



Sipelia Release Notes

2.0 SR3

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

Copyright notice

© Genetec Inc., 2015

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", "OMNICAST", "SYNERGIS", "AUTOVU", "FEDERATION", "STRATOCAST", "SIPELIA", "CITYWISE", and the Omnicast, Synergis, AutoVu, and Stratocast logos 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 Release Notes 2.0 SR3

Document number: EN.704.001-V2.0.C3(1)

Document update date: January 4, 2016

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

Notes and notices

The following notes and notices might appear in this guide.

- **Tip.** Provides a useful hint, suggestion, or practical application of a topic or step.
- **Note.** Describes a special case or expands on an important point.
- **Important.** Points out critical information about a topic or step.
- **Caution.** Indicates that an action or step might cause loss of data, security problems, or performance issues.
- **Warning.** Indicates that an action or step might cause physical harm or damage the 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.

Contents

Preface: Preface

Copyright notice	ii
Notes and notices	iii

Chapter 1: Release notes

What's new in Sipelia 2.0 SR3	2
What's new in Sipelia 2.0 SR2	3
New supported SIP devices in Sipelia 2.0 SR2	3
Resolved issues in Sipelia 2.0 SR2	3
What's new in Sipelia 2.0 SR1	4
New supported SIP devices in Sipelia 2.0 SR1	4
Resolved issues in Sipelia 2.0 SR1	4
What's new in Sipelia 2.0 GA	6
Resolved issues in Sipelia 2.0 GA	9
Known issues in Sipelia 2.0 SR3	10
Limitations in Sipelia 2.0 SR3	12
System requirements for Sipelia 2.0 SR3	13
Supported languages for Sipelia 2.0 SR3	14
Product compatibility for Sipelia 2.0 SR3	15
Supported SIP devices for Sipelia 2.0 SR3	16
Product documentation	18
Where to find product information	19
Technical support	20

Release notes

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 2.0 SR3 is a service release that improves the reliability and performance of Sipelia. This document describes the release in detail, and provides late-breaking or other information that supplements the Genetec Sipelia documentation.

This section includes the following topics:

- ["What's new in Sipelia 2.0 SR3"](#) on page 2
- ["What's new in Sipelia 2.0 SR2"](#) on page 3
- ["What's new in Sipelia 2.0 SR1"](#) on page 4
- ["What's new in Sipelia 2.0 GA"](#) on page 6
- ["Known issues in Sipelia 2.0 SR3"](#) on page 10
- ["Limitations in Sipelia 2.0 SR3"](#) on page 12
- ["System requirements for Sipelia 2.0 SR3"](#) on page 13
- ["Supported languages for Sipelia 2.0 SR3"](#) on page 14
- ["Product compatibility for Sipelia 2.0 SR3"](#) on page 15
- ["Supported SIP devices for Sipelia 2.0 SR3"](#) on page 16
- ["Product documentation"](#) on page 18

What's new in Sipelia 2.0 SR3

With each release, new features, enhancements, or resolved issues are added to the product.

Sipelia 2.0 SR3 is a service release that improves the reliability and performance of Sipelia.

Enhancements:

- **Support for Security Center 5.4:** Sipelia 2.0 SR3 now supports Security Center 5.4.

What's new in Sipelia 2.0 SR2

With each release, new features, enhancements, or resolved issues are added to the product.

Sipelia 2.0 SR2 is a service release that improves the reliability and performance of Sipelia.

Related Topics

[What's new in Sipelia 2.0 SR1](#) on page 4

[What's new in Sipelia 2.0 GA](#) on page 6

New supported SIP devices in Sipelia 2.0 SR2

The following SIP devices have been added to the supported devices list.

Manufacturer	Devices	Support
Cisco	SPA8000 - VoIP Gateway for analog devices	Certified
Jacques	VSL-351W+	Certified

Resolved issues in Sipelia 2.0 SR2

Resolved issues are software issues from previous releases which have been fixed in the current release.

Solution/ Unit	Issue	Description
All	237071	(Call report task) If there is a failed transfer during a call, the recorded call duration is not saved correctly in the archive. The call is not replayed completely in the report.
All	269832	When failover is activated, the user must log off Security Desk and log on again to use Sipelia client.
All	281158	If a Ring Group is configured with the "all at once" property and contains duplicate entries, a call destined to that group crashes the Sipelia server.

What's new in Sipelia 2.0 SR1

With each release, new features, enhancements, or resolved issues are added to the product.

Sipelia 2.0 SR1 is a service release that improves the reliability and performance of Sipelia. Here is what's new in this release:

Enhancements:

- **Enabling and disabling codecs:** Users can select which audio or video codecs are enabled on the Sipelia server.

Related Topics

[What's new in Sipelia 2.0 SR2](#) on page 3

New supported SIP devices in Sipelia 2.0 SR1

The following SIP devices have been added to the supported devices list.

Manufacturer	Devices	Support
Axis	A8004-VE	Certified
CodeBlue	IP5000	Certified
	IP1500, IP2500	Supported by design

Resolved issues in Sipelia 2.0 SR1

Resolved issues are software issues from previous releases which have been fixed in the current release.

NOTE: Former issue IDs are shown in parentheses.

Solution/ Unit	Issue	Description
All	217869	(Sipelia Server) Video from a SIP camera (webcam, intercom built-in camera), that is, a camera not connected to an Archiver, is not recorded.
All	221134	(Monitoring task) When viewing a call with associated cameras, if the camera selection menu is open, single clicking in the tile replaces the intercom by the associated camera.
All	221152	When a Sipelia configuration page is open on a remote Config Tool, users might observe an unusually high CPU usage.
All	221385	When a dial plan rule which has a "New source" defined is used to call a ring group, the caller's extension is shown to the recipients instead of the new source extension.

Solution/ Unit	Issue	Description
All	222532	(Sipelia Client) When a call is forwarded and is not answered, the caller remains in the transferring state and cannot forward the same call to other recipients.
All	222536	(Sipelia Client) The video from a forwarded call is not visible to the recipient.
All	222539	Calls that cannot be transferred are ended instead of being returned to the previous participants. This behavior only occurs when the call recipient is initiating the transfer.
All	223825	(Security Desk) Changing the camera in Sipelia options prevents video from that camera to be displayed during the next calls.
All	224388	The recording option is available on the configuration pages for intercoms and users, regardless of whether you have a recording license.
All	225780	(Security Desk) From the tile, the recipient of a forwarded call can only see the entities associated with the person who forwarded the call instead of the entities associated with the original caller.
All	234705	(Sipelia Server) Calls to ring groups are audio only, no video is shown to the participants.
All	235414	(Sipelia Client) On computers that provide multiple network interfaces (cards), if the network interface used by Sipelia is not configured with the highest priority in Windows, Security Desk cannot register to Sipelia Server.
All	235749	During a call, if you click 'Forward call' multiple times, a transfer window opens for each click.
All	241261	During a call between the Sipelia Client on Security Desk and an intercom with a SIP embedded camera, the video from the intercom camera is not available in the Security Desk tile if the Security Desk machine's webcam is not connected.
All	244688	A missing certificate in the Sipelia installation prevents you from configuring the Sipelia module from Config Tool, but only if Sipelia is on a remote server.
All	246462	In certain network architectures, Security Desk client cannot connect to the server if the Notification Service (RabbitMQ) address is set to "localhost".
All	255199	During a call, if Security Desk with Sipelia client has no microphone or speaker, it does not receive the video.
All	256171	When calling a ring group, the call cannot be established if the recipient is connected to a SIP trunk.

What's new in Sipelia 2.0 GA

With each release, new features, enhancements, or resolved issues are added to the product.

Sipelia 2.0 GA is the initial Sipelia release that includes all of the product features. Here's what's new in this release:

Security Desk features

- **Making and receiving calls:** Users can initiate and receive calls from the call dialog box or from the logical view of the *Monitoring* task.
- **Managing calls:** Users can answer or decline incoming calls. When a call has been answered (active call), all parties within that call session can place the call on hold. If users are placed on hold, they can still initiate a new call, and this new call will subsequently be placed on hold once the preceding call has resumed. Once on a call, users can forward the call to other SIP extensions.
- **Call notification:** Along with an audible alert, the call dialog box appears from the notification tray to notify users of incoming calls. From the call dialog box, users can answer or decline incoming calls.
- **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.. Once the Sipelia module is installed, Security Desk tiles support Sipelia-related controls, such as the ability to display an active conversation.
- **DTMF support:** In the call dialog box, users can send DTMF tones using the keypad. This can be used to send commands to an intercom for example.
- **Call-related controls in Security Desk tiles:** Security Desk tiles display active conversations. Security Desk users can choose to display their incoming and outgoing calls in either the conversation window or a tile. From the tiles, users can manage multiple conversations, forward calls and view associated camera video when available.
- **Indicating the availability status of a user:** In the call dialog box, users can set their availability status, thereby indicating to other users whether they are available, away, or busy.
- **List of contacts:** In the call dialog box, users can view and manage their list of contacts. From the list of contacts, users can do the following:
 - Call a contact by simply double-clicking the contact name.
 - See the availability status of their contacts (users and intercoms).
 - In detailed view mode, quickly display a contact's information, such as photo, name, and number.
 - Filter their contacts by type (device or user).
 - Add and remove contacts from their favorites.
 - Search for and call numbers that appear in the contact list.
- **Selecting audio and video devices:** From the *Options* dialog box, users can select the audio device (microphone or speaker) and local camera (webcam) that they want to use for their voice and video calls. Users can also select the video codecs they want to use for their video communication.
- **User-specific call options:** From the *Options* dialog box, users can select whether they want incoming calls to automatically open in a tile within the *Monitoring* task (as opposed to the conversation window), and whether they want an audible ring to sound when receiving an incoming call.

- **Status of SIP devices:** Users can see the status of the SIP devices that are registered to Sipelia Server, so that they can easily identify which devices are online or offline.
- **Controlling cameras, doors, zones, and device outputs:** During a call with a SIP intercom, users can control cameras (including PTZ cameras) that are associated with the SIP intercoms. Users can also open and close associated doors for remote users, arm and disarm zones, and activate outputs along with their respective behaviors. All of these entities can be controlled from either the conversation window or a tile within the *Monitoring* task. Furthermore, users can drag SIP intercoms and camera entities into available tiles within the *Monitoring* task.
- **Call report task:** 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. Users can also view communication events (calls accepted, calls rejected, and so on) and events from a SIP device's associated entities (door opened, zone armed, and so on). Users can also generate reports based on the criteria that they set. The layout of the *Call report* task resembles that of similar report tasks found in Security Desk.
- **Watching recorded video:** From the *Call report* task, users can access video that was recorded from cameras that are associated to users and intercoms.
- **Exporting call sessions:** In the *Call report* task, users can export the video and audio for multiple call sessions at once. Exported video files also contain all events and actions that are associated to a call session. Users can watch the exported video files directly from the *Call report* task.

Config Tool features

- **Sipelia Server and Sipelia Client:** The Sipelia module contains two components: Sipelia Server and Sipelia Client. 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 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.
- **Installation of SIP freeware:** SIP freeware comes bundled with Sipelia. As a result, all of the required SIP freeware is installed automatically when administrators install Sipelia.
- **SIP intercoms:** Administrators can add SIP intercoms. 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. A SIP phone can also be added as an intercom.
- **SIP entities:** Administrators can create SIP entities based on intercom devices and existing Security Center entities. 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..
- **Configuration pages:** Upon installing Sipelia Server, administrators can configure the various Sipelia features through the following six pages:
 - **General:** used to configure the system communication service, configuration service, and port settings.
 - **Servers:** to configure the Sipelia Server SIP port, and define the ranges of SIP extensions.
 - **Ring groups:** used to create and manage custom ring groups.
 - **Dial plans:** used to import and manage rules related to the routing of inbound and outbound calls within the local SIP server, or across different SIP servers.
 - **SIP trunks:** used to connect SIP servers to other servers, thus extending your VoIP capabilities.
 - **Recording:** used to define recording options for users and SIP devices.

- **Creating a SIP accounts for Security Center users:** Upon installing Sipelia, administrators can create a SIP account for individual Security Center users by accessing the VoIP page of the user entities. In the VoIP page, administrators can choose to manually or automatically assign a SIP phone extension and password, and configure other parameters.
- **Recording call sessions:** Administrators can select to record call sessions in which users and SIP devices participate.
- **Retention period for recordings of call sessions:** Administrators can set the number of days and hours that recordings of call sessions are kept stored in the system.
- **Associating entities with SIP intercoms:** Administrators can associate multiple cameras (including PTZ cameras), doors, and zones, and device outputs (along with their respective behaviors) with SIP intercoms. Administrators can also set the order by which a SIP intercom's entities are displayed within the *Monitoring* task in Security Desk. If associating PTZ cameras, administrators can select which position presets are associated with the SIP intercom. You can associate these entities to a SIP intercoms regardless of whether the intercoms have been assigned SIP extensions.
- **Creating ring groups:** Administrators can create ring groups, so that a group of selected SIP entities get called simultaneously whenever someone calls the SIP extension of the ring group. 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. Custom ring groups are created in the Sipelia *Plugins* task, but administrators can also create basic ring groups from the respective VoIP pages of Security Center user 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 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.
- **Storing call preferences:** Administrators can select whether two user-specific call preferences are stored locally on a user's Security Desk workstation or stored in a central database (roaming profile). If the latter is selected, Security Desk users can log on to any Security Desk workstation that is on the same network and keep their user options.
- **Support for failover:** Administrators can protect the Sipelia Plugin role against hardware failures by assigning standby servers for the role.
- **Establishing dial plan rules:** With dial plans, administrators can import and manage rules related to routes for inbound and outbound calls. 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.
- **Adding SIP trunks:** Administrators can add trunks so that they can connect their SIP servers to other servers, thus extending their VoIP capabilities and allowing them to migrate their old PBX systems to a unified VoIP system.
- **User privileges:** Administrators can decide whether users and user groups have the right to use the call dialog box to make new calls, transfer calls or reject calls, or use the *Call report* task.
- **Licensing:** With the *Certificates* tab of the *About* page, administrators can view their respective license restrictions and usage levels for various components, such as intercom servers, external phones, and so on.
- **Product upgrade wizard:** Administrators can upgrade their versions of Sipelia through an automated upgrade wizard, thereby facilitating upgrades and eliminating the need to reconfigure systems.
- **Custom events:** Administrators can associate Security Center custom events to each user and SIP intercom. The custom events will be generated upon specific call states, for example, trigger an alarm when a call is not answered by a user. You can select a different custom event for each one of the following call states: *Ringing*, *On a call*, *Busy*, *Not answered*, *Error*, *End call*.

Related Topics

[What's new in Sipelia 2.0 SR2](#) on page 3

Resolved issues in Sipelia 2.0 GA

The following issues were resolved in Sipelia 2.0 GA.

NOTE: Former issue IDs are shown in parentheses.

Solution/ Unit	Issue	Description
All	196478	(Config Tool) The <i>Servers</i> page does not include Apply and Cancel buttons. As a result, when changes are made, they are automatically applied.
All	198982	(<i>Call report</i> task) When a user is watching a recorded call session, the video of the call session freezes if the user receives a call. The video's progress bar continues to move, but the video remains frozen. The video stream resumes once the call has ended, and an error message is displayed at the end of the call session.
All	199195	(<i>Call report</i> task) Users cannot watch a recorded call session if the associated camera, from which the video recording was captured, is currently offline.
All	199442	(Config Tool) In the <i>VoIP</i> tab of the user entity, administrators cannot change the order of the user's associated cameras. As a result, during an active call, when users click the camera entity button to select a video stream in either the conversation window or tile, the order in which the camera names appear is randomly set.
All	199839	(<i>Call report</i> task) When exporting a call session, the Start export button remains disabled, regardless of whether the filepath to the destination folder that was entered is valid. Workaround: When choosing the destination folder, use the short browse button (...).
All	225771 (197467)	(Server) When associated Security Center entities are deleted from a federated system, they remain stored in the database. As a result, if the federated system is removed, and then added again, the associated entities (which had previously been deleted) are once again displayed in the respective <i>VoIP</i> tab of the user and intercom entities.

Known issues in Sipelia 2.0 SR3

Known issues are software issues that have been discovered in the current release or a previous release, and have not yet been resolved.

NOTE: Former issue IDs are shown in parentheses.

Solution/ Unit	Issue	Description
All	218981	(Security Desk) Video of a previous operator to operator call session can still be observed for few seconds on the next call.
All	221159	When an intercom is deleted, the number of intercom connections permitted is not properly updated.
All	222083	(Sipelia Client) Video preview is not displayed when an intercom with a built-in SIP camera is calling a Security Desk user.
All	224963	(Call report task) Calling a ring group shows more call sessions than expected in the report.
All	225769 (196308)	(Licensing) When the number of allowed SIP devices has been reached, the following incorrect warning message appears in the <i>VoIP</i> tab: <i>Unable to establish communication with the server. Check the connection.</i> The message should inform administrators that they have exceeded the maximum amount of SIP devices authorized by their license.
All	225772 (198980)	(Call report task) When playback of a call session recording, which contains video, has ended, the message <i>No recorded video at this time</i> is displayed on the first frame of the video file. This message appears even though the recording does contain recorded video.
All	225773 (199211)	(Security Desk) In some cases, when users have an active call in a tile, but they want to move the call to the conversation window instead, Security Desk opens the conversation window, but does not remove the call from the tile. Even though the call is displayed in the conversation window, Security Desk freezes and needs to be restarted.
All	225774 (199836)	(Sipelia Client) When users call a ring group extension, the extension, name, and photo of the ring group member that accepts the call is not displayed. As a result, users might not know who they are speaking with.
All	225775 (200629)	(Sipelia Client) When a dial plan rule is in effect to reroute local calls from one extension (the source) to the other extension (the destination) in Security Desk, the extension originally dialed is displayed to the caller. For example, let's assume that we have imported a dial plan rule that reroutes calls that were originally destined to extension 2001 to extension 2002. When extension 2001 is called, and extension 2002 accepts the call (as defined by the rule), the extension 2001 is displayed to the caller in Security Desk.
All	225912	(Call report task) Canceling an export is blocking the user from using Security Desk until the cancellation operation is completed.

Solution/ Unit	Issue	Description
All	237473	(Security Desk) New incoming calls are not displayed in tiles when all the tiles are already used. Workaround: Use the call dialog box, change the Sipelia options in Security Desk to receive new calls in popup windows, or select a tile pattern that provides additional tiles.
All	256380	When a call is transferred to a ring group, the call is dropped approximately 30 seconds. after a member of the ring group accepts it.
All	272236	(Sipelia Server) Video from a SIP camera (webcam, intercom built-in camera) is not recorded properly when the call is on HOLD. The end of the video is missing.
All	292597	The Advanced menu from the Call window does not close after a failed call transfer.
Axis	260416	When an Axis intercom sends a standard SIP re-INVITE message to Security Desk during an active call, video freezes and features like Hold and Transfer are not available anymore. Workaround: Enable only the two following codecs on the server: the H264 video codec and the PCMA audio codec.
Axis	272872	When a call is established from the Axis A8004-VE to a Security Desk user, the video file from the intercom camera is corrupted, which makes the replay of the session from the report task incorrect. Workaround: Add the intercom camera as an associated camera of the intercom entity. To do so: Go to the Area view in the Config Tool and select the Axis A8004-VE entity. From the VoIP tab, click on the "+" in the associations list. In the wizard, click on camera, select the Axis unit and then apply. The camera will now be available as an associated camera in the Call Report.
Castel	222975	(Sipelia Server) It is not possible to hear audio for several seconds after resuming a call with a Castel intercom.
Commend	258491	When a Commend GE800 unit is used to create a SIP trunk, a ring group call cannot be established when the recipient is a SIP client connected to that trunk.

Limitations in Sipelia 2.0 SR3

Limitations are software or hardware issues that cannot be fixed. For certain limitations, workarounds are documented.

NOTE: Former issue IDs are shown in parentheses.

Solution/ Unit	Issue	Description
All	221212	(Call report task) Cannot play back video from previous call sessions when Security Desk is running on Windows Server 2008 R2 with the Desktop Experience feature enabled. As stated by Microsoft: "This problem occurs because the Desktop Experience feature in Windows Server 2008 R2 does not include decoders for the H.264 and AAC formats." To resolve this issue, install the "Update for Desktop Experience Decoder for Windows Server 2008 R2" (KB2483177).
All	260960	Network Address Translation (NAT) is not supported with Sipelia. Security Desk must use the server's private IP address to connect.
All	263587	Security Desk with Sipelia installed does not start if the application Microsoft Process Monitor is running.
All	265106 (148346)	When calling devices that share the same extension, and that are registered on the same server, the calls are not received on any of the devices.
All	265107 (193273)	(Sipelia Server) When deactivating the Sipelia plugin role, you can reactivate the role before the deactivation process has been fully completed. As a result, Sipelia cannot start. Workaround: Deactivate the role and wait until it is disabled (the GenetecPlugin.exe process is terminated) before reactivating it.
All	265108 (198171)	(Call report task) Users cannot watch video from exported call sessions through remote desktop. In such cases, the audio from the call session can be heard, but the video is not visible.

System requirements for Sipelia 2.0 SR3

System requirements are the recommended hardware and software components that are required for your product and system to run optimally.

Software requirements

The following table lists the software requirements for and .

Component	Requirements
Sipelia Server	- Security Center 5.2 SR7 and later - One of the following: 32-bit or 64-bit Windows 7, 2008, 2008R2 32-bit or 64-bit Windows Server 2012 Standard or Enterprise Edition
Sipelia Client	- Security Center 5.2 SR7 and later 32-bit or 64-bit Windows 7 or 8

Hardware requirements

Sipelia Server must be hosted on a Security Center server, and Sipelia Client must be hosted on a Security Desk workstation. As a result, the general hardware requirements for Sipelia must follow those of Security Center. Refer to the release notes of the Security Center version you are using for the applicable Security Center system requirements.

The following table lists hardware requirements specific for the 2.0 release of Sipelia.

Component	System characteristics	Requirements
Sipelia Server	A maximum of: - One Sipelia Plugin role per directory 32 simultaneous calls (active or recording) 1000 registered SIP intercoms 10 SIP trunks	- For systems recording call sessions, a dedicated high-end server is required. - For systems handling only active calls (not recording call sessions), the Sipelia Plugin role can share a high-end server with a 20% impact on server resources.
Sipelia Client	A maximum of 10 simultaneous calls	High-end workstations only

Supported languages for Sipelia 2.0 SR3

The supported languages are the languages in which the software is available.

Sipelia 2.0 is available in the following languages:

- Arabic
- Chinese (Simplified and Traditional)
- Czech
- Dutch
- English
- French
- German
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Persian
- Polish
- Portuguese-Brazil
- Spanish
- Thai
- Turkish

Product compatibility for Sipelia 2.0 SR3

Product compatibility indicates that the product supports and can run with specific versions of other products.

Sipelia 2.0 is compatible with the following products and software components:

- Security Center 5.2 SR7 and later
- Plan Manager 10.3 SR2 and later

Supported SIP devices for Sipelia 2.0 SR3

Sipelia supports a number of industry-leading SIP devices from various manufacturers. Before adding a device, make sure that your model is supported and that the latest firmware is installed.

The following SIP devices are supported with Sipelia 2.0.

Manufacturer	Devices	Support
Axis	A8004-VE	Certified
Cisco	SPA8000	Certified
CodeBlue	IP5000	Certified
	IP1500, IP2500	Supported by design
Commend	GE800 Server	Certified
	SIP-WS 800P	
	SIP-ET 908A, SIP-ET 908A-1	Supported by design
	SIP-WS 200P, SIP-WS 200V	
	SIP-WS 201P, SIP-WS 201V, SIP-WS 201V CA	
	SIP-WS 202P, SIP-WS 202V	
	SIP-WS 203P, SIP-WS 203V	
	SIP-WS 210V	
	SIP-WS 211V DA	
	SIP-WS 212V	
	SIP-WS 500F, SIP-WS 500P	
	SIP-WS 800F, SIP-WS 800FMD, SIP-WS 800V	
	VirtuoSIS	
Jacques	VSL-351W+	Certified
Zenitel	1008111020	Certified
	1009601003	
	1008000000, 1008001000, 1008007000	Supported by design
	1008015000, 1008031000, 1008041100	
	1008041150, 1008051000, 1008070000	
	1008072100, 1008072120, 1008072200	
	1008072220, 1008090200, 1008090250	
	1008093000, 1008111010, 1008111030	
	1008111040, 1008111050, 1008111060	

Manufacturer	Devices	Support
	1008131020, 1009608000, 1009608100	
	1009608106, 1009608300, 1009621000	
	1009627000, 1009627001, 1009627100	
	1009627200, 1401110100, 1401110200	

Product documentation

The documentation that is provided with a product is subject to change. With each product release, new documents might be added, current ones updated, and older ones replaced.

Available documents

- Sipelia User Guide
- Sipelia Release Notes

Available languages

The documentation for Sipelia 2.0 is available in English and French.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec Technical Information Site:** The latest version of the documentation is available from the [Documents](#) page of the Technical Information Site. To access the Technical Information Site, simply log on to [GTAP](#) and click the tab for the Technical Information Site.
- **Installation package:** The documentation is available in the Documentation folder of the installation package. Some of the 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 Genetec customer, 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:** Browse over 5000 articles or download one of our many technical publications to find information on how to deploy and use Genetec products. Prior to 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, simply log on to [GTAP](#) and click the tab for the Technical Information Site.
- **Genetec Technical Assistance Center (GTAC):** Live support is available during business hours over the phone or using GTAP chat at <https://gtap.genetec.com/Cases>. For GTAC's contact information in your region see the Contact page at <https://gtap.genetec.com>.

NOTE: To obtain phone support, you must provide a certification number and the last six digits of your system ID. Refer to the [Genetec Training FAQ](#) for more information.

NOTE: To open a case with GTAC, you must provide your System ID (Omnicast, Synergis and Security Center) and/or SMA contract number. In addition, for Genetec hardware controllers and appliances, you'll need the software revision number (image version).

Additional resources

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

- **GTAP Forum:** The Forum is an easy-to-use message board that allows clients and Genetec staff 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/Services>.