



Sipelia User Guide 2.3

Click [here](#) for the most recent version of this document

Copyright notice

© Genetec Inc., 2017

Genetec Inc. distributes this document with software that includes an end-user license agreement and is furnished under license and may be used only in accordance with the terms of the license agreement. The contents of this document are protected under copyright law.

The contents of this guide are furnished for informational use only and are subject to change without notice. Genetec Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

This publication may not be copied, modified, or reproduced in any form or for any purpose, nor can any derivative works be created therefrom without Genetec Inc.'s prior written consent.

Genetec Inc. reserves the right to revise and improve its products as it sees fit. This document describes the state of a product at the time of document's last revision, and may not reflect the product at all times in the future.

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein. The use of this document is subject to the disclaimer of liability found in the end-user license agreement.

Genetec, Genetec Clearance, Omnicast, Synergis, AutoVu, Federation, Stratocast, Sipelia, Citywise, the Genetec Logo, the Mobius Strip Logo, the Genetec Clearance Logo, the Omnicast Logo, the Synergis Logo, the AutoVu Logo, and the Stratocast Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

All specifications are subject to change without notice.

Document information

Document title: Sipelia User Guide 2.3 GA

Document number: EN.704.004-V2.3.B(1)

Document update date: January 13, 2017

You can send your comments, corrections, and suggestions about this guide to documentation@genetec.com.

About this guide

This guide is intended for Sipelia administrators. It describes how to set up, configure, and manage the Sipelia module as part of your Security Center system.

Notes and notices

The following notes and notices might appear in this guide:

- **Tip.** Suggests how to apply the information in a topic or step.
- **Note.** Explains a special case, or expands on an important point.
- **Important.** Points out critical information concerning a topic or step.
- **Caution.** Indicates that an action or step can cause loss of data, security problems, or performance issues.
- **Warning.** Indicates that an action or step can result in physical harm, or cause damage to hardware.

IMPORTANT: Topics appearing in this guide that reference information found on third-party websites were accurate at the time of publication, however, this information is subject to change without prior notice to Genetec Inc.

Contents

Preface: Preface

Copyright notice	ii
About this guide	iii

Chapter 1: Getting started

What is Sipelia?	2
How licensing works in Sipelia	4
Deploying Sipelia	5
User interface tour of Sipelia	6
Call management in Sipelia	6
Call report task in Sipelia	7

Chapter 2: Installation

About Sipelia Server	9
Default ports for Sipelia Server	10
About Sipelia Client	12
Default ports for Sipelia Client	13
Installing Sipelia Server	14
Uninstalling Sipelia Server	16
Installing Sipelia Client	17
Uninstalling Sipelia Client	18

Chapter 3: Configuration

Creating the Sipelia Plugin role	21
Configuring the Sipelia system communication service	22
Configuring the SIP port of Sipelia Server	23
Defining the ranges of SIP phone extensions	24
Installing additional instances of RabbitMQ	26
Modifying the RabbitMQ ports	27
Disabling SSL communication	29
Recording the audio and video of call sessions	30
Configuring SIP accounts for Security Center users	31
Allowing users to see pictures of other users	33
Associating Security Center cameras with users	34
Adding SIP intercoms	36
Associating Security Center entities with SIP intercoms	38
Registering your SIP intercom with Sipelia Server	40
Associating Security Center custom events with Sipelia entity states and call states	41
Configuring Sipelia role failover	43
Ring groups	44
Creating basic ring groups	45
Creating custom ring groups	47
Configuring Sipelia Client	50
Changing the ringtone for incoming Sipelia calls	51
Configuring two-way communication between Sipelia Server and other SIP servers	52

Configuring your SIP intercom to call a specific extension	54
Adding SIP intercom objects to a Plan Manager map	55
How to determine the Sipelia Server IP address	56
Selecting a network interface	57
Enabling and Disabling codecs on Sipelia servers	58
Configuring the device registration margin for SIP intercoms	59
Configuring the SIP trunk state timeout period	60

Chapter 4: SIP trunks and dial plans

Adding SIP trunks	62
Associating Security Center custom events with SIP trunk states	63
Dial plans	64
Dial plan rules	65
Regular expressions in Sipelia	67
Defining dial plan rules	69
Importing dial plans	70
Dial plan scenario 1: Forwarding to a SIP trunk all calls starting with a prefix	71
Dial plan scenario 2: Reserving a range of SIP extensions for local calls	73
Dial plan scenario 3: Reserving a range of SIP extensions for calls to a SIP trunk	76
Dial plan scenario 4: Replacing source SIP extensions	79
Dial plan scenario 5: Removing prefix on source SIP extensions from a SIP trunk	81
Dial plan scenario 6: Forwarding calls to another SIP extension on schedule	83

Chapter 5: Troubleshooting

Unable to establish communication with the Sipelia Server	87
Message broker connection failed to all the configured hosts	88
Lost login credentials to RabbitMQ or modifying RabbitMQ credentials	90
Missing communication service connection for Sipelia Security Desk	91
Message broker connection failed because of invalid credentials	92
Cannot add SIP intercom devices	93
Cannot see the Sipelia icon in the notification tray	94
Security Desk cannot connect to Sipelia Server	95
Cannot register to Sipelia Server Server from Security Desk	96
Cannot make calls between two SIP endpoints	97
Sipelia calls from Security Desk are delayed or are not delivered	98
No video displayed during Sipelia calls	99
Audio and video not being recorded during Sipelia calls	100
No audio, or distorted audio in Sipelia calls	101
DTMF tones not working in Sipelia	102
Users cannot view recorded video from Sipelia calls	103
Enabling file logging for debug traces on the Sipelia Server	104

Additional resources

Appendix A: Common VoIP terms	106
Common VoIP terms	107
Glossary	108
Where to find product information	112

Technical support 113

Getting started

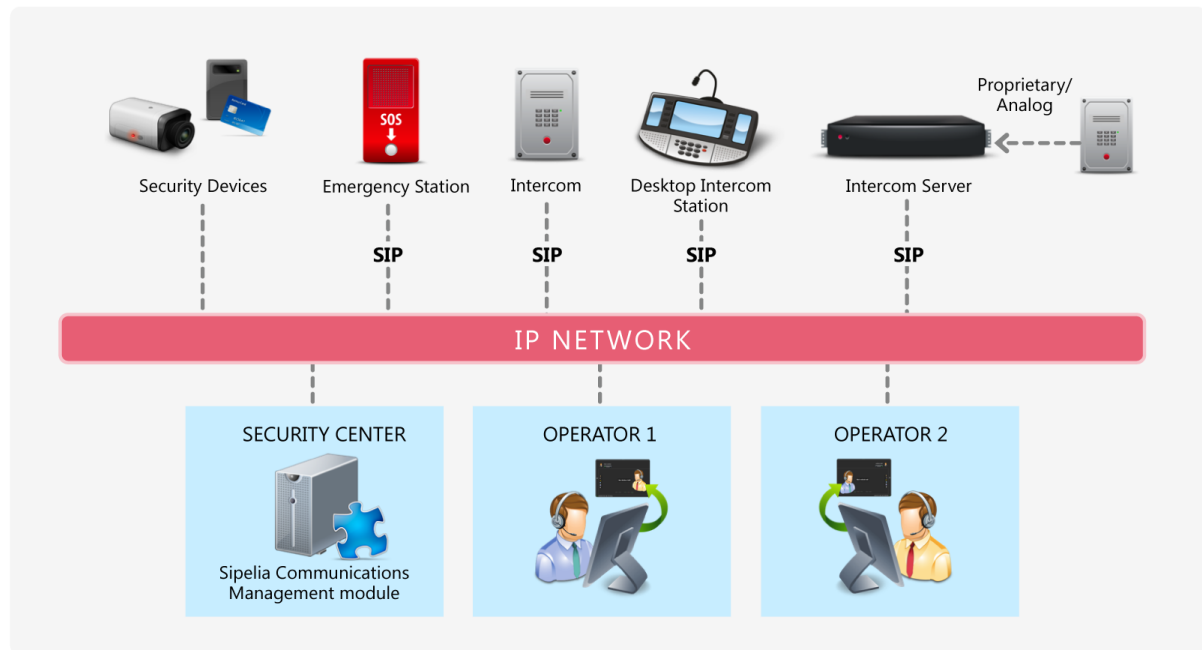
This section includes the following topics:

- ["What is Sipelia?"](#) on page 2
- ["How licensing works in Sipelia"](#) on page 4
- ["Deploying Sipelia "](#) on page 5
- ["User interface tour of Sipelia"](#) on page 6

What is Sipelia™?

Sipelia is a core module of Security Center that allows Security Center users to make, receive, and manage SIP-based voice and video calls over a network. Running on the open source Session Initiation Protocol (SIP), Sipelia also integrates existing video and access control platforms with intercom systems, and allows users to log call activities.

Overview of Sipelia Communications Management



Main features

With Sipelia™ installed within Security Center, you can do the following:

- Connect standard USB headsets and webcams to Security Desk workstations, so that you can make voice and video calls through Security Center.
- Receive incoming call notifications directly through the notification tray in Security Desk.
- Initiate, answer, forward, place on hold, or cancel calls from a dedicated call dialog box.
- Generate reports to investigate the activities within specific call sessions.
- Watch call sessions that have associated video.
- Control cameras, doors, zones, and device outputs during a call.
- Deploy a SIP-based solution that makes it easy to leverage your existing communications infrastructure.
- Connect to SIP intercom devices, intercom exchange servers, and mobile apps through the SIP standard.
- Create a customizable list of contacts, so that users can quickly call their contacts. Contact lists can include other Security Center users, as well as SIP devices.
- Create ring groups so that multiple Security Center users and *SIP entities* can receive incoming calls at the same time or one after another until a user takes the call.

Typical applications

A Sipelia™ integration within Security Center can help you in the following applications:

- Responding to and investigating an emergency
- Responding to employees who have lost their cards
- Granting access to high-security rooms
- Monitoring and managing who enters and exits a parking lot
- User to user video calls, thus making communication more efficient

How licensing works in Sipelia™

Sipelia™ requires a set of licenses that allow the installation and use of the plugin in Security Center and to enable more advanced features.

Sipelia™ requires the following licenses:

- **GSC-Sipelia-Base:** The base system license is required to install the Sipelia™ plugin on Security Center and to allow the operators to make and receive calls.
- **GSC-Sipelia-1SIP-STD:** The standard license allows a SIP device (such as a SIP intercom) to be used in Security Center, whether it registers directly to Sipelia Server or is made available via a SIP trunk. You need one standard license per SIP device that you will be adding to your system.
- **GSC-Sipelia-1SIP-ADV:** The advanced license enables the recording of call sessions and failover of the Sipelia™ Plugin role to a second server when needed. You need one advanced license for each standard license that you will be adding to your system.

NOTE: If the standard and advanced license counts do not match, the system will choose the lower count for both types of licenses, as shown in the example below.

- **GSC-Sipelia-1Trunk:** The trunk license allows you to add and configure a SIP trunk. You need one trunk license for each SIP trunk that you will be adding to your system.

Example

The following sample license shows how the system will apply the license counts when they do not match:

License type	Number of licenses installed	Number of licenses applied
GSC-Sipelia-Base	1	1
GSC-Sipelia-1SIP-STD	100	50
GSC-Sipelia-1SIP-ADV	50	50
GSC-Sipelia-1Trunk	4	4

Deploying Sipelia™

To integrate SIP-based communication into Security Center, so that users can communicate through VoIP, you can deploy Sipelia™ as part of your Security Center system.

Before you begin

- Read the *Sipelia™ 2.3 Release Notes*.
- Familiarize yourself with the [default ports for Sipelia Server](#).
- Familiarize yourself with the [common VoIP terms](#) and the Sipelia™ glossary of terms that are used throughout this guide.

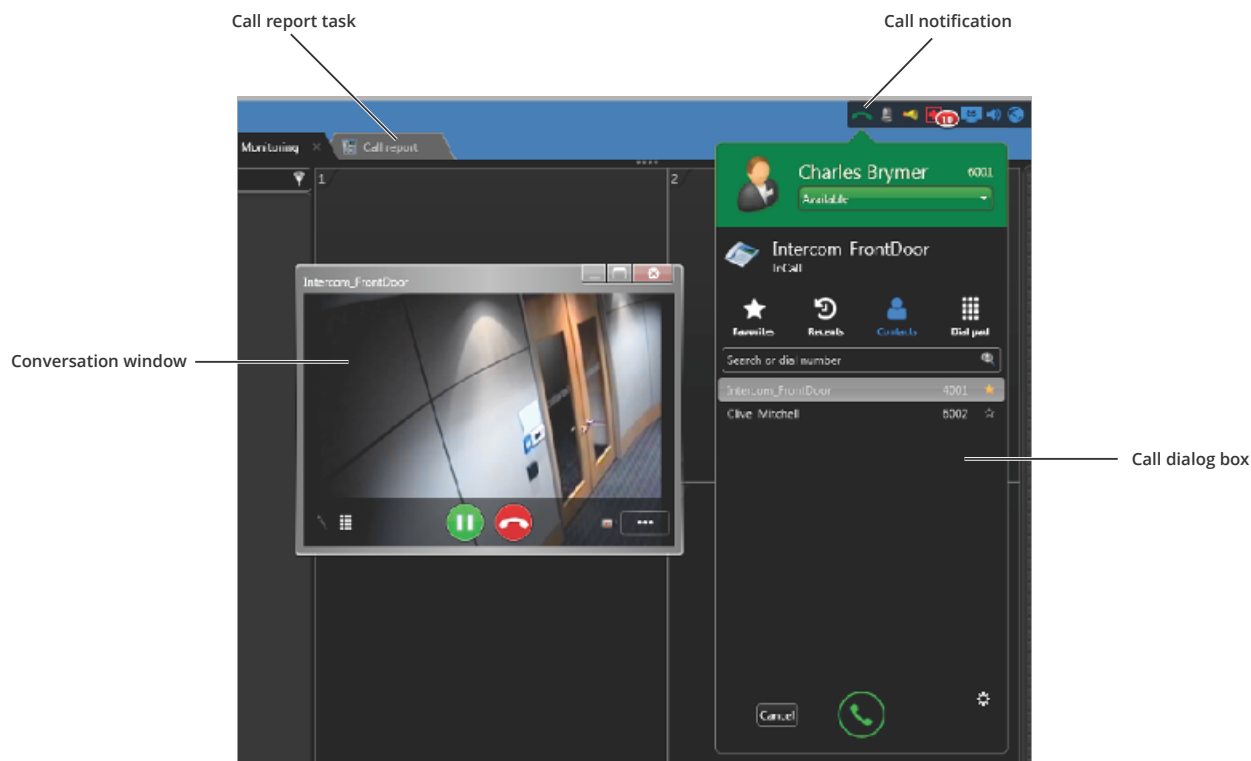
To deploy Sipelia™:

- 1 [Install Sipelia Server](#).
- 2 [Create the Sipelia™ Plugin role](#).
- 3 [Configure the system communication service](#).
- 4 [Configure the SIP port of Sipelia Server](#).
- 5 [Define the ranges of your SIP phone extensions](#).
- 6 [Configure the audio and video recording of call sessions](#).
- 7 [Configure SIP accounts for your Security Center users](#).
- 8 [Create basic ring groups](#).
- 9 [Add your SIP intercoms](#).
- 10 [Register your SIP intercoms with Sipelia Server](#).
- 11 [Create custom ring groups](#).
- 12 [Install Sipelia Client](#) on each of the Security Desk workstations that will run Sipelia™.
- 13 [Configure your devices for voice and video calls in Security Desk](#).
- 14 [Configure two-way communication between Sipelia Server and other SIP servers](#).

User interface tour of Sipelia™

Sipelia is a core module of Security Center that allows Security Center users to make, receive, and manage SIP-based voice and video calls over a network.

Sipelia Client must be installed on every Security Desk workstation that is running Sipelia, thus turning Security Desk into a SIP client (or softphone). The following image shows some of the components of Sipelia Client.



Example

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



Call management in Sipelia™

Integrating Sipelia™ within your Security Center environment provides you with an array of features to help you manage your calls directly from Security Desk.

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



Call report task in Sipelia™

In the *Call report* task, users can investigate call sessions, view the call logs for all sessions, watch playback video and audio of call sessions, and switch between the different video sources that are linked to a session.

Watch this video to learn more. Click the **Captions** icon (CC) to turn on video captions in one of the available languages.



Installation

This section includes the following topics:

- ["About Sipelia Server"](#) on page 9
- ["Default ports for Sipelia Server "](#) on page 10
- ["About Sipelia Client"](#) on page 12
- ["Default ports for Sipelia Client "](#) on page 13
- ["Installing Sipelia Server "](#) on page 14
- ["Uninstalling Sipelia Server"](#) on page 16
- ["Installing Sipelia Client"](#) on page 17
- ["Uninstalling Sipelia Client"](#) on page 18

About Sipelia Server

Sipelia Server is the SIP server component of Sipelia. It receives and administers information about the different SIP endpoints, and essentially facilitates the communication between two or more endpoints that are communicating in a SIP environment. Sipelia Server also collates and stores important data, such as contact list information, SIP server settings, and call session recordings.

Sipelia Server is a server plugin (🔧) that must be run by a Security Center Plugin role. As a result, Sipelia Server must be installed on every Security Center server where you intend to host this Plugin role.

Sipelia Server stores the following data:

- User options
- List of contacts
- Session information (for example: users, time and duration of phone calls, and associated entities)
- Audio and video files related to call sessions
- Configurations of SIP phone extensions for users and devices
- SIP server settings
- Ring group configuration
- SIP trunk configuration
- Dial plan configuration
- Recording settings for users and devices
- Security Center events that are linked to the SIP intercom entity

Default ports for Sipelia Server

To ensure that Sipelia™ works properly, the ports used by Sipelia Server modules must be open and redirected for firewall purposes.

IMPORTANT: When configuring ports, make sure that the ports are open and that they are not being used by another application on the same workstation. For example, if Sipelia Server is installed on the same machine that hosts the Genetec Server, you cannot use the same port that is already being used by Security Center or another application.

Sipelia Server component	Default port number	Protocol	Description
Sipelia Server: SIP port	5060	UDP (SIP)	The port used to enable the SIP protocol on Sipelia Server. As a result, it is the basis of all SIP communication in Sipelia™. The default value is 5060 . Every SIP endpoint, such as softphones and SIP intercoms, that needs to connect to the Sipelia Server must have this port value in their respective configurations.
SIP trunks: SIP port	5060	UDP (SIP)	The port used by the SIP trunk to communicate with the Sipelia Server. Because SIP trunks are SIP servers, the default value is 5060 . SIP trunks are needed if you have a device that is connected to an external IP PBX , and you want to connect this device to Sipelia™.
System communication port	5671	TCP	The port that Sipelia™ uses for SSL communication with the RabbitMQ system communication service. The default value is 5671 , which is a standard of the RabbitMQ service configuration. Sipelia™ uses SSL communication by default.
System communication port	5672	TCP	The port that Sipelia™ uses for non-SSL communication with the RabbitMQ system communication service. The default value is 5672 , which is a standard of the RabbitMQ service configuration. By default, this port is not used. Sipelia™ uses SSL communication by default.
Configuration service port	8201	TCP	The port that Config Tool uses to communicate configuration settings with the Sipelia Server. The default value is 8201 . If there are issues with this port number, you can enter another applicable value.

Sipelia Server component	Default port number	Protocol	Description
Session transfer port	8202	TCP	The port that Sipelia Server uses to download recordings of call sessions to the <i>Call report</i> task in Security Desk. The default value is 8202 . If there are issues with this port number, you can enter another applicable value.
Sipelia Server UDP port range	20000-20500	UDP (RTP)	<p>The port range for the User Datagram Protocol (UDP). The UDP ports are used by the different SIP clients to send and receive communication data. The default range is from 20000 to 20500. It is recommended to keep the default settings, and to change them only if Sipelia logs any port-related issues about making or receiving calls with Security Desk.</p> <p>The UDP port range used by Sipelia Server is set with the <i>MinimumPortRange</i> and <i>MaximumPortRange</i> properties found in <i>C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config</i>.</p>

About Sipelia Client

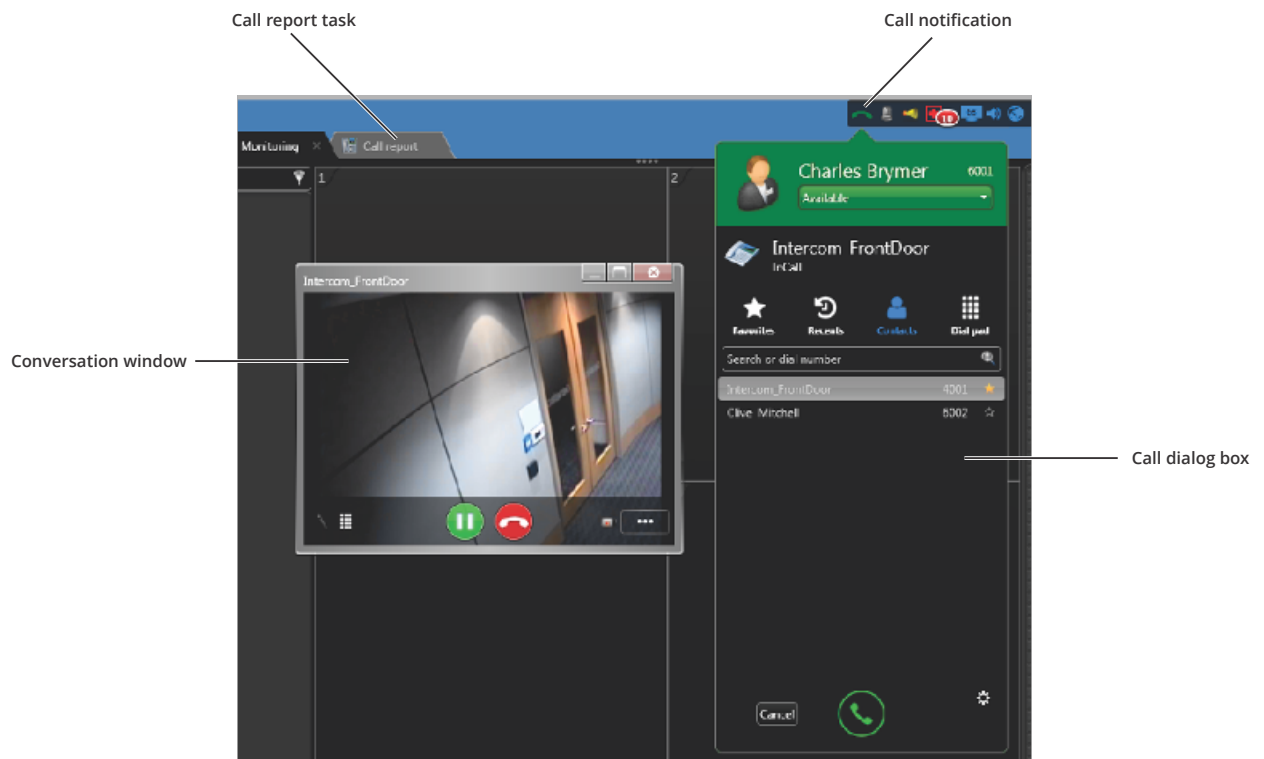
Sipelia Client is the softphone component of Sipelia. As a result, it installs the various user interface features of the Sipelia module, such as the call dialog box and conversation window.

By installing Sipelia Client, you install the following components:

- Notification tray
- Call dialog box
- Conversation window
- *Call report* task

Although not mandatory, it is recommended that you install Sipelia Client after installing and deploying Sipelia Server. If Sipelia Client is installed before Sipelia Server, the user interface in Sipelia™ will not be enabled.

Sipelia Client must be installed on every Security Desk workstation that is running Sipelia, thus turning Security Desk into a SIP client (or softphone). The following image shows some of the components of Sipelia Client.



Default ports for Sipelia Client

To ensure that Sipelia™ works properly, the ports used by Sipelia Client must be properly set in Security Desk.

IMPORTANT: When configuring ports, make sure that the ports are open and that they are not being used by another application on the same workstation.

Sipelia Client component	Default port number	Protocol	Description
System communication port	5671	TCP	The port that Sipelia™ uses for SSL communication with the RabbitMQ system communication service. The default value is 5671 , which is a standard of the RabbitMQ service configuration. Sipelia™ uses SSL communication by default.
System communication port	5672	TCP	The port that Sipelia™ uses for non-SSL communication with the RabbitMQ system communication service. The default value is 5672 , which is a standard of the RabbitMQ service configuration. By default, this port is not used. Sipelia™ uses SSL communication by default.
Sipelia client: SIP port	5060	UDP (SIP)	The port used to enable the SIP protocol on Sipelia Client. This port is used for all basic SIP protocol communication. The default value is 5060 . This value is retrieved from the Sipelia Server and cannot be changed on the Client side.
Advanced: UDP port range	20000-20500	UDP (RTP)	The port range for the User Datagram Protocol (UDP). The UDP ports are used by the different SIP clients to send and receive communication data. The default range is from 20000 to 20500 . It is recommended to keep the default settings, and to change them only if Sipelia logs any port-related issues about making or receiving calls with Security Desk. You can change the UDP port range by clicking Options > Sipelia > Advanced in Security Desk.

Installing Sipelia Server

To integrate SIP functions into Security Center, and allow your system to store data such as phone book contacts and the recordings of call sessions, you must first install *Sipelia Server* before configuring the Sipelia module in Config Tool.

Before you begin

Make sure of the following:

- Your servers meet the hardware requirements described in the *Sipelia™ Release Notes*.
- Config Tool is installed on the system on which you plan to install Sipelia Server.

IMPORTANT: It is recommended to install Sipelia Server on a dedicated Security Center expansion server. Refer to the *Security Center Administrator Guide* for details on how to add an expansion server to your Security Center system.

WARNING: If you already have Sipelia™ installed (2.0 and earlier) and you are upgrading to a newer version (2.1 and up) and that you are also upgrading to a new version of Security Center (from 5.3 and earlier to 5.4 and up), you need to delete the Sipelia™ plugin role before upgrading Security Center. You can then install your new version of Sipelia™ and make it point to your previous database.

What you should know

Sipelia Server is a server plugin (🔧) that must be run by a Security Center Plugin role. As a result, Sipelia Server must be installed on every Security Center server where you intend to host this Plugin role.

Although not mandatory, it is recommended that you install Sipelia Client after installing and deploying Sipelia Server. If Sipelia Client is installed before Sipelia Server, the user interface in Sipelia™ will not be enabled.

To install Sipelia Server:

- 1 Download the product from GTAP (<https://gtap.genetec.com>). You need a username and password to log on to GTAP.
- 2 Double-click on **setup.exe** to run the product's setup. The product's *InstallShield Wizard* dialog box opens.
- 3 Select the installation language, and then click **OK**.

This language selection does not limit the language availability of the installed software. The Sipelia™ user interface appears in the language that is selected for Security Center.

- 4 Click **Next**.
- 5 Read the license agreement, accept the terms, and then click **Next**.
- 6 Select a folder location to install the product, and then click **Next**.
- 7 In the *Custom Setup* dialog box, select the **Server** check box.
- 8 To secure communication between Sipelia Server and Sipelia Client, RabbitMQ and Erlang software are installed. Choose a **Username** and **Password** for RabbitMQ. This account will be created after the RabbitMQ installation.

IMPORTANT: You cannot choose the username *guest* as this username is already used for the default RabbitMQ *guest* account.

NOTE: The RabbitMQ credentials are required later when configuring the Sipelia™ plugin.

- 9 By default, RabbitMQ uses port 5671 for secure SSL communication. You can modify the port if the default does not match your network architecture or requirements.

NOTE: If you modify the RabbitMQ port, you must then [change the port in the Message Broker server settings](#).

10 Click **Install**.

The installation might take a few minutes.

11 Once completed, select **Restart Genetec Server**, and then click **Finish**.

IMPORTANT: You must restart the *Genetec Server* for the system to detect that a new plugin has been installed.

Restarting the Genetec Server causes a short interruption of the service on the server. If you cannot afford to interrupt the service at this time, you can restart the Genetec Server later, as long as you do so before configuring Sipelia™ in Config Tool. To avoid interruptions, it is recommended to install Sipelia Server on a dedicated Security Center expansion server.

Along with Sipelia Server, the RabbitMQ system communication service, which comes bundled with the Sipelia Server installation, is installed automatically. RabbitMQ is the communication channel between Security Desk and Sipelia Server. It is an essential service for ensuring that Sipelia™ works properly.

After you finish

In Config Tool, [create the Sipelia™ Plugin role](#).

Uninstalling Sipelia Server

To completely remove Sipelia Server from your system, you must perform a series of steps.

What you should know

To uninstall Sipelia Server from your system:

- 1 Close all Security Center applications (Security Desk, Config Tool, and Server Admin).
- 2 Click **Start > Control Panel > Programs and Features**.
- 3 In the *Programs and Features* window, right-click **Genetec Sipelia Installer**, and then click **Uninstall**.

NOTE: There are two applications associated with Sipelia™: *Genetec Sipelia Installer*, and *Genetec Sipelia X.X*. Uninstalling *Genetec Sipelia Installer* removes both applications.

- 4 In the *Remove the Program* dialog box, click **Remove**.
- 5 When the message *Uninstallation Completed* is displayed, click **Finish**.
- 6 Restart the computer.

The Genetec™ Sipelia Server application is removed from the system.

Installing Sipelia Client

To turn Security Desk into a *SIP client* and use the various features of the Sipelia module, you must install Sipelia Client on every Security Desk workstation that is running Sipelia.

Before you begin

Make sure of the following:

- [Sipelia Server](#) is installed on your Security Center system.
- Security Center Client is installed on the computer on which you want to install Sipelia Client.
- On computers that provide multiple network interfaces (cards), the network interface to be used by Sipelia Client must be [selected](#) in the Security Desk options.

What you should know

Although not mandatory, it is recommended that you install Sipelia Client after installing and deploying Sipelia Server. If Sipelia Client is installed before Sipelia Server, the user interface in Sipelia™ will not be enabled.

To install Sipelia Client:

- 1 Download the product from GTAP (<https://gtap.genetec.com>). You need a username and password to log on to GTAP.
- 2 Double-click on **setup.exe** to run the product's setup.
The product's *InstallShield Wizard* dialog box opens.
- 3 Select the installation language, and then click **OK**.

This language selection does not limit the language availability of the installed software. The Sipelia™ user interface appears in the language that is selected for Security Center.
- 4 Click **Next**.
- 5 Read the license agreement, accept the terms, and then click **Next**.
- 6 Select a folder location to install the product, and then click **Next**.
- 7 In the *Custom Setup* dialog box, expand the **Client** node.
- 8 If the Plan Manager plugin is installed, and you want to add SIP intercoms on maps, select **Plan Manager Intercom Object**, and then click **Next**.
- 9 Click **Install**.

The installation might take a few minutes.
- 10 When completed, click **Finish**.
- 11 Restart the Security Center applications (Security Desk and Config Tool).

After you finish

If deploying Sipelia, [configure your audio and video devices](#), so that Security Center users can make and receive voice and video calls.

Uninstalling Sipelia™ Client

To completely remove Sipelia™ Client from your system, you must perform a series of steps.

What you should know

To uninstall Sipelia™ Client from your system:

- 1 Close all Security Center applications (Security Desk, Config Tool, and Server Admin).
- 2 Click **Start > Control Panel > Programs and Features**.
- 3 In the *Programs and Features* window, right-click **Genetec Sipelia Installer**, and then click **Uninstall**.

NOTE: There are two applications associated with Sipelia™: *Genetec Sipelia Installer*, and *Genetec Sipelia X.X*. Uninstalling *Genetec Sipelia Installer* removes both applications.

- 4 In the *Remove the Program* dialog box, click **Remove**.
- 5 When the message *Uninstallation Completed* is displayed, click **Finish**.

Configuration

This section includes the following topics:

- ["Creating the Sipelia Plugin role" on page 21](#)
- ["Configuring the Sipelia system communication service" on page 22](#)
- ["Configuring the SIP port of Sipelia Server " on page 23](#)
- ["Defining the ranges of SIP phone extensions" on page 24](#)
- ["Installing additional instances of RabbitMQ" on page 26](#)
- ["Modifying the RabbitMQ ports" on page 27](#)
- ["Disabling SSL communication " on page 29](#)
- ["Recording the audio and video of call sessions" on page 30](#)
- ["Configuring SIP accounts for Security Center users" on page 31](#)
- ["Allowing users to see pictures of other users" on page 33](#)
- ["Associating Security Center cameras with users" on page 34](#)
- ["Adding SIP intercoms" on page 36](#)
- ["Associating Security Center entities with SIP intercoms" on page 38](#)
- ["Registering your SIP intercom with Sipelia Server" on page 40](#)
- ["Associating Security Center custom events with Sipelia entity states and call states" on page 41](#)
- ["Configuring Sipelia role failover" on page 43](#)
- ["Ring groups" on page 44](#)
- ["Creating basic ring groups" on page 45](#)
- ["Creating custom ring groups" on page 47](#)
- ["Configuring Sipelia Client" on page 50](#)
- ["Changing the ringtone for incoming Sipelia calls" on page 51](#)
- ["Configuring two-way communication between Sipelia Server and other SIP servers" on page 52](#)
- ["Configuring your SIP intercom to call a specific extension" on page 54](#)
- ["Adding SIP intercom objects to a Plan Manager map" on page 55](#)
- ["How to determine the Sipelia Server IP address" on page 56](#)
- ["Selecting a network interface" on page 57](#)
- ["Enabling and Disabling codecs on Sipelia servers" on page 58](#)
- ["Configuring the device registration margin for SIP intercoms" on page 59](#)

- ["Configuring the SIP trunk state timeout period"](#) on page 60

Creating the Sipelia™ Plugin role

Once you have installed Sipelia Server on a Security Center server machine, you can create the Sipelia™ plugin role in Config Tool.

Before you begin

Make sure that [Sipelia Server is installed](#).

To create the Sipelia™ Plugin role:

- 1 Log on to Security Center with Config Tool.
- 2 Open the *Plugins* task, click (+) Add an entity, and select **Plugin**.
The *Creating a role: Plugin* wizard appears.
- 3 In the **Server** drop-down list, select the server that is going to host the Sipelia Server role.
- 4 In the **Select plugin type** field, select **Sipelia™**.
- 5 Enter the values for **Database server** and **Database** for the Sipelia™ database, or use the default values which are already provided.
- 6 Click **Next**, enter the entity name and description, and then select the desired partition for this role.
- 7 Click **Next** and check that the information that you have entered is correct.
- 8 Click **Create**, and then click **Close**.

Sipelia™ appears in the list of Plugin roles (🔧). It might take a few minutes for the role to create its database.

After you finish

If deploying Sipelia™, [configure the system communication service](#).

Configuring the Sipelia™ system communication service

As part of the Sipelia™ plugin installation, the RabbitMQ Message broker is also installed. You must configure the Message broker credentials to match those that you entered for RabbitMQ.

What you should know

- As part of the Sipelia™ plugin installation, the RabbitMQ Message broker is also installed. You must configure the Message broker credentials to match those that you entered for RabbitMQ during the installation of Sipelia Server.
- The system communication service for Sipelia™ is RabbitMQ. RabbitMQ is an open source, external Windows service that allows applications that are running on different servers, and at different times, to communicate across dissimilar networks and computers, regardless of whether they are online. Sipelia Server needs this service in order to properly communicate with Security Desk. As a result, this is an essential requirement for a Sipelia™ installation.
- By default, Message broker adds the *guest* account. The *guest* account is only available within the localhost. You can still use the *guest* account for testing purposes, but only when Sipelia™ Server and Sipelia™ Client are installed on the same machine as the RabbitMQ server.
- The default localhost RabbitMQ Message broker connection is added during the Sipelia™ Server installation and is configured to use the default RabbitMQ *guest* account and the default SSL port (5671). If required, you can [modify the default RabbitMQ port](#). You can also [disable the SSL connection](#) to RabbitMQ.

To configure the Sipelia™ Message broker:

- 1 Log on to Security Center using Config Tool.
- 2 Open the *Plugins* task and click the Sipelia™ plugin.
- 3 Click the **General** tab.
- 4 In the **Message broker** section, enter the **Username and Password** that you created for RabbitMQ during the Sipelia™ plugin installation.
- 5 To prevent a loss of communication in the event that the server hosting RabbitMQ is not available, you can install RabbitMQ on multiple servers. Sipelia™ attempts to reach an instance of RabbitMQ beginning with the first server listed in the Message broker configuration. To add additional RabbitMQ servers, click (+), and add the machine name or IP address, as well as the communication port used by that instance of RabbitMQ. Click **Add**.

NOTE: All instances of RabbitMQ must use the same username and password.

The system communication service is configured. If there are issues with the RabbitMQ connection, descriptions of these issues appear in the *Plugin Diagnose* window.

For a description of the other ports shown on the *General* page, see [Default ports for Sipelia Server](#) on page 10.

After you finish

If deploying Sipelia™, [configure the SIP port of Sipelia Server](#).

Configuring the SIP port of Sipelia Server

To enable the SIP protocol on Sipelia Server, you must configure the SIP port of Sipelia Server, and ensure that all connected *SIP endpoints* use the same port value.

Before you begin

If deploying Sipelia™, [configure the system communication service](#).

What you should know

When configuring ports, make sure that the ports are open and that they are not being used by another application on the same workstation. For example, if Sipelia Server is installed on the same machine that hosts the Genetec Server, you cannot use the same port that is already being used by Security Center or another application.

To configure the SIP port of Sipelia Server:

- 1 Log on to Security Center using Config Tool, and then open the *Plugins* task.
- 2 Select the Sipelia™ Plugin role, and then click **Servers**.
- 3 Set the following:
 - **SIP port:** The port used to enable the SIP protocol on Sipelia Server. As a result, it is the basis of all SIP communication in Sipelia™. The default value is **5060**. Every SIP endpoint, such as softphones and SIP intercoms, that needs to connect to the Sipelia Server must have this port value in their respective configurations.
- 4 If you changed the default value of the SIP port, make sure that all SIP clients that are connected to Sipelia Server also use the new port value.

After you finish

If deploying Sipelia™, [define the ranges for the SIP phone extensions](#).

Defining the ranges of SIP phone extensions

Before assigning a SIP extension for a given user, *ring group*, or SIP intercom, you can define multiple ranges of SIP extensions, and then choose a different range for each *SIP entity*.

Before you begin

If deploying Sipelia™, [configure the SIP port of Sipelia Server](#).

What you should know

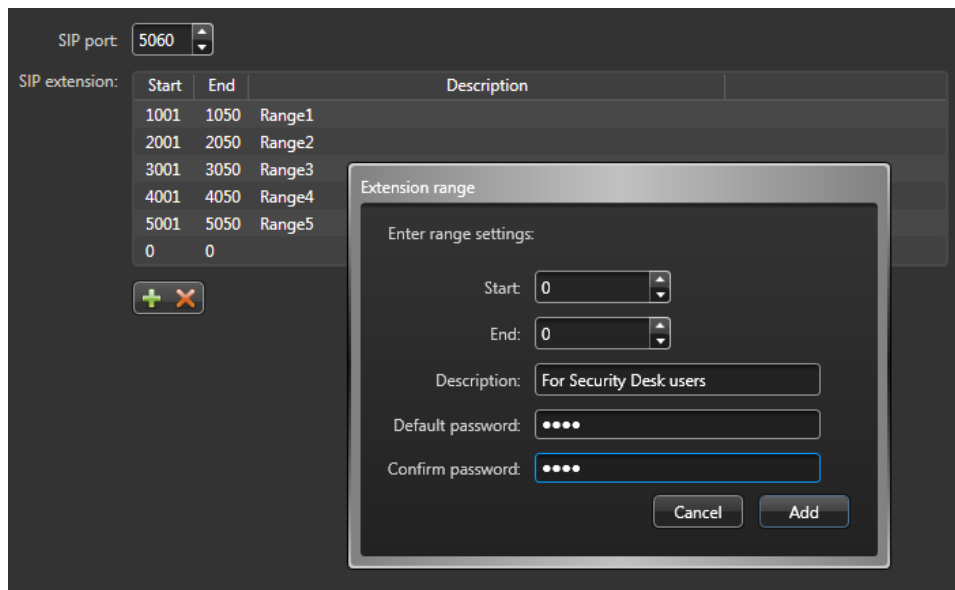
The phone extension ranges are sets of SIP extensions from which you can assign an extension number to each of your SIP entities. Each extension range must have a default password for the extensions, you can only have a maximum of 1000 extensions per range, and you must have a minimum of one defined extension range to be able to connect a SIP entity to Sipelia™. By default, Sipelia™ provides five extension ranges (*Range 1 to Range 5*), each with a default password of 1234.

To define a range of SIP phone extensions:

- 1 Log on to Security Center using Config Tool, and then open the *Plugins* task.
 - 2 Select the Sipelia™ Plugin role, and then click **Servers**.
 - 3 Note the extension ranges that are already defined, and decide on how to assign them to your various SIP entities.
 - 4 To add an extension range, click **Add range** (+).
 - 5 Enter the following:
 - **Start:** The start value of the SIP extension range. The start value must be unique and cannot be greater than the end value.
 - **End:** The end value of the SIP extension range. The end value must be unique and cannot be less than the start value.
 - **Description:** A phrase that describes the range, and perhaps indicates what SIP entity the range is reserved for.
 - **Default password:** The password for every SIP extension within the range. All SIP entities whose respective extensions lie within this range must know this password. Every SIP endpoint, such as softphones and SIP intercoms, that needs to connect to the Sipelia Server must have this password value (along with the extension) in their respective configurations.
 - **Confirm password:** The confirmation of the default password. Values in both password fields must match.
- NOTE:** The start and end values for the extension ranges are inclusive.
- 6 Click **Add**, and then click **Apply**.

Example

As shown in the following image, let's assume that you want to define an extension range reserved solely for Security Center users, and you want to limit the number of extensions to 50. Add a unique extension range that spans 50 numbers, and then enter a default password that applies to every extension within this range. When configuring SIP accounts for your Security Center users, you can assign each user an extension number within this new range, but you can only assign a maximum of 50 users to this range.



After you finish

If deploying Sipelia™, [configure the recording of the audio and video of call sessions.](#)

Installing additional instances of RabbitMQ

If communication with the Message broker server is lost, the Sipelia™ plugin cannot function. To reduce the possibility of system downtime, you can install RabbitMQ on multiple servers.

What you should know

- If communication with the Message broker server is lost, the Sipelia™ plugin shows the error *Message broker connection failed to all the configured hosts*.
- Servers are prioritized according to the order in which they appear in Config Tool. Sipelia™ connects to the topmost Message Broker server first. If it fails to connect, Sipelia™ continues down the server list until a connection is established.

To install multiple instances of RabbitMQ:

- 1 [Install Sipelia Server](#) on one or more additional servers.

NOTE: By default, RabbitMQ uses port 5671 for SSL communication, and port 5672 for non-SSL communication. [These ports can be changed](#) if they do not match your network architecture.

- 2 Add the additional servers in the Message broker configuration.
 - a) In Config Tool, open the *Plugins* task and click the Sipelia™ plugin.
 - b) Click the **General** tab.
 - c) In **Message broker > Servers**, click **Add** (+).
 - d) Enter the **Address** and the configured **Port** of the server. Click **Add**.

NOTE: By default, Sipelia™ uses the SSL connection for communication with RabbitMQ. If you [disable the SSL connection in Sipelia™](#), enter the non-SSL port (5672) here.

- e) Click **Apply** to save your changes.

Modifying the RabbitMQ ports

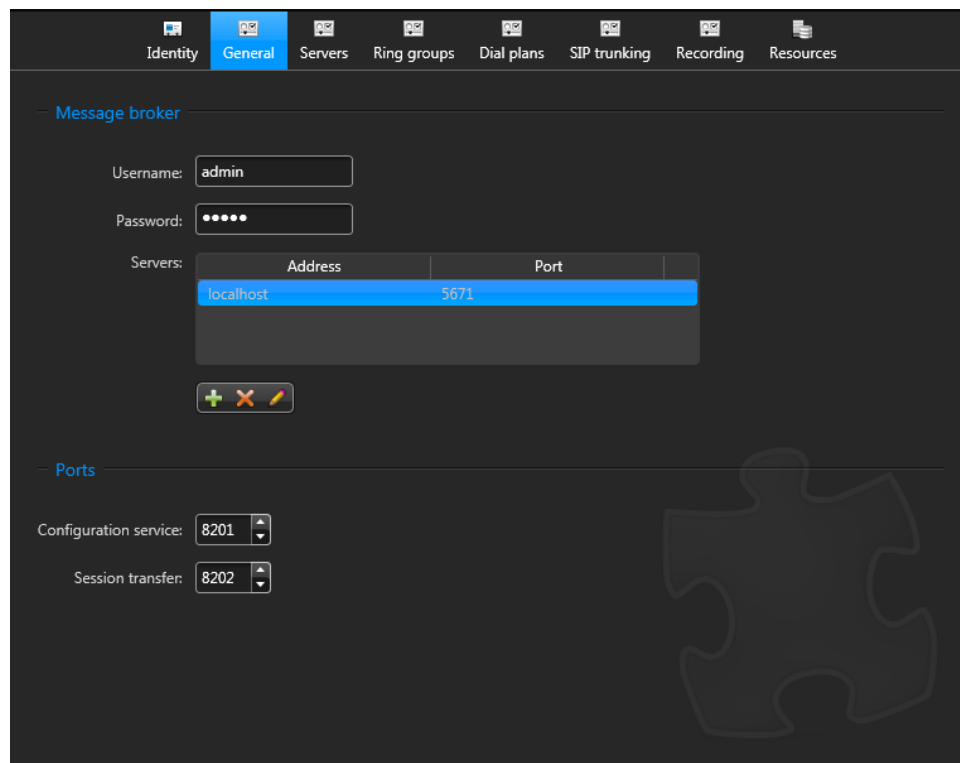
By default, RabbitMQ uses port 5671 for SSL communication, and port 5672 for non-SSL communication. If you change the default port numbers used by Sipelia™, you must also change the port in the Message broker settings.

What you should know

During the Sipelia™ plugin installation procedure, there is an option to modify the SSL port. You can modify the RabbitMQ SSL port and also the non-SSL port at any time using the following procedure.

To modify the Sipelia™ SSL port:

- 1 Update the *RabbitMQ.config* file.
 - a) On the machine where Sipelia™ Server is installed, open File Explorer, and navigate to *Computer > [Local Disk (C:)] > Program Files (x86) > Genetec > RabbitMQ*.
 - b) Open the *RabbitMQ.config* file in a text editor.
 - c) To change the **SSL** port from the default (5671), modify the line: `{ssl_listeners, [5671]}`.
 - d) To change the **non-SSL** port from the default (5672), modify the line: `{tcp_listeners, [5672]}`.
 - e) Save and closed the *RabbitMQ.config* file.
- 2 In the **Services** tab of the Windows Task Manager, restart the RabbitMQ service.
- 3 Update the Message broker port in the Sipelia™ plugin to match the port in the *RabbitMQ.config* file.
 - a) Log on to Security Center using Config Tool.
 - b) Open the *Plugins* task and click the **Sipelia™** plugin.
 - c) Click the **General** tab.
 - d) In **Message broker > Servers**, select the RabbitMQ server for which you have modified the ports and click edit (✎).



- e) Modify the **Port** to match the port you configured in the *RabbitMQ.config* file, and click **OK**.

NOTE: By default, Sipelia™ use the SSL connection to RabbitMQ, so the port entered here must be the SSL port you change in the *RabbitMQ.config* file in the previous steps. If you have [disabled the Sipelia™ SSL connection](#), then you must enter the non-SSL port here.

- f) Click **Apply**.
- g) If you have modified the ports on more than one RabbitMQ server, and if those servers are listed here in Message broker configuration, then you must also edit the port for those servers.

Disabling SSL communication

By default, Sipelia™ uses a Secure Socket Layer (SSL) connection for communication with RabbitMQ. You can disable SSL by modifying the *Sipelia.config* file.

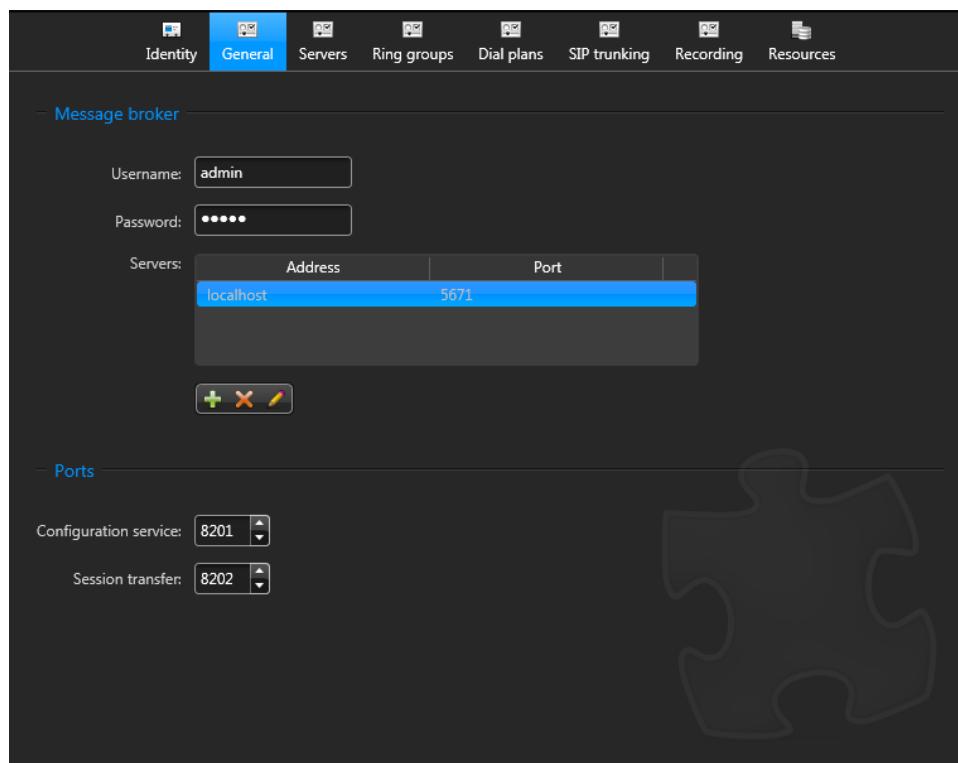
Before you begin

Create a backup copy of the existing *C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config* and save under a new filename.

To disable SSL communication:

- 1 Modify the *Sipelia.config* file.
 - a) Deactivate the Sipelia™ plugin role (see *Security Center Administrator Guide*).
 - b) Open the following configuration file in a text editor:
C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config
 - c) Under <CommunicationService>, locate the entry <IsSslEnabled Value="True"/> and modify the entry to <IsSslEnabled Value="False"/>.
 - d) Save the file and reactivate the Sipelia™ plugin role.
- 2 Configure Sipelia™ to use the non-SSL port.
 - a) Log on to Security Center with Config Tool.
 - b) Open the *Plugins* task and click the Sipelia™ plugin.
 - c) Click the **General** tab.
 - d) In **Message broker** > **Servers**, select the server entry on the list and click edit (✎)

NOTE: If your system includes multiple Message broker servers, you must edit all of them to use the non-SSL port.



- 3 Modify the port to use the non-SSL port (5672).

NOTE: By default, RabbitMQ uses port 5672 as the non-SSL port. If required, you can modify the port used for non-SSL communication.

Recording the audio and video of call sessions

To record the audio and video of call sessions involving users and SIP intercoms, you must configure the recording settings provided in the Recording page of the Sipelia™ Plugin role.

Before you begin

Make sure that you have advanced licenses installed on your system.

What you should know

The **User recording** and **Device recording** options apply to all user and SIP intercom entities, unless an entity is configured differently in which case it will not inherit the default values from the Sipelia™ Plugin role anymore.

To record the audio and video of call sessions:

- 1 Log on to Security Center using Config Tool, and then open the *Plugins* task.
- 2 Select the Sipelia™ Plugin role, and then click Recording.
- 3 Enter the following:
 - **User recording:** Enables the recording of call sessions in which user entities participate (either as a caller or recipient of a call). Once recorded, call sessions can later be reviewed and exported through the *Call report* task in Security Desk. The default value is defined here at the role level, and is inherited by all user entities. It is possible to turn the recording on or off for only specific user entities via the **Recording audio and video** setting provided in the VoIP page of the user entity without affecting all of them.
 - **Device recording:** Enables the recording of call sessions in which the SIP intercom entities participate (either as a caller or recipient of a call). Once recorded, sessions can later be reviewed and exported through the *Call report* task. The default value is defined here at the role level, and is inherited by all SIP intercom entities. It is possible to turn the recording on or off for only specific SIP intercom entities via the **Recording audio and video** setting provided in the VoIP page of the SIP intercom entity without affecting all of them.
 - **Recording folder:** The directory in which the recorded files are stored. It can be a local or a network directory. The Sipelia Plugin role displays an error when the path format is not valid, the local path is not accessible, or the network path does not exist or is unreachable. If a directory specified with a local path does not exist, it will automatically be created. If a path becomes invalid, the call session recording will stop and the recorded files will be lost.
 - **Automatic cleanup:** Enables automatic deletion of the recorded files. This option is enabled by default with a retention period of 30 days.
- 4 Click **Apply**.

After you finish

If deploying Sipelia™, [configure SIP accounts for Security Desk users](#).

Configuring SIP accounts for Security Center users

To allow Security Center users to communicate with one another using the SIP-related controls in Security Desk, you must configure a SIP account for each of your users and assign the appropriate privileges.

Before you begin

- Create the users that you want to configure SIP accounts for (see the *Security Center Administrator Guide* for details).
- Ensure that all users have access rights to the partition where the Sipelia plugin is located. For more information on granting access rights for partitions, refer to the *Security Center Administrator Guide*.
- If you do not want to use the default extension ranges which are already provided, [define your own ranges of SIP phone extensions](#).

What you should know

Once a SIP account has been configured for a Security Center user, that user becomes a SIP entity. A SIP entity is a Security Center entity that has SIP-related capabilities. In Security Center, examples of SIP entities are users, ring groups, and SIP devices such as SIP intercoms.

To configure a SIP account for a Security Center user:

- 1 Log on to Security Center with Config Tool, and then open the *User Management* task.
- 2 Select a user from the list.
- 3 Click the **VoIP** tab to set up this SIP entity as a SIP endpoint.
- 4 Assign a SIP extension to your SIP entity in one of the following ways:
 - Click **Auto-assign**. Auto-assign automatically assigns the SIP entity the next available phone extension in a given range. As a result, it is the recommended way of assigning a SIP extension to users, ring groups, and SIP intercoms. Simply click this button, choose an existing range, and then click **Apply**.
 - Enter the following:
 - **SIP extension:** The SIP entity's phone extension. To be able to communicate with other SIP endpoints, every SIP entity (user, ring group, or intercom) in Security Center must have a unique SIP extension assigned to it. Either enter the extension manually, or use the recommended approach of clicking **Auto-assign**.
 - **Password:** The password for the extension. This password was specified when creating the extension range. Each SIP extension within a given range has its password automatically set to match the default password for that range. Clicking **Auto-assign** automatically populates this field with the correct password for the range, and is therefore the recommended approach.

IMPORTANT: Although you can change the password for a given SIP extension by simply entering a new password, it is not recommended to do so here. It is recommended to change passwords for phone extensions only in the *Servers* tab of the Sipelia™ Plugin role.
- 5 Set the following:
 - **Record audio and video:** Allows you to record the call sessions that the SIP entity participates in (either caller or recipient of a call). Once recorded, sessions can later be reviewed and exported through the *Call report* task. The default value is inherited from the global recording settings which are found on the *Recording* page of the Sipelia Plugin role. Changing this setting at the entity level forces the entity to no longer inherit the value from the global setting, thus allowing you to turn recording on or off for only specific entities, without affecting all of them.
 - **Roaming profile:** When it is turned on (default value), it stores a user's respective Security Desk option settings in the database. As a result, users can log on to Security Desk from a different

computer on the same network and keep their settings. For example, if a user has set the option to have incoming calls always open in a tile, this option will remain intact for this user even on a different Security Desk workstation that is on the same network.

- 6 Click the *Privileges* tab to set up the user's privileges for Sipelia™.
- 7 Under **All privileges** > **Application privileges** > **Sipelia**, select the privileges corresponding to the actions the user is allowed to perform.

IMPORTANT: By default, privileges are set to *Undefined*. For users to make and receive calls, you must explicitly grant the appropriate privileges.

- 8 Click **Apply**.

After you finish

If deploying Sipelia™, [create basic ring groups](#).

Allowing users to see pictures of other users

If you want Security Center users to see the picture of other users in Sipelia™, you must manually add them in the security settings of the associated custom field.

Before you begin

- [Create the Sipelia™ Plugin role.](#)

What you should know

When created, the Sipelia™ Plugin role automatically adds the *Photo* custom field in Security Center. The picture of each user, shown in the list of contacts for example, is provided by this custom field. To be able to see the pictures, users must be added to the *Security* property of the custom field.

To allow a user to see the pictures:

- 1 Log on to Security Center with Config Tool, and then open the *System* task.
- 2 Click Custom fields, select *Photo* in the list, and then click **Edit the item** (✎).
- 3 Under *Security*, click **Add an item** (+), and then select the user.

BEST PRACTICE: You can add all your Sipelia™ users to a single user group, and then add this group to the custom field. This way, each time new users are added to the group, the pictures will automatically be made visible to them.

- 4 Click **OK** > **Save and close** > **Apply**.

Associating Security Center cameras with users

To extend your monitoring capabilities within Security Desk, you can associate Security Center cameras with users that have SIP accounts, so that the live video stream from Security Center cameras is displayed during active phone calls between these users.

Before you begin

- Create your Security Center users (see the *Security Center Administrator Guide* for details).
- [Configure SIP accounts for your Security Center users.](#)

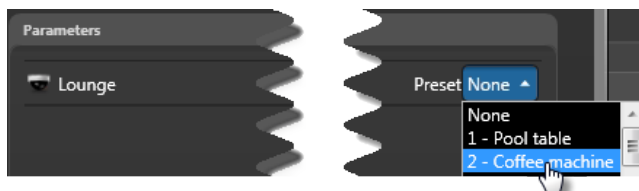
What you should know


Video streams from a Security Center camera do not require a SIP connection, and are therefore not considered video calls. To configure video calls between SIP entities, you must [configure the required audio and video devices in Security Desk](#).

As opposed to SIP intercoms, which allow you to associate cameras, doors, zones, and output devices to them, you can only associate a camera to a Security Center user.

To associate a Security Center camera with a user:

- 1 Log on to Security Center with Config Tool, and then open the *User Management* task.
- 2 Select a user from the list.
- 3 Click the **VoIP** tab.
- 4 In the *Associated entities* section, click **Add an entity** (+).
- 5 In the *Entity association wizard* search for and select the camera entity that you want to associate to your user, and then click **Next**. If you select a PTZ camera, you can select the PTZ preset whose video stream you want to appear during an active call.

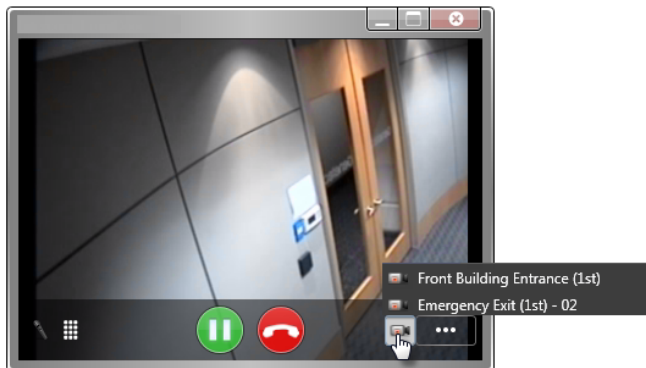


- 6 Confirm your selection by clicking **Next**, and then **Apply**.
- 7 Once the *Entity association wizard* has closed, click **Apply** to save your changes.
The entity that you selected appears in the list of associated entities.
- 8 (Optional) To configure the associated entity that you added, click .
- 9 (Optional) [Associate custom events to call states or Sipelia entity states.](#)
- 10 Associate additional cameras to your user by repeating the steps above.

The camera you have selected is linked to the user. During an active call, the live video stream from this camera appears in the conversation window or Security Desk tile of the users with which this user is communicating. If you have associated multiple cameras, users are able to switch between the different video streams.

Example

Let's assume that you have associated the following two cameras to user Charles: *Front Building Entrance* and *Emergency Exit*. As shown in the following image, when Charles is in an active call with Security Center users, those users can switch between the live video streams of both cameras.



Adding SIP intercoms

To increase the security of your premises and grant access to people upon confirming their identities, you can add a SIP intercom, and then associate it to various Security Center entities such as a camera or door.


Before you begin

- Install the SIP intercom according to the recommendations of the intercom manufacturer.
- If you want to connect a SIP intercom to a *SIP trunk* and not Sipelia Server, [add a SIP trunk](#), and then [define associated dial plan rules](#).
- [Define a range of phone extensions](#) for your SIP intercoms. It is recommended to dedicate extension ranges for each particular SIP entity, especially intercoms that communicate with Sipelia Server through a *SIP trunk*.

What you should know

A SIP intercom is an intelligent SIP endpoint that provides two-way phone connectivity in a SIP environment. In Security Center, a SIP intercom is one of the established SIP entities, and it is the only SIP entity that is an actual device. The other SIP entities are Security Center users and ring groups.

To add a SIP intercom:

- 1 Log on to Security Center using Config Tool, and then open the *Plugins* task.
- 2 Select the **Sipelia™** Plugin role.
- 3 At the bottom of the page, click **Add intercom** .
- 4 Enter a descriptive name for your SIP intercom, and then click **Add**.
The *Logical view* task opens, and the intercom you added appears in the list of entities.
- 5 Click the **VoIP** tab to set up this SIP entity as a SIP endpoint.
- 6 Assign a SIP extension to your SIP entity in one of the following ways:
 - Click **Auto-assign**. Auto-assign automatically assigns the SIP entity the next available phone extension in a given range. As a result, it is the recommended way of assigning a SIP extension to users, ring groups, and SIP intercoms. Simply click this button, choose an existing range, and then click **Apply**.
 - Enter the following:
 - **SIP extension:** The SIP entity's phone extension. To be able to communicate with other SIP endpoints, every SIP entity (user, ring group, or intercom) in Security Center must have a unique SIP extension assigned to it. Either enter the extension manually, or use the recommended approach of clicking **Auto-assign**.
 - **Password:** The password for the extension. This password was specified when creating the extension range. Each SIP extension within a given range has its password automatically set to match the default password for that range. Clicking **Auto-assign** automatically populates this field with the correct password for the range, and is therefore the recommended approach.

IMPORTANT: Although you can change the password for a given SIP extension by simply entering a new password, it is not recommended to do so here. It is recommended to change passwords for phone extensions only in the *Servers* tab of the Sipelia™ Plugin role.
- 7 Set the following:
 - **Record audio and video:** Allows you to record the call sessions that the SIP entity participates in (either caller or recipient of a call). Once recorded, sessions can later be reviewed and exported through the *Call report* task. The default value is inherited from the global recording settings which are found on the *Recording* page of the Sipelia Plugin role. Changing this setting at the entity level

forces the entity to no longer inherit the value from the global setting, thus allowing you to turn recording on or off for only specific entities, without affecting all of them.

- 8 Click **Apply**.
- 9 Add additional SIP intercoms by repeating the steps above.

After you finish

- [Register your SIP intercom.](#)
- [Associate a Security Center entity with your SIP intercom.](#)

Associating Security Center entities with SIP intercoms

To confirm caller identification through live video and grant access to the premises through access controlled doors, you can associate various Security Center entities to a SIP intercom, and then control everything through Security Desk.

Before you begin



Add and configure your SIP intercom in Config Tool.

What you should know

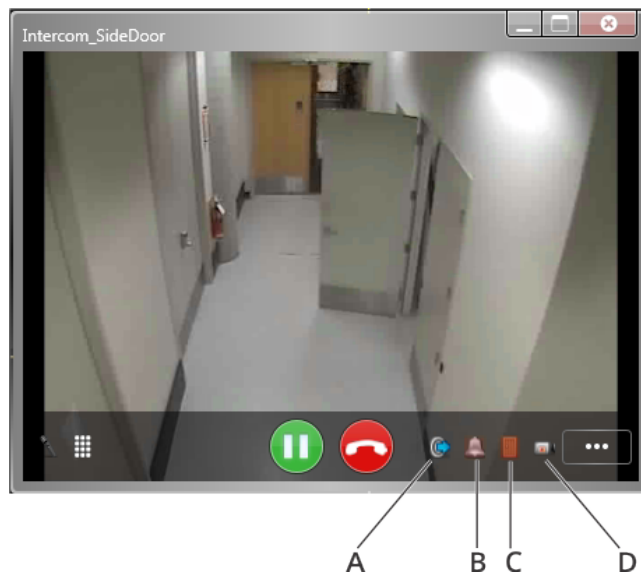
- With SIP intercoms, you can associate cameras, doors, zones, and device outputs along with their respective output behaviors.
- When you associate Security Center entities, the icons that appear in the Sipelia™ conversation window indicate the action that can be performed on the entity. The icons do NOT indicate the current state of the entity. For example, if a door is associated with the intercom, an "unlock" icon (🔓) that appears in the conversation window indicates that the door is currently locked, and you can unlock the door by clicking the icon.

To associate a Security Center entity to a SIP intercom:

- 1 Log on to Security Center with Config Tool, and then open the *Logical view* task.
- 2 From the logical view, select a SIP intercom, and then click the **VoIP** tab.
- 3 In the *Associated entities* section, click **Add an entity** (+).
- 4 In the *Entity association wizard*, select one of the following entities, and then click **Next**. Follow the onscreen instructions to complete the entity association.
 - **Camera:** The camera that you want to associate with the SIP entity. You can associate a camera so that the live video stream from this Security Center camera is displayed during active phone calls between SIP entities.
 - **Door:** The door that you want to associate with the SIP intercom. You can associate a door so that you can unlock it to grant access to callers that use the intercom, and then lock it once the callers have entered.
 - **Zone:** The zone that you want to associate with the SIP intercom. You can associate a zone so that you can arm and disarm it based on the callers that use the intercom. As a result, you can grant or deny callers access to a particular section of your premises. Once set up, in the Security Desk conversation window or tile, click 🔔 to disarm the zone.
 - **Device:** The output of a device that you want to associate with the SIP intercom. Each output must have an associated output behavior; for example, sounding a buzzer (via an output relay) when a window that is equipped with a glass break sensor (connected to an input) is shattered. Once set up, you can trigger the selected output behavior during a call.
- 5 If you selected a device output, do the following to define the output behavior:
 - a) In the **Alias** field, enter a short, descriptive name that allows you to quickly identify the output behavior.
 - b) Select an applicable output type (*Normal*, *Active*, or a custom one). You can create multiple custom output types based on the *State*, *Pulse*, and *Periodic* types. For more information on output behaviors, see the *Security Desk Administrator Guide*.
- 6 Once the *Entity association wizard* has closed, click **Apply** to save your changes. The entity that you selected appears in the list of associated entities.
- 7 (Optional) If your SIP intercom has a built-in camera, and you want the video stream from this camera to be displayed in conversations involving the intercom, you can associate that built-in camera by clicking 📹.

- 8 (Optional) To configure the associated entity that you added, click .
- 9 (Optional) [Associate custom events to call states or Sipelia entity states.](#)
- 10 Repeat the above steps to associate additional entities to the SIP intercom.
- 11 For multiple entities of the same type, use the arrow buttons in the *Associations* panel to define the order in which the entities appear within the conversation window or tile in Security Desk. For example, if you have associated multiple cameras, the live video stream from the camera that appears first in the list is the default stream. Users can switch to the video streams of other cameras by clicking , and then selecting another camera.

If you associate all of the possible entities with a SIP intercom, all of the entities appear within the conversation window or tile in Security Desk. As shown in the following image, each entity can be controlled during an active call.



- **A:** Trigger the output behavior of a device
- **B:** Arm and disarm a zone
- **C:** Open and close a door
- **D:** View the video stream of the selected camera

Example

Let's assume that you want to facilitate how operators respond to lost card requests. With a SIP intercom installed at the main entrance of the building, you can associate the following two entities with that intercom: the camera at the main entrance, and the door at the main entrance. When Charles calls from that SIP intercom, claiming that he has lost his card and cannot enter the building, you can confirm Charles' identity by comparing the live video against his cardholder profile, and then granting or denying access to the building accordingly.

Registering your SIP intercom with Sipelia Server

To make calls from your SIP intercom to Security Center users, you must register the intercom with Sipelia Server.

Before you begin

- Install the SIP intercom according to the recommendations of the intercom manufacturer.
- [Add and configure your SIP intercom in Config Tool.](#)

What you should know

Because there are a variety of SIP intercoms that you can install, the way they are configured and registered to Sipelia Server might differ. The steps below provide a general overview of the settings that must be configured. Always refer to the documentation provided by the manufacturer of the SIP intercom for information on how to configure and register the intercom.

To register your SIP intercom with Sipelia Server:

- Create a SIP account on your intercom.
- Enter an applicable name for your SIP account. This name can be the same as the one given to the intercom when adding it to Security Center, but it does not need to be. The SIP account name is not used during SIP communications.
- Enter the domain or IP address of Sipelia Server.
You can find the IP address of Sipelia Server in **Config Tool > Network view > Properties.**
- For the SIP port value, enter the value you have configured. The default value used by the *Session Initiation Protocol* is **5060**.
- Enter the SIP extension which was assigned to this intercom in Security Center. In certain SIP clients, you must enter the extension number as the username.
- Enter the password for the SIP extension that has been assigned to the intercom.
- Register the intercom so that it can communicate with Sipelia Server.

The SIP intercom is ready to make and receive calls.

After you finish

To create ring groups that include other ring groups and SIP intercoms, [create custom ring groups.](#)

Associating Security Center custom events with Sipelia™ entity states and call states

You can associate custom events to Sipelia™ entities to monitor when a device or a user registers to your SIP server, for example, or goes offline. You can also associate custom events to call states to be notified, for example, when a call was missed or to monitor errors on intercom devices.

Before you begin

- Create the Security Center custom events that you want to associate with entity states or call states. See the *Security Center Administrator Guide, Creating custom events* for details.
- If you want to monitor the state of SIP intercoms, you need to [configure the registration timeout delay for your intercoms](#).

What you should know

Any type of custom events from Security Center can be associated to a Sipelia™ entity state or to a call state. A call state represents the different phases of a call. It tells us, for example, that the call is ringing, busy or in progress. The entity state shows when the entity is online or offline. Two types of entities can be associated to custom events: users and intercoms.

IMPORTANT: You can associate custom events in the following way:

- **Call states:** They can be associated with users, local intercoms (intercoms connected directly to Sipelia™ server, not to a trunk) and with intercoms connected to a trunk.
- **Entity states:** They can be associated with users and local intercoms only. To get the state of an intercom connected to a trunk, you need to [monitor the state of the trunk itself](#).

To associate a Security Center custom event with the state of a Sipelia entity or the state of a call:

- 1 Open Config Tool and choose one of the following:
 - **For users:** Open the **User Management** task and select the user you want to associate with the event.
 - **For intercoms:** Open the **Area view** task and select the intercom you want to associate with the event.
- 2 Click the **VoIP** tab to access the Sipelia parameters.

To associate a custom event to a call state:

- 1 In the *Custom events association* section, under the *Call state events* list, click **Add an item** (+).
- 2 In the *Assign custom event to call state* window, select the call state you want from the **Call state** drop-down list:
 - **Ringng:** A call to or from an intercom or user is ringing.
 - **On a call:** A call with an intercom or user is established.
 - **Busy:** A call with an intercom or user cannot be established for any of the following reasons:
 - The intercom or user is already in a call with another participant.
 - The intercom or user rejects the call.
 - The intercom is connected through a trunk server and the trunk server is not able to reach this intercom.
 - **Not answered:** The intercom or user does not accept or reject the call. The call stops after the ringing timeout.
 - **Error:** Unexpected errors occurred during the call.
 - **End call:** A call was established without error and is properly closed by any of the participants.

- 3 Select the required custom event from the list and click **Add**.
- 4 Click **Apply** to confirm your selection.
The associated event now appears in the Call state events list.

To associate a custom event to an entity state:

- 1 In the *Custom events association* section, under the *Entity state events* list, click **Add an item** (+).
- 2 In the *Assign custom event to entity state* window, select the entity state you want to associate from the **Entity state** drop-down list:
 - **Online:** The entity first registers or registers back after being offline.
 - **Offline:** The entity fails to register or to re-register within the configured period of time.
- 3 Select the required custom event from the list and click **Add**.
- 4 Click **Apply** to confirm your selection.
The associated event now appears in the Entity state events list.

The custom events you have selected are now linked to the Sipelia entity or call states of your choice. You can now associate an action to these events, monitor them or include these events in a report.

Configuring Sipelia™ role failover

You can protect the Sipelia™ role against hardware failures by assigning standby servers to the role.

Before you begin

- Your SIP devices (intercoms, SIP phones, etc.) need to be able to connect to two SIP servers to get failover on Sipelia™. Verify with your manufacturer that your devices support that configuration type.
- [Install Sipelia™ Server](#) on a main and at least one expansion server to use as a standby server for the Sipelia™ role.
- The Sipelia servers need access to a shared database and a shared network drive.

To configure the Sipelia™ role failover:

- 1 Log on to Security Center with Config Tool.
- 2 Open the *Plugins* task, select the Sipelia™ role (🔧) and click **Resources**.
- 3 Under the Servers list, click **Add an item** (+) and select a server where *Sipelia™ Server* has been installed.
- 4 After a failover occurs, if you want the primary server to take control of the role once it is restored, select the **Force execution on highest priority server** option.

By default, the role remains on the secondary server after a failover occurs to minimize system disruptions.

- 5 Configure the Sipelia™ database to be shared with both the primary and secondary servers.
The database is set up when you [create the plugin role](#).
- 6 [Configure the recording folder](#) of each server to point to the shared network drive.

After you finish

You can [register your SIP devices](#) to the primary and the secondary SIP servers that you configured. See your manufacturer's user guide to get detailed information about your SIP device configuration.

Ring groups

A ring group is a group of SIP entities that has its own unique SIP phone extension. All entities (or members) within a ring group are part of a call list, and all members get called when the ring group extension is called. The members of a ring group can either be called all at once, or successively at a set interval. The call stops ringing once any one of the members within a call list answers the call.

In Security Center, there are two types of ring groups: basic and custom.

Basic ring groups

A basic ring group is a Security Center user group which has been assigned its own unique extension. In a basic ring group, you can only include Security Center users and other Security Center user groups.

A basic ring group has the following characteristics:

- It is a Security Center user group.
- It can only include Security Center users and other Security Center user groups.
- It can be assigned its own unique SIP extension.
- Once the extension is dialed, all members of the user group set with a SIP extension are called.
- To be able to receive a call, users that are part of a basic ring group must have their own dedicated SIP extension.
- If users do not have a SIP extension, they are bypassed when the ring group that they are a part of is called.

Custom ring groups

A custom ring group is a ring group that can include any combination of the following entities: users, user groups, and SIP devices. Whereas basic ring groups can only include users and user groups, custom ring groups can also include SIP devices.

A custom ring group has the following characteristics:

- It can include any combination of the following entities: users, user groups, and SIP devices.
- It can be assigned its own unique SIP extension.
- To be able to receive a call, users and SIP devices within a custom ring group must have their own unique SIP extensions.
- If users and SIP devices do not have a SIP extension, they are bypassed when the custom ring group that they are a part of is called.
- Security Center user groups that are part of a custom ring group do not need to have their own unique extensions, but each user entity included in the custom ring group must provide one. User entities that do not have a SIP extension will be omitted when the group is called.

Creating basic ring groups

To call multiple Security Center users at the same time, you can create a basic *ring group* by simply assigning a SIP extension to a Security Center user group.

Before you begin

[Configure SIP accounts for your Security Center users.](#)

What you should know

A basic ring group is a Security Center user group which has been assigned its own unique extension. In a basic ring group, you can only include Security Center users and other Security Center user groups.

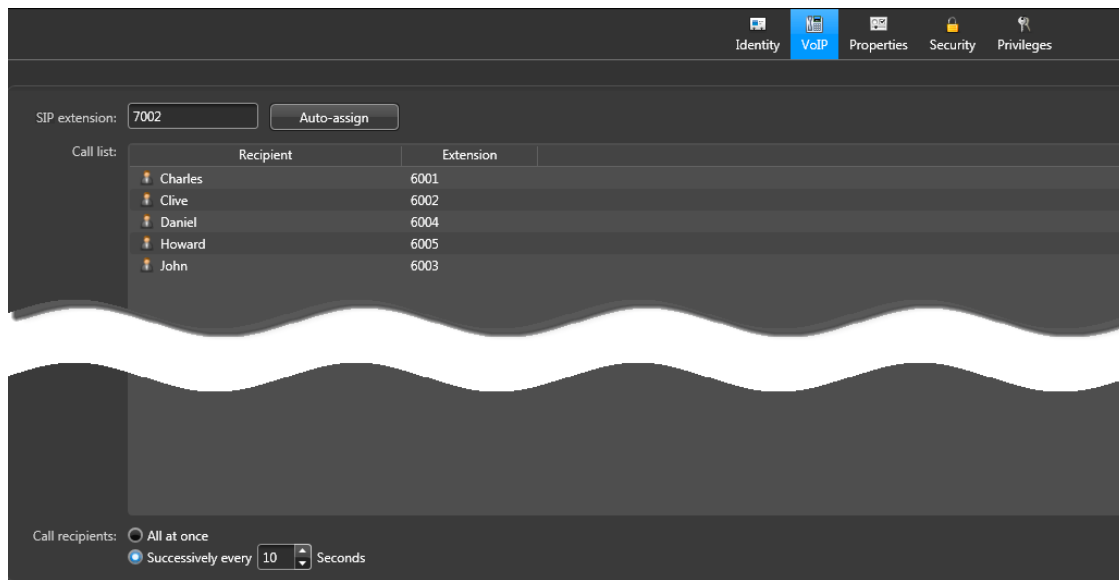
To create a basic ring group:

- 1 Log on to Security Center with Config Tool, and then open the *User Management* task.
- 2 Click **User groups**, and then select one from the list.
- 3 Create a Security Center user group that contains all of the users you want as part of your ring group. For information on creating user groups in Config Tool, see the *Security Center Administrator Guide*.
- 4 Click the **VoIP** tab.
The members of the user group appear in the **Call list** field.
- 5 Assign a SIP extension to your ring group in one of the following ways:
 - Click **Auto-assign**. Auto-assign automatically assigns the SIP entity the next available phone extension in a given range. As a result, it is the recommended way of assigning a SIP extension to users, ring groups, and SIP intercoms. Simply click this button, choose an existing range, and then click **Apply**.
 - Enter the following:
 - **SIP extension:** The SIP entity's phone extension. To be able to communicate with other SIP endpoints, every SIP entity (user, ring group, or intercom) in Security Center must have a unique SIP extension assigned to it. Either enter the extension manually, or use the recommended approach of clicking **Auto-assign**.
- 6 In the **Call recipients** field, select one of the following:
 - **All at once:** All members of a call list are called at the same time. The call stops ringing once any one of the members within a call list answers the call.
 - **Successively every:** Members get called one after another in sequence, with a set delay between each call. The order in which the members are called is based on the order in which they appear in the call list. This sequence of calls is repeated until any one of the members within a call list answers the call. If a member declines the call, the next member in the call list is immediately called, regardless of whether the set delay between calls has elapsed. The minimum delay is 10 seconds. Because it might affect how long a call to a ring group goes unanswered, it is not recommended to set a delay that is too high.
- 7 (Optional) To change the order in which the members of the ring group are called, use the arrow buttons to move the members up or down. This is available only when **Successively every** is selected.
- 8 Click **Apply**.

Example

As shown in the image below, this basic ring group includes five Security Center users, each with their own dedicated extensions. The call sequence for this ring group is set at *Successively every 10 seconds*. As a result, when the ring group extension (7002) is called, Charles' extension (6001) is called first. If Charles

does not answer or decline the call within 10 seconds, Clive's extension (6002) is called. The same sequence continues until one of the members in the call list answers the call.



The screenshot shows a configuration interface for a SIP extension. At the top, there are navigation tabs: Identity, VoIP (selected), Properties, Security, and Privileges. Below the tabs, the SIP extension is set to 7002, with an Auto-assign button. A call list table is displayed with the following data:

Recipient	Extension
Charles	6001
Clive	6002
Daniel	6004
Howard	6005
John	6003

At the bottom, the Call recipients settings are shown: All at once and Successively every 10 Seconds.

After you finish

If deploying Sipelia, [add your SIP intercoms](#).

Creating custom ring groups

To call multiple SIP entities at the same time, you can create a custom *ring group* in Config Tool.

Before you begin

Depending on which entities you want to include in your custom ring group, do one or more of the following:

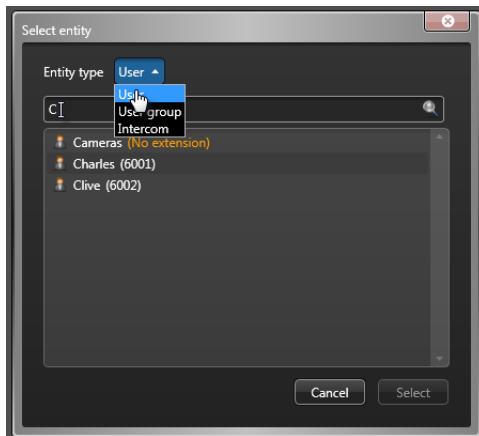
- [Configure SIP accounts for your Security Center users.](#)
- [Create a basic ring group.](#)
- [Add your SIP intercoms.](#)


What you should know

A custom ring group is a ring group that can include any combination of the following entities: users, user groups, and SIP devices. Whereas basic ring groups can only include users and user groups, custom ring groups can also include SIP devices.

To create a custom ring group:

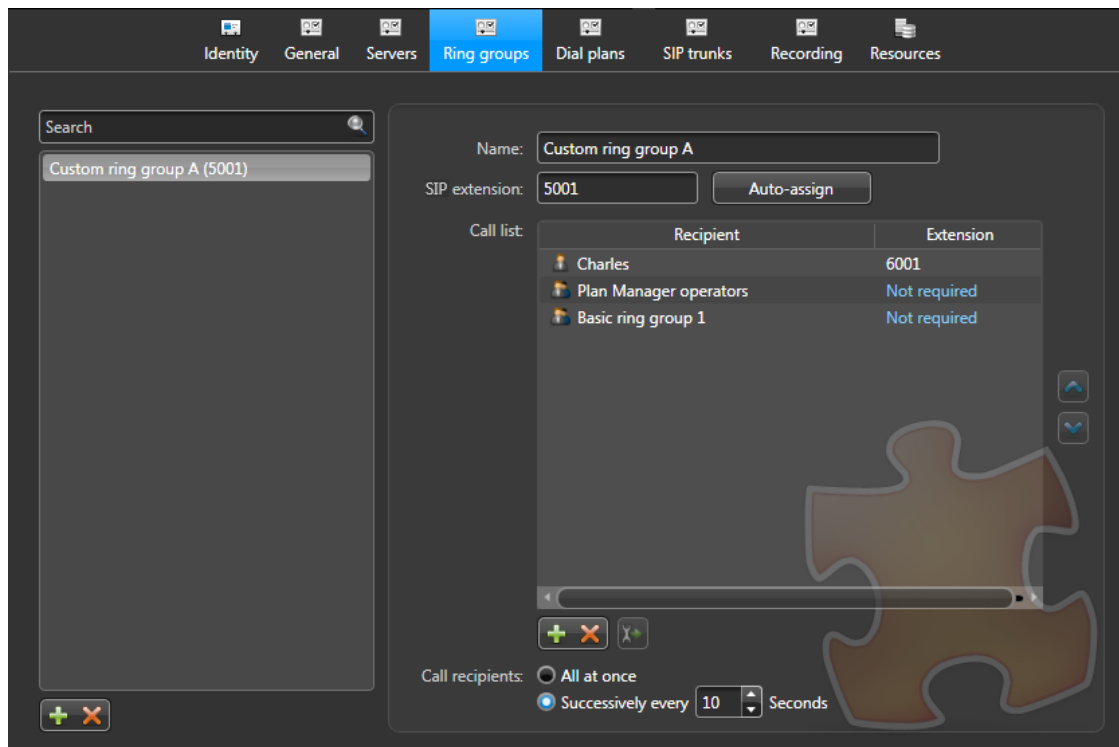
- 1 Log on to Security Center using Config Tool, and then open the *Plugins* task.
- 2 Select the **Sipelia™** Plugin role, and then click **Ring groups**.
- 3 Click **Add ring group** (+).
- 4 Enter a descriptive name for your custom ring group, and then click **Add**.
- 5 Assign a SIP extension to your ring group in one of the following ways:
 - Click **Auto-assign**. Auto-assign automatically assigns the SIP entity the next available phone extension in a given range. As a result, it is the recommended way of assigning a SIP extension to users, ring groups, and SIP intercoms. Simply click this button, choose an existing range, and then click **Apply**.
 - Enter the following:
 - **SIP extension:** The SIP entity's phone extension. To be able to communicate with other SIP endpoints, every SIP entity (user, ring group, or intercom) in Security Center must have a unique SIP extension assigned to it. Either enter the extension manually, or use the recommended approach of clicking **Auto-assign**.
- 6 In the **Call list** field, click **Add entity** (+).
- 7 In the *Select entity* dialog box, choose the different entities that you want to include in your custom ring group. As shown in the following image, you can use the **Entity type** drop-down list to filter by entity type, and then search for the entities by name.



- 8 Once you have selected all of your entities, click **Select**.
- 9 (Optional) To configure the associated entity that you added, click .
- 10 In the **Call recipients** field, select one of the following:
 - **All at once:** All members of a call list are called at the same time. The call stops ringing once any one of the members within a call list answers the call.
 - **Successively every:** Members get called one after another in sequence, with a set delay between each call. The order in which the members are called is based on the order in which they appear in the call list. This sequence of calls is repeated until any one of the members within a call list answers the call. If a member declines the call, the next member in the call list is immediately called, regardless of whether the set delay between calls has elapsed. The minimum delay is 10 seconds. Because it might affect how long a call to a ring group goes unanswered, it is not recommended to set a delay that is too high.
- 11 (Optional) To change the order in which the members of the ring group are called, use the arrow buttons to move the members up or down. This is available only when **Successively every** is selected.
- 12 Click **Apply**.

Example

As shown in the image below, this custom ring group includes three entities: one user, one user group, and one basic ring group. The call sequence for this custom ring group is set at *Successively every 10 seconds*. As a result, when the ring group extension (5001) is called, Charles' extension (6001) is called first. If Charles does not answer or decline the call within 10 seconds, the users that make up the *Plan Manager operators* user group, and that already have an assigned extension, are each called. The same sequence continues until one of the members in the call list answers the call.



After you finish

If deploying Sipelia, [install Sipelia Client](#).

Configuring Sipelia Client

To participate in voice and video calls, you can connect the required audio and video equipment to the Security Desk workstations onto which Sipelia Client is installed, and then configure relevant configuration settings for each Security Center user.

Before you begin

- [Configure SIP accounts for your Security Center users.](#)
- [Install Sipelia Client](#) on each of the Security Desk workstations that run Sipelia.
- Install the required headsets and webcams. For optimal audio quality, it is recommended to use headsets instead of microphones and speakers.

To configure devices for voice and video calls:

- 1 Log on to Security Center with Security Desk.
- 2 Click **Options** > **Sipelia**.
- 3 In the *Audio and video* section, select the physical audio and video devices that are used for calls.
IMPORTANT: Make sure that the devices are properly connected to the Security Desk workstations that run Sipelia™ and that the devices are properly configured in the Windows operating system.
- 4 Click to expand the *Advanced* section, and set the following settings, as required:
 - **Video codecs:** The video codecs that are supported by Security Desk for video communication. By default, the H.264 and H.263 codecs are turned on, and should suffice for most cases. As a result, it is recommended to keep the default settings, and to be aware that changing video codecs can disrupt the video that is streamed during video calls. To be able to view video during a SIP video call, the SIP clients that are involved in a call must all support at least one common video codec. For example, if *SIP client A* only supports the H.264 codec and *SIP client B* only supports H.263, no video is streamed during a call session between the two SIP clients.
 - **UDP port range:** The port range for the User Datagram Protocol (UDP). The UDP ports are used by the different SIP clients to send and receive communication data. The default range is from **20000** to **20500**. It is recommended to keep the default settings, and to change them only if Sipelia logs any port-related issues about making or receiving calls with Security Desk.
- 5 Set the following call-related options, as required:
 - **Open new calls in:** Select whether you want all incoming calls to automatically open in the conversation window or in a tile within the *Monitoring* task in Security Desk.
 - **Ringer:** Use this to enable or disable ringtones for incoming calls.
 - **Ringtone:** Use the **Test** button to test the current *Default* ringtone. Use the **Volume** slider to set the ringtone volume for incoming calls.
NOTE: The **Volume** slider changes the volume of the ringtone, it does not affect the volume of the voice call.
- 6 Repeat these steps on each of the Security Desk workstations that run Sipelia.

After you finish

- Test the audio and video devices by making voice and video calls between SIP clients.
- If deploying Sipelia, [configure two-way communication between Sipelia Server and other SIP servers.](#)

Related Topics

[Changing the ringtone for incoming Sipelia calls](#) on page 51

Changing the ringtone for incoming Sipelia™ calls

You can select a new WAV audio file to be used as the ringtone for Sipelia™ calls. The ringtone can be customized for each Security Desk workstation.

Before you begin

Ensure that the new ringtone audio file you want to use is in WAV format and is accessible from the client machine.

What you should know

In **Security Desk > Options > Sipelia**, the **Ringtone** drop-down list displays the *Default* ringtone. You cannot add new ringtones to the drop-down list, but you can save a new WAV file as the *Default* ringtone.

To change the ringtone for incoming Sipelia™ calls:

- 1 On the machine where Sipelia™ Client is installed, open File Explorer, and navigate to *Computer\Local Disk (C:)\Program Files (x86)\Genetec Sipelia\Sounds*.
- 2 Create a backup copy of the existing *ringtone.wav* and save under a new filename.
- 3 Save the new ringtone WAV file you want to use as *ringtone.wav*.
- 4 Log on to Security Desk.

NOTE: If you are already logged on, you do not need to log off/log on nor do you need to restart the application.

- 5 Click **Options > Sipelia**.
- 6 Click the **Test** button which is located next to the **Ringtone** drop-down list.
The system plays the new ringtone you saved as *ringtone.wav*.
- 7 Move the **Volume** slider to set the ringtone volume.

NOTE: The **Volume** slider changes the volume of the ringtone, and does not affect the volume of the voice call.

Configuring two-way communication between Sipelia Server and other SIP servers

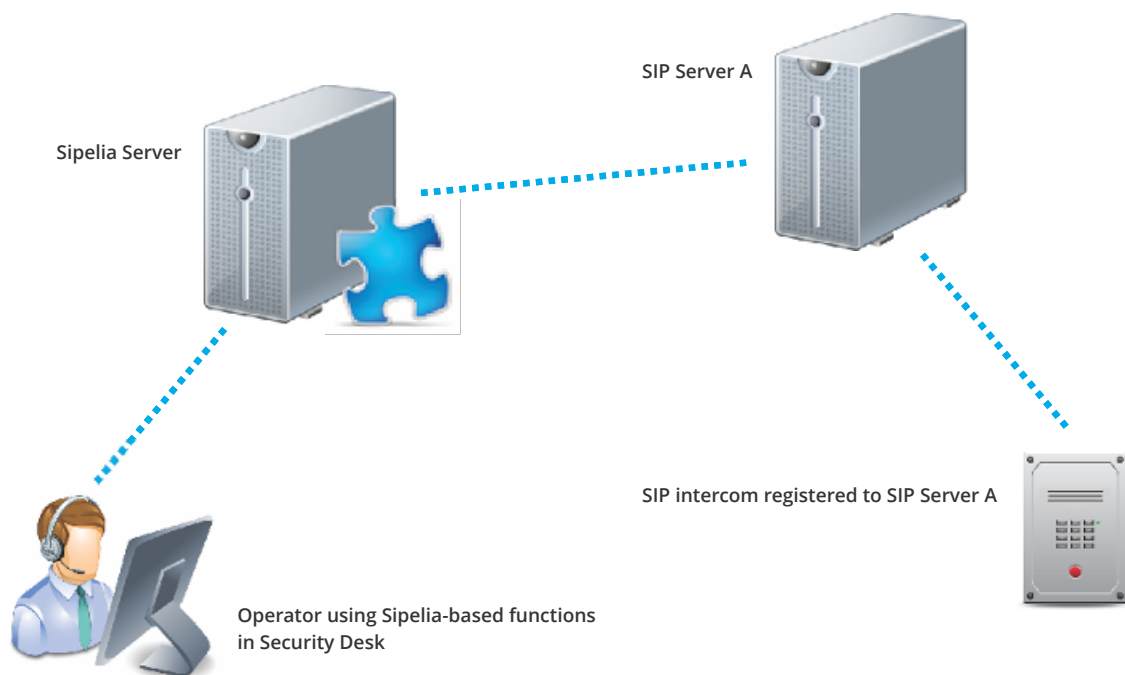
To expand your SIP capabilities, you can configure two-way communication between Sipelia Server and other SIP servers, so SIP extensions from either server can call each other.

Before you begin

- Read the documentation provided by the manufacturer of the SIP server that you want to connect to Sipelia Server.
NOTE: For the purpose of this topic, we will refer to the SIP server that you want to connect to as *SIP Server A*.
- Make sure that *SIP Server A* supports trunking and is able to connect to other SIP servers (in our case, Sipelia Server). Some SIP servers do not support trunking, and therefore, cannot call extensions registered to other SIP servers.
- Make sure that *SIP Server A* has been certified by Genetec as a compatible hardware component, and that it is included in Sipelia's supported hardware list for SIP servers and intercom servers.

What you should know

To have a SIP environment like the one shown in the following image, you must properly configure two-way communication between the two SIP servers (Sipelia Server and *SIP Server A* which, for example, is embedded within an intercom server). In this illustration, Sipelia Server must add *SIP Server A* as a SIP trunk, and *SIP Server A* also needs to add and configure Sipelia Server as a SIP trunk. Also, each SIP server must define appropriate dial plans to be able to contact the other SIP server.



Because there are many different SIP servers available on the market, and numerous possible implementations for each, the method used to configure a SIP trunk and dial plan process differs for each SIP server. As a result, the steps listed below only provide general instructions on how to set up a two-

way communication between Sipelia Server and *SIP Server A*. However, in this topic, and in the related topics about SIP trunks and dial plans, specific instructions are provided for how to set up a one-way communication between Sipelia Server and the SIP trunk for *SIP Server A*. This way, extensions on Sipelia Server can call those on *SIP server A*.

To connect Sipelia Server to *SIP Server A*:

- 1 [Add *SIP Server A* as a SIP trunk](#).
- 2 [Define dial plan rules](#) that allow SIP extensions registered to Sipelia Server to call SIP extensions registered to *SIP Server A*.
- 3 [Import the dial plan rules](#) in Config Tool.

To connect *SIP Server A* to Sipelia Server:

- 1 Add Sipelia Server as a SIP trunk. Refer to the documentation of *SIP Server A* for details on how to add SIP trunks.
- 2 Define and implement dial plan rules that allow SIP extensions registered to *SIP Server A* to call SIP extensions registered to Sipelia Server. Refer to the documentation of *SIP Server A* for details on how to define and implement dial plan rules.

Configuring your SIP intercom to call a specific extension

When your SIP intercom can only be configured to call a specific extension when a button is pressed, it is recommended to configure your SIP intercom to call the SIP extension of a ring group, so that you can manage the list of users who will receive the call.

Before you begin

- Install the SIP intercom according to the recommendations of the intercom manufacturer.
- [Add and configure your SIP intercom in Config Tool.](#)

What you should know

When your SIP intercom only allows the configuration of one SIP extension, it is recommended that you use the extension of a ring group. With a ring group you can then decide who will be called when the button is pressed on the SIP intercom and it calls the extension. The ring group also provides you with the flexibility to adjust the list of recipients to meet your needs.

Because there are a variety of SIP intercoms that you can install, the way they are configured and registered to Sipelia Server might differ. The steps below provide a general overview of the settings that must be configured. Always refer to the documentation provided by the manufacturer of the SIP intercom for information on how to configure and register the intercom.

To configure your SIP intercom to call the SIP extension of a ring group:

- 1 [Add and configure a ring group](#) in Config Tool.
- 2 Take note of the SIP extension that you assigned to the ring group.
- 3 Create a SIP account on your intercom.
- 4 Enter an applicable name for your SIP account. This name can be the same as the one given to the intercom when adding it to Security Center, but it does not need to be. The SIP account name is not used during SIP communications.
- 5 Enter the domain or IP address of Sipelia Server.
You can find the IP address of Sipelia Server in **Config Tool > Network view > Properties.**
- 6 For the SIP port value, enter the value you have configured. The default value used by the [Session Initiation Protocol](#) is **5060**.
- 7 Enter the SIP extension which was assigned to the ring group in Security Center. In certain SIP clients, you must enter the extension number as the username.

The SIP intercom will call the extension of the ring group when its button is pressed. This means that one or more recipients could be called all at once or one after another according to the ring group configuration.


Adding SIP intercom objects to a Plan Manager map

In a system where both Sipelia™ and Plan Manager are installed, you can add SIP intercom objects to your maps so that they are displayed in Security Desk and can be used by the operators to make and receive calls.

What you should know

The Maps role is included with Security Center 5.4 and later.

To add a SIP intercom object to a Plan Manager map:

- 1 Log on to Security Center with Config Tool.
- 2 Open the *Map Designer* task and select a map.
- 3 Navigate to the location on the map where you want to add the SIP intercom object.
- 4 From the **Entities** list in the toolbar, select **Area view** ().
- 5 From the **Area view** list, drag the SIP intercom to the required location on the map.
- 6 Adjust the size, position, and orientation of the SIP intercom object with the mouse. From the panel displayed on the right, you can make precise adjustments to the size and position coordinates of the SIP intercom icon.
- 7 Click **Apply**.

The SIP intercom now appears on the map in the Security Desk *Maps* task. Make a test call to the SIP intercom to test functionality.

How to determine the Sipelia Server IP address

The Security Center main server can be connected to multiple network interfaces and respond to many private IP addresses. The Sipelia Server only uses the first one in the list.

What you should know

In order to connect SIP intercoms to Sipelia Server, you need to determine which IP address the server is using.

To determine which IP address is used by the Sipelia Server:

- 1 From the Config Tool home page, click on the *Network view* task.
- 2 In the left panel, select the server on which Sipelia™ is running.
- 3 Click on the *Properties* tab.

The Sipelia Server IP address is the first one on the *Private addresses* list.

Selecting a network interface

If the computer on which Security Desk is running has multiple network interfaces, to ensure that communication between Security Desk and Sipelia Server works properly, you must select which network interface is to be used for Sipelia™.

What you should know

Applications such as VPN can automatically modify the network interface priorities in Windows, for example, when establishing a connection. Selecting a network interface in Security Desk will ensure that the same interface will always be used, regardless of any priority changes.

To select a network interface:

- 1 From the Security Desk home page, click **Options > General**.
- 2 In the **Network Options** section, select the required network interface from the **Network Card** drop-down list.
- 3 To apply changes, log off then log back on.

The selected network interface will be used by Security Desk to connect and to register to Sipelia Server.

Enabling and Disabling codecs on Sipelia™ servers

To change the default codecs that are allowed to run on Sipelia servers, you must enable or disable them through a configuration file.

Before you begin

- Create a backup of the following file:
`C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config`

What you should know

Enabling and disabling video and audio codecs is done through an XML configuration file. In this file, you can find the following XML elements: **AudioCodecs** and **VideoCodecs**. The **Codec** element within them contains the **Enabled** attribute that defines the state of each codec.

To enable or disable a specific audio or video codec:

- 1 Deactivate the Sipelia™ plugin role (see *Security Center Administrator Guide*).
- 2 Open the following configuration file:
`C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config`
- 3 In the chosen **Codec** element, modify the **Enabled** attribute to `False` to disable the codec or to `True` to enable it.

CAUTION: You must only change the **Enabled** attribute, never the **Name** attribute. It is not possible to add new types of codecs directly by editing this configuration file.

- 4 Save the file and reactivate the Sipelia™ plugin role.

To restore default values without a backup file:

- 1 Deactivate the Sipelia™ plugin role.
- 2 Delete the configuration file:
`C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config`
- 3 Reactivate the Sipelia™ plugin role.
The configuration file will be regenerated with the default values.

Configuring the device registration margin for SIP intercoms

SIP intercoms send regular *keepalive* messages to the Sipelia™ Server to indicate that they are still running and connected. The Sipelia™ Server knows how often to expect a *keepalive* message based on the *registration timeout* which is sent from each SIP intercom. You can configure a *device registration margin* as a safeguard for SIP intercoms that might exceed their *registration timeout* period.

Before you begin

- Create a backup of the following file:
`C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config`
- Investigate the *registration timeout* for the SIP intercoms in the system. Depending on the devices you have connected, this setting might be configurable or hardcoded.

What you should know

- SIP intercoms can sometimes send their *keepalive* message shortly after their *registration timeout* period has elapsed. When this happens, Security Center reports that the device is fluctuating between online and offline states. This issue can be solved by increasing the *device registration margin* which adds additional time to the device's *registration timeout* period.
- The default value of the *device registration margin* is 60 seconds. The minimum accepted value is 0 seconds.

To configure the SIP intercom's *device registration margin*:

- 1 Deactivate the Sipelia™ plugin role (see *Security Center Administrator Guide*).
- 2 Open the following configuration file:
`C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config`
- 3 To adjust the *device registration margin*, locate the DeviceRegistrationMargin element and modify the value (in seconds).
- 4 Save the file and reactivate the Sipelia™ plugin role.

Configuring the SIP trunk state timeout period

The Sipelia™ Server monitors the SIP Trunks to ensure that they are still running and connected. You can modify how often the Sipelia™ Server monitors the SIP Trunk through a configuration file on the Sipelia™ Server.

Before you begin

- Create a backup of the following file:
C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config

What you should know

- Unlike SIP intercoms, SIP Trunks do not send a keepalive message to the Sipelia™ Server. The Sipelia™ Server checks the status of SIP Trunks using the configurable *trunk state timeout period*.
- The default value of the *trunk state timeout* is 60 seconds. The minimum accepted value is 40 seconds.

To modify the SIP Trunk state timeout period:

- 1 Deactivate the Sipelia™ plugin role (see *Security Center Administrator Guide*).
- 2 Open the following configuration file:
C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config
- 3 Locate the TrunkStateTimeout element and modify the value (in seconds).
- 4 Save the file and reactivate the Sipelia™ plugin role.

SIP trunks and dial plans

This section includes the following topics:

- ["Adding SIP trunks"](#) on page 62
- ["Associating Security Center custom events with SIP trunk states"](#) on page 63
- ["Dial plans"](#) on page 64
- ["Dial plan rules"](#) on page 65
- ["Regular expressions in Sipelia"](#) on page 67
- ["Defining dial plan rules"](#) on page 69
- ["Importing dial plans"](#) on page 70
- ["Dial plan scenario 1: Forwarding to a SIP trunk all calls starting with a prefix"](#) on page 71
- ["Dial plan scenario 2: Reserving a range of SIP extensions for local calls"](#) on page 73
- ["Dial plan scenario 3: Reserving a range of SIP extensions for calls to a SIP trunk"](#) on page 76
- ["Dial plan scenario 4: Replacing source SIP extensions"](#) on page 79
- ["Dial plan scenario 5: Removing prefix on source SIP extensions from a SIP trunk"](#) on page 81
- ["Dial plan scenario 6: Forwarding calls to another SIP extension on schedule"](#) on page 83

Adding SIP trunks

To connect to SIP servers other than Sipelia Server, you can add a *SIP trunk* in Config Tool, and then define applicable *dial plan* rules to make and receive calls between the SIP servers.

Before you begin

Configure the time interval Sipelia™ uses to check SIP trunk status.

What you should know

SIP trunks work together with dial plans. For example, to connect Sipelia Server to another SIP server (*SIP Server A*) through a SIP trunk, you must [define dial plan rules](#) that instruct Sipelia Server about which calls to reroute through the trunk and on towards the new SIP extension destinations that are registered to *SIP Server A*. Furthermore, if you want proper [two-way communication](#) between Sipelia Server and *SIP Server A*, both SIP servers need to be configured accordingly.


To add a SIP trunk:

- 1 Log on to Security Center using Config Tool, and then open the *Plugins* task.
- 2 Select the **Sipelia™** Plugin role, and then click **SIP trunks**.
- 3 Click **Add SIP trunk** (+).
- 4 In the **Name** field, enter a descriptive name for your SIP trunk. The name of the SIP trunk must be unique, because it will be used in the dial plan rules involving this SIP trunk.
Example: For the purposes of this example, let's name the SIP trunk *TrunkSIPServerA* for *SIP Server A*.
- 5 Enter the following:
 - **IP address:** The IP address of the SIP server that you want to connect Sipelia Server to.
 - **SIP port:** The port used by the SIP trunk to communicate with the Sipelia Server. Because SIP trunks are SIP servers, the default value is **5060**.

Example: Let's assume that the IP address of *TrunkSIPServerA* is the following: **10.150.4.100**. And, as stated above, the default port is **5060**.

- 6 Click **Add**, and then click **Apply**.

The SIP trunk *TrunkSIPServerA* has been added. The LED in the first column indicates the state of the trunk: green for online and red for offline.

	Name	Address	SIP port
	TrunkSIPServerA	10.150.4.100	5060

IMPORTANT: The SIP extension configured for an intercom entity in Security Center is the unique identifier of this entity. For intercoms connected to an Intercom Exchange Server connected with a trunk to Sipelia, this SIP extension must be the extension used to call the intercom. This extension must also be the identifier used by the intercom to call Sipelia clients. The [Dial Plan rules](#) must be properly configured for these extensions to match.

After you finish

To call extensions registered on *TrunkSIPServerA*, [define the applicable dial plan rules](#).

Associating Security Center custom events with SIP trunk states

You can associate custom events to SIP trunk states to monitor when the connection with the trunk is established, for example, or goes offline.

Before you begin

- Create the Security Center custom events that you want to associate with a trunk state. See the *Security Center Administrator Guide, Creating custom events* for details.
- [Configure the time interval Sipelia™ uses to check SIP trunk status.](#)
- [Add your SIP trunks.](#)

What you should know

Any type of custom events from Security Center can be associated to a SIP trunk state. The trunk states show when it is online or offline.

To associate a Security Center custom event with the state of a SIP trunk:

- 1 Open Config Tool and select the **Plugins** task.
- 2 Select the **SIP trunk** tab of the Sipelia™ plugin.
- 3 Click on the trunk that you want to monitor.
The *Trunk state event* section appears on the page.
- 4 click **Add an item** (+) under the *Trunk state events* control.
- 5 In the *Assign custom event to trunk state* window, select the state you want from the **Trunk state** drop-down list:
 - **Online:** The connection to the trunk is available when the periodic check is performed.
 - **Offline:** There is no connection with the trunk when the periodic check is performed.
- 6 Select the required custom event from the *Custom event* list and click **Add**.
- 7 Click **Apply** to confirm your selection.
The associated event now appears in the Trunk state events list.

The custom event you have selected is now linked to the SIP trunk state of your choice. You can now associate an action to this event, monitor it or include this event in a report. You can also add more events, delete them or modify them by using the buttons under the events list.

Dial plans

A dial plan is a collection of rules that defines how calls are routed locally or between two SIP trunks. Dial plans ensure that calls are routed and rerouted correctly, and they also allow administrators to block calls to certain geographic locations or ensure the privacy of the callers.

A dial plan defines one or multiple rules to specify the following:

- How calls can reach SIP extensions that reside on other SIP servers.
- How calls coming from other SIP servers can reach SIP extensions that reside on Sipelia Server.
- How calls can be forwarded even when they remain local to Sipelia Server.
- How Sipelia Server can modify dialing information such as source or destination SIP extensions during call routing.

For example, if a SIP extension registered to Sipelia Server needs to call an extension that resides on *SIP Server A*, you must first configure a SIP trunk in Sipelia Server to connect to *SIP Server A*. Then you must define a dial plan to route the call from Sipelia Server to *SIP Server A*. In Sipelia™, dial plans can also be used to route local calls, that is, calls that must remain in Sipelia Server.

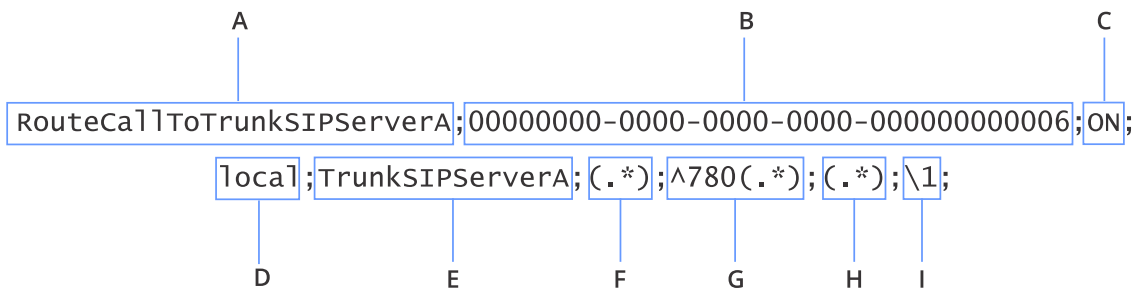
NOTE: Dial plans also need to be configured on *SIP Server A* to route calls from and to Sipelia Server. Refer to the documentation provided by the manufacturer of *SIP Server A* for information on how to configure dial plans.

Dial plan rules

Dial plan rules are stored in comma-separated values (CSV) text files, and these files can contain multiple rules. Each rule appears on a separate line and each comma-separated value (or value field) of a rule is separated by a semicolon (;).

Although CSV files support different types of separators (or delimiters), dial plan rules in Sipelia™ only support the semicolon (;) separator. You can define dial plan rules for a number of reasons. Most commonly, dial plan rules are used to call SIP extensions that are registered to SIP servers other than Sipelia Server, and to redirect local calls from extensions residing within Sipelia Server.

Each dial plan rule must define the values as shown in the following example.



- **Name (A):** The name of the dial plan rule. If the name is not provided, a default value is used upon import (*DialplanRule1*). Enter a name that will help you remember the purpose of the rule.
- **Schedule (B):** The schedule that defines when this rule must be in effect. The long string of digits for this value represent a GUID (Globally Unique Identifier). If this GUID is not provided, or it is incorrect, the default value of *Always* is used upon import.

TIP: The schedule can be changed graphically from the *Dial plans* page in Config Tool once the dial plan rule has been imported, so you can leave it empty here and let the system assign the default schedule.

- **Status (C):** The status of the rule (On = Active; Off = Inactive). This value is not case sensitive. If this value is not provided, the default value *Off* is used upon import.
- **Direction from (D):** The SIP server from where the call is originating (the source server). Possible values are *local* or the name of a SIP trunk. Sipelia Server is always the *local* SIP server. If a SIP trunk name is entered here and does not exist in the Sipelia Server configuration, a warning will be displayed and this value will revert to *local* during import.
- **Direction to (E):** The SIP server that receives the call (the destination server). Possible values are *local* or the name of a SIP trunk. The name of the SIP trunk must be unique, and must match the name that was entered in the *SIP trunks* tab when adding the SIP trunk. Sipelia Server is always the *local* SIP server. If a SIP trunk name is entered here and does not exist in the Sipelia Server configuration, a warning will be displayed and this value will revert to *local* during import.

TIP: After adding the SIP trunk in Config Tool, you can copy its name by right-clicking on the name. It is recommended to copy the name, and then paste it within your dial plan rule to avoid misspelling it.

- **Source (F):** The [regular expression](#) that identifies the extension of the caller (the source caller). The dial plan rule is only applied if there is a match between the regular expression and the caller's extension. This field is mandatory.
- **Destination (G):** The regular expression that identifies the extension of the recipient (the destination recipient). The dial plan rule is only applied if there is a match between the regular expression and the recipient's extension. This field is mandatory.
- **New source (H):** The value that changes the caller's extension (if the rule is applied). For example, if the caller at extension 1001 calls the recipient at extension 2001, and the *New source* value is 4001, the

recipient at extension 2001 sees that the incoming call is coming from extension 4001, not 1001. Possible values can also include regular expressions.

- **New destination (D):** The SIP extension that is receiving the call (if the rule is applied). Possible values can also include regular expressions.

Order of priority for dial plan rules

Rules defined in a dial plan are listed in order of priority. A rule located in a previous row is considered to be a higher priority rule. If a call matches two or more rules, the first rule listed in the dial plan will always apply. The order of priority can be changed after they were imported in Config Tool using the arrows located on the right side of the list.

Sample scenarios

For more information on how to use regular expressions in dial plan rules, you can refer to the following sample scenarios for some of the more common uses for dial plans:

- [Forwarding to a SIP trunk all calls starting with a prefix.](#)
- [Reserving a range of SIP extensions for local calls.](#)
- [Reserving a range of SIP extensions for calls to a SIP trunk.](#)
- [Replacing source SIP extensions.](#)
- [Removing the prefix on source SIP extensions from a SIP trunk.](#)
- [Forwarding calls to another SIP extension on schedule.](#)

In the Sipelia™ installation folder (typically *C:\Program Files (x86)\Genetec Sipelia*), the *Samples* folder contains a ZIP file from which you can extract the sample dial plans for common scenarios.

Regular expressions in Sipelia

A regular expression is a sequence of symbols used by a regular expression engine to identify all the strings of characters that match a specific search pattern without having to list all the possible discrete values that must be returned. The Microsoft's .NET Framework Regular Expression engine is the engine used in Sipelia™.

In Sipelia™, regular expressions are used in dial plan rules to do the following:

- Look for specific SIP extensions from which calls are made.
- Look for destination SIP extensions to which calls are made.
- Look for specific prefixes added to SIP extensions.
- Change SIP extensions from which calls are received.
- Change SIP extensions to which calls are sent.

Regular expression elements

Regular expressions used in dial plan rules typically include the following elements:

- **(.*)**: Match any value.
 - Use this element in the **Source (F)** or **Destination (G)** fields to request Sipelia Server to look for any source or destination extension when calls are made.
 - Use this element in the **New source (H)** or **New destination (I)** fields to ensure that the source or destination extension will remain unchanged when routed by Sipelia Server.
- **\n**: Match the value of a capturing group from a previous related field. A capturing group is one or more regular expression elements that are typically specified between parentheses and match a specific pattern.
 - Use this element in the **New source (H)** field to specify the capturing group from the *Source* field to be used as the new source value. **n** represents the ranking of the capturing group (\1; \2; \5, etc.) of the regular expression. For example, if *Source* contains **550[1-5](.*)**, enter \2 to use **(.*)** as the *New source* value, which in this case will remove the prefix **550** and the following digit.
 - Use this element in the **New destination (I)** field to specify the capturing group from the *Destination* field to be used as the new destination value.
- **n**: Match a specific value. In Sipelia, this value generally represents a specific SIP extension.
 - Use this element in the **New source (H)** field to specify a different extension number from which the calls are made. This is useful if you want calls to come from an extension which differs from the original source extension.
 - Use this element in the **New destination (I)** field to specify the extension number that will receive the calls. This is useful if you want to forwards calls to an extension which differs from the original destination extension.
- **[first - last]**: Match any single character in the range from **first** to **last**.
- **{n}**: Match the previous element exactly **n** times.
- **^**: Match value at the beginning of the string.
- **\b**: Use at the beginning and at the end of a series of regular expression elements to match on whole word only (not only a part of it).

Example

For example, the regular expression `\b6[0-9]{2}\b` could be used to look for SIP extensions 600 to 699.

Regular expression construct	Description
<code>\b</code>	SIP extension boundary. Used together with the same <code>\b</code> element at the end of the expression, this requires the whole SIP extension to be matched. Starting or ending characters will not be omitted.
<code>6</code>	Look for a SIP extension that begins with 6 .
<code>[0-9]</code>	Look for the digits 0 through 9 .
<code>{2}</code>	Look for 2 occurrences of the above digits following the 6 .
<code>\b</code>	Match a SIP extension boundary.

For more information on regular expressions, see [Microsoft's website](#).

Defining dial plan rules

To call SIP extensions registered to SIP servers other than Sipelia Server, or simply redirect calls from within Sipelia Server, you must define dial plan rules, and then import the rules into Config Tool.

Before you begin

- If you want to call SIP extensions that are registered to other SIP servers, [add a SIP trunk](#) for that SIP server.
- Familiarize yourself with [dial plans](#) and [dial plan rules](#) used in Sipelia™.

What you should know

Rules defined in a dial plan are listed in order of priority. A rule located in a previous row is considered to be a higher priority rule. If a call matches two or more rules, the first rule listed in the dial plan will always apply. The order of priority can be changed after they were imported in Config Tool using the arrows located on the right side of the list.

To define a dial plan rule:

- 1 Create a new text file for your dial plan with the `.txt` or `.csv` extension, or open an existing one.
- 2 Write an applicable dial plan rule. Depending on what your dial plan rule is for, you can base your rule on a [sample scenario](#) or create a rule of your own.
- 3 Enter a value for each field required by the rule.

IMPORTANT: A dial plan rule must contain the correct number of comma-separated values for it to be imported successfully. Each comma-separated value of a rule must be separated by a semicolon (;).

- 4 Repeat the same steps for additional rules that you require in your plan.
- 5 Save and close the dial plan file.

After you finish

Import your [dial plan rule](#) in Config Tool.


Importing dial plans

Once dial plan rules have been defined and a SIP trunk has been added, you must import the dial plan files into Config Tool so that the rules can be applied accordingly.

Before you begin


- [Add a SIP trunk.](#)
- [Define applicable dial plan rules.](#)

What you should know

If you delete  a dial plan rule that you have imported, the rule is no longer available to the dial plan system of Sipelia Server. If you want the deleted rule to be available again, you must reimport the dial plan file which contains the rule. If you want the dial plan system to no longer apply a rule, simply make the rule inactive, and keep it as part of your imported rules in case you ever want to reapply the rule again.

When updating a dial plan rule that has already been imported once, you do not need to delete the existing rule from the *Dial plans* page. In the dial plan file, simply make the necessary changes to the rule, make sure not to change the name of the rule, and then reimport the rule. Upon import, dial plan rules with new names get added to the list of rules; those whose names are already part of the list, are simply updated.

To import a dial plan:

- 1 Log on to Security Center using Config Tool, and then open the *Plugins* task.
- 2 Select the **Sipelia™** Plugin role, and then click **Dial plans**.
- 3 Click **Import dial plan rules from file** .
- 4 Select the dial plan file, and then click **OK**.

The dial plan is imported and the rules contained within your file appear on separate lines on the *Dial plans* page.

IMPORTANT: If a dial plan rule does not have the correct number of comma-separated values, the rule is not imported and an error is generated.

- 5 If your dial plan file contains issues, click the **Show errors and warnings** button to open the *Parser result* window.

This window classifies the issues by type (error or warning), and provides information on each issue. Warnings do not need to be corrected, but errors do. Simply modify the dial plan file accordingly, and then reimport the file.

- 6 For each dial plan rule that you import, you can edit the following:
 - **Schedule:** The Security Center schedule that defines when this rule must be in effect. The rule is applied only if the schedule condition is met.
 - **Status:** The status of the rule. Only *Active* rules are applied.
- 7 (Optional) To change the order in which the dial plan rules are applied, use the arrow buttons to move the rules up or down.
- 8 Click **Apply**.

Dial plan scenario 1: Forwarding to a SIP trunk all calls starting with a prefix

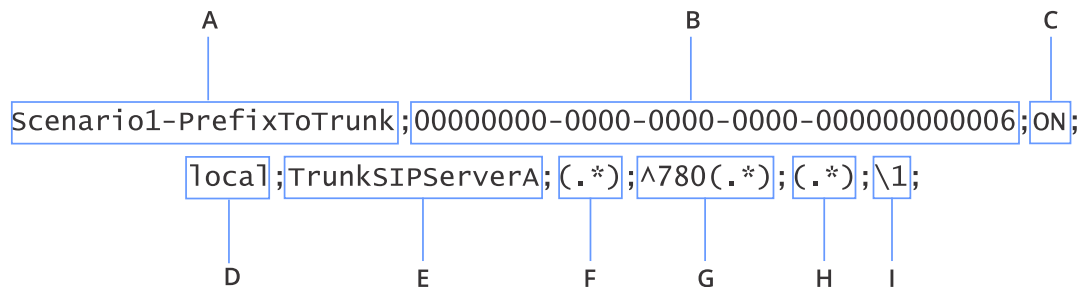
In this scenario, a dial plan rule is used to route to a SIP trunk any call that begins with a specific prefix.

Scenario

- **What do you want to do?** Your SIP extension is registered to Sipelia Server and you need to connect to *SIP Server A* because you want to call SIP extensions (SIP client, SIP intercom, etc.) that are registered to that SIP trunk. Doing so allows you to establish a one-way communication with *SIP Server A*.
- **What you need to do before defining the rule?** Add a SIP trunk in Config Tool for *SIP Server A* and name it *TrunkSIPServerA*. This trunk name must be unique, so that the dial plan rule that you will create will not conflict with other rules, and your rule will be applied correctly.
- **How can you do it?** To route calls to *TrunkSIPServerA*, you can use a dialing prefix; for example, the prefix **780**. This means that SIP extensions on Sipelia Server must dial this prefix if they want to call SIP extensions on *TrunkSIPServerA*. The prefix approach mimics that of dialing 9 to get an outside line in a typical PBX system. The prefix can be any number that you want, as long as it is defined in your dial plan rule.

Example of the dial plan rule

The following is an example of a [dial plan rule](#) that accomplishes the above mentioned scenario.



The value labels identified below correspond to the column labels which appear on the *Dial plans* page of the **Sipelia** Plugin role.

Value letter	Value label	Description
A	Name	The name of the rule indicates that calls made from Sipelia Server and starting with a prefix will be routed to the SIP trunk.
B	Schedule	The schedule is set to <i>Always</i> , meaning that the rule will always be verified.
C	Status	The status is set <i>On</i> , meaning that the rule is currently active.
D	Direction from	The field is set to <i>local</i> to look for calls that will be originating from Sipelia Server.
E	Direction to	The field is set to <i>TrunkSIPServerA</i> because calls will be routed to the SIP trunk.

Value letter	Value label	Description
F	Source	The regular expression is set to (.*) , meaning that the call can be made from <i>any</i> SIP extension registered to Sipelia Server. If you choose to enter a specific SIP extension, make sure that the regular expression corresponds to the caller's extension.
G	Destination	<p>The prefix ^780 is used. This means that SIP extensions on Sipelia Server must first dial 780 to be able to communicate with <i>TrunkSIPServerA</i>. Furthermore, the prefix is followed by the regular expression (.*) This regular expression creates a regular expression capturing group for all digits that follow the prefix.</p> <p>Example: If you want to call extension 1001 on <i>TrunkSIPServerA</i>, you must dial 7801001. The regular expression (.*) creates a group index of extensions that begin with <i>1</i>. As a result, the extension 1001 is included in this index. If you call 7801002, the extension 1002 will also be included in this index.</p>
H	New source	<p>The regular expression (.*) is used. This means that the caller's extension on Sipelia Server remains unchanged.</p> <p>Example: If the source extension registered on Sipelia Server is 6001, the dial plan rule will not cause it to change. With this rule, the same applies to all other registered extensions on Sipelia Server. However, if you enter a <i>New source</i> value of 7001, and you make a call from your extension (6001), the recipient sees that the incoming call is coming from extension 7001, not 6001.</p>
I	New destination	Because the <i>New destination</i> value is linked to the <i>Destination</i> field, the \1 indicates that the rule must use the value of the first regular expression group of <i>Destination</i> . In this scenario, the <i>Destination</i> value is 780(.*) , so using \1 will correspond to (.*) which is actually the destination SIP extension without the prefix.

Result

Once this dial plan rule is imported into Config Tool, if any SIP extension registered to Sipelia Server dials **7801001**, the extension **1001** on *SIP Server A* will ring.

Dial plan scenario 2: Reserving a range of SIP extensions for local calls

In this scenario, dial plan rules are used to define a range of SIP extensions for calls that remain local to Sipelia Server, while calls made to any other SIP extensions are automatically routed to a SIP trunk.

Scenario

- **What do you want to do?** You want the SIP extensions 4000 to 4500 reserved for calls that must remain local to Sipelia Server, while calls made to other SIP extensions are routed to *SIP Server A*.
- **What you need to do before defining the rule?** Add a SIP trunk in Config Tool for *SIP Server A* and name it *TrunkSIPServerA*. This trunk name must be unique, so that the dial plan rule that you will create will not conflict with other rules, and your rule will be applied correctly.
- **How can you do it?** You need to define two separate rules listed in the right order in your dial plan.
 - The first rule will keep the calls local when the destination SIP extensions are between 4000 and 4500.
 - The second rule will take calls to any other SIP extensions and route them to *TrunkSIPServerA*.

IMPORTANT: The rules need to be in the right order in the dial plan to work as described in this scenario.

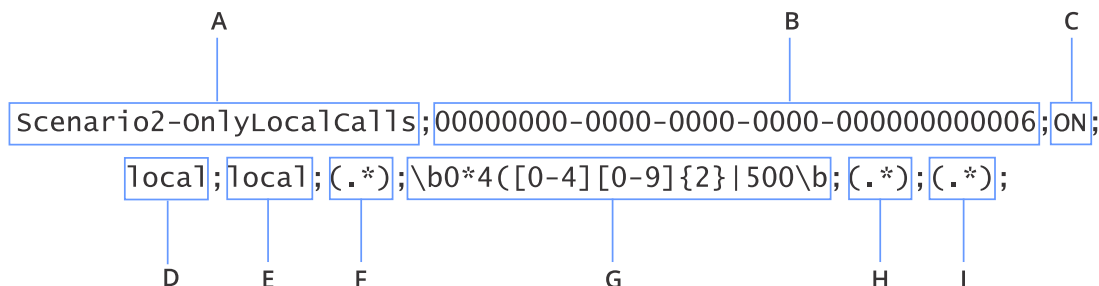
Example of the dial plan

The following is an example of a [dial plan](#) that accomplishes the above mentioned scenario.

- 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;(.*);(.*);(.*);

Rule 1: Only local calls

The first rule listed in the dial plan and shown below tells Sipelia Server to look for source SIP extensions between 4000 and 4500, and keep them local.



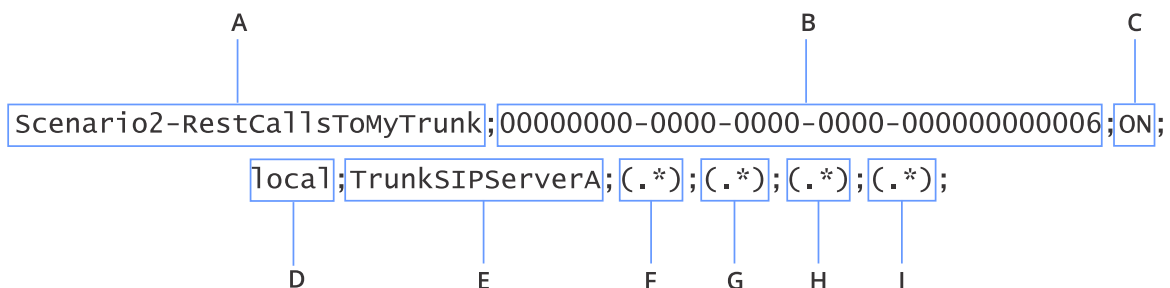
The value labels identified below correspond to the column labels which appear on the *Dial plans* page of the **Sipelia** Plugin role.

Value letter	Value label	Description
A	Name	The name indicates that this rule will route local calls.

Value letter	Value label	Description
B	Schedule	The schedule is set to <i>Always</i> , meaning that the rule will always be verified.
C	Status	The status is set <i>On</i> , meaning that the rule is currently active.
D	Direction from	The field is set to <i>local</i> to look for calls that will be originating from Sipelia Server.
E	Direction to	The field is set to <i>local</i> because the calls that match the rule will remain local to Sipelia Server.
F	Source	The regular expression is set to <i>(.*)</i> , meaning that the call can be made from <i>any</i> SIP extension registered to Sipelia Server.
G	Destination	The regular expression is set to <code>\b0*4([0-4][0-9]{2} 500)\b</code> to look for destination SIP extensions between 4000 and 4500, as described below: <ul style="list-style-type: none"> • \b: SIP extension boundary. Used together with the same \b element at the end of the expression, this requires the whole SIP extension to be matched. Starting or ending characters will not be omitted. • 0*: Look for any number of zeros before the next character, which is 4. • 4: Look for a SIP extension that begins with 4. • ([0-4]: Look for a single occurrence of digits 0 through 4 after the first 4. • [0-9]{2}: Look for 2 following occurrences of digits 0 through 9, which now covers extension 4000 to 4499. • 500): Look specifically for 500 to add 4500 in the search pattern. • \b: Match a SIP extension boundary.
H	New source	The regular expression <i>(.*)</i> is used. This means that your extension (the source caller) on Sipelia Server remains unchanged.
I	New destination	The regular expression <i>(.*)</i> is used. This means that the called extension remains unchanged.

Rule 2: Other calls routed to the SIP trunk

The second rule listed in the dial plan and shown below tells Sipelia Server to route to *TrunkSIPServerA* any call that is not matching the first rule.



Value letter	Value label	Description
A	Name	The name indicates that this rule will route any other call to <i>TrunkSIPServerA</i> .
B	Schedule	The schedule is set to <i>Always</i> , meaning that the rule will always be verified.
C	Status	The status is set <i>On</i> , meaning that the rule is currently active.
D	Direction from	The field is set to <i>local</i> to look for calls that will be originating from Sipelia Server.
E	Direction to	The field is set to <i>TrunkSIPServerA</i> to route the calls to that SIP trunk.
F	Source	The regular expression is set to <i>(.*)</i> , meaning that the call can be made from <i>any</i> SIP extension registered to Sipelia Server.
G	Destination	The regular expression is set to <i>(.*)</i> , meaning that the call can be made to reach <i>any</i> SIP extension.
H	New source	The regular expression <i>(.*)</i> is used. This means that your extension (the source caller) on Sipelia Server remains unchanged.
I	New destination	The regular expression <i>(.*)</i> is used. This means that the called extension remains unchanged.

Result

Once the dial plan is imported into Config Tool, only the highest priority rule will apply. This dial plan results in the following:

- 1 If any SIP extension dials a number between 4000 and 4500, the call will remain local to Sipelia Server.
- 2 If any SIP extension dials any other number, the call will automatically be routed to *SIP Server A*.

Dial plan scenario 3: Reserving a range of SIP extensions for calls to a SIP trunk

In this scenario, dial plan rules are used to define a range of SIP extensions for calls that are automatically routed to a SIP trunk.

Scenario

- **What do you want to do?** You want to reserve SIP extensions 4000 to 4500 for calls that must automatically be routed to *SIP Server A*.
- **What you need to do before defining the rule?** Add a SIP trunk in Config Tool for *SIP Server A* and name it *TrunkSIPServerA*. This trunk name must be unique, so that the dial plan rule that you will create will not conflict with other rules, and your rule will be applied correctly.
- **How can you do it?** You need to define two separate rules listed in the right order in your dial plan.
 - The first rule will take any call made to a SIP extension that is between 4000 and 4500 and automatically route it to *TrunkSIPServerA*.
 - The second rule will take calls to any other SIP extension and will keep it local to Sipelia Server.

IMPORTANT: The rules need to be in the right order in the dial plan to work as described in this scenario.

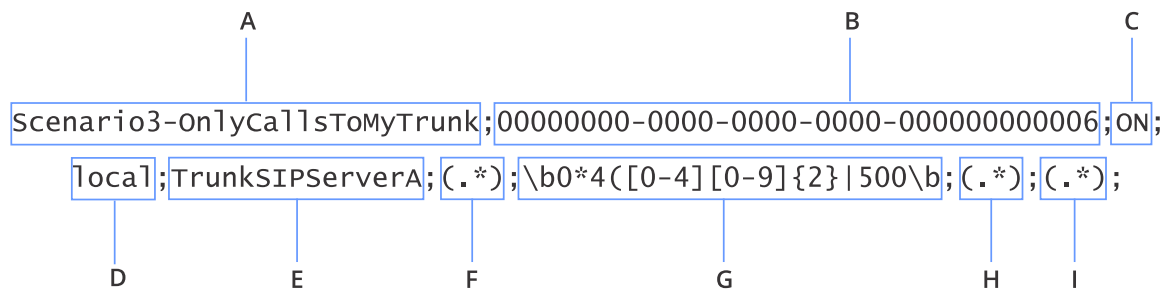
Example of the dial plan

The following is an example of a [dial plan](#) that accomplishes the above mentioned scenario.

- 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;(*);(*);(*);(*);

Rule 1: Calls to the SIP trunk only

The first rule listed in the dial plan and shown below tells Sipelia Server to look for destination SIP extensions between 4000 and 4500, and forward them to the SIP trunk.



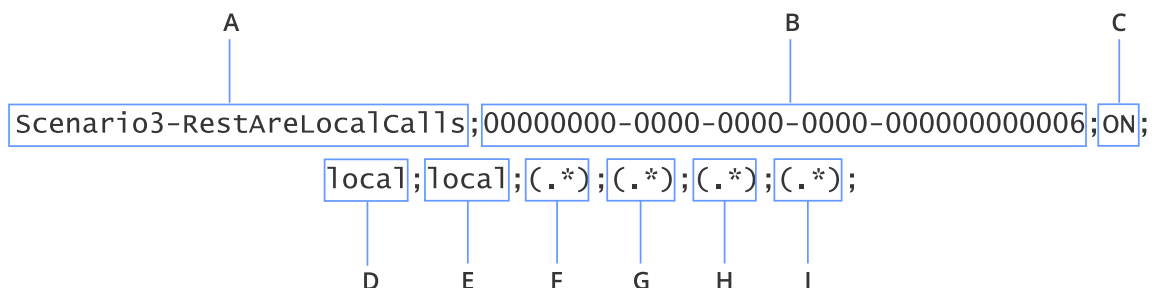
The value labels identified below correspond to the column labels which appear on the *Dial plans* page of the **Sipelia** Plugin role.

Value letter	Value label	Description
A	Name	The name indicates that this rule will route to the SIP trunk calls made with specific SIP extensions.

Value letter	Value label	Description
B	Schedule	The schedule is set to <i>Always</i> , meaning that the rule will always be verified.
C	Status	The status is set <i>On</i> , meaning that the rule is currently active.
D	Direction from	The field is set to <i>local</i> to look for calls that will be originating from Sipelia Server.
E	Direction to	The field is set to <i>TrunkSIPServerA</i> to route the calls to that SIP trunk.
F	Source	The regular expression is set to <i>(.*)</i> , meaning that the call can be made from <i>any</i> SIP extension registered to Sipelia Server.
G	Destination	<p>The regular expression is set to <code>\b0*4([0-4][0-9]{2} 500)\b</code>, meaning the Sipelia Server must to look for destination SIP extensions between 4000 and 4500, as described below:</p> <ul style="list-style-type: none"> • \b: SIP extension boundary. Used together with the same \b element at the end of the expression, this requires the whole SIP extension to be matched. Starting or ending characters will not be omitted. • 0*: Look for any number of zeros before the next character, which is 4. • 4: Look for a SIP extension that begins with 4. • ([0-4]: Look for a single occurrence of digits 0 through 4 after the first 4. • [0-9]{2}: Look for 2 following occurrences of digits 0 through 9, which now covers extension 4000 to 4499. • 500): Look specifically for 500 to add 4500 in the search pattern. • \b: Match a SIP extension boundary.
H	New source	The regular expression <i>(.*)</i> is used. This means that your extension (the source caller) on Sipelia Server remains unchanged.
I	New destination	The regular expression <i>(.*)</i> is used. This means that the called extension remains unchanged.

Rule 2: Other calls routed locally

The second rule listed in the dial plan and shown below tells Sipelia Server to route to *TrunkSIPServerA* any other call that does not match the first rule.



Value letter	Value label	Description
A	Name	The name indicates that this rule will keep local any other call.
B	Schedule	The schedule is set to <i>Always</i> , meaning that the rule will always be verified.
C	Status	The status is set <i>On</i> , meaning that the rule is currently active.
D	Direction from	The field is set to <i>local</i> to look for calls that will be originating from Sipelia Server.
E	Direction to	The field is set to <i>local</i> to keep the calls local to Sipelia Server.
F	Source	The regular expression is set to <i>(.*)</i> , meaning that the call can be made from <i>any</i> SIP extension registered to Sipelia Server.
G	Destination	The regular expression is set to <i>(.*)</i> , meaning that the call can be made to reach <i>any</i> SIP extension.
H	New source	The regular expression <i>(.*)</i> is used. This means that your extension (the source caller) on Sipelia Server remains unchanged.
I	New destination	The regular expression <i>(.*)</i> is used. This means that the called extension remains unchanged.

Result

Once the dial plan is imported into Config Tool, only the highest priority rule will be apply. This dial plan results in the following:

- 1 If any SIP extension dials a number between 4000 and 4500, the call will be routed to *TrunkSIPServerA*.
- 2 If any SIP extension dials any other number, the call will remain local to Sipelia Server.

Dial plan scenario 4: Replacing source SIP extensions

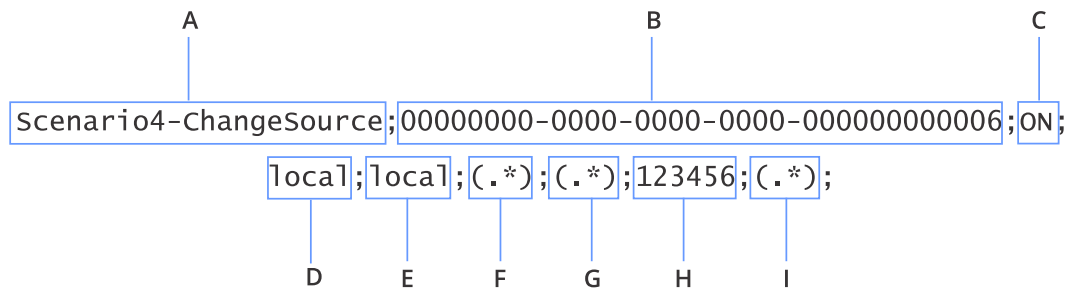
In this scenario, a dial plan rule is used to replace the source SIP extensions with a unique SIP extension that will be displayed to the recipients. This rule can be used to ensure the privacy of the callers.

Scenario

- **What do you want to do?** Display a unique source SIP extension for any call that is made.
- **What you need to do before defining the rule?** Select the SIP extension that will always be used as the source. In this scenario, 123456 is the selected SIP extension.
- **How can you do it?** You need to create a rule that takes any call from Sipelia Server and replace the source SIP extension with 123456.

Example of the dial plan rule

The following is an example of a [dial plan rule](#) that accomplishes the above mentioned scenario.



The value labels identified below correspond to the column labels which appear on the *Dial plans* page of the **Sipelia** Plugin role.

Value letter	Value label	Description
A	Name	The name of the rule indicates that it will replace the source SIP extension.
B	Schedule	The schedule is set to <i>Always</i> , meaning that the rule will always be verified.
C	Status	The status is set <i>On</i> , meaning that the rule is currently active.
D	Direction from	The field is set to <i>local</i> to look for calls that will be originating from Sipelia Server.
E	Direction to	The field is set to <i>local</i> to keep the calls local to Sipelia Server.
F	Source	The regular expression is set to <i>(.*)</i> , meaning that the call can be made from <i>any</i> SIP extension registered to Sipelia Server.
G	Destination	The regular expression is set to <i>(.*)</i> , meaning that the call can be made to reach <i>any</i> SIP extension.

Value letter	Value label	Description
H	New source	The regular expression is set to 123456 to change the SIP extension with this constant value.
I	New destination	The regular expression (.*) is used. This means that the called extension remains unchanged.

Result

Once this dial plan rule is imported into Config Tool, if any SIP extension registered to Sipelia Server dials any other SIP extension, the source extension 123456 will be displayed to the recipients.

Dial plan scenario 5: Removing prefix on source SIP extensions from a SIP trunk

In this scenario, a dial plan rule is used to remove the prefix used in source SIP extensions for calls received from a SIP trunk, so that it is not displayed to the recipients. This scenario can be combined with scenario 1 to have the source extensions displayed with no prefix when received by the recipients registered to *SIP Server A*.

Scenario

- **What do you want to do?** Remove the prefix included in source SIP extensions when calls are received from a SIP trunk.
- **What you need to do before defining the rule?** Add a SIP trunk in Config Tool for *SIP Server A* and name it *TrunkSIPServerA*. This trunk name must be unique, so that the dial plan rule that you will create will not conflict with other rules, and your rule will be applied correctly. You also need to know the prefix used by the SIP trunk for its extensions.
- **How can you do it?** Create a rule that takes any call from a SIP trunk and remove the prefix used in the source SIP extension.

Example of the dial plan rule

The following is an example of a [dial plan rule](#) that accomplishes the above mentioned scenario.

```

Scenario5-RemoveSourceHeaderFromTrunk;00000000-0000-0000-0000-0000000000006;
ON;TrunkSIPServerA;local;^551(. *);(. *);\1;(. *);

```

The diagram shows the following labels pointing to parts of the rule:

- A**: Points to the rule name 'Scenario5-RemoveSourceHeaderFromTrunk'.
- B**: Points to the schedule '00000000-0000-0000-0000-0000000000006'.
- C**: Points to the status 'ON'.
- D**: Points to the direction from 'TrunkSIPServerA'.
- E**: Points to the direction to 'local'.
- F**: Points to the first regex pattern '^551(. *)'.
- G**: Points to the second regex pattern '(. *)'.
- H**: Points to the replacement '\1'.
- I**: Points to the final regex pattern '(. *)'.

The value labels identified below correspond to the column labels which appear on the *Dial plans* page of the **Sipelia** Plugin role.

Value letter	Value label	Description
A	Name	The name of the rule indicates that it will remove the prefix from source SIP extensions received from the SIP trunk.
B	Schedule	The schedule is set to <i>Always</i> , meaning that the rule will always be verified.
C	Status	The status is set <i>On</i> , meaning that the rule is currently active.
D	Direction from	The field is set to <i>TrunkSIPServerA</i> to look for calls that will be originating from the SIP trunk.
E	Direction to	The field is set to <i>local</i> to route the calls to Sipelia Server.

Value letter	Value label	Description
F	Source	The regular expression is set to <code>^551(.*)</code> to look for <i>any</i> source SIP extension that begins with prefix 551.
G	Destination	The regular expression is set to <code>(.*)</code> , meaning that the call can be made to reach <i>any</i> SIP extension.
H	New source	The regular expression is set to <code>\1</code> , which indicates that the rule will use the value of the first regular expression group, which was defined in the <i>Source</i> value. This means that the prefix will be discarded and the source SIP extension becomes <code>(.*)</code> .
I	New destination	The regular expression <code>(.*)</code> is used. This means that the called extension remains unchanged.

Result

Once this dial plan rule is imported into Config Tool, any source SIP extension with prefix 551 received from *TrunkSIPServerA* will be displayed without the prefix to the recipients. For example, if a call received from the SIP trunk is made from extension 5513005, the recipient registered to Sipelia Server will only see 3005.

Dial plan scenario 6: Forwarding calls to another SIP extension on schedule

In this scenario, dial plan rules are used to define a range of SIP extensions for calls that must always reach the recipients, while other SIP extensions are automatically forwarded to a new destination. This can be useful to route calls from SIP intercoms to a call center during the night for example.

Scenario

- **What do you want to do?** During off-hours for example, calls made to SIP extensions between 4000 and 4500 must be routed normally to the requested recipients, while other calls must be forwarded to extension 1001, which can be the extension of a SIP endpoint (or SIP client) in a security office for example.
- **What you need to do before defining the rule?** Define the range of SIP extensions that must always be routed and the specific SIP extension to which other calls will be forwarded. You also need to have a schedule defined in Security Center to be used in the dial plan rule.
- **How can you do it?** You need to define two separate rules listed in the right order in your dial plan:
 - The first rule looks for any call made to reach SIP extensions between 4000 to 4500, and route them normally.
 - The second rule will take calls to any other SIP extension and forward them to extension 1001.

IMPORTANT: The rules need to be in the right order in the dial plan to work as described in this scenario.

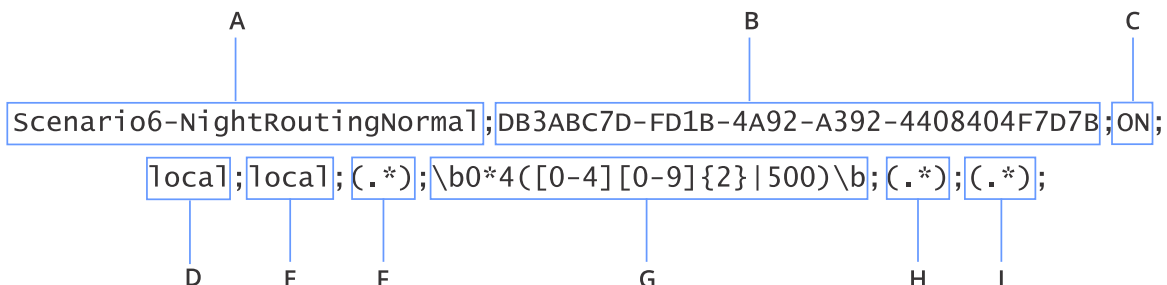
Example of the dial plan

The following is an example of a [dial plan](#) that accomplishes the above mentioned scenario.

- 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;

Rule 1: Normal night routing

The first rule listed in the dial plan shown below tells Sipelia Server to look for destination SIP extensions between 4000 and 4500, and route them normally.

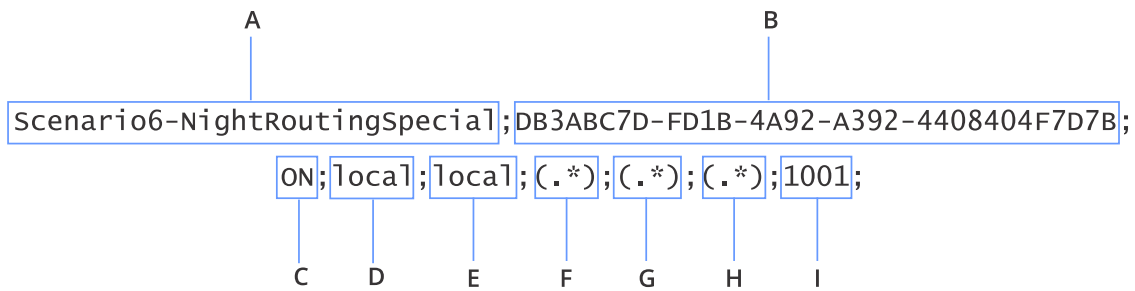


The value labels identified below correspond to the column labels which appear on the *Dial plans* page of the **Sipelia** Plugin role.

Value letter	Value label	Description
A	Name	The name of the rule indicates that the calls are routed normally.
B	Schedule	The schedule is set to <i>Off-hours</i> , meaning that the rule will be applied only during that time.
C	Status	The status is set <i>On</i> , meaning that the rule is currently active.
D	Direction from	The field is set to <i>local</i> to look for calls that will be originating from Sipelia Server.
E	Direction to	The field is set to <i>local</i> because the calls will remain local to Sipelia Server when the rule is applied.
F	Source	The regular expression is set to <i>(.*)</i> , meaning that the call can be made from <i>any</i> SIP extension.
G	Destination	<p>The regular expression is set to <code>\b0*4([0-4][0-9]{2} 500)\b</code>, meaning that Sipelia Server must look for called SIP extensions between 4000 and 4500, as described below:</p> <ul style="list-style-type: none"> • <code>\b</code>: SIP extension boundary. Used together with the same <code>\b</code> element at the end of the expression, this requires the whole SIP extension to be matched. Starting or ending characters will not be omitted. • <code>0*</code>: Look for any number of zeros before the next character, which is <code>4</code>. • <code>4</code>: Look for a SIP extension that begins with <code>4</code>. • <code>([0-4]</code>: Look for a single occurrence of digits <code>0</code> through <code>4</code> after the first <code>4</code>. • <code>[0-9]{2}</code>: Look for 2 following occurrences of digits <code>0</code> through <code>9</code>, which now covers extension 4000 to 4499. • <code> 500)</code>: Look specifically for <code>500</code> to add 4500 in the search pattern. • <code>\b</code>: Match a SIP extension boundary.
H	New source	The regular expression <i>(.*)</i> is used. This means that your extension (the source caller) on Sipelia Server remains unchanged.
I	New destination	The regular expression <i>(.*)</i> is used. This means that the called extension remains unchanged.

Rule 2: Special night routing

The second rule listed in the dial plan and shown below tells Sipelia Server to look for any call that does not match the first rule, and forward it to extension 1001.



The value labels identified below correspond to the column labels which appear on the *Dial plans* page of the **Sipelia** Plugin role.

Value letter	Value label	Description
A	Name	The name of the rule indicates that the calls are following a special route.
B	Schedule	The schedule is set to <i>Off-hours</i> , meaning that the rule will be applied only during time.
C	Status	The status is set <i>On</i> , meaning that the rule is currently active.
D	Direction from	The field is set to <i>local</i> to look for calls that will be originating from Sipelia Server.
E	Direction to	The field is set to <i>local</i> because the calls will remain local to Sipelia Server when the rule is applied.
F	Source	The regular expression is set to <i>(.*)</i> , meaning that the call can be made from <i>any</i> SIP extension.
G	Destination	The regular expression is set to <i>(.*)</i> , meaning that the call can be made to reach <i>any</i> SIP extension.
H	New source	The regular expression <i>(.*)</i> is used. This means that your extension (the source caller) on Sipelia Server remains unchanged.
I	New destination	The regular expression 1001 is used. This means that the call will always be forwarded to SIP extension 1001.

Result

Once the dial plan is imported into Config Tool, only the highest priority rule will apply. This dial plan results in the following:

- 1 When the schedule is satisfied, if any SIP extension dials a number between 4000 and 4500, the call will remain local to Sipelia Server and will be routed normally to the requested recipient.
- 2 When the schedule is satisfied, if any SIP extension dials any other number, the call will automatically be forwarded to SIP extension 1001.

Troubleshooting

This section includes the following topics:

- ["Unable to establish communication with the Sipelia Server"](#) on page 87
- ["Message broker connection failed to all the configured hosts"](#) on page 88
- ["Lost login credentials to RabbitMQ or modifying RabbitMQ credentials"](#) on page 90
- ["Missing communication service connection for Sipelia Security Desk"](#) on page 91
- ["Message broker connection failed because of invalid credentials"](#) on page 92
- ["Cannot add SIP intercom devices"](#) on page 93
- ["Cannot see the Sipelia icon in the notification tray"](#) on page 94
- ["Security Desk cannot connect to Sipelia Server"](#) on page 95
- ["Cannot register to Sipelia Server Server from Security Desk"](#) on page 96
- ["Cannot make calls between two SIP endpoints"](#) on page 97
- ["Sipelia calls from Security Desk are delayed or are not delivered"](#) on page 98
- ["No video displayed during Sipelia calls"](#) on page 99
- ["Audio and video not being recorded during Sipelia calls"](#) on page 100
- ["No audio, or distorted audio in Sipelia calls"](#) on page 101
- ["DTMF tones not working in Sipelia"](#) on page 102
- ["Users cannot view recorded video from Sipelia calls"](#) on page 103
- ["Enabling file logging for debug traces on the Sipelia Server"](#) on page 104

Unable to establish communication with the Sipelia Server

When adding a SIP intercom in Config Tool, the error message **Unable to establish communication with the server** is displayed.

What you should know

This error typically occurs when there is a connection issue with the configuration service between Config Tool and Sipelia Server.

To troubleshoot this issue, try the following:

- 1 Log on to Security Center using Config Tool, and then open the *Plugins* task.
- 2 Select the Sipelia™ plugin role, and then click **General**.
- 3 Make sure that **Configuration service port** is set to the proper value.
- 4 Make sure that this port is not being blocked anywhere on the network.

Message broker connection failed to all the configured hosts

The Sipelia™ plugin role displays the error message **Message broker connection failed to all the configured hosts**: and the connection to Sipelia Server is not possible from Security Desk.

Before you begin

- Ensure that you are not [logging on to RabbitMQ using the "guest" account](#) as it works only with the localhost.
- Ensure that the [RabbitMQ username and password](#) you have entered are correct.
- Ensure that the Message broker server parameters are correct.
 - The server address must be reachable from the machine where Sipelia Server and Sipelia Client are installed.
 - The correct ports must be selected. By default, Sipelia™ uses the SSL connection to RabbitMQ which works on the RabbitMQ SSL port. [If this connection is disabled in Sipelia™](#), the Message broker server port must be changed to use the RabbitMQ non-SSL port. If required, you can also [change the ports used by RabbitMQ](#).

What you should know

- This error typically occurs when your Sipelia™ Message broker configuration is incorrect. Your Message broker server is not reachable from the machine hosting the Sipelia™ system, or the RabbitMQ server is offline or is not working.
- You can increase the reliability of your system by [deploying and configuring multiple RabbitMQ servers](#). If one of the servers fails, Sipelia™ automatically connects to the next server. This ensures that Sipelia™ is always operational.

IMPORTANT: It is strongly recommended that you use the RabbitMQ version that is included with the Sipelia™ installation package. Differences between RabbitMQ releases prevent the use of older versions. Sipelia™ Server installation always installs or upgrades to the correct RabbitMQ version.

To establish a connection with the Message broker, do the following:

- 1 Restart the Sipelia™ plugin role. If the problem is still present, continue with the next step.
- 2 Ensure that your Message broker configuration is correct. Verify the username, password, address, and port. If the problem is still present, continue with the next step.
- 3 Ensure that there are no network issues that prevent the Sipelia™ plugin or Sipelia™ Security Desk from reaching the RabbitMQ server that is installed with the Sipelia™ plugin. Depending on your network architecture, you might need to update your networking system to allow the required traffic to pass. RabbitMQ uses the AMPQ (TCP) protocol, the default SSL port is 5671, and the default port for non-SSL communication is 5672. If the problem is still present, continue with the next step.
- 4 On the machine where RabbitMQ server is installed, verify that the RabbitMQ service is running, then restart the RabbitMQ service.

NOTE: To access the RabbitMQ service, open the Windows Services panel (services.msc) and look for RabbitMQ.

- 5 If the RabbitMQ service fails to start, check the RabbitMQ service logs (file path: %APPDATA%\RabbitMQ\log) for an explanation of the failure.
- 6 If the problem is still present, reinstall RabbitMQ server.

To reinstall the RabbitMQ server:

- 1 Uninstall Sipelia™ from your computer.

- 2 Uninstall RabbitMQ from your computer.

NOTE: You do not need to uninstall Erlang.

- 3 Restart the computer.
- 4 Start the [Sipelia Server installation](#), which deploys RabbitMQ.

Lost login credentials to RabbitMQ or modifying RabbitMQ credentials

If you lose the RabbitMQ username and password that were created during the Sipelia Server installation, or if you would like to modify the existing username and password, you can manage the credentials in the RabbitMQ web portal.

What you should know

- During the installation of the Sipelia™ plugin, you must enter credentials for the RabbitMQ account which is created by the installer. If you lose your credential, or if you would like to modify them, you can do it in the RabbitMQ web portal using the following steps. You must then update the Message Broker settings in the Sipelia™ plugin according to your changes.
- You can [temporarily use the guest account](#) (guest/guest), but it will only work if RabbitMQ, Sipelia Server, and Sipelia Client are installed on the same machine.
- If you enter incorrect credentials in Sipelia™, an entity warning is generated with the message: *Message broker connection failed because of invalid credentials.*
- To learn more about RabbitMQ configuration, visit the [RabbitMQ](#) website.

To troubleshoot this issue, try the following:

- 1 Create new credentials or modify the existing credentials for the user in the RabbitMQ web portal.
 - a) From the workstation where RabbitMQ is installed, start the RabbitMQ web portal (<http://localhost:15672>), and log on using the *guest* account (guest/guest).
 - b) Select the **Admin** tab.

NOTE: If required, you can create a new account by clicking **Add user**.
 - c) Click the user that you added or modified during the Sipelia™ installation.
 - d) In the **Update this user** section, create a new password for the user.
 - e) Click **Update user** to save your changes.
- 2 Update the credentials used in Sipelia™.
 - a) In Config Tool, open the *Plugins* task and click the Sipelia™ plugin.
 - b) Click the **General** tab.
 - c) In the **Message broker** configuration, modify the **Username** and **Password** to match the new credentials you added in the RabbitMQ web portal.
 - d) Click **Apply** to save your changes.

Missing communication service connection for Sipelia™ Security Desk

If Sipelia Client cannot connect to RabbitMQ, it may be because you are using the RabbitMQ *guest* account or because Sipelia™ failed to connect to all the configured RabbitMQ servers.

What you should know

The *guest* account is only available within the localhost. You can use the guest account for testing purposes if Sipelia Client and Sipelia Server are both installed on the same machine as RabbitMQ server.

To troubleshoot this issue, try the following:

- 1 Ensure that the Sipelia™ plugin is not configured to use the *guest* account.
- 2 Ensure that you are using the correct logon credentials for RabbitMQ.
- 3 Ensure that Sipelia™ can connect to all the configured hosts.

Message broker connection failed because of invalid credentials

If the Sipelia™ plugin has an entity warning with the message: *Message broker connection failed because of invalid credentials*, it means that the RabbitMQ message broker username and/or password is incorrect in the Sipelia™ configuration.

What you should know

- During the installation of Sipelia Server, you must provide the RabbitMQ message broker username and password which are then created on the RabbitMQ server by the installer.
- A default RabbitMQ *guest* account is created, but it is only available within the localhost. You can use the *guest* account for testing purposes if Sipelia Client and Sipelia Server are both installed on the same machine as RabbitMQ server.

To modify the SSL port in the Message broker server settings:

- 1 [Ensure that the Sipelia™ plugin is not configured to use the *guest* account.](#)
- 2 [Ensure that you are using the correct logon credentials for RabbitMQ.](#)

Cannot add SIP intercom devices

When adding a SIP intercom in Config Tool, the error message **The number of Sipelia licenses (standard or advanced) has been exceeded.** is displayed.

What you should know

This error typically occurs when you do not have enough standard and/or advanced licenses in your system to support the number of SIP intercom devices that you want to add.

To be able to add new SIP intercom devices, do one of the following:

- Remove one or more SIP intercom devices from your system.
- [Increase the number of licenses.](#)

Cannot see the Sipelia™ icon in the notification tray

A user cannot see the Sipelia™ icon in the notification tray of Security Desk.

What you should know

This issue typically occurs when the Sipelia Client has not been installed properly.

To troubleshoot this issue, try the following:

- 1 Restart Security Desk.
- 2 If the problem is still present, restart the computer on which Security Desk is running.
- 3 If you are still unable to see the icon in the notification tray, try to uninstall and [re-install Sipelia Client](#) on the computer.

Security Desk cannot connect to Sipelia Server

If Security Desk cannot connect to the Sipelia Server, verify that the IP address and port properties are properly set.

What you should know

Connection issues typically occur when IP addresses or ports are not configured properly, or when the network is blocking packets from being exchanged between two endpoints.

To troubleshoot connection issues to the Sipelia Server, try the following:

- 1 If the computer on which Security Desk is running provides multiple network interfaces (cards), verify that the network interface used for Sipelia™ is [selected](#).
- 2 Verify that the RabbitMQ Server is installed and is running on both the client (Security Desk) and server (Sipelia Server).
- 3 Log on to Security Center using Config Tool, and then open the *Plugins* task.
- 4 Select the Sipelia™ Plugin role, and verify that the role is up and running.
- 5 Click **General**, and make sure that the address and port properties are set to the proper values.
- 6 Click **Servers**, and make sure that **SIP port** is set to the proper value.
- 7 Make sure that the ports are not being blocked anywhere on the network.
- 8 Open the *Network* task, and then select the server that is hosting the Sipelia™ Plugin role.
- 9 Click **Properties**, and make sure that the first IP address shown in **Private addresses**, that is, the IP address listed at the top, is the one that you want to be used by the server.
Sipelia Server automatically uses the first IP address shown in the list.
- 10 Log on to Security Center with Security Desk.
- 11 Click **Options > Sipelia > Advanced**, and make sure that **UDP port range** is set properly.
- 12 On the Sipelia Server, browse to folder *C:\ProgramData\Genetec Sipelia\SipServer* and open *SipServer.config*.
- 13 Make sure that *MinimumPortRange* and *MaximumPortRange* values are set properly in the file.

Cannot register to Sipelia Server Server from Security Desk

If users cannot register to Sipelia Server from Security Desk, you should verify that the VoIP properties are properly set for those users.

What you should know

Registration issues typically occur when Security Desk can connect to the Sipelia Server but SIP extensions or passwords are not configured properly.

To troubleshoot this issue, try the following:

- 1 Log on to Security Center with Config Tool.
- 2 Open the *Security* task, and then select the user entity involved in the connection issue.
- 3 In the VoIP page, make sure that the **SIP extension and Password** properties have been configured with the proper values.

Cannot make calls between two SIP endpoints

If users cannot make or receive Sipelia™ calls with Security Desk, the messages might be blocked somewhere on the network.

What you should know

When users are registered to Sipelia Server but cannot make or receive calls, this typically occurs when the network is blocking packets from being exchanged between two SIP endpoints.

To troubleshoot this issue, try the following:

- 1 Log on to Security Center with Security Desk.
- 2 Using a network protocol analyzer (Wireshark, for example), try to make a call and verify that SIP messages are exchanged between the two SIP endpoints.
- 3 If SIP packets are being exchanged, verify that SDP and RTP packets are also exchanged.
- 4 Make sure that the IP addresses and port numbers used in the SIP and SDP packets are correct.
- 5 If you can see SIP, SDP, and RTP packets exchanged on the network between the two SIP endpoints, but users are still not able to make or receive calls, try to restart the Genetec Server.

Sipelia™ calls from Security Desk are delayed or are not delivered

If calls are delayed or not delivered from Security Desk to another SIP client or endpoint, you might have to disable *NAT Traversal mode* on the Sipelia™ Server.

What you should know

This issue typically occurs when:

- Calls are made from Security Desk to another SIP client or endpoint.
- Security Desk is inside a different subnet or different network than the Sipelia™ Plugin.
- Systems with the Sipelia™ Plugin do not have access to the Internet.

To troubleshoot this issue, try the following:

- 1 Deactivate the Sipelia™ Plugin role.
In the *Plugins* task, right-click the Sipelia™ Plugin and select **Maintenance > Deactivate role**.
- 2 Open the Sipelia™ Server configuration file (*C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config*).
- 3 Change the value of the *NatTraversalMethod* property from *Default* to *None*.
- 4 Activate the Sipelia Plugin role.
In the *Plugins* task, right-click the Sipelia™ Plugin and select **Maintenance > Activate role**.

No video displayed during Sipelia™ calls

If you cannot see video during SIP video calls, you might have video codec options that are not configured properly.

To troubleshoot this issue, try the following:

- 1 Log on to Security Center with Security Desk.
 - 2 Click **Options > Sipelia > Advanced**.
 - 3 Make sure that the following is set correctly:
 - **Video codecs:** The video codecs that are supported by Security Desk for video communication. By default, the H.264 and H.263 codecs are turned on, and should suffice for most cases. As a result, it is recommended to keep the default settings, and to be aware that changing video codecs can disrupt the video that is streamed during video calls. To be able to view video during a SIP video call, the SIP clients that are involved in a call must all support at least one common video codec. For example, if *SIP client A* only supports the H.264 codec and *SIP client B* only supports H.263, no video is streamed during a call session between the two SIP clients.
 - **UDP port range:** The port range for the User Datagram Protocol (UDP). The UDP ports are used by the different SIP clients to send and receive communication data. The default range is from **20000** to **20500**. It is recommended to keep the default settings, and to change them only if Sipelia logs any port-related issues about making or receiving calls with Security Desk.
- NOTE:** The highest matching preference will be chosen. If both endpoints support H.264 and H.263, the connection will be established using H.264.
- 4 If you still have an issue, using a network protocol analyzer (Wireshark, for example), verify that SDP and RTP packets are exchanged between the two SIP endpoints.
 - 5 If you can see SDP and RTP packets exchanged on the network, but there is still no video displayed during calls, try to restart the Genetec Server.

Audio and video not being recorded during Sipelia™ calls

If you can see video during SIP video calls but you have no recording in the database, you might have recording options that are not configured properly.

To make sure that audio and video are recorded during call sessions:

- 1 Make sure that your [license supports the recording](#) of call sessions.
- 2 Log on to Security Center using Config Tool, and then open the *Plugins* task.
- 3 Select the Sipelia™ Plugin role, and then click **Recording**.
- 4 Make sure that **User recording** and **Device recording** are enabled.
- 5 If you have no recording associated with specific users, open the *Security* task, and then select the user entity involved in the issue.
- 6 In the VoIP page, make sure that the **Record audio and video** property is turned on or inherits the default value from the Sipelia™ Plugin role.
- 7 If you still have problems recording call sessions, try restarting the Genetec Server.

No audio, or distorted audio in Sipelia™ calls

If there is no audio, or if you are experiencing poor audio quality when making Sipelia™ calls, it might be possible to improve audio quality by using a different audio codec, and by verifying the RTP packet size defined for the SIP intercoms.

Before you begin

- [Ensure that the USB headset you are using is configured and is working properly.](#)
- Create a backup of the following file:

`C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config`

What you should know

- Enabling and disabling video and audio codecs is done through an XML configuration file. In this file, you can find the following XML elements: **AudioCodecs** and **VideoCodecs**. The **Codec** element within them contains the **Enabled** attribute that defines the state of each codec.

No audio:

- The Sipelia™ Server supports several audio codecs. Your choice of which codecs to enable in the Sipelia™ system depends on what codecs are supported by the SIP intercoms.
- Intercoms can support one or multiple audio codecs. The most commonly used audio codecs are PCMA, PCMU, and G722. Research the audio quality and network usage associated with the supported codecs.
- The following instructions describe enabling or disabling codecs at the Sipelia Server level. It might also be required to configure the audio codecs used by the SIP intercoms. To investigate this, refer to the configuration page of each SIP intercom. You can also run a Wireshark capture to verify which codecs each device is using.
- For communication to occur, the same audio codec must be enabled on each device, as well as on the Sipelia Server. For example, for a system that includes two SIP intercoms (intercom A <-> Sipelia Server <-> intercom B) which both support PCMA, PCMU, and G722 codecs, configuring Sipelia Server to enable only PCMA forces all communication between the SIP intercoms to use the PCMA audio codec.

Distorted audio:

- All systems that you use with Sipelia™ (intercoms, servers, hardware, and software) should use an RTP packet size of 20 ms. Refer the documentation provided with the intercom hardware to see if the RTP packet size is configurable.
- The distorted audio maybe also be caused by particular audio codec. Reconfigure the system to use a different audio codec, then test the system and evaluate the audio quality. If the audio quality is poor, enable a different audio codec and perform another audio quality test.

To configure which codecs are enabled on the Sipelia™ Server:

- 1 Deactivate the Sipelia™ plugin role (see *Security Center Administrator Guide*).
- 2 Open the following configuration file:
`C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config`
- 3 In the *AudioCodecs* section of the configuration file, note whether the **Enabled** attribute is `True` or `False` for each of the audio codecs.
- 4 Enable or disable audio codecs as required to ensure that the Sipelia™ Server and all SIP intercoms share an audio codec.
- 5 Save the file and reactivate the Sipelia™ plugin role.
- 6 Test the system and evaluate the audio quality. If the audio quality is poor, enable a different audio codec and perform another audio quality test.

DTMF tones not working in Sipelia™

If pressing a number button on the Security Desk keypad does not produce an audible touch-tone signal (DTMF) at the SIP intercom, verify that the **telephone-event** audio codec is enabled on the Sipelia™ Server, and that an audio channel is established between the Sipelia™ Server and the SIP intercom.

Before you begin

- Create a backup of the following file:
`C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config`

What you should know

- DTMF tones in Sipelia™ are transported by the RTP protocol as the RTP EVENT payload (RFC 2833).
- DTMF tones do not depend on the type of audio codec which was used to enable the audio channel between the call participants. For more information on configuring which codecs are used for audio communication, refer to the related [audio troubleshooting](#) information.

To enable the required audio codecs to support DTMF in a Sipelia™ system:

- 1 Deactivate the Sipelia™ plugin role (see *Security Center Administrator Guide*).
- 2 Open the following configuration file:
`C:\ProgramData\Genetec Sipelia\SipServer\SipServer.config`
- 3 In the *AudioCodecs* section of the configuration file, note whether the **Enabled** attribute is **True** or **False** for each of the audio codecs.
- 4 To enable DTMF, set the **telephone-event** codec to **True**.
- 5 Enable or disable audio codecs as required to ensure that Sipelia™ Server and all SIP intercoms share an audio codec.
- 6 Save the file and reactivate the Sipelia™ plugin role.

Users cannot view recorded video from Sipelia™ calls

If a user cannot see the video that was recorded during previous SIP call sessions, you might have user privileges that are not set properly.

What you should know

This issue typically occurs when the user does not have the privilege to view recorded video in Security Center.

To enable users to watch recorded video:

- 1 Log on to Security Center with Config Tool.
- 2 Open the *Security* task, and then select the user entity involved in the issue.
- 3 In the **Privileges** page, make sure that the **View playback** privilege is allowed for the user.

Enabling file logging for debug traces on the Sipelia™ Server

File logging for debug traces can be enabled on the Sipelia™ Server side, the Sipelia™ Client side, or both. The nature of the problem to be investigated will determine if and where the debugging traces need to be enabled.

Before you begin

You need administrator privileges to be able to modify the required configuration files.

To enable file logging for debug traces on the Server side:

1 Stop the Sipelia Server.

2 Go to the configuration folder for the server logs.

It is located under the Sipelia program data folder as shown in the following example:

```
C:\ProgramData\Genetec Sipelia\Logs\Server
```

3 Open the file *NLog.dll.nLog*.

4 On line 12, replace text A with text B:

```
Text A: logger name="*" levels="Info,Warn" writeTo="RegularLogFile"
```

```
Text B: logger name="*" levels="Trace,Debug,Info,Warn" writeTo="RegularLogFile"
```

5 Save the file and restart the Sipelia Server

To enable file logging for debug traces on the Client side:

1 Go to the configuration folder for the client logs.

It is located under the Sipelia program data folder as shown in the following example:

```
C:\ProgramData\Genetec Sipelia\Logs\Client
```

2 Open the file *NLog.dll.nLog*.

3 On line 12, replace text A with text B:

```
Text A: logger name="*" levels="Info,Warn" writeTo="RegularLogFile"
```

```
Text B: logger name="*" levels="Trace,Debug,Info,Warn" writeTo="RegularLogFile"
```

4 Save the file.

The system will now log debugging traces in log files. The output files can be found in the following directory:

```
C:\ProgramData\Genetec Sipelia\Logs
```

IMPORTANT:

To avoid filling the hard disk with unnecessary information, it is recommended to revert the changes to the original configuration as soon as the required investigation has been completed.

Appendices

Additional resources

This section includes the following topics:

- ["Common VoIP terms"](#) on page 106



Common VoIP terms

This section includes the following topics:

- ["Common VoIP terms"](#) on page 107

Common VoIP terms

A VoIP (voice over Internet Protocol) environment needs many interacting components to work properly. Familiarizing yourself with these common terms can help you gain a better understanding of the Sipelia™ module.

- **dual-tone multifrequency (DTMF):** Dual-tone multifrequency is the standard for the audible signal that is sent to the phone company once a key is pressed on a telephone keypad. There is an audible tone to represent each digit on a keypad.
- **IP phone:** An Internet Protocol (IP) phone is a device that is used to make and receive calls over the Internet. An IP phone can use any of the existing communication standards or protocols, such as SIP, to transmit calls across a network. Although an IP phone can look like a traditional phone, an IP phone is not connected to a phone-line jack found in typical POTS installations; an IP phone is connected to a router or RJ-45 Ethernet connector.
- **plain old telephone system (POTS):** The plain old telephone system (POTS) is the basic form of telephone service that is used by most homes and businesses worldwide. Apart from being a different technology, what separates a non-POTS service from a POTS service is speed and bandwidth. POTS is also known as the public switched telephone network (PSTN).
- **private branch exchange (PBX):** A private branch exchange (PBX) is a private phone network that is used within a company. A PBX is a switching station that is used to connect many internal phone extensions to one outside line, thereby making it more efficient and cost effective for companies to adopt a phone system. In a company that uses a PBX network, incoming calls are redirected by the PBX to one or more internal extensions within the same enterprise.
- **IP private branch exchange (IP PBX):** An IP PBX is a private branch exchange (telephone switching system within an enterprise) that switches calls between VoIP (voice over Internet Protocol or IP) users on local lines while allowing all users to share a certain number of external phone lines.
- **SIP trunking:** SIP trunking is the process of using VoIP technology to connect existing PBX systems to other PBX systems. SIP trunking replaces traditional phone trunks with an IP network and consolidates voice, data, and video into a single trunk (or line). SIP trunking ensures a more reliable communication service and cost reductions.
- **softphone:** A softphone is a software for managing inbound and outbound calls over a network, using your computer rather than a phone. Softphones are designed to simulate the functions found on traditional phones. Also known as *SIP client*.
- **Voice over Internet Protocol (VoIP):** Voice over Internet Protocol (VoIP) is the technology for routing two-way voice and video communications over the web or other IP networks.

Glossary

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

C

- call dialog box** The call dialog box is a Sipelia-related dialog box that appears from the notification tray within Security Desk once an incoming call comes in from a SIP endpoint. In the call dialog box, users can manage their calls and their list of contacts and favorites, and set their availability status.
- Call report** The *Call report* task is a type of investigation task that allows users to review call sessions and generate reports. Among the possible actions that can be performed in this task, users can view the call logs for all sessions, watch playback video of all recorded call sessions, and see the bookmarks that have been added to video sequences of associated cameras.
- call session** A call session is the sequence of events or activities that occur from the time a SIP call is initiated to the time that it ends, including all call transfers. For example, if a call is transferred twice, the sequence of events that occur in both those transfers are all part of the same call session. In a Security Center system equipped with the Sipelia module, call sessions can be reviewed and exported through the *Call report* task within Security Desk.
- Config Tool** Config Tool is a Security Center administrative application used to manage all Security Center users, and configure all Security Center entities such as areas, cameras, doors, schedules, cardholders, Patroller/LPR units, and hardware devices.
- conversation window** The conversation window is a Sipelia-related window that opens within Security Desk once a SIP call has been accepted by either the caller or the recipient of a call. From the conversation window, Security Center users can manage conversations, forward calls, and view associated video when available.

D

- dial plan** A dial plan is a collection of rules that defines how calls are routed locally or between two SIP trunks. Dial plans ensure that calls are routed and rerouted correctly, and they also allow administrators to block calls to certain geographic locations or ensure the privacy of the callers.

E

entity Entities are the basic building blocks of Security Center. Everything that requires configuration is represented by an entity. An entity can represent a physical device, such as a camera or a door, or an abstract concept, such as an alarm, a schedule, a user, a role, a plugin, or an add-on.

G

Genetec Server Genetec Server is the Windows service that is at the core of Security Center architecture, and that must be installed on every computer that is part of the Security Center's pool of servers. Every such server is a generic computing resource capable of taking on any role (set of functions) you assign to it.

N

notification tray The notification tray contains icons that allow quick access to certain system features, and also displays indicators for system events and status information. The notification tray display settings are saved as part of your user profile and apply to both Security Desk and Config Tool.

R

regular expression A regular expression is a sequence of symbols used by a regular expression engine to identify all the strings of characters that match a specific search pattern without having to list all the possible discrete values that must be returned. The Microsoft's .NET Framework Regular Expression engine is the engine used in Sipelia™.

ring group A ring group is a group of SIP entities that has its own unique SIP phone extension. All entities (or members) within a ring group are part of a call list, and all members get called when the ring group extension is called. The members of a ring group can either be called all at once, or successively at a set interval. The call stops ringing once any one of the members within a call list answers the call.

role A role is a software module that performs a specific job within Security Center. Roles must be assigned to one or more servers for their execution.

S

Security Center Security Center is the unified security platform that seamlessly blends Genetec™ security and safety systems within a single innovative solution. The systems unified under Security Center include Genetec™ Omnicast™ IP video surveillance system, Synergis™ IP access control system, and AutoVu™ IP license plate recognition (LPR) system.

Security Desk	Security Desk is the unified user interface of Security Center. It provides consistent operator flow across all of the Security Center's main systems, Omnicast™, Synergis™, and AutoVu™. Security Desk's unique task-based design lets operators efficiently control and monitor multiple security and public safety applications.
Session Initiation Protocol	The Session Initiation Protocol (SIP) is a signalling standard that is used to control the exchange of data between two or more parties in multimedia communications. Sipelia, the Security Center core module that allows users to make, receive, and manage voice and video calls over the web, is based on the SIP standard.
SIP client	A SIP client is a program with softphone functionality that users can install on their computers or mobile devices to make and receive voice or video calls from other SIP clients. A SIP client requires a SIP account, and typically includes a user interface from which users can manage calls and also view call-related video streams, if such a feature is supported. Examples of SIP clients are SIP phones, softphones, and SIP intercoms. Once Sipelia Client is installed and configured, Security Desk is also an example of a SIP client.
Sipelia	Sipelia is a core module of Security Center that allows Security Center users to make, receive, and manage SIP-based voice and video calls over a network. Running on the open source Session Initiation Protocol (SIP), Sipelia also integrates existing video and access control platforms with intercom systems, and allows users to log call activities.
Sipelia Client	Sipelia Client is the softphone component of Sipelia. As a result, it installs the various user interface features of the Sipelia module, such as the call dialog box and conversation window. Sipelia Client must be installed on every Security Desk workstation that is running Sipelia, thus turning Security Desk into a SIP client (or softphone).
Sipelia Server	Sipelia Server is the SIP server component of Sipelia. It receives and administers information about the different SIP endpoints, and essentially facilitates the communication between two or more endpoints that are communicating in a SIP environment. Sipelia Server also collates and stores important data, such as contact list information, SIP server settings, and call session recordings. Sipelia Server must be run by a Security Center Plugin role, and therefore, must be installed on every Security Center server on which you intend to host the Plugin role.
SIP endpoint	A SIP endpoint is the device or system that is at each end of a SIP call session. Examples of endpoints are hard-wired phones, voice mail systems, and intercoms. A SIP client such as a softphone, is another example of an endpoint. Once Sipelia

Client is installed and configured, Security Desk is considered both an endpoint and a SIP client.

SIP entity

A SIP entity is a Security Center entity that has SIP-related capabilities. In Security Center, examples of SIP entities are users, ring groups, and SIP devices such as SIP intercoms.

SIP extension

A SIP extension is a numeric value assigned to a SIP device so that the device can make and receive SIP calls. Typically, a SIP extension is also used to register the SIP device (to which it is assigned) to a SIP server. To be able to communicate with other SIP endpoints, every SIP entity (user, ring group, or intercom) in Security Center must have a unique SIP extension assigned to it.

SIP intercom

A SIP intercom is an intelligent SIP endpoint that provides two-way phone connectivity in a SIP environment. In Security Center, a SIP intercom is one of the established SIP entities, and it is the only SIP entity that is an actual device. The other SIP entities are Security Center users and ring groups.

SIP trunk

A SIP trunk is a SIP server that allows users to connect their existing SIP servers to other servers, thus extending their VoIP capabilities and allowing them to migrate their old PBX systems to a unified VoIP system. With an integrated dial plan, SIP trunks make it possible for SIP extensions that reside on different SIP servers to communicate with one another.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ Technical Information Site:** The latest documentation is available on the Technical Information Site. To access the Technical Information Site, log on to [Genetec™ Portal](#) and click [Technical Information](#). Can't find what you're looking for? Contact documentation@genetec.com.
- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explain how the product works and provide instructions on how to use the product features. Patroller and the Sharp Portal also include context-sensitive help for each screen. To access the help, click **Help**, press F1, or tap the ? (question mark) in the different client applications.

Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to the Genetec™ Technical Information Site, where you can find information and search for answers to your product questions.

- **Genetec™ Technical Information Site:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

Before contacting GTAC or opening a support case, it is recommended to search the Technical Information Site for potential fixes, workarounds, or known issues.

To access the Technical Information Site, log on to [Genetec™ Portal](#) and click [Technical Information](#). Can't find what you're looking for? Contact documentation@genetec.com.

- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: [EN_GLM_ASSURANCE](#) and [EN_GLM_ADVANTAGE](#).

Additional resources

If you require additional resources other than the Genetec™ Technical Assistance Center, the following is available to you:

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss a variety of topics, ranging from technical questions to technology tips. You can log in or sign up at <https://gtapforum.genetec.com>.
- **Technical training:** In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to <http://www.genetec.com/support/training/training-calendar>.

Licensing

- For license activations or resets, please contact GTAC at <https://gtap.genetec.com>.
- For issues with license content or part numbers, or concerns about an order, please contact Genetec™ Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, please contact Genetec™ Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Please contact GTAC at <https://gtap.genetec.com> to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.