être configurés. Reportez-vous toujours à la documentation fournie par le fabricant de l'interphone SIP pour des détails sur comment le configurer et l'inscrire.

Pour configurer un interphone SIP pour appeler le poste SIP d'un groupe d'appel :

1 Ajoutez et configurez un groupe d'appel dans Config Tool.

2 Notez le poste SIP que vous avez affecté au groupe d'appel.

3 Créez un compte SIP sur l'interphone.

4 Donnez un nom pertinent au compte SIP. Il peut s'agir du nom donné à l'interphone lors de son ajout à Security Center, mais ce n'est pas obligatoire. Le nom de compte SIP n'est pas utilisé dans le cadre des communications SIP.

5 Entrez le nom de domaine ou l'adresse IP de Sipelia Server.

Vous trouverez l'adresse IP de Sipelia Server dans **Config Tool** > **Vue réseau** > **Propriétés**.

6 Pour le port SIP, entrez la valeur que vous avez configurée. La valeur par défaut utilisée par *Session Initiation Protocol (SIP)* est **5060**.

7 Entrez le poste SIP qui a été affecté au groupe d'appel dans Security Center. Certains clients SIP utilisent le numéro de poste en tant que nom d'utilisateur.

L'interphone SIP appellera le poste du groupe d'appel lorsque son bouton sera actionné. Cela signifie qu'un ou plusieurs destinataires peuvent être appelés en même temps ou en séquence, selon la configuration du groupe d'appel.

Ajouter des icônes d'interphone SIP à une carte Plan Manager

Lorsque Sipelia et Plan Manager sont installés sur un même système, vous pouvez ajouter des icônes d'interphones SIP aux cartes afin qu'ils soient affichés dans Security Desk et puissent être utilisés par les opérateurs pour passer et recevoir des appels.

Avant de commencer

- Plan Manager déployé sur votre système. Pour en savoir plus sur comment déployer, configurer et utiliser Plan Manager, voir le Guide de l'utilisateur de Plan Manager.

Pour ajouter une icône d'interphone SIP à une carte Plan Manager :

1 Connectez-vous à Security Center avec Security Desk et ouvrez la tâche *Surveillance*.

2 Dans la vue *Logique*, cliquez deux fois sur une carte Plan Manager ( ) ou faites glisser la carte sur une tuile.

3 Naviguez jusqu'à l'emplacement de la carte où vous souhaitez ajouter l'interphone SIP.

4 Dans la tuile Plan Manager, sélectionnez le ruban **Modifier**.

Un cadre rouge apparaît autour de l'espace de travail Plan Manager.

5 Dans la vue *Logique*, cliquez sur l'interphone SIP concerné et faites-le glisser au bon endroit sur la carte.

6 Réglez la taille, la position et l'orientation de l'icône de l'interphone SIP à la souris.

7 Dans le volet affiché à gauche, configurez les propriétés de l'icône d'interphone SIP.

Les propriétés sont regroupées par catégorie. Cliquez sur un en-tête de groupe pour l'ouvrir.

- **Identité:** Nom de l'icône d'interphone SIP qui sera affiché sur la carte.
- **États:** Ensembles de propriétés (image, taille d'image, couleur, opacité, vitesse de clignotement) représentant chaque état possible de l'icône d'interphone SIP sur la carte.
- **Position:** Propriétés affectant l'aspect général de l'icône d'interphone SIP sur la carte.
- **Entité associée:** Liste des entités liées à l'interphone SIP.

8 Dans le ruban **Modifier**, cliquez sur **Enregistrer les modifications** ( ).

Lorsque vous avez terminé

Cliquez sur le ruban **Accueil** et essayez de passer et de recevoir un appel avec l'icône d'interphone SIP que vous venez d'ajouter.

Configurer une interface réseau avec la plus haute priorité

Pour que la communication entre Security Desk et Sipelia Server fonctionne correctement lorsque le poste Security Desk qui exécute Sipelia possède plus d'une interface (carte) réseau, vous devez configurer l'interface réseau à être utilisée pour Sipelia avec la plus haute priorité.

À savoir

Des applications telles que VPN peuvent automatiquement modifier l'ordre de priorité des interfaces réseau dans Windows, lorsqu'une connexion est établie par exemple. Dans ce cas vous aurez probablement à reconfigurer l'ordre de priorité après avoir utilisé ces applications, ou bien tentez de dédier un seul ordinateur pour exécuter Security Desk.

Pour configurer une interface réseau avec la plus haute priorité:

1. Dans le **Panneau de configuration** de Windows, cliquez sur **Réseau et Internet** > **Centre Réseau et partage**.
2. Dans le panneau de gauche, cliquez sur **Modifier les paramètres de la carte**.
3. Appuyez sur la touche **ALT** pour afficher le menu, et cliquez sur **Avancé** > **Paramètres avancés**.
4. Dans la fenêtre de configuration *Paramètres avancés*, cliquez sur **Cartes et liaisons**.
5. Sous **Connexions**, sélectionnez l'interface réseau à être utilisée par Sipelia et déplacez cette interface vers le haut de la liste en utilisant les flèches situées à droite.

   L'interface réseau affichée dans le haut de la liste est configurée avec la plus haute priorité.
6. Cliquez sur **OK** afin de confirmer les changements.
7. Pour vérifier que les changements ont été sauvegardés correctement, ouvrez une fenêtre de commande, tapez `ipconfig`, et appuyez sur **ENTRÉE**.
8. Vérifiez que l'ordre des interfaces réseau listées dans la fenêtre de commande est le même que celui configuré dans **Cartes et liaisons**.

L'interface réseau sélectionnée pour Sipelia est configurée avec la plus haute priorité dans Windows et sera utilisée par Security Desk pour se connecter et s'inscrire sur Sipelia Server.

4

Jonctions SIP et plans de numérotation

Cette section aborde les sujets suivants:

Ajouter des jonctions SIP

Pour vous connecter à des serveurs SIP autres que Sipelia Server, vous pouvez ajouter une jonction SIP dans Config Tool, puis définir des règles de *plan de numérotation* adaptées pour acheminer les appels entre les serveurs SIP.

À savoir

Les jonctions SIP fonctionnent avec des plans de numérotation. Par exemple, pour connecter Sipelia Server à un autre serveur SIP (*SIP Server A*) par le biais d'une jonction SIP, vous devez définir des règles de plan de numérotation qui indiquent à Sipelia Server les appels à réacheminer par la jonction vers les nouvelles destinations de postes SIP inscrites sur *SIP Server A*. En outre, pour bénéficier de la communication bidirectionnelle entre Sipelia Server et *Serveur SIP A*, les deux serveurs SIP doivent être configurés en conséquence.

Pour ajouter une jonction SIP :

1 Connectez-vous à Security Center avec Config Tool, et ouvrez la tâche Modules externes.

2 Sélectionnez le rôle Module externe **Sipelia**, puis cliquez sur **Jonctions SIP**

3 Cliquez sur **Ajouter une jonction SIP** ( ).

4 Dans le champ **Nom**, donnez un nom descriptif à la jonction SIP. Le nom de la jonction SIP doit être unique, car il sera utilisé dans les règles de plan de numérotation impliquant la jonction.

Exemple: Dans le cadre de cet exemple, nommons la jonction SIP *TrunkSIPServerA* pour *SIP Server A*.

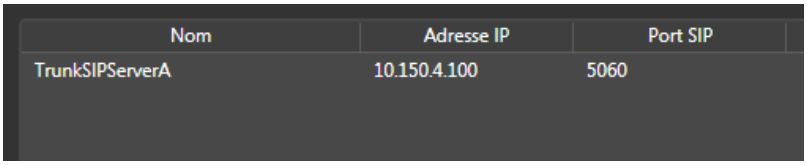
5 Entrez les informations suivantes :

- **Adresse IP:** L'adresse IP de la jonction SIP à laquelle vous souhaitez connecter Sipelia Server.
- **Port SIP:** Le port utilisé par la jonction SIP pour communiquer avec Sipelia Server. Puisque les jonctions SIP sont des serveurs, la valeur par défaut est **5060**.

Exemple: Imaginons que l'adresse IP de *TrunkSIPServerA* est la suivante : **10.150.4.100**. Et comme indiqué plus haut, que le port par défaut est **5060**.

6 Cliquez sur **Ajouter**, puis sur **Appliquer**.

La jonction SIP *TrunkSIPServerA* est ajoutée.



Lorsque vous avez terminé

Pour appeler les postes inscrits sur *TrunkSIPServerA*, créez les règles de plan de numérotation adaptées.

Plans de numérotation

Un plan de numérotation est un ensemble de règles qui définit la manière d'acheminer les appels en local ou entre deux jonctions SIP. Les plans de numérotation assurent le bon acheminement des appels, et permettent aux administrateurs de restreindre les appels à des sites géographiques ou d'assurer la confidentialité des appelants.

Un plan de numérotation définit une ou plusieurs règles qui régissent :

- Comment les appels peuvent joindre les postes SIP résidant sur d'autres serveurs SIP.
- Comment les appels provenant d'autres serveurs SIP peuvent joindre les postes résidant sur Sipelia Server.
- Comment les appels peuvent être transférés, même en local sur Sipelia Server.
- Comment Sipelia Server peut modifier les informations de numérotation comme les postes SIP source ou cible durant l'acheminement des appels.

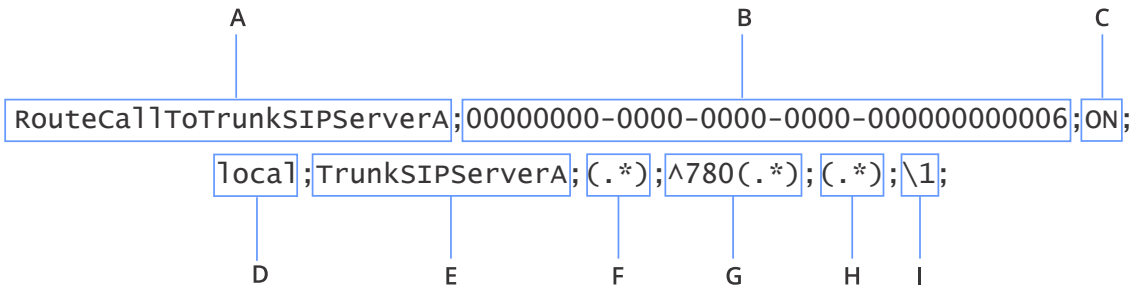
Par exemple, si un poste SIP inscrit sur Sipelia Server doit appeler un poste hébergé sur *SIP Server A*, vous devez d'abord configurer une Jonction SIP dans Sipelia Server pour pouvoir vous connecter à *SIP Server A*. Vous devez ensuite définir un plan de numérotation pour acheminer l'appel de Sipelia Server vers *SIP Server A*. Dans Sipelia, les plans de numérotation peuvent servir à acheminer les appels locaux, c'est-à-dire les appels qui doivent rester sur Sipelia Server.

REMARQUE : Les plans de numérotation doivent être configurés sur *SIP Server A* pour acheminer les appels depuis et vers Sipelia Server. Reportez-vous à la documentation fournie par le fabricant du *SIP Server A* pour en savoir plus sur la configuration des plans de numérotation.

Règles de plan de numérotation

Les règles de plans de numérotation sont stockées dans des fichiers texte CSV (valeurs séparées par un point-virgule) qui peuvent contenir plusieurs règles. Le fichier contient une règle par ligne et chaque valeur (ou champ) d'une règle est séparée des autres par un point-virgule (**;**). Bien que les fichiers CSV prennent en charge différents séparateurs (ou délimiteurs), les règles de plan de numérotation Sipelia ne prennent en charge que le point-virgule (**;**). Vous pouvez définir des règles de plan de numérotation à différentes fins. Généralement, les règles de plan de numérotation servent à appeler des serveurs SIP autres que Sipelia Server, et à rediriger les appels en local provenant de postes hébergés par Sipelia Server.

Chaque règle de plan de numérotation doit spécifier les valeurs présentées dans l'exemple suivant.



- **Nom (A):** Le nom de la règle de plan de numérotation. Si le nom n'est pas fourni, une valeur par défaut est utilisée à l'importation (*DialplanRule1*). Entrez un nom qui vous aidera à identifier l'objectif de la règle.

- **Horaire (B):** L'horaire durant lequel la règle doit être en vigueur. La longue chaîne de chiffres de cette valeur représente un identifiant global unique (GUID). Si ce GUID n'est pas fourni ou n'est pas valable, la valeur par défaut *Toujours* est utilisée à l'importation.

  CONSEIL : L'horaire peut être modifié avec l'interface graphique sur la page Plans de numérotation de Config Tool une fois que la règle de plan de numérotation a été importée. Vous pouvez donc la laisser vide ici et laisser le système affecter l'horaire par défaut.
- **État (C):** L'état de la règle (On = Active ; Off = Inactive). Cette valeur n'est pas sensible à la casse. Si cette valeur n'est pas fournie, la valeur par défaut *Off* est utilisée à l'importation.
- **Direction de (D):** Le serveur SIP d'où provient l'appel (le serveur source). Les valeurs possibles sont *local* ou le nom d'une jonction SIP.Sipelia Server est toujours le serveur SIP *local*. Si vous spécifiez un nom de jonction SIP qui n'existe pas dans les réglages de Sipelia Server, une alerte est affichée et la valeur *local* est rétablie à l'importation.
- **Direction cible (E):** Le serveur SIP qui reçoit l'appel (le serveur de destination). Les valeurs autorisées sont *local* ou le nom d'une jonction SIP. Le nom de la jonction SIP doit être unique et doit correspondre à un nom spécifié dans l'onglet Jonctions SIP à l'ajout de la jonction SIP. Sipelia Server est toujours le serveur SIP *local*. Si vous spécifiez un nom de jonction SIP qui n'existe pas dans les réglages de Sipelia Server, une alerte est affichée et la valeur *local* est rétablie à l'importation.

  CONSEIL : Après l'ajout de la jonction SIP dans Config Tool, vous pouvez copier son nom en faisant un clic droit sur le nom. Il est conseillé de copier le nom puis de le coller dans votre règle de plan de numérotation pour éviter les erreurs de saisie.
- **Source (F):** L'expression régulière qui identifie le poste de l'appelant (l'appelant source). La règle de plan de numérotation n'est appliquée qu'en cas de correspondance entre l'expression régulière et le poste de l'appelant. Ce champ est obligatoire.
- **Destination (G):** L'expression régulière qui identifie le poste du destinataire (le destinataire cible). La règle de plan de numérotation n'est appliquée qu'en cas de correspondance entre l'expression régulière et le poste du destinataire. Ce champ est obligatoire.
- **Nouvelle source (H):** La valeur qui modifie le poste de l'appelant (si la règle est appliquée). Par exemple, si l'appelant du poste 1001 appelle le destinataire au poste 2001 et que la valeur *Nouvelle source* est 4001, le destinataire voit que l'appel provient du poste 4001 au lieu du poste 1001. Les valeurs autorisées peuvent également contenir des expressions régulières.
- **Nouvelle destination (I):** Le poste SIP qui reçoit l'appel (si la règle est appliquée). Les valeurs autorisées peuvent également contenir des expressions régulières.

Priorité de règles de plan de numérotation

Les règles définies dans un plan de numérotation sont affichées par ordre de priorité. Une règle située sur une ligne précédente a une priorité plus élevée. Si un appel correspond à plusieurs règles, la première règle qui apparaît dans le plan de numérotation sera toujours appliquée. L'ordre de priorité après importation des règles dans Config Tool peut être modifié à l'aide des flèches situées à droite de la liste.

Scénarios exemples

Pour en savoir plus sur l'utilisation des expressions régulières dans les règles de plan de numérotation, examinez les scénarios suivants :

- Transférer vers une jonction SIP tous les appels dotés d'un préfixe.
- Réserver une plage de postes SIP pour les appels en local.
- Réserver une plage de postes SIP pour les appels vers une jonction SIP.
- Remplacer les postes SIP source.
- Supprimer le préfixe des postes SIP source provenant d'une jonction SIP.

- Transférer les appels vers un autre poste SIP sur horaire.

Dans le dossier d'installation de Sipelia, généralement *C:\Program Files (x86)\Genetec Sipelia*, le dossier *Samples* contient un fichier *zip* avec les fichiers de plan de numérotation exemple correspondant aux scénarios ci-dessus.

Expressions régulières dans Sipelia

Une expression régulière est une séquence de signes interprétés par un moteur d'expression régulière pour identifier toutes les chaînes de caractères qui correspondent à un critère de recherche particulier, sans qu'il soit nécessaire d'énumérer toutes les valeurs individuelles possibles qui doivent être recherchées. Le moteur utilisé dans Sipelia est celui de Microsoft .NET.

Dans Sipelia, les expressions régulières sont utilisées dans les règles de plan de numérotation pour effectuer les tâches suivantes :

- Rechercher des postes SIP particuliers d'où proviennent les appels.
- Rechercher des postes SIP de destination des appels.
- Rechercher des préfixes particuliers ajoutés aux postes SIP.
- Modifier les postes SIP d'où proviennent les appels.
- Modifier les postes SIP de destination des appels.

Éléments des expressions régulières

Les expressions régulières utilisées dans les règles de plan de numérotation utilisent généralement les éléments suivants :

- **(.*):** Rechercher n'importe quelle valeur.
  - Utilisez cet élément dans les champs **Source (F)** ou **Destination (G)** pour indiquer à Sipelia Server de rechercher n'importe quel poste source ou cible lors des appels.
  - Utilisez cet élément dans les champs **Nouvelle source (H)** ou **Nouvelle destination (I)** pour garantir que le poste source ou cible ne sera pas modifié lorsqu'il est acheminé par Sipelia Server.
- **\n:** Rechercher la valeur d'un groupe de capture d'un précédent champ associé. Un groupe de capture regroupe un ou plusieurs éléments d'expression régulière généralement spécifiés entre parenthèses, et représente un motif particulier.
  - Utilisez cet élément dans le champ **Nouvelle source (H)** pour spécifier le groupe de capture du champ *Source* qui doit servir de nouvelle valeur source. **n** représente l'ordre du groupe de capture (\1 ; \2 ; \5, etc.) de l'expression régulière. Par exemple, si *Source* contient **550[1-5](.*)**, entrez \2 pour utiliser **(.*)** en tant que valeur de *Nouvelle source*, ce qui dans ce cas supprimera le préfixe **550** ainsi que le chiffre suivant.
  - Utilisez cet élément dans le champ **Nouvelle destination (H)** pour spécifier le groupe de capture du champ *Destination* qui doit servir de nouvelle valeur cible.
- **n:** Rechercher une valeur particulière. Dans Sipelia, cette valeur représente généralement un poste SIP particulier.
  - Utilisez cet élément dans le champ **Nouvelle source (H)** pour spécifier un numéro de poste différent pour la provenance des appels. Cela peut être utile si vous souhaitez que les appels proviennent d'un poste autre que le poste source d'origine.
  - Utilisez cet élément dans le champ **Nouvelle destination (I)** pour spécifier le numéro de poste qui recevra les appels. Cela peut être utile si vous souhaitez transférer les appels vers un poste autre que le poste cible d'origine.
- **[premier - dernier]:** Rechercher un caractère dans la plage **premier** à **dernier**.
- **{n}:** Rechercher l'élément précédent exactement **n** fois.

- **\b:** Utilisez cet élément au début et à la fin d'une série d'éléments d'expression régulière pour rechercher un mot entier seulement (pas seulement une partie du mot).

Exemple

Par exemple, l'expression régulière **\b6[0-9]{2}\b** permet de rechercher les postes SIP 600 à 699.

Déconstruction de l'expression régulière	Description
\b	Limite des postes SIP. En tandem avec le même élément **\b** à la fin de l'expression, cette option indique que le numéro de poste SIP entier doit correspondre. Les caractères de début ou de fin ne seront pas ignorés.
6	Rechercher un poste SIP qui commence par **6**.
[0-9]	Rechercher les chiffres **0** à **9**.
{2}	Rechercher 2 occurrences des chiffres ci-dessus après le **6**.
\b	Limite de fin des postes SIP.

Pour en savoir plus sur les expressions régulières, voir le site de Microsoft.

Définir les règles de plan de numérotation

Pour appeler des postes SIP inscrits sur des serveurs SIP autres que Sipelia Server, ou simplement pour rediriger des appels au sein de Sipelia Server, vous devez définir des règles de plan de numérotation, puis les importer dans Config Tool.

Avant de commencer

- Si vous voulez appeler des postes SIP inscrits sur d'autres serveurs SIP, ajoutez une jonction SIP pour le serveur concerné.
- Prenez connaissance des plans de numérotation et des règles de plan de numérotation utilisés par Sipelia.

À savoir

Les règles définies dans un plan de numérotation sont affichées par ordre de priorité. Une règle située sur une ligne précédente a une priorité plus élevée. Si un appel correspond à plusieurs règles, la première règle qui apparaît dans le plan de numérotation sera toujours appliquée. L'ordre de priorité après importation des règles dans Config Tool peut être modifié à l'aide des flèches situées à droite de la liste.

Pour définir une règle de plan de numérotation :

1 Créez un fichier texte pour le plan de numérotation avec une extension *.txt* ou *.csv*, ou ouvrez un fichier existant.

2 Rédigez une règle de plan de numérotation adaptée. En fonction de l'objectif de la règle de plan de numérotation, vous pouvez baser la règle sur un scénario exemple, ou créer votre propre règle.

3 Entrez une valeur dans chaque champ requis par la règle.

IMPORTANT : Une règle de plan de numérotation doit contenir le bon nombre de valeurs pour pouvoir être importée correctement. Chaque valeur d'une règle doit être séparée par un point-virgule (**;**).

4 Répétez les mêmes étapes pour chaque règle supplémentaire nécessaire.

5 Enregistrez et fermez le fichier de plan de numérotation.

Lorsque vous avez terminé

Importez le plan de numérotation dans Config Tool.

Importer un plan de numérotation

Une fois que vous avez défini des règles de plan de numérotation, vous devez importer les fichiers de plan de numérotation dans Config Tool pour qu'elles soient appliquées.

Avant de commencer

- Ajoutez une jonction SIP.
- Définissez les règles de plan de numérotation nécessaires.

À savoir

Si vous supprimez (✕) une règle de plan de numérotation que vous avez importée, la règle n'est plus disponible dans le système de plan de numérotation de Sipelia Server. Si vous souhaitez à nouveau utiliser la règle supprimée, vous devez réimporter le fichier de plan de numérotation qui contient la règle. Si vous souhaitez que le système cesse d'appliquer une règle, désactivez tout simplement la règle, mais conservez-la dans vos règles importées, pour pouvoir l'utiliser à nouveau en cas de besoin.

Si vous faites la mise à jour d'une règle de plan de numérotation précédemment importée, il est inutile de supprimer la règle existante de la page Plans de numérotation. Dans le fichier de plan de numérotation, apportez les modifications nécessaires à la règle en veillant à ne pas changer son nom, puis réimportez la règle. Durant l'importation, les règles de plan de numérotation avec un nouveau nom sont ajoutées à la liste de règles, tandis que celles dont les noms sont déjà présents dans la liste sont mises à jour.

Pour importer un plan de numérotation :

1 Connectez-vous à Security Center avec Config Tool, et ouvrez la tâche Modules externes.

2 Sélectionnez le rôle Module externe **Sipelia**, puis cliquez sur **Plans de numérotation**

3 Cliquez sur **Importer les règles de plan de numérotation depuis un fichier** ( ).

4 Sélectionnez le fichier de plan de numérotation, puis cliquez sur **OK**.

Le plan de numérotation est importé et les règles contenues dans le fichier apparaissent sur des lignes distinctes de la page Plans de numérotation.

IMPORTANT : Lorsqu'une règle n'a pas le bon nombre de valeurs séparées par un point-virgule, la règle n'est pas importée et une erreur est signalée.

5 Si votre fichier de plan de numérotation génère des problèmes, cliquez sur le bouton **Afficher les erreurs et avertissements** pour ouvrir la fenêtre *Résultat de l'analyse*.

Cette fenêtre classe les problèmes par type (erreur ou avertissement) et fournit des informations sur chaque problème. Les avertissements ne nécessitent pas de correction, mais les erreurs doivent être corrigées. Modifiez le plan de numérotation en conséquence, puis réimportez le fichier.

6 Pour chaque règle de plan de numérotation que vous importez, vous pouvez modifier les éléments suivants :

- **Horaire:** L'horaire Security Center durant lequel la règle doit être en vigueur. La règle n'est appliquée que si les conditions horaires sont remplies.
- **État:** L'état de la règle. Seules les règles *actives* sont appliquées.

7 (Facultatif) Pour modifier l'ordre d'application des règles de plan de numérotation, utilisez les boutons fléchés pour déplacer les règles dans la liste.

8 Cliquez sur **Appliquer**.

Scénario de plan de numérotation 1 : Transférer vers une jonction SIP tous les appels dotés d'un préfixe

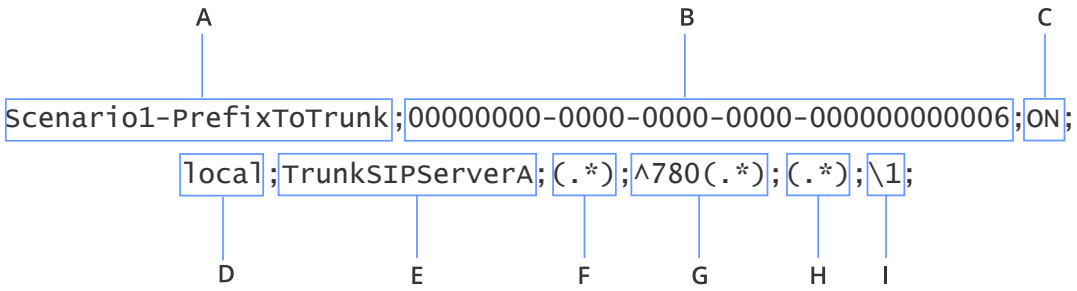
Dans ce scénario, une règle de plan de numérotation achemine vers une jonction SIP tout appel doté d'un préfixe particulier.

Scénario

- **Objectif** Votre poste SIP est inscrit sur Sipelia Server et vous devez vous connecter au *SIP Server A*, car vous souhaitez appeler des postes SIP (client SIP, interphone SIP, etc.) inscrits sur cette jonction SIP. Cela vous permet d'établir une communication unidirectionnelle avec *SIP Server A*.
- **À faire avant de définir la règle** Ajoutez une jonction SIP dans Config Tool pour *SIP Server A* et nommez-la *TrunkSIPServerA*. Ce nom de jonction doit être unique, afin que la règle de plan de numérotation que vous créez n'entre pas en conflit avec d'autres règles et qu'elle soit appliquée correctement.
- **Marche à suivre** Pour acheminer les appels vers *TrunkSIPServerA*, vous pouvez utiliser un préfixe de numérotation, comme **780**. Cela signifie que les postes SIP sur Sipelia Server doivent composer ce préfixe pour pouvoir appeler les postes SIP sur *TrunkSIPServerA*. L'approche par préfixe correspond à l'utilisation du 9 pour obtenir une ligne extérieure avec un système PBX traditionnel. Le préfixe peut être le numéro de votre choix, dès lors qu'il est défini dans votre règle de plan de numérotation.

Exemple de règle de plan de numérotation

Voici un exemple de règle de plan de numérotation pour atteindre l'objectif du scénario ci-dessus.



Les étiquettes de valeur identifiées ci-dessous correspondent aux étiquettes de colonne qui apparaissent sur la page Plans de numérotation du rôle Module externe **Sipelia**.

Lettre de valeur	Étiquette de valeur	Description
A	**Nom**	Le nom de la règle indique que les appels effectués depuis Sipelia Server et dotés d'un préfixe seront acheminés vers la jonction SIP.
B	**Horaire**	L'horaire est réglé sur *Toujours*, ce qui signifie que la règle sera toujours évaluée.
C	**État**	L'état est réglé sur *On*, ce qui signifie que la règle est actuellement active.

Lettre de valeur	Étiquette de valeur	Description
D	**Direction de**	Le champ est réglé sur *local* pour rechercher les appels provenant de Sipelia Server.
E	**Direction cible**	Le champ est réglé sur *TrunkSIPServerA* car les appels seront acheminés vers la jonction SIP.
F	**Source**	L'expression régulière est réglée sur **(.*)**, ce qui signifie que l'appel peut être passé depuis *tout* poste SIP inscrit sur Sipelia Server. Si vous choisissez d'indiquer un poste SIP particulier, vérifiez que l'expression régulière correspond au poste de l'appelant.
G	**Destination**	Le préfixe **^780** est utilisé. Cela signifie que les postes SIP sur Sipelia Server doivent premièrement composer le 780 pour pouvoir communiquer avec le *TrunkSIPServerA*. En outre, le préfixe est suivi de l'expression régulière **(.*)** Cette expression régulière capture tous les chiffres qui suivent le préfixe. **Exemple** : Pour appeler le poste 1001 sur *TrunkSIPServerA*, vous devez composer le **7801001**. L'expression régulière **(.*)** crée un index de groupe de postes qui commence par *1*. Dès lors, le poste 1001 fait partie de cet index. Si vous appelez le **7801002**, le poste 1002 est également inclus dans l'index.
H	**Nouvelle source**	L'expression régulière **(.*)** est utilisée. Cela signifie que le poste de l'appelant sur Sipelia Server n'est pas modifié. **Exemple** : Si le poste source inscrit sur Sipelia Server est 6001, la règle de plan de numérotation ne le modifiera pas. Avec cette règle, ce sera le cas pour tous les postes inscrits sur Sipelia Server. Toutefois, si vous entrez la valeur 7001 dans *Nouvelle source* et que vous passez un appel depuis votre poste (6001), le destinataire voit que l'appel entrant vient du poste 7001 au lieu de 6001.
I	**Nouvelle destination**	Puisque la valeur *Nouvelle destination* est liée au champ *Destination*, le **\1** indique que la règle doit utiliser la valeur du premier groupe d'expression régulière de *Destination*. Dans ce scénario, *Destination* a une valeur de **780(.*)**, donc l'utilisation de **\1** renvoie **(.*)**, qui correspond au poste SIP de destination, sans le préfixe.

Résultat

Une fois que cette règle de plan de numérotation est importée dans Config Tool, si un poste SIP inscrit sur Sipelia Server compose le **7801001**, le poste **1001** sur *SIP Server A* sonne.

Scénario de plan de numérotation 2 : Réserver une plage de postes SIP pour les appels en local

Dans ce scénario, les règles de plan de numérotation servent à définir une plage de postes SIP pour les appels en local sur Sipelia Server, tandis que les appels passés vers d'autres postes SIP seront automatiquement acheminés vers une jonction SIP.

Scénario

- **Objectif** Réserver les postes SIP 4000 à 4500 pour les appels qui doivent rester en local sur Sipelia Server, et acheminer les autres postes SIP vers *SIP Server A*.
- **À faire avant de définir la règle** Ajoutez une jonction SIP dans Config Tool pour *SIP Server A* et nommez-la *TrunkSIPServerA*. Ce nom de jonction doit être unique, afin que la règle de plan de numérotation que vous créez n'entre pas en conflit avec d'autres règles et qu'elle soit appliquée correctement.
- **Marche à suivre** Vous devez définir deux règles distinctes et les placer dans le bon ordre dans votre plan de numérotation.
  - La première règle conserve les appels en local lorsque les postes SIP de destination sont entre 4000 et 4500.
  - La seconde règle traitera les appels vers les autres postes SIP en les acheminant vers *TrunkSIPServerA*.

IMPORTANT : Les règles doivent être placées dans le bon ordre dans le plan de numérotation pour que ce scénario fonctionne correctement.

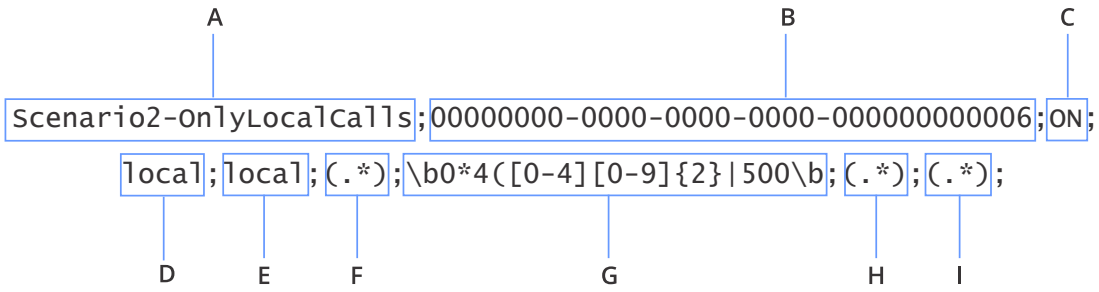
Exemple de plan de numérotation

Voici un exemple de plan de numérotation pour atteindre l'objectif du scénario ci-dessus.

1 Scenario2-OnlyLocalCalls;00000000-0000-0000-0000-000000000006;ON;local;local;(.*);\b0*4([0-4][0-9]{2}|500)\b;(.*);(.*);
2 Scenario2-RestCallsToMyTrunk;00000000-0000-0000-0000-000000000006;ON;local;TrunkSIPServerA;(.*);(.*);(.*);(.*);

Règle 1 : Appels en local seulement

La première règle du plan de numérotation indiquée ci-dessous indique à Sipelia Server de rechercher les postes SIP entre 4000 et 4500, et de les acheminer en local.

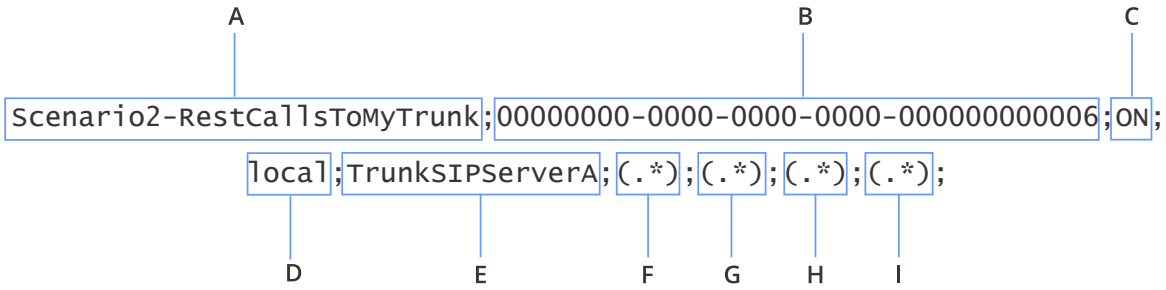


Les étiquettes de valeur identifiées ci-dessous correspondent aux étiquettes de colonne qui apparaissent sur la page Plans de numérotation du rôle Module externe **Sipelia**.

Lettre de valeur	Étiquette de valeur	Description
A	**Nom**	Le nom indique que cette règle n'acheminera que les appels en local.
B	**Horaire**	L'horaire est réglé sur *Toujours*, ce qui signifie que la règle sera toujours évaluée.
C	**État**	L'état est réglé sur *On*, ce qui signifie que la règle est actuellement active.
D	**Direction de**	Le champ est réglé sur *local* pour rechercher les appels provenant de Sipelia Server.
E	**Direction cible**	Ce champ est réglé sur *local* car les appels correspondant à la règle resteront en local sur Sipelia Server.
F	**Source**	L'expression régulière est réglée sur **(.*)**, ce qui signifie que l'appel peut être passé depuis *tout* poste SIP inscrit sur Sipelia Server.
G	**Destination**	L'expression régulière est réglée sur **\b0*4([0-4][0-9]{2}|500)\b** pour rechercher les postes SIP entre 4000 et 4500, selon les modalités suivantes : • **\b:** Limite des postes SIP. En tandem avec le même élément **\b** à la fin de l'expression, cette option indique que le numéro de poste SIP entier doit correspondre. Les caractères de début ou de fin ne seront pas ignorés. • **0*:** Rechercher n'importe quel nombre de zéros avant le caractère suivant, qui est le **4**. • **4:** Rechercher un poste SIP qui commence par **4**. • **([0-4]:** Rechercher une seule occurrence des chiffres **0** à **4** après le premier **4**. • **[0-9]{2}:** Rechercher 2 occurrences suivantes des chiffres **0** à **9**, pour couvrir les postes 4000 à 4499. • **|500):** Rechercher spécifiquement **500** pour ajouter 4500 aux critères de recherche. • **\b:** Limite de fin des postes SIP.
H	**Nouvelle source**	L'expression régulière **(.*)** est utilisée. Cela signifie que votre poste (l'appelant source) surSipelia Server n'est pas modifié.
I	**Nouvelle destination**	L'expression régulière **(.*)** est utilisée. Cela signifie que le poste appelé n'est pas modifié.

Règle 2 : Acheminement des autres appels vers la jonction SIP.

La seconde règle du plan de numérotation indiquée ci-dessous indique à Sipelia Server d'acheminer vers *TrunkSIPServerA* tout appel qui ne correspond pas à la première règle.



Lettre de valeur	Étiquette de valeur	Description
A	**Nom**	Le nom indique que cette règle acheminera tous les autres appels vers *TrunkSIPServerA*.
B	**Horaire**	L'horaire est réglé sur *Toujours*, ce qui signifie que la règle sera toujours évaluée.
C	**État**	L'état est réglé sur *On*, ce qui signifie que la règle est actuellement active.
D	**Direction de**	Le champ est réglé sur *local* pour rechercher les appels provenant de Sipelia Server.
E	**Direction cible**	Le champ est réglé sur *TrunkSIPServerA* pour acheminer les appels vers cette jonction SIP.
F	**Source**	L'expression régulière est réglée sur **(.*)**, ce qui signifie que l'appel peut être passé depuis *tout* poste SIP inscrit sur Sipelia Server.
G	**Destination**	L'expression régulière est réglée sur **(.*)**, ce qui signifie que l'appel peut atteindre *tout* poste SIP.
H	**Nouvelle source**	L'expression régulière **(.*)** est utilisée. Cela signifie que votre poste (l'appelant source) surSipelia Server n'est pas modifié.
I	**Nouvelle destination**	L'expression régulière **(.*)** est utilisée. Cela signifie que le poste appelé n'est pas modifié.

Résultat

Une fois que le plan de numérotation est importé dans Config Tool, seule la règle prioritaire sera appliquée. Le résultat du plan de numérotation est le suivant :

1 Si un poste SIP compose un numéro entre 4000 et 4500, l'appel reste en local sur Sipelia Server.
2 Si un poste SIP compose un autre numéro, il sera automatiquement acheminé vers *SIP Server A*.

Scénario de plan de numérotation 3 : Réserver une plage de postes SIP pour les appels vers une jonction SIP

Dans ce scénario, les règles de plan de numérotation servent à définir une plage de postes SIP qui sont automatiquement acheminés vers une jonction SIP.

Scénario

- **Objectif** Réserver les postes SIP 4000 à 4500 pour les appels devant être automatiquement acheminés vers *SIP Server A*.
- **À faire avant de définir la règle** Ajoutez une jonction SIP dans Config Tool pour *SIP Server A* et nommez-la *TrunkSIPServerA*. Ce nom de jonction doit être unique, afin que la règle de plan de numérotation que vous créez n'entre pas en conflit avec d'autres règles et qu'elle soit appliquée correctement.
- **Marche à suivre** Vous devez définir deux règles distinctes et les placer dans le bon ordre dans votre plan de numérotation.
  - La première règle redirige automatiquement tout appel effectué vers un poste SIP entre 4000 et 4500 vers *TrunkSIPServerA*.
  - La seconde règle traitera les appels vers les autres postes SIP en les conservant en local sur Sipelia Server.

IMPORTANT : Les règles doivent être placées dans le bon ordre dans le plan de numérotation pour que ce scénario fonctionne correctement.

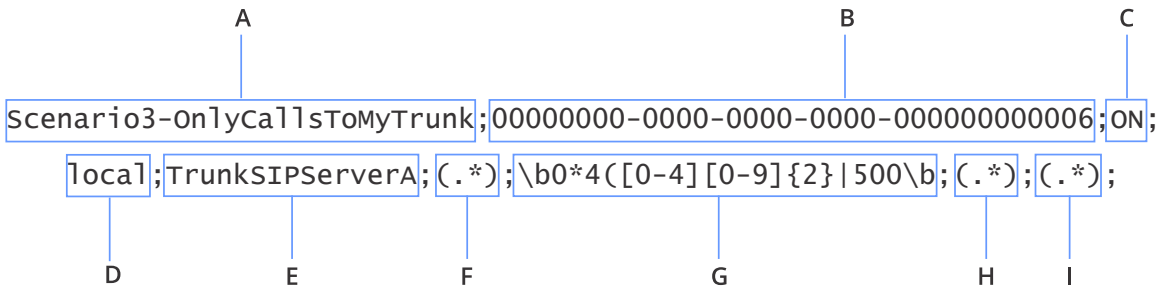
Exemple de plan de numérotation

Voici un exemple de plan de numérotation pour atteindre l'objectif du scénario ci-dessus.

1 Scenario3-OnlyCallsToMyTrunk;00000000-0000-0000-0000-000000000006;ON;local;TrunkSIPServerA;(.*);\b0*4([0-4][0-9]{2}|500)\b;(.*);(.*);
2 Scenario3-RestAreLocalCalls;00000000-0000-0000-0000-000000000006;ON;local;local;(.*);(.*);(.*);(.*);

Règle 1 : Appels vers la jonction SIP seulement

La première règle du plan de numérotation indiquée ci-dessous indique à Sipelia Server de rechercher les postes SIP de destination entre 4000 et 4500, et de les transférer vers la jonction SIP.

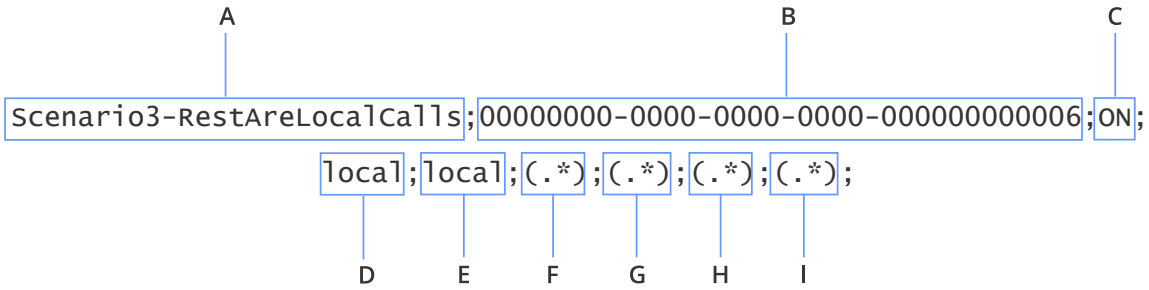


Les étiquettes de valeur identifiées ci-dessous correspondent aux étiquettes de colonne qui apparaissent sur la page Plans de numérotation du rôle Module externe **Sipelia**.

Lettre de valeur	Étiquette de valeur	Description
A	**Nom**	Le nom indique que cette règle acheminera vers la jonction SIP les appels passés vers des postes SIP particuliers.
B	**Horaire**	L'horaire est réglé sur *Toujours*, ce qui signifie que la règle sera toujours évaluée.
C	**État**	L'état est réglé sur *On*, ce qui signifie que la règle est actuellement active.
D	**Direction de**	Le champ est réglé sur *local* pour rechercher les appels provenant de Sipelia Server.
E	**Direction cible**	Le champ est réglé sur *TrunkSIPServerA* pour acheminer les appels vers cette jonction SIP.
F	**Source**	L'expression régulière est réglée sur **(.*)**, ce qui signifie que l'appel peut être passé depuis *tout* poste SIP inscrit sur Sipelia Server.
G	**Destination**	L'expression régulière est réglée sur **\b0*4([0-4][0-9]{2}|500)\b** pour que Sipelia Server recherche les postes SIP de destination entre 4000 et 4500, selon les modalités suivantes : • **\b:** Limite des postes SIP. En tandem avec le même élément **\b** à la fin de l'expression, cette option indique que le numéro de poste SIP entier doit correspondre. Les caractères de début ou de fin ne seront pas ignorés. • **0*:** Rechercher n'importe quel nombre de zéros avant le caractère suivant, qui est le **4**. • **4:** Rechercher un poste SIP qui commence par **4**. • **([0-4]:** Rechercher une seule occurrence des chiffres **0** à **4** après le premier **4**. • **[0-9]{2}:** Rechercher 2 occurrences suivantes des chiffres **0** à **9**, pour couvrir les postes 4000 à 4499. • **|500):** Rechercher spécifiquement **500** pour ajouter 4500 aux critères de recherche. • **\b:** Limite de fin des postes SIP.
H	**Nouvelle source**	L'expression régulière **(.*)** est utilisée. Cela signifie que votre poste (l'appelant source) surSipelia Server n'est pas modifié.
I	**Nouvelle destination**	L'expression régulière **(.*)** est utilisée. Cela signifie que le poste appelé n'est pas modifié.

Règle 2 : Autres appels acheminés en local

La seconde règle du plan de numérotation indiquée ci-dessous indique à Sipelia Server d'acheminer vers *TrunkSIPServerA* tout appel qui ne correspond pas à la première règle.



Lettre de valeur	Étiquette de valeur	Description
A	**Nom**	Le nom indique que cette règle acheminera tous les autres appels en local.
B	**Horaire**	L'horaire est réglé sur *Toujours*, ce qui signifie que la règle sera toujours évaluée.
C	**État**	L'état est réglé sur *On*, ce qui signifie que la règle est actuellement active.
D	**Direction de**	Le champ est réglé sur *local* pour rechercher les appels provenant de Sipelia Server.
E	**Direction cible**	Le champ est réglé sur *local* pour acheminer les appels en local sur Sipelia Server.
F	**Source**	L'expression régulière est réglée sur **(.*)**, ce qui signifie que l'appel peut être passé depuis *tout* poste SIP inscrit sur Sipelia Server.
G	**Destination**	L'expression régulière est réglée sur **(.*)**, ce qui signifie que l'appel peut atteindre *tout* poste SIP.
H	**Nouvelle source**	L'expression régulière **(.*)** est utilisée. Cela signifie que votre poste (l'appelant source) surSipelia Server n'est pas modifié.
I	**Nouvelle destination**	L'expression régulière **(.*)** est utilisée. Cela signifie que le poste appelé n'est pas modifié.

Résultat

Une fois que le plan de numérotation est importé dans Config Tool, seule la règle prioritaire sera appliquée. Le résultat du plan de numérotation est le suivant :

1 Si un poste SIP compose un numéro entre 4000 et 4500, l'appel est acheminé en vers *TrunkSIPServerA*.
2 Si un poste SIP compose un autre numéro, l'appel sera acheminé en local vers Sipelia Server.

Scénario de plan de numérotation 4 : Remplacer les postes SIP source

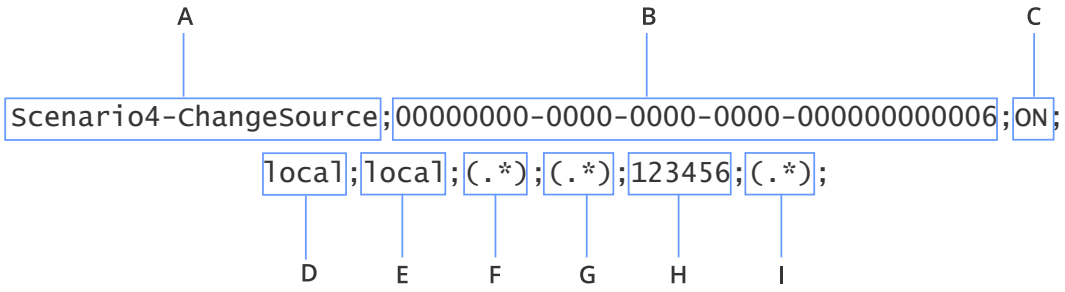
Dans ce scénario, une règle de plan de numérotation remplace les postes SIP source par un numéro de poste SIP unique qui sera présenté aux destinataires. Cette règle peut servir à assurer la confidentialité des appelants.

Scénario

- **Objectif** Afficher un numéro de poste SIP unique pour tout appel passé.
- **À faire avant de définir la règle** Sélectionnez le poste SIP qui servira toujours de source. Dans ce scénario, 123456 est le poste SIP utilisé.
- **Marche à suivre** Vous devez créer une règle qui prend tout appel provenant de Sipelia Server et remplace le poste SIP source par 123456.

Exemple de règle de plan de numérotation

Voici un exemple de règle de plan de numérotation pour atteindre l'objectif du scénario ci-dessus.



Les étiquettes de valeur identifiées ci-dessous correspondent aux étiquettes de colonne qui apparaissent sur la page Plans de numérotation du rôle Module externe **Sipelia**.

Lettre de valeur	Étiquette de valeur	Description
A	**Nom**	Le nom de la règle indique qu'elle remplacer le poste SIP source.
B	**Horaire**	L'horaire est réglé sur *Toujours*, ce qui signifie que la règle sera toujours évaluée.
C	**État**	L'état est réglé sur *On*, ce qui signifie que la règle est actuellement active.
D	**Direction de**	Le champ est réglé sur *local* pour rechercher les appels provenant de Sipelia Server.
E	**Direction cible**	Le champ est réglé sur *local* pour acheminer les appels en local sur Sipelia Server.

Lettre de valeur	Étiquette de valeur	Description
F	**Source**	L'expression régulière est réglée sur **(.*)**, ce qui signifie que l'appel peut être passé depuis *tout* poste SIP inscrit sur Sipelia Server.
G	**Destination**	L'expression régulière est réglée sur **(.*)**, ce qui signifie que l'appel peut atteindre *tout* poste SIP.
H	**Nouvelle source**	L'expression régulière est réglée sur **123456** afin de transformer le poste SIP par cette valeur constante.
I	**Nouvelle destination**	L'expression régulière **(.*)** est utilisée. Cela signifie que le poste appelé n'est pas modifié.

Résultat

Une fois que cette règle de plan de numérotation est importée dans Config Tool, lorsqu'un poste SIP inscrit sur Sipelia Server appelle un autre poste SIP, le destinataire voit s'afficher le poste SIP source 123456.

Scénario de plan de numérotation 5 : Supprimer le préfixe des postes SIP source provenant d'une jonction SIP

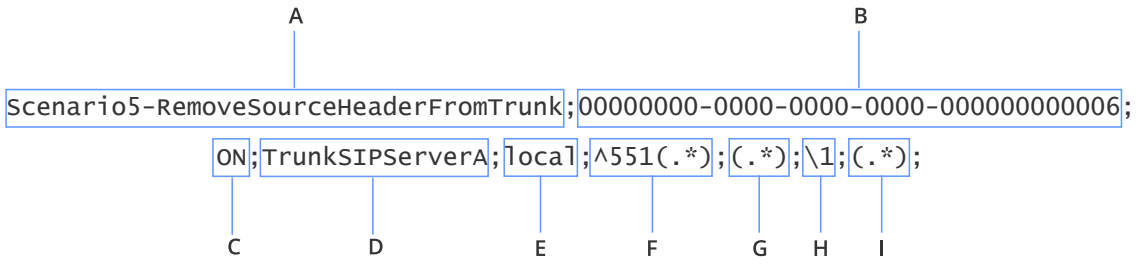
Dans ce scénario, une règle de plan de numérotation sert à supprimer le préfixe utilisé par des postes SIP source pour des appels provenant d'une jonction SIP, afin que les destinataires ne voient pas le préfixe. Ce scénario peut être associé au scénario 1 pour que les postes SIP source soient affichés sans préfixe lors des appels reçus par les destinataires inscrits sur *SIP Server A*.

Scénario

- **Objectif** Supprimer le préfixe des postes SIP source lorsque les appels proviennent d'une jonction SIP.
- **À faire avant de définir la règle** Ajoutez une jonction SIP dans Config Tool pour *SIP Server A* et nommez-la *TrunkSIPServerA*. Ce nom de jonction doit être unique, afin que la règle de plan de numérotation que vous créez n'entre pas en conflit avec d'autres règles et qu'elle soit appliquée correctement. Vous devez également connaître le préfixe utilisé par la jonction SIP pour ses postes.
- **Marche à suivre** Créez une règle qui prend tout appel provenant d'une jonction SIP et supprime le préfixe utilisé par le poste SIP source.

Exemple de règle de plan de numérotation

Voici un exemple de règle de plan de numérotation pour atteindre l'objectif du scénario ci-dessus.



Les étiquettes de valeur identifiées ci-dessous correspondent aux étiquettes de colonne qui apparaissent sur la page Plans de numérotation du rôle Module externe **Sipelia**.

Lettre de valeur	Étiquette de valeur	Description
A	**Nom**	Le nom de la règle indique qu'elle supprimera le préfixe des postes SIP source qui appellent depuis la jonction SIP.
B	**Horaire**	L'horaire est réglé sur *Toujours*, ce qui signifie que la règle sera toujours évaluée.
C	**État**	L'état est réglé sur *On*, ce qui signifie que la règle est actuellement active.
D	**Direction de**	Le champ est réglé sur *TrunkSIPServerA* pour rechercher les appels provenant de la jonction SIP.

Lettre de valeur	Étiquette de valeur	Description
E	**Direction cible**	Le champ est réglé sur *local* pour acheminer les appels vers Sipelia Server.
F	**Source**	L'expression régulière est réglée sur **^551(.*)** pour rechercher *tout* poste SIP source doté du préfixe 551.
G	**Destination**	L'expression régulière est réglée sur **(.*)**, ce qui signifie que l'appel peut atteindre *tout* poste SIP.
H	**Nouvelle source**	L'expression régulière est réglée sur **\1**, qui indique que la règle utilisera la valeur du premier groupe d'expression régulière, défini dans *Source*. Cela signifie que le préfixe sera supprimé et que le poste SIP source correspondra à **(.*)**.
I	**Nouvelle destination**	L'expression régulière **(.*)** est utilisée. Cela signifie que le poste appelé n'est pas modifié.

Résultat

Une fois que cette règle de plan de numérotation est importée dans Config Tool, tout appel d'un poste SIP source doté du préfixe 551 provenant de *TrunkSIPServerA* sera affiché sans le préfixe. Par exemple, si un appel est reçu de la jonction SIP depuis le poste 5513005, le destinataire inscrit sur Sipelia Server ne verra que 3005.

Scénario de plan de numérotation 6 : Transférer les appels vers un autre poste SIP sur horaire

Dans ce scénario, les règles de plan de numérotation servent à définir une plage de postes SIP pour des appels qui doivent toujours parvenir aux destinataires, tandis que les autres postes SIP sont automatiquement transférés. Cela permet d'acheminer les appels d'interphones SIP vers un centre d'appels la nuit par exemple.

Scénario

- **Objectif** Durant les heures non travaillées, les appels passés vers les postes SIP entre 4000 et 4500 doivent être acheminés vers les destinataires demandés, tandis que les autres appels doivent être transférés vers le poste 1001, qui peut être le poste d'une extrémité SIP (ou d'un client SIP) d'un service de sécurité par exemple.
- **À faire avant de définir la règle** Définissez la plage de postes SIP qui doivent toujours être acheminés et le poste SIP vers lequel les autres appels doivent être transférés. Vous devez également avoir défini un horaire dans Security Center qui servira dans la règle de plan de numérotation.
- **Marche à suivre** Vous devez définir deux règles distinctes et les placer dans le bon ordre dans votre plan de numérotation :
  - La première règle recherche les appels passés vers les postes SIP entre 4000 et 4500, puis les achemine normalement.
  - La seconde règle traitera les appels vers les autres postes SIP en les transférant vers le poste 1001.

IMPORTANT : Les règles doivent être placées dans le bon ordre dans le plan de numérotation pour que ce scénario fonctionne correctement.

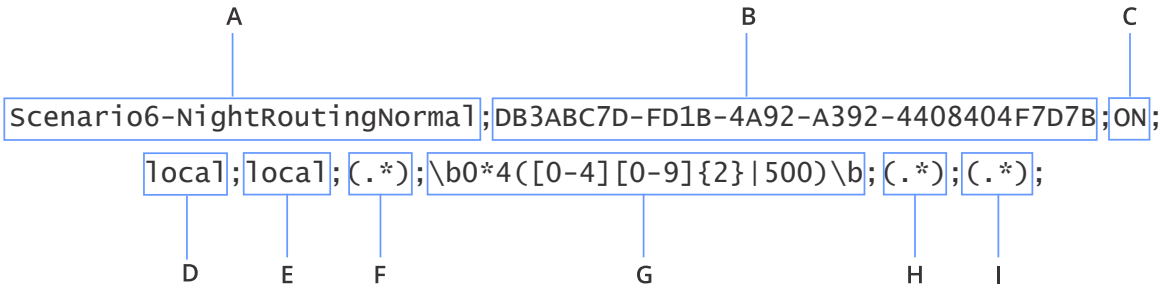
Exemple de plan de numérotation

Voici un exemple de plan de numérotation pour atteindre l'objectif du scénario ci-dessus.

1 Scenario6-NightRoutingNormal;DB3ABC7D-FD1B-4A92-A392-4408404F7D7B;ON;local;local;(.*);\b0*4([0-4][0-9]{2}|500)\b;(.*);(.*);
2 Scenario6-NightRoutingSpecial;DB3ABC7D-FD1B-4A92-A392-4408404F7D7B;ON;local;local;(.*);(.*);(.*);1001;

Règle 1 : Acheminement normal la nuit

La première règle du plan de numérotation indiquée ci-dessous indique à Sipelia Server de rechercher les postes SIP de destination entre 4000 et 4500, et de les acheminer normalement.

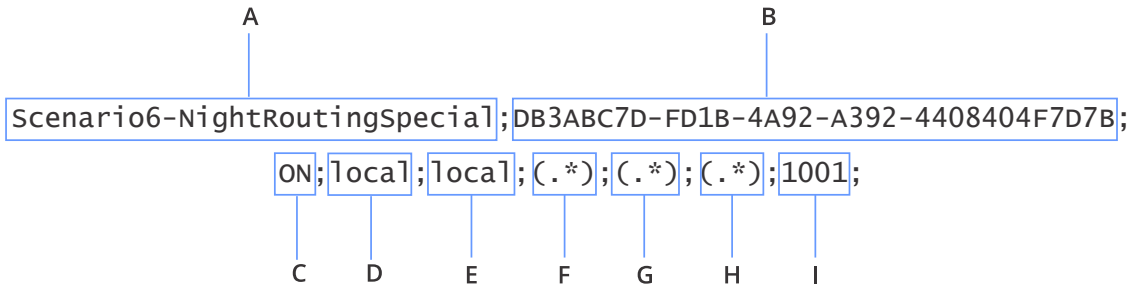


Les étiquettes de valeur identifiées ci-dessous correspondent aux étiquettes de colonne qui apparaissent sur la page Plans de numérotation du rôle Module externe **Sipelia**.

Lettre de valeur	Étiquette de valeur	Description
A	**Nom**	Le nom de la règle indique que les appels sont acheminés normalement.
B	**Horaire**	L'horaire est réglé sur *Heures creuses*, ce qui signifie que la règle ne sera appliquée que durant la période correspondante.
C	**État**	L'état est réglé sur *On*, ce qui signifie que la règle est actuellement active.
D	**Direction de**	Le champ est réglé sur *local* pour rechercher les appels provenant de Sipelia Server.
E	**Direction cible**	Ce champ est réglé sur *local* car les appels seront acheminés en local sur Sipelia Server lorsque la règle sera appliquée.
F	**Source**	L'expression régulière est réglée sur **(.*)**, ce qui signifie que l'appel peut provenir de *tout* poste SIP.
G	**Destination**	L'expression régulière est réglée sur **\b0*4([0-4][0-9]{2}|500)\b** pour que Sipelia Server recherche les postes SIP appelés entre 4000 et 4500, selon les modalités suivantes : • **\b:** Limite des postes SIP. En tandem avec le même élément **\b** à la fin de l'expression, cette option indique que le numéro de poste SIP entier doit correspondre. Les caractères de début ou de fin ne seront pas ignorés. • **0*:** Rechercher n'importe quel nombre de zéros avant le caractère suivant, qui est le **4**. • **4:** Rechercher un poste SIP qui commence par **4**. • **([0-4]:** Rechercher une seule occurrence des chiffres **0** à **4** après le premier **4**. • **[0-9]{2}:** Rechercher 2 occurrences suivantes des chiffres **0** à **9**, pour couvrir les postes 4000 à 4499. • **|500):** Rechercher spécifiquement **500** pour ajouter 4500 aux critères de recherche. • **\b:** Limite de fin des postes SIP.
H	**Nouvelle source**	L'expression régulière **(.*)** est utilisée. Cela signifie que votre poste (l'appelant source) surSipelia Server n'est pas modifié.
I	**Nouvelle destination**	L'expression régulière **(.*)** est utilisée. Cela signifie que le poste appelé n'est pas modifié.

Règle 2 : Acheminement spécial de nuit

La seconde règle du plan de numérotation indiquée ci-dessous indique à Sipelia Server de rechercher tout appel qui ne correspond pas à la première règle, et de le transférer vers le poste 1001.



Les étiquettes de valeur identifiées ci-dessous correspondent aux étiquettes de colonne qui apparaissent sur la page Plans de numérotation du rôle Module externe **Sipelia**.

Lettre de valeur	Étiquette de valeur	Description
A	**Nom**	Le nom de la règle indique que les appels sont acheminés selon des modalités particulières.
B	**Horaire**	L'horaire est réglé sur *Heures creuses*, ce qui signifie que la règle ne sera appliquée que durant la période correspondante.
C	**État**	L'état est réglé sur *On*, ce qui signifie que la règle est actuellement active.
D	**Direction de**	Le champ est réglé sur *local* pour rechercher les appels provenant de Sipelia Server.
E	**Direction cible**	Ce champ est réglé sur *local* car les appels seront acheminés en local sur Sipelia Server lorsque la règle sera appliquée.
F	**Source**	L'expression régulière est réglée sur **(.*)**, ce qui signifie que l'appel peut provenir de *tout* poste SIP.
G	**Destination**	L'expression régulière est réglée sur **(.*)**, ce qui signifie que l'appel peut atteindre *tout* poste SIP.
H	**Nouvelle source**	L'expression régulière **(.*)** est utilisée. Cela signifie que votre poste (l'appelant source) surSipelia Server n'est pas modifié.
I	**Nouvelle destination**	l'expression régulière **1001** est utilisée. Cela signifie que l'appel sera toujours transféré vers le poste SIP 1001.

Résultat

Une fois que le plan de numérotation est importé dans Config Tool, seule la règle prioritaire sera appliquée. Le résultat du plan de numérotation est le suivant :

1 Lorsque l'horaire est en vigueur, tout poste SIP qui compose un numéro entre 4000 et 4500 sera conservé en local sur Sipelia Server et sera acheminé normalement vers le destinataire demandé.

2 Lorsque l'horaire est en vigueur, tout poste SIP qui compose un autre numéro verra son appel automatiquement transféré vers le poste SIP 1001.

5

Dépannage

Cette section aborde les sujets suivants:

Dépannage : Impossible d'établir une connexion au serveur

Lorsque vous ajoutez un interphone SIP dans Config Tool, le message d'erreur **Impossible d'établir une connexion au serveur** est affiché.

À savoir

Cette erreur se produit généralement en cas de problème de connexion lié au service de configuration entre hConfig Tool et Sipelia Server.

Pour résoudre ce problème, procédez de la manière suivante :

1 Connectez-vous à Security Center avec Config Tool, et ouvrez la tâche Modules externes.

2 Sélectionnez le rôle Module externe Sipelia, puis cliquez sur **Général**.

3 Vérifiez que **Port du service de configuration** est réglé sur la bonne valeur.

4 Vérifiez que ce port n'est pas bloqué ailleurs sur le réseau.

Dépannage : Échec de la connexion de l'agent de messages

Le rôle Module externe Sipelia affiche le message d'erreur Échec de la connexion de l'agent de messages : et la connexion à Sipelia Server depuis Security Desk est impossible.

À savoir

Cette erreur survient généralement lorsque la version de RabbitMQ déjà installée sur votre serveur est plus récente que la version requise par Sipelia. Des modifications apportées aux versions successives de RabbitMQ empêchent l'utilisation de versions plus récentes. Il est conseillé d'installer la version incluse dans le pack d'installation de Sipelia.

Pour établir une connexion avec l'agent de messages, procédez de la manière suivante :

1 Redémarrez le service Genetec Server.

2 Si le problème persiste, passez aux étapes suivantes.

3 Désinstallez RabbitMQ Server de votre ordinateur.

4 Supprimez tous les fichiers situés dans *C:\Users\<votre_nom_d_utilisateur>\AppData\Roaming\RabbitMQ*.

REMARQUE : <votre_nom_d_utilisateur> correspond au compte utilisé lors de l'installation initiale de RabbitMQ.

5 Si vous voyez le message **Vous devez disposer d'une autorisation pour effectuer cette action**, supprimez d'abord les fichiers, puis les dossiers.

6 Installez la version de RabbitMQ incluse dans le pack d'installation de Sipelia.

REMARQUE : Le programme d'installation de RabbitMQ est généralement situé dans le dossier *ISSetupPrerequisites*.

7 Sélectionnez tous les composants, et cliquez sur **Suivant**.

8 Sélectionnez le dossier de destination, et cliquez sur **Installer**.

9 Lorsque l'installation est finie, cliquez sur **Terminer**.

10 Redémarrez le rôle Module externe Sipelia.

Dépannage : Impossible d'ajouter des interphones SIP

Lorsque vous ajoutez un interphone SIP dans Config Tool, le message d'erreur **Le nombre de licences Sipelia (standard ou advanced) a été dépassé** est affiché.

À savoir

Cette erreur se produit généralement si vous n'avez pas suffisamment de licences standard ou advanced pour la prise en charge du nombre d'interphone SIP que vous souhaitez ajouter.

Pour pouvoir ajouter un nouvel interphone SIP, procédez de l'une des manières suivantes :

- Supprimez des interphone SIP de votre système.
- Augmentez le nombre de licences.

Dépannage : L'icône de Sipelia n'apparaît pas dans la zone de notification

L'utilisateur ne voit pas l'icône Sipelia dans la zone de notification de Security Desk.

À savoir

Ce problème survient généralement lorsque Sipelia Client n'est pas correctement installé.

Pour résoudre ce problème, procédez de la manière suivante :

1 Redémarrez Security Desk.

2 Si le problème persiste, redémarrez l'ordinateur qui exécute Security Desk.

3 Si vous ne voyez toujours pas l'icône dans la zone de notification, essayez de désinstaller puis de réinstaller Sipelia Client sur l'ordinateur.

Dépannage : Security Desk ne se connecte pas à Sipelia Server

Si Security Desk ne parvient pas à se connecter à Sipelia Server, vérifiez que les adresses IP et numéros de port sont configurés correctement.

À savoir

Les problèmes de connexion surviennent généralement lorsque les adresses IP ou ports ne sont pas configurés correctement, ou lorsque le réseau bloque l'échange des paquets entre les deux extrémités.

Pour résoudre les problèmes de connexion à Sipelia Server, procédez de la manière suivante :

1. Si le poste Security Desk possède plusieurs interfaces (cartes) réseau, vérifiez que l'interface réseau utilisée pour Sipelia est configurée avec la plus haute priorité.
2. Vérifiez que RabbitMQ Server est installé et lancé sur le client (Security Desk) et le serveur (Sipelia Server).
3. Connectez-vous à Security Center avec Config Tool, et ouvrez la tâche Modules externes.
4. Sélectionnez le rôle Module externe Sipelia, et vérifiez qu'il est en cours d'exécution.
5. Cliquez sur **Général**, et vérifiez que les propriétés d'adresse IP et de port sont réglées sur les bonnes valeurs.
6. Cliquez sur **Serveurs**, et vérifiez que **Port SIP** utilise la bonne valeur.
7. Vérifiez que les ports ne sont pas bloqués ailleurs sur le réseau.
8. Ouvrez la tâche *Réseau*, puis sélectionnez le serveur qui héberge le rôle Module externe Sipelia.
9. Cliquez sur **Propriétés**, et vérifiez que la première adresse IP indiquée dans **Adresses privées** (la première de la liste), est celle qui est censée être utilisée par le serveur.
10. Connectez-vous à Security Center avec Security Desk.
11. Cliquez sur **Options** > **Sipelia** > **Avancé**, et vérifiez que **Plage de ports UDP** est configurée comme il faut.
12. Sur l'ordinateur Sipelia Server, naviguez jusqu'au dossier *C:\ProgramData\Genetec Sipelia 2.0\SipServer* et ouvrez *SipServer.config*.
13. Vérifiez que les valeurs *MinimumPortRange* et *MaximumPortRange* sont configurées correctement dans le fichier.

Dépannage : Inscription sur Sipelia Server impossible depuis Security Desk

Si les utilisateurs ne parviennent pas à s'inscrire sur Sipelia Server depuis Security Desk, vérifiez que les propriétés VoIP des utilisateurs concernés sont configurées correctement.

À savoir

Les problèmes d'inscription surviennent généralement lorsque Security Desk parvient à se connecter à Sipelia Server, mais que les postes ou mots de passe SIP ne sont pas configurés correctement.

Pour résoudre ce problème, procédez de la manière suivante :

1 Connectez-vous à Security Center avec Config Tool.

2 Ouvrez la tâche *Sécurité*, puis sélectionnez l'entité utilisateur impactée par le problème de connexion.

3 Sur la page VoIP, vérifiez que les propriétés **Poste SIP** et **Mot de passe** sont configurées avec les bonnes valeurs.

Dépannage : Appels impossibles entre deux extrémités SIP

Si les utilisateurs ne parviennent pas à passer ou recevoir des appels avec Security Desk, les messages sont peut-être bloqués quelque part sur le réseau.

À savoir

Lorsque les utilisateurs sont inscrits sur Sipelia Server mais ne peuvent pas passer ou recevoir d'appels, cela signifie généralement que le réseau bloque l'échange des paquets entre les deux extrémités SIP.

Pour résoudre ce problème, procédez de la manière suivante :

1. Connectez-vous à Security Center avec Security Desk.
2. À l'aide d'un outil d'analyse de protocoles réseau (comme Wireshark), essayez de passer un appel pour voir si les messages SIP sont échangés entre les deux extrémités SIP.
3. Si les paquets SIP sont échangés, vérifiez que c'est aussi le cas des paquets SDP et RTP.
4. Vérifiez que toutes les adresses IP et numéros de port utilisés pas les paquets SIP et SDP sont valables.
5. Si vous pouvez voir que les paquets SIP, SDP et RTP sont échangés sur le réseau entre les deux extrémités SIP, mais que les utilisateurs ne parviennent toujours pas à passer ou recevoir des appels, essayez de redémarrer Genetec Server.

Dépannage : Aucune vidéo affichée durant les appels

Si vous ne voyez pas de vidéo durant les appels, les options de codecs vidéo ne sont peut-être pas configurées correctement.

Pour résoudre ce problème, procédez de la manière suivante :

1 Connectez-vous à Security Center avec Security Desk.

2 Cliquez sur **Options** > **Sipelia** > **Avancé**.

3 Vérifiez que les options suivantes sont réglées correctement :

- **Codecs vidéo:** Les codecs vidéo pris en charge par Security Desk pour les communications vidéo. Par défaut, les codecs H.264 et H.263 sont activés et devraient convenir dans la plupart des cas. Par conséquent, il est recommandé de conserver les réglages par défaut, sachant que changer les codecs vidéo peut perturber la vidéo diffusée durant les appels vidéo. Pour pouvoir afficher la vidéo durant un appel vidéo SIP, les clients SIP impliqués doivent tous prendre en charge au moins un codec vidéo en commun. Par exemple, si le Client SIP A ne prend en charge que le codec H.264 et le Client SIP B ne prend en charge que le codec H.263, aucune vidéo ne sera diffusée durant une session d'appel entre ces deux clients SIP.
- **Plage de ports UDP:** La plage de ports pour le protocole UDP (User Diagram Protocol). Les ports UDP sont utilisés par les différents clients SIP pour émettre et recevoir des données de communication. La plage par défaut va de **20000** à **20500**. Il est recommandé de conserver les réglages par défaut et de ne les modifier que si Sipelia signale des problèmes de communication avec Security Desk liés aux ports.

REMARQUE : La préférence avec la meilleure correspondance sera sélectionnée. Si les deux extrémités prennent en charge les codecs H.264 et H.263, la connexion sera établie en H.264.

4 Si le problème n'est pas résolu, utilisez un outil d'analyse de protocoles réseau (comme Wireshark), et vérifiez que les paquets SDP et RTP sont échangés entre les deux extrémités SIP.

5 Si vous voyez que les paquets SDP et RTP sont échangés mais que la vidéo ne s'affiche toujours pas pendant les appels, essayez de redémarrer Genetec Server.

Dépannage : L'enregistrement audio et vidéo ne fonctionne pas

Si vous pouvez voir de la vidéo pendant les appels, mais que la base de données ne contient pas d'enregistrements, vos options d'enregistrement sont probablement mal configurées.

Pour vérifier que les données audio et vidéo sont enregistrées pendant les sessions d'appel :

1. Vérifiez que votre licence prend en charge l'enregistrement des sessions d'appel.
2. Connectez-vous à Security Center avec Config Tool, et ouvrez la tâche Modules externes.
3. Sélectionnez le rôle Module externe Sipelia, puis cliquez sur **Enregistrement**.
4. Vérifiez que **Utilisateur qui enregistre :** et **Appareil qui enregistre :** sont activés.
5. Si vous n'avez pas d'enregistrement associé à un utilisateur particulier, ouvrez la tâche *Sécurité*, puis sélectionnez l'utilisateur qui pose problème.
6. Sur la page VoIP, vérifiez que la propriété **Enregistrer le son et la vidéo** est activée ou qu'elle hérite la valeur par défaut du rôle Module externe Sipelia.
7. Si vous rencontrez toujours des problèmes d'enregistrement des sessions, essayez de redémarrer Genetec Server.

Dépannage : Les utilisateurs ne peuvent pas visionner les enregistrements vidéo

Si un utilisateur ne parvient pas à afficher de la vidéo enregistrée lors de sessions d'appel précédentes, il peut s'agir d'un problème de configuration de ses privilèges utilisateur.

À savoir

Ce problème survient généralement lorsque l'utilisateur n'a pas le privilège nécessaire pour visionner les enregistrements vidéo dans Security Center.

Pour permettre aux utilisateurs de visionner les enregistrements vidéo :

1 Connectez-vous à Security Center avec Config Tool.

2 Ouvrez la tâche *Sécurité*, puis sélectionnez l'entité utilisateur impactée par le problème.

3 Sur la page **Privilèges**, vérifiez que **Visionner la reprise vidéo** est autorisé pour l'utilisateur.

Ressources supplémentaires

Cette section aborde les sujets suivants:

A

Vocabulaire VoIP courant

Cette section aborde les sujets suivants:

Vocabulaire VoIP courant

Un environnement VoIP (Voice over Internet Protocol ou Voix sur IP) dépend de nombreux composants interconnectés pour fonctionner correctement. Voici une liste de termes techniques couramment utilisés dans ce domaine, et dans les différents manuels Sipelia.

- **signal multifréquence à double tonalité (DTMF ou dual-tone multifrequency):** Le signal multifréquence à double tonalité est la norme pour le signal audible envoyé à l'opérateur téléphonique lorsqu'une touche est activée sur le clavier du téléphone. Chaque touche du clavier est représentée par une tonalité audible différente.
- **téléphone IP:** Un téléphone IP (Internet Protocol) est un appareil utilisé pour passer et recevoir des appels via Internet. Un téléphone IP peut utiliser n'importe quel standard ou protocole de communication existant, comme SIP, pour transmettre les appels sur le réseau. Bien qu'un téléphone IP peut ressembler à un téléphone traditionnel, il n'est pas connecté à une prise de téléphone classique, mais à un routeur ou à un connecteur Ethernet RJ-45.
- **service téléphonique traditionnel (POTS ou plain old telephone system):** Le service téléphonique traditionnel est le service utilisé par la majorité des particuliers et des entreprises dans le monde. Il s'agit non seulement d'une technologie différente, mais d'un service qui se distingue des autres par des différences de débit et de bande passante. Le service téléphonique traditionnel est également appelé réseau téléphonique public commuté (RTPC).
- **PBX (private branch exchange ou autocommutateur privé):** Un autocommutateur privé ou PBX est un réseau téléphonique privé utilisé au sein d'une société. Il s'agit d'un commutateur servant à connecter les nombreux numéros de poste internes à une ligne extérieure, ce qui rend l'installation d'un système téléphonique au sein de l'entreprise plus simple et moins onéreuse. Dans une société équipée d'un réseau PBX, les appels entrants sont redirigés par le commutateur vers un ou plusieurs postes internes.
- **jonctions SIP:** Les jonctions SIP consistent à utiliser la technologie VoIP pour connecter des systèmes PBX existants à d'autres systèmes PBX. Les jonctions SIP remplacent les jonctions téléphoniques traditionnelles par un réseau IP qui consolide la voix, les données et la vidéo sur une même ligne. Les jonctions SIP assurent un service de communication plus fiable à moindre coût.
- **téléphone logiciel:** Un téléphone logiciel est un logiciel qui gère les appels entrants et sortants sur un réseau en passant par un ordinateur au lieu d'un téléphone. Les téléphones logiciels sont conçus pour simuler les fonctionnalités d'un téléphone traditionnel. Également appelé *Client SIP*.
- **Voice over Internet Protocol (VoIP ou Voix sur IP):** Le protocole VoIP (Voice over Internet Protocol) est la technologie servant à acheminer les communications voix et vidéo bidirectionnelles sur le Web et les réseaux IP en général.

Glossaire

B

boîte de dialogue d'appel

La boîte de dialogue d'appel est une boîte de dialogue Sipelia qui apparaît dans la zone de notification de Security Desk lorsqu'un appel arrive d'une extrémité SIP. Dans la boîte de dialogue d'appel, les utilisateurs peuvent gérer leurs appels, leurs contacts et leurs favoris, et régler leur état de disponibilité.

C

Config Tool

Application d'administration de Security Center qui sert à gérer tous les utilisateurs de Security Center et à configurer toutes les entités Security Center, comme les secteurs, caméras, portes, horaires, titulaires de cartes, unités Patroller/RAPI et périphériques matériels.

Client SIP

Un client SIP est un logiciel doté de fonctions de téléphonie que les utilisateurs peuvent installer sur leur ordinateur ou appareil mobile pour échanger des appels audio et vidéo avec d'autres clients SIP. Un client SIP nécessite un compte SIP, et propose généralement une interface qui permet aux utilisateurs de gérer les appels et le cas échéant d'afficher les flux vidéo associés. Les téléphones SIP, téléphones logiciels ou encore les interphones SIP sont des exemples de clients SIP. Une fois que Sipelia Client est installé et configuré, Security Desk devient également un client SIP.

E

entité

Les entités sont les composants de base de Security Center. Tout ce qui requiert une configuration est représenté par une entité. Les entités peuvent représenter un objet physique, comme une caméra ou une porte, ou une notion abstraite, comme une alarme, un horaire, un utilisateur, un rôle, un module externe ou un composant logiciel.

expression régulière

Une expression régulière est une séquence de signes interprétés par un moteur d'expression régulière pour identifier toutes les chaînes de caractères qui correspondent à un critère de recherche particulier, sans qu'il soit nécessaire d'énumérer toutes les valeurs individuelles possibles qui doivent être recherchées. Le moteur utilisé dans Sipelia est celui de Microsoft .NET.

extrémité SIP

Une extrémité SIP est un appareil ou système à chaque bout d'une session d'appel SIP. Il peut s'agir de téléphones filaires, de systèmes de messagerie vocale ou d'interphones. Un client comme un téléphone logiciel est également une extrémité. Une fois que Sipelia Client est installé et configuré, Security Desk devient une extrémité SIP ainsi qu'un client SIP.

entité SIP

Une entité SIP est une entité Security Center dotée de fonctionnalités SIP. Dans Security Center, il peut s'agir d'utilisateurs, de groupes d'appel ou d'appareils SIP comme des interphones SIP.

F

fenêtre de conversation La fenêtre de conversation est une fenêtre Sipelia qui apparaît dans Security Desk lorsqu'un appel SIP est accepté soit par l'appelant, soit par le destinataire de l'appel. Dans la fenêtre de conversation, les utilisateurs de Security Center peuvent gérer les conversations, transférer les appels, et visionner la vidéo associée, si disponible.

G

Genetec Server Genetec Server est le service Windows au cœur de l'architecture de Security Center devant être installé sur tout ordinateur faisant partie de l'ensemble de serveurs de Security Center. Chacun de ces serveurs est une ressource informatique générique apte à accueillir n'importe quel rôle (ensemble de fonctions) que vous lui affectez.

groupe d'appel Un groupe d'appel est un ensemble d'entités SIP qui dispose de son propre numéro de poste. Toutes les entités (ou membres) d'un groupe d'appel font partie d'une liste d'appel, et les membres reçoivent tous les appels reçus par le groupe d'appel. Les membres d'un groupe d'appel peuvent être appelés tous en même temps, ou successivement selon un intervalle prédéfini. L'appel cesse de sonner lorsqu'un membre du groupe d'appel répond à l'appel.

I

interphone SIP Un interphone SIP est une extrémité SIP intelligente qui offre une connectivité bidirectionnelle en environnement SIP. Dans Security Center, un interphone SIP est une entité SIP reconnue, et la seule à correspondre à un appareil réel. Les autres entités SIP dans Security Center sont les utilisateurs et les groupes d'appel.

J

Jonction SIP Une jonction SIP est un serveur SIP qui permet aux utilisateurs de connecter leurs serveurs SIP existants à d'autres serveurs, afin d'étendre leurs capacités VoIP et migrer d'anciens systèmes PBX vers un système VoIP unifié. Avec un plan de numérotation intégré, une jonction SIP permet aux postes SIP inscrits sur différents serveurs SIP de communiquer entre eux.

P

plan de numérotation Un plan de numérotation est un ensemble de règles qui définit la manière d'acheminer les appels en local ou entre deux jonctions SIP. Les plans de numérotation assurent le bon acheminement des appels, et permettent aux administrateurs de restreindre les appels à des sites géographiques ou d'assurer la confidentialité des appelants.

Poste SIP Un poste SIP est une valeur numérique attribuée à un appareil SIP afin qu'il puisse passer et recevoir des appels SIP. Généralement, les numéros de poste SIP servent également à inscrire l'appareil SIP associé à un serveur SIP. Pour pouvoir communiquer avec d'autres extrémités SIP, chaque entité SIP (utilisateur, groupe d'appel ou interphone) dans Security Center doit avoir un numéro de poste attitré.

R

Rapport d'appels

La tâche *Rapport d'appels* est un type de tâche d'investigation qui permet aux utilisateurs d'analyser les sessions d'appel et de créer des rapports. Cette tâche permet notamment aux utilisateurs d'analyser les journaux d'appels de toutes les sessions, de visionner les enregistrements vidéo de toutes les sessions d'appel enregistrées, et de voir les signets qui ont été ajoutés aux séquences vidéo des caméras associées.

rôle

Un rôle est un module logiciel qui effectue une tâche particulière au sein de Security Center. Les rôles doivent être affectés à un ou plusieurs serveurs pour exécution.

S

session d'appel

Une session d'appel est la séquence d'événements ou d'activités qui surviennent du moment de l'initiation d'un appel SIP à la fin de l'appel, y compris tous les transferts. Par exemple, si un appel est transféré deux fois, la séquence d'événements qui survient lors des deux transferts fait partie de la même session d'appel. Dans un système Security Center équipé du module Sipelia, les sessions d'appel peuvent être analysées et exportées avec la tâche *Rapport d'appels* de Security Desk.

Security Center

Security Center est la plate-forme de sécurité unifiée qui intègre de manière transparente les systèmes de sécurité sur IP de Genetec au sein d'une même solution innovante. Les systèmes unifiés au sein de Security Center sont Omnicast, le système de vidéosurveillance sur IP de Genetec, Synergis, son système de contrôle d'accès sur IP, ainsi que le système AutoVu de reconnaissance automatique de plaques d'immatriculation (RAPI).

Security Desk

Security Desk est l'interface utilisateur unifiée de Security Center. Il fournit des processus cohérents à l'échelle d'Omnicast, Synergis et AutoVu, les principaux composants de Security Center. La conception centrée sur les tâches de Security Desk permet aux opérateurs de contrôler et surveiller efficacement de nombreuses applications de sécurité et de sûreté.

Session Initiation Protocol

Le protocole SIP ou Session Initiation Protocol est une norme de signalisation utilisée pour contrôler l'échange de données entre plusieurs interlocuteurs dans le cadre de communications multimédias. Sipelia, le module principal qui permet aux utilisateurs de Security Center de passer, recevoir et gérer les appels audio et vidéo via le Web, est basé sur la norme SIP.

Sipelia

Sipelia est un module principal de Security Center qui permet aux utilisateurs de passer, recevoir et gérer les appels audio et vidéo basés sur la norme SIP sur le réseau. Exploitant le protocole open source SIP (Session Initiation Protocol), Sipelia gère aussi l'intégration de plates-formes de vidéosurveillance et de contrôle d'accès comprenant des systèmes d'interphone, et permet aux utilisateurs de consigner les activités d'appel.

Sipelia Client

Sipelia Client est le composant téléphone logiciel de Sipelia. Par conséquent, il installe les éléments d'interface utilisateur du module Sipelia, comme la boîte de dialogue d'appel et la fenêtre de conversation. Sipelia Client doit être installé sur

chaque poste Security Desk exécutant Sipelia, et transforme ainsi Security Desk en client SIP (ou téléphone logiciel).

Sipelia Server

Sipelia Server est le composant serveur SIP de Sipelia. Il reçoit et gère les informations sur les diverses extrémités SIP, puis permet les échanges entre extrémités communiquant en environnement SIP. Sipelia Server recueille et stocke également des informations importantes, comme les données de listes de contact, les réglages de serveur SIP et les enregistrements de sessions d'appel. Sipelia Server doit être exécuté par un rôle Module externe Security Center, et doit donc être installé sur chaque serveur Security Center qui hébergera le rôle Module externe.

Z

zone de notification

La zone de notification est la partie de l'interface utilisateur qui apparaît dans le coin supérieur droit de Security Desk et de Config Tool. 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 configurés pour la zone de notification sont stockés avec le profil des utilisateurs et s'appliquent à Security Desk et à Config Tool.

Informations complémentaires sur les produits

Vous trouverez la documentation sur les produits aux endroits suivants :

- **Pack d'installation:** La documentation est disponible dans le dossier Documentation du pack d'installation. Certains documents intègrent par ailleurs un lien permettant de télécharger la dernière version du document.
- **Portail d'assistance technique de Genetec (GTAP):** La dernière version de la documentation est disponible sur la page Documents de GTAP. Vous devez disposer d'un nom d'utilisateur et d'un mot de passe pour vous connecter à GTAP.
- **Aide:** Security Center Les applications client et web offrent une aide en ligne qui décrit le fonctionnement du produit et la marche à suivre pour utiliser ses fonctionnalités. Patroller et le Sharp Portal proposent également une aide contextuelle pour chaque écran. Pour accéder à l'aide en ligne, cliquez sur Aide, appuyez sur F1 ou touchez le ? (point d'interrogation) au sein des différentes applications client.

Assistance technique

Le centre d'assistance technique de Genetec (GTAC) s'engage à fournir le meilleur service d'assistance technique possible à ses clients du monde entier. En tant que client Genetec, vous avez accès au Portail d'assistance technique de Genetec (GTAP), où vous pouvez trouver des informations et chercher des réponses à vos questions sur les produits.

- **Portail d'assistance technique de Genetec (GTAP):** GTAP est un site Web d'assistance qui offre des informations techniques détaillées, dont des FAQ, une base de connaissances, des manuels d'utilisation, des listes de périphériques pris en charge, des vidéos de formation, des outils et bien plus encore.

  Avant de contacter GTAC ou d'ouvrir un ticket d'assistance, il est important de consulter ce site qui propose des informations sur comment corriger ou contourner certains problèmes et sur les problèmes connus. Vous pouvez vous connecter à GTAP à l'adresse http://gtap.genetec.com.
- **Centre d'assistance technique de Genetec (GTAC):** Si vous ne trouvez pas la réponse sur GTAP, vous pouvez ouvrir un ticket d'assistance en ligne sur https://gtap.genetec.com. Pour obtenir des coordonnées GTAC dans votre pays, consultez la page contact sur https://gtap.genetec.com.

  NOTE: Avant de contacter GTAC, veuillez vous munir de votre ID système (disponible via le bouton À propos de votre application client) et le cas échéant de votre numéro de contrat CMA.
- **Licences:**
  - Pour l'activation ou la réinitialisation de licences, veuillez contacter GTAC sur https://gtap.genetec.com.
  - Pour des problèmes de contenu de licences ou de références ou concernant une commande, veuillez contacter le service clientèle de Genetec à l'adresse customerservice@genetec.com, ou appelez le 1-866-684-8006 (option 3).
  - Pour obtenir une licence de démo ou pour des questions sur les tarifs, veuillez contacter le service commercial de Genetec à l'adresse sales@genetec.com, ou appelez le 1-866-684-8006 (option 2).

Ressources complémentaires

Si vous souhaitez obtenir une assistance complémentaire, en plus du centre d'assistance technique Genetec, vous disposez des ressources suivantes :

- **Forum GTAP:** Le Forum est un forum de discussion convivial qui permet aux clients et aux employés de Genetec de communiquer et de converser sur différents sujets, qu'il s'agisse de questions ou de conseils techniques. Vous pouvez vous y connecter ou vous y inscrire sur https://gtapforum.genetec.com.
- **Formation technique:** Nos formateurs agréés peuvent vous aider à concevoir, installer, exploiter et dépanner votre système dans un environnement de formation professionnel ou dans vos propres locaux. Des services de formation technique sont proposés pour tous les produits et pour différents niveaux d'expérience, et peuvent en outre être personnalisés pour répondre à vos besoins ou objectifs particuliers. Pour plus de détails, reportez-vous à http://www.genetec.com/Services.