Call Recorder Apresa
Admin Manual
V2.14
VC2019

Care and Maintenance

	Keep the CR Apresa dry. If it gets wet, wipe it dry immediately with a soft, clean cloth. Liquids might contain minerals that corrode the electronic circuits.
0° to 40°	Use and store the CR Apresa only in temperature conditions between 0 and 40 degrees Celsius. Temperature extremes can shorten the life of electronic devices and distort or melt plastic parts.
	Keep the CR Apresa away from excessive dust and dirt.
	Do not use aggressive chemicals, cleaning solvents or strong detergents to clean CR Apresa.

Contents

---

1   Introduction

This is the manual of the Vidicode Call Recorder Apresa web interface. It is intended for users and administrators as well.

Call Recorder Apresa is a system for systematically recording VoIP (Voice over IP), ISDN T1/E1, Digital TDM, and analog telephone calls.

Note: When you want to use Full disk encryption, it needs to be configured in the earliest stages of the installation. When enabled you must enter a passphrase (on a keyboard connected to the machine) every time you reboot. This feature offers some additional security, but is inconvenient. When the passphrase is lost, the Apresa system won't boot and all data on the disk(s) is inaccessible. If, like in most cases, you only need to store the calls encrypted, switching on encryption in the normal settings is enough.

Do you need to install hardware and software yourself? Do you need to configure the telephone wiring or the LAN? Ask Vidicode for the elaborate **Apresa Installation manual**.

1.1   Apresa Variants

The Apresa system can be supplied in a number of variants:

- **Apresa Server (rack equipment):**
This is a Vidicode supplied server system pre-installed with all needed hardware. This unit can handle a mix of all inputs possible on an Apresa system.

- **Apresa Compact Server for VoIP channels:**
This version is built around a small cabinet and records up to 10 simultaneous VoIP channels.

- **Apresa Compact Server for analog or digital channels:**
The Apresa solution for smaller applications up to 8 TDM digital or 8 analog lines.

- **Apresa Software-only:**
You can install the Apresa recorder on a virtual machine or on other preferred locally sourced hardware. Base software and licenses and (if needed) recording cards are supplied by Vidicode for local installation.

1.2   Apresa Call Recording Solutions

1.2.1   VoIP

Call Recorder Apresa

VoIP Phones

PBX

VOIP / SIP
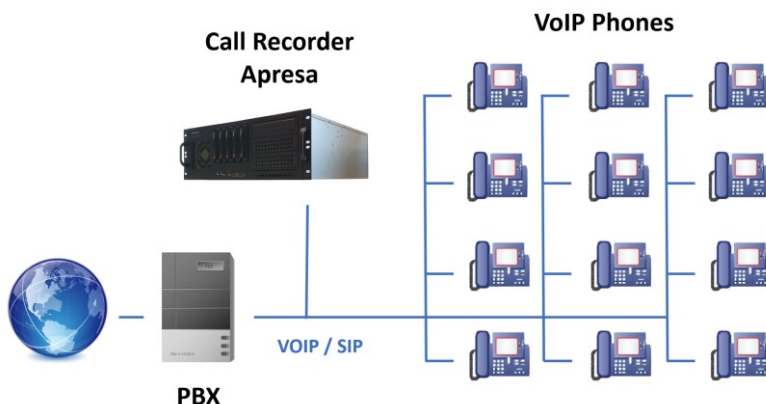
VoIP recording using internal port-mirroring (SPAN). Apresa receives copies of network packets sent between the PBX and the phones.
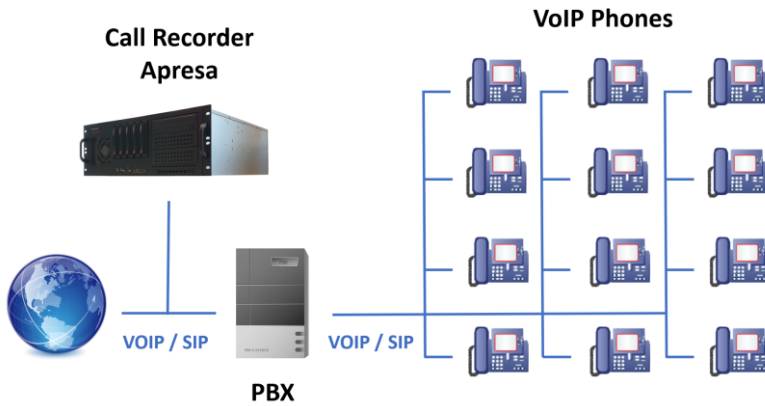
VoIP recording on the trunk, using external port-mirroring (SPAN).

1.2.2 Analog
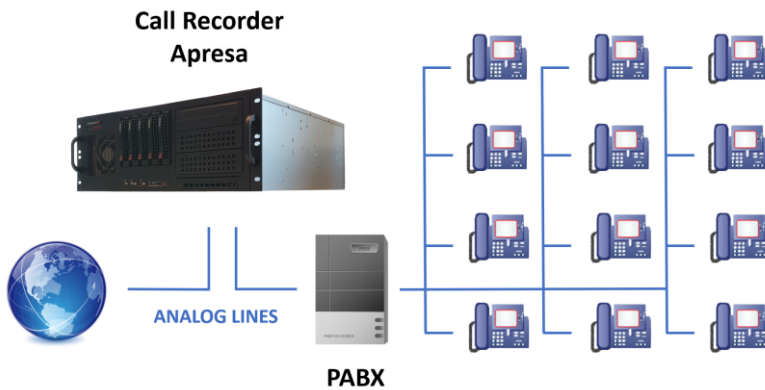
Recording from Analog lines, regardless of the protocol the phones.
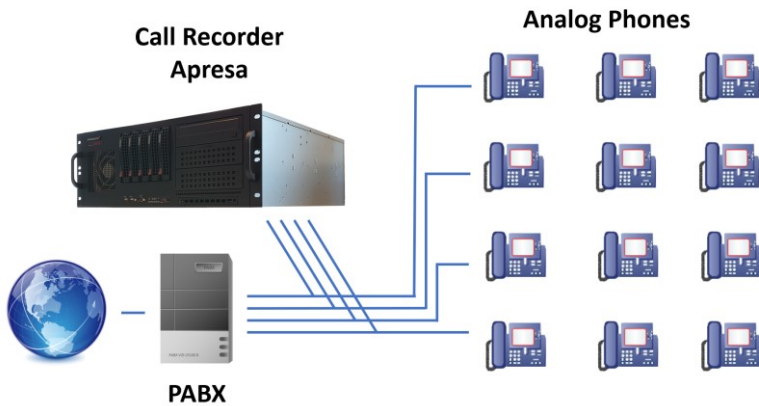
Recording from Analog Phones.

1.2.3 TDM
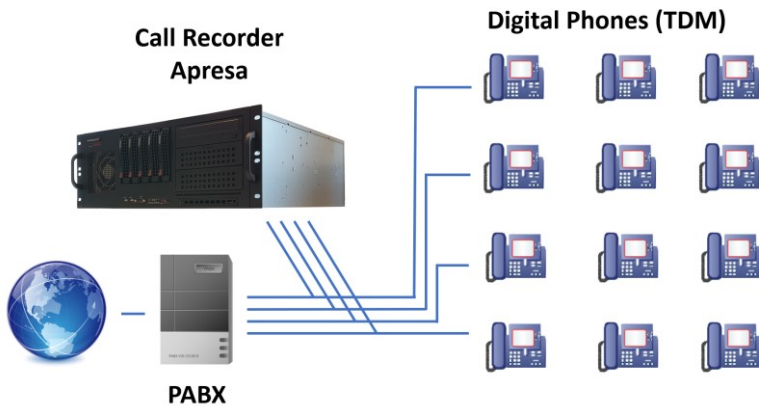
Recording from Digital Phones (TDM).

1.2.4 ISDN PRI

Call Recorder
Apresa

ISDN PRI LINES

PBX
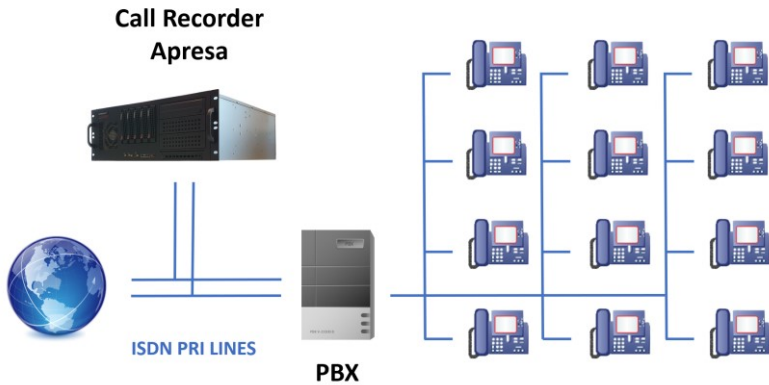
Recording from ISDN PRI lines.

1.2.5 Apresa and V-Tap
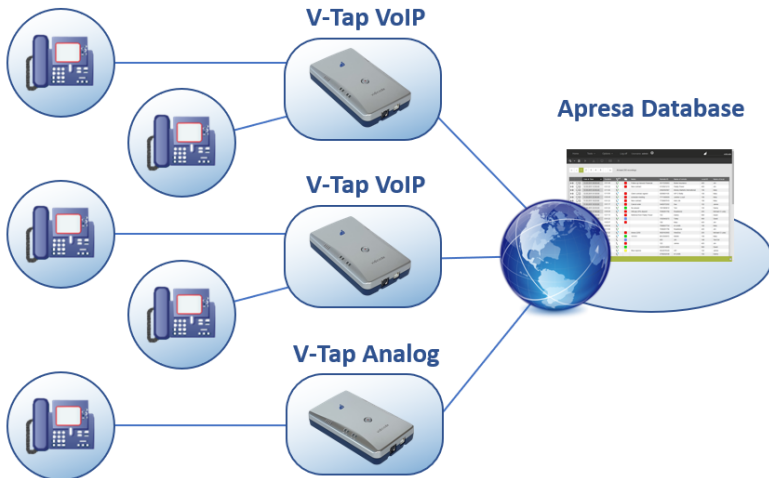
Recordings made by local Vidicode V-Tap units can be transported safely via a secured tunnel and stored encrypted in the central Apresa database. This can be done over LAN, WAN or even the internet.

1.2.6 Apresa and Call Recorder Oygo software

Vidicode's Call Recorder Oygo is software to record telephone calls from **soft phones** and **headsets**. With an additional **screen recording** license, you can record the screen during the call. Oygo can upload the recordings to Call Recorder Apresa.
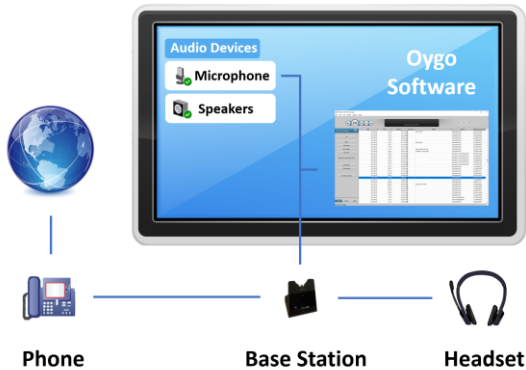
1.2.7 Apresa and OpenScape Xpert
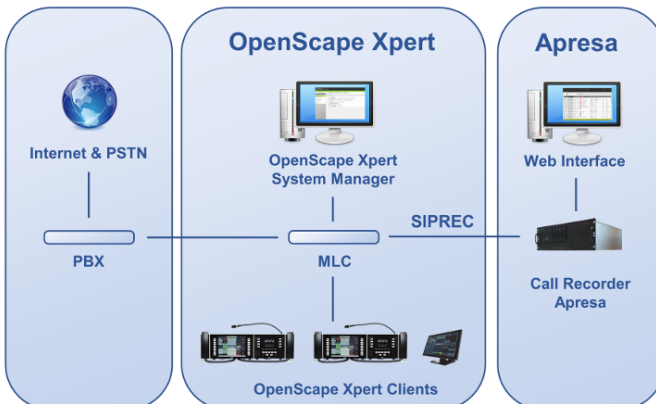
Apresa features a certified recording solution for Unify OpenScape Xpert to record all communication and telephone calls using the Session Recording Protocol (SIPREC).

Other SIPREC solutions are available for: NEC Univerge SV9500, AudioCodes Mediant, BroadWorks and others.

1.2.8   Active Recording

Active Recording solutions are available for: Unify OpenScape 3000 and 4000, OpenScape Voice, Avaya Aura, Cisco CUCM, and others.
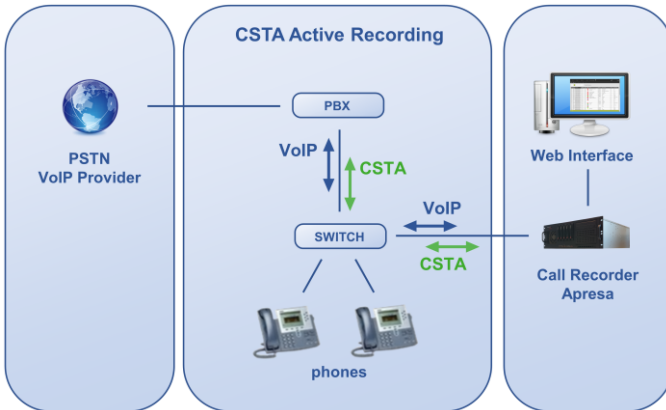
The image shows Active Recording using VoIP data and the CSTA protocol. See CSTA Active recording.

1.2.9   Passive Recording

CSTA Passive Recording solutions are available for: Mitel (Aastra) 400 series, Unify OpenScape 3000 and 4000, and others.
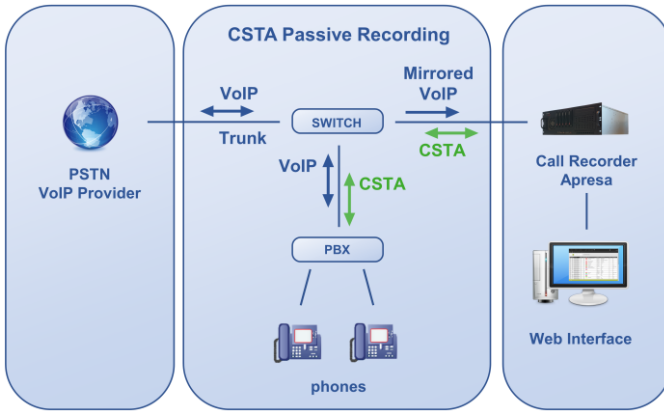
The image shows Passive Recording using mirrored VoIP data and the CSTA protocol.

There are separate documents available about configuring CSTA Recording. Contact Vidicode for more information.

1.2.10 Microsoft Teams Recording

Apresa records telephone calls and video conferences from Microsoft Teams. Recording of shared screens is featured as well. Video meetings and Screen sharing can be stored in mp4 format.
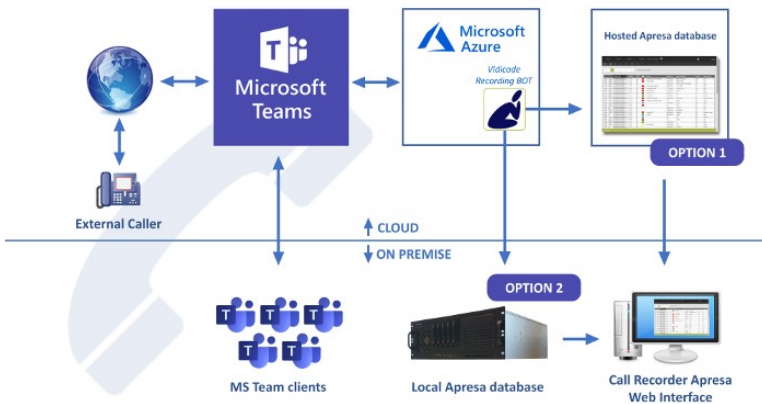
In the Microsoft Teams interface, you can add notes to a recording, pause a recording (insert silence or blank a screen) or stop a recording.
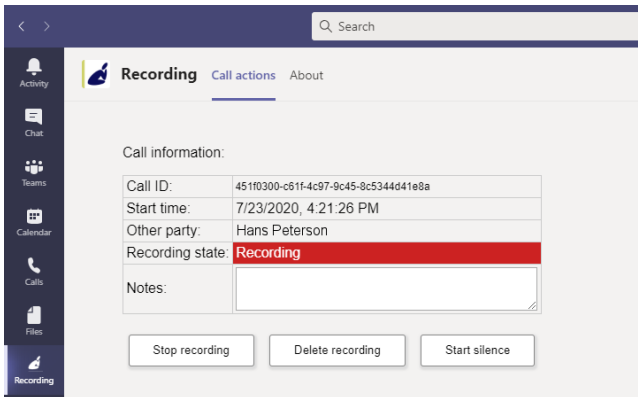
The audio and video recordings are available in the Apresa web interface.

There are separate documents available on Apresa and Microsoft Teams Recording, for example about configuring MS Teams, the Recording Bot in Azure, and Apresa itself. Contact Vidicode for more information.

2   Setting up the Apresa

The Call Recorder Apresa can be set up via the web interface. This set up has to be done by a person with Administrator rights on the Apresa.

2.1   Log on

To access the Call Recorder Apresa and log on:

•   open a browser.

•   Enter the IP address for the Apresa web interface.

•   Enter your user name and password.
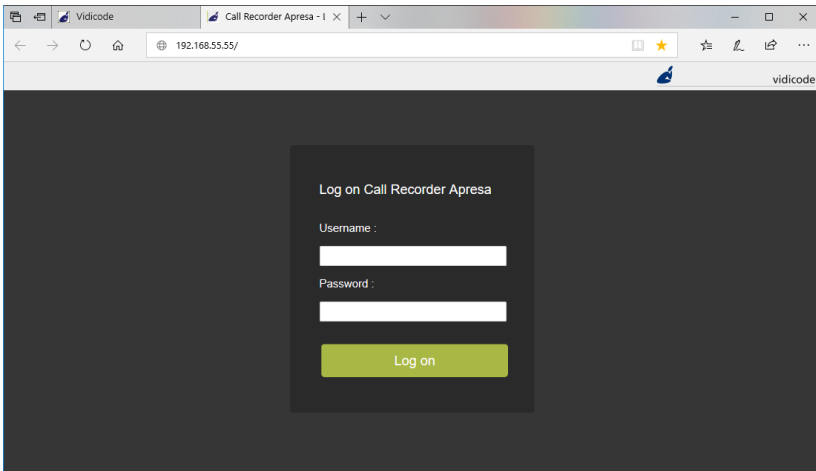
2.2   Quick start

If you want to record SIP calls right away, install the VoIP licenses and send the SIP data to Apresa using port-mirroring on a network switch. You don't have to create users, because licensing is not per user. Licensing is per simultaneously recorded call (recording channels).

2.3 Licenses

You'll need to install licenses when you, after receiving the Apresa hardware, want to do the following:

- Expand your system with extra licenses to record more phone calls at the same time. We call these channel licenses.
- Enhance your system with an optional feature, like Agent Evaluation.
- Renew your Support & Upgrade license. The first year is free.

Base Key License
A base key license is needed for the Apresa to work. If you bought the Apresa "Software Only" version, install the Apresa on a server (or virtual server) and then activate the base key license.

Channel licenses
Vidicode offers, among others, the following licenses to record telephone calls:

- VoIP channel licenses
- Analog channel licenses
- TDM channel licenses
- ISDN E1/T1 channel licenses
- External device recording licenses
- MS Teams BOT audio recording licenses
- MS Teams BOT video recording licenses

Support & Upgrade license
Install this license after you have installed your channel licenses.

See Apresa License Activation on how to activate licenses.

2.4 Security

Setup Data Encryption as soon as possible.

This includes, depending on your preferences:

- Encryption of the communication
- Full disk encryption
- Encryption of call content
- Per-tenant encryption of call content

Recommendations:
- Please change the admin password.
- Don't make the Apresa accessible from the internet, unless necessary.
- Use HTTPS
- Use strong passwords.
- Don't grant a user more privileges than necessary (e.g. seldomly grant permission to delete calls).

2.5 Defining user groups and permissions

Place every user in the group Organization or a sub-group of Organization. Apresa will still record calls if you don't create sub-groups. If the only user is "admin" the system still work.

It is recommended to start with defining the **user group** structure, and then define the user list. You can do this in the web interface, or by importing it from an external file. The easiest way to set the permissions correctly for all users and their managers or supervisors is following these recommendations:

User groups in Apresa reflect the hierarchical structure of an organization. At the root of the structure is the group Organization. This group is defined by default. When you add a user group, always make it a part of the group Organization.

This is an example of an hierarchical group structure:

- Organization
  - o Finance Management
    - ▪ Finance
  - o Development Management
    - ▪ Development

Active Directory (LDAP) log-on in Apresa

Note: Are you using Active Directory in your organization? Let Apresa create (and synchronize) a user group for you by importing an Active Directory user group(s). And/or choose "LDAP log-on" for a user.

Apresa will check his or her password using LDAP communication with the Active Directory server. See the chapter Active Directory on how to configure this.

Create the user groups as described here: User groups.

Then create the users as described here: Users. Make sure you place every new user in the group he or she belongs to. In this example:

● The Overall manager in the top-level group "Organization".
● The Finance manager in the group "Finance Management."
● The Development manager (or managers) in the group "Development Management".
● Regular workers of the Finance department in the group Finance.
● Regular workers of the Development department in the group Development.

A useful set of default permissions has already been defined at the Organization level. These permissions apply recursively through the whole organization. The result of these default permissions is the following:

● Everyone in the organization can playback their own calls.
● Management has full access to the calls of the people they manage (people in subgroups). The Finance manager has access to calls of the Finance department. The overall manager has access to all calls, including the calls of the managers.

It is possible to change the default permissions, or to define extra permissions on the level of groups and users, if the need for this would arise. See Permissions.

If ADFS is used for logging on, Apresa redirects the browser of the user to the website of ADFS. If the user has an active session, the user is redirected back immediately. If the user has no active session, the user needs to input username and password.

3   Overview

See [Setting up the Apresa](#).

3.1   Help

The Apresa web interface has a built-in help. Click on the question mark. This will open a window with help about the page you're currently on.
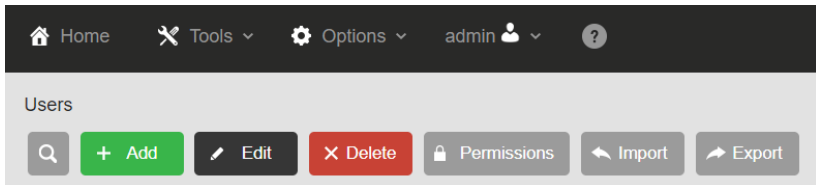
3.2   License Activation

See [Apresa License Activation](#) on how to activate licenses. Licensing is not per user, but per simultaneously recorded call.

3.3   Security Set-up

- [Data Encryption](#)
- [Encryption of the communication](#) (HTTPS)
- [Full disk encryption](#)
- [Encryption of call content](#)

3.4   Import users to autocreate user accounts

If you don't want to create every Apresa user account manually, you can import the users from [Active Directory (LDAP)](#).

3.5 Creating User Accounts and User Groups

- Creating a user group structure.
- Creating user accounts.
- Creating user groups.
- Using Active Directory (LDAP) for sign-on.
- Using ADFS for sign-on.

3.6 Permissions

You can set up Permissions for:
- Call access
- User account editing
- System access

3.7 Users and their telephone numbers

When the required licenses are activated, user groups are defined and users are defined, check if you have all telephone numbers of every user in place.

In the example above, telephone number 122 is assigned to Eric. If Eric logs on to the Apresa, he will be able to listen (on default) to recordings of all telephone calls made by 122. Only those recordings will be shown in his list. They are visible in the Home tab when he logs in. If you want to grant Eric access to all recordings of the group "West", then place him in a higher level group. That is group "Organization" in this case.

3.8   Access Recordings

You can access the call listing by clicking on Home. Here you can play, search for, import and export recordings. See chapter <u>Home, the call listing</u>.

3.9   Recording Features

See <u>recording features</u> about:
- store on demand
- delete on demand
- silence on demand
- recording on demand
- CSTA active recording
- and more

3.10 CSTA active recording

In active recording, Apresa takes part in the call as a third party. There are separate documents available about configuring Apresa for CSTA. Please contact Vidicode for more information. See <u>recording features</u> for a summary.

3.11 Ask the caller permission to store the call

- Store on demand (of the complete call)

Use the <u>VoIP Service</u> to play a notification message and create a rule to store the call when a certain key is pressed.

Or, as a local caller, you can ask the remote caller permission to store the call and use a dial key on your phone to start a recording. See recording features.

- Delete on demand (of the complete call)
See recording features

3.12 Silence a part of the call for privacy reasons

- Silence on demand (to silence a part of the call)
Silence a part of the call, for example if you ask customers for their credit card numbers, and you don't want to include this information in the recordings. See recording features.

- Recording on demand (to record a part of the call)
With recording on demand, you can record a part of the call. See recording features.

3.13 Delete multiple calls

Enable the "Delete recordings" permission and the "Delete multiple calls" permission. Turn on the Recycle Bin when desired. Go to the Home page.

Click on the magnifying glass and perform a search query. Search for the recordings you want to delete.

Click on the List button and select "Delete all calls resulting from search query."

3.14 Delete old calls for privacy reasons

Options → System settings → System tab → Delete calls older than…
Tools → Export & Import → Backup

Let Apresa delete calls older than a number of days, for example to comply with General Data Protection Regulation (GDPR). The retention period of calls in the backup is set separately.

3.15 Screen Recording

Screen recording is possible if the Apresa Client for Windows is running on a pc. The screen of this pc will be recorded during a call.

In the call listing of the Apresa web interface, you will easily see which recordings have screen recordings attached to them. You can watch them and download them.

3.16 Blank a part of a screen recording

See Apresa Client for Windows. You can hide the screen during a screen recording, using the "Silence on demand" feature. This is useful when for example a credit card number is show on your screen. Apresa Client is able to stop screen recording automatically when you open a window with a certain title, for example when you visit the website of a bank in a browser. You can also use hotkeys.

3.17 Start or stop a recording in the web interface

Tools → Web Client

Web Client is a page in the Apresa web interface. After the required permissions and settings are in place, a user can perform actions on active calls, like silencing a part of a call by clicking on a button.

3.18 Start and stop a recording in a Windows app

Apresa Client is PC software for Windows that communicates with the Apresa server. You can use it to start, stop, store and delete a recording.

(In addition, you can use it for screen recording during a call and Free Seating.)

3.19 Adding a note to a call in a Windows app

Apresa Client is PC software for Windows make it possible to add a note during a call.

3.20 Audio Transcription

Stored recordings can be transcribed using VoiceCrunch, an online service that analyses the audio and creates text. In Apresa, the text appears in a note field or in a special transcription field of the recording. These fields are searchable in the Apresa web interface. For this feature a VoiceCrunch account is needed.

3.21 Recording Problems

If you are recording VoIP using port-mirroring, have a quick look at Solving Problems for Passive Recording. This chapter will be a help when you encounter VoIP problems.

3.22 Check the authenticity of a recording

Options → System settings → System → Calculate checksum

Fingerprinting (SHA-2) is a safety feature that will create a "fingerprint" for every recording. The checksum that is generated can be used to prove a recording is the original and has not been tampered with.

3.23 Free Seating

Use the Free Seating feature when employees don't have a fixed desk, but you want to assign recordings to the employee anyway. Use the Apresa Client software for Windows PCs.

3.24 Multi-Tenancy

Multi-Tenancy is a set of features for having multiple tenants on the same installation.

3.25 Software Update

Tools → System → Software Update

The Software update screen is intended for Apresa updates and Debian operating system updates.

3.26 Import, Export and Backup

Make sure to regularly backup your data. See Export and Import for import call data, export call data, backup call data, and configuration backup.

3.27 Watch over Actions of Users with Audit Trail

Tools → System → Audit Trail

The Audit Trail, if enabled, contains information about the actions that each user has performed.

3.28 Monitor Calling Agents with Agent Evaluation

Tools → Agent Evaluation

Agent Evaluation is an add-on which requires an Agent Evaluation License. Agent Evaluation monitors the performance of an agent. Using Call Evaluation, you can assign a score to each call.

3.29 Listen near real-time to calls of your employees

Apresa Call Monitor is PC software to listen to currently active calls in near real-time. The Apresa Call Monitor is PC software that communicates with the Apresa.

3.30 View Apresa Usage with Graphs and Charts
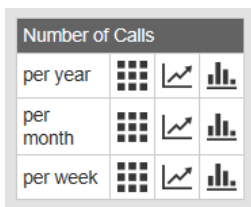
Tools → Statistics

Reach the statistics via the Tools menu.

There are charts for number of calls, local caller, remote caller, time of day, wait time before answer, etc.

3.31 Mobile Phone Recording Set-up

Record calls with your mobile phone and upload them to the Apresa with the Vidicode V-Upload app on your mobile phone. On the Apresa you'll need an External Phone Recording License.

3.32 Recycle Bin

Options → System Settings → System
Tools → Recycle Bin

The Recycle Bin is disabled on default. This means that on default a recording is removed permanently if you delete it.

Enable it by checking the Recycle Bin checkbox at Options, System Settings, System tab. If you delete a recording from this point on, you can restore it from the Recycle Bin of the Tools menu.

Note: From the list button, it is also possible to restore or delete all calls that result from a search query. To use these options, the global 'Delete multiple calls' permission is required and the 'Delete recordings' permission is required for each individual call that you try to restore or delete with these options.

3.33 Integration with CRM or DMS (Apresa API)

Third party software can send commands via HTTPS to the Apresa using the Apresa API to perform certain actions on a recording, such as:
- starting, stopping, storing, and deleting a recording
- requesting a list of active calls
- edit properties of a recording, for example to store the client number of the caller in the notes field of the recording in the Apresa database.

3.34 Integration with SalesForce (CRM)

Options → System settings → Network

Apresa offers integration with SalesForce. When configured, telephone calls recorded by Apresa appear as completed Tasks of the type "Call" in SalesForce. Access the recording by clicking on the link in SalesForce.

Type
Call

Call recording
http://apresa.example.com/play.php?
rem=20210510_145355_o5077

Completed time:
10-05-2021 14:54

3.35 VoIP Service

Tools → VoIP Service

You can use the VoIP Service of Apresa if the call is looped through the Apresa or when the Apresa is involved in the call as a caller, which is the case with CSTA active recording. See recording features.

The VoIP Service supports four actions to apply on SIP telephone calls: Reject, Accept, Forward the call, and Play notification message.

3.36 Play notification messages

Tools → VoIP Service

The VoIP Service plays audio messages based on rules you choose. For example, it plays a certain audio message when a certain telephone number is called or a certain key on the dial pad is pressed.

3.37 Forward calls automatically

Tools → VoIP Service

The VoIP Service forwards calls based on rules you choose. For example it can forward a call to a certain telephone number when the caller presses a certain key.

3.38 Notify the caller that the call will be recorded

The VoIP Service is able to play notification messages, for example if you are using CSTA active recording.

3.39 Call Recording for FRITZ!Box®

Configure the Apresa's VoIP Service to record calls from the FRITZ!Box®. Details are available in a separate FritzBox document.

3.40 Multiple Apresa Servers

Tools → Export & Import → Export to Apresa server

Multiple Apresa Servers can work together using export and import functions. This is useful if you need more than one Apresa:
- if you want to record calls at two or more geographically separated locations.
- if there's a large amount of data that one Apresa can't handle alone.

3.41 Remote access to the Apresa web interface

Tools → System → Encryption → Certificates (HTTPS)
Options → System settings → Network

If you allow access to the Apresa from outside your LAN via the web interface, make sure the connection is encrypted (HTTPS). Create and enable a **certificate** on the Encryption page. Set the Browser protocol to **https** in the Network settings. See Encryption of the communication.

3.42 Customize the login page and page headers

To create a custom login page, and use a custom header for all other pages, upload two required html files to Apresa using SFTP. Details are available in a separate document.

3.43 Automatic system check

Tools → System Information → System Health
Options → System Settings → E-mail

Crucial features and hardware of the Apresa are automatically checked. Errors result in an alarm e-mail notification to a system administrator and / or (optionally) an audio/visual warning. The Apresa is able to send alarm messages and other notifications via SNMP.

4 Home, the call listing

To reach the main call listing, click the "Home" button.

The main call listing displays the list of recorded calls for which you have the "View listing" permission. To view only your own calls, click the "My calls" button.

Menu buttons on the main screen

The Options button may not be visible to you depending on the permissions you were granted by the organization's administrator.

Tool buttons on the main screen

Icon	Description
🔍	Search
📄	Export table (and Delete multiple calls)
▶	Play
⬇	Download recording
🖥	Download screen recording *)
✉	E-mail
✕	Delete

*) This button will only be active if a screen recording has actually been made. It will be greyed out if there is no screen recording associated with the call.

In the example below the user has 'Administrator' permission. This means he or she has access to all calls, the Options menu and the Tools

menu. The columns that are displayed in the call listing can be configured in the Display Settings page.
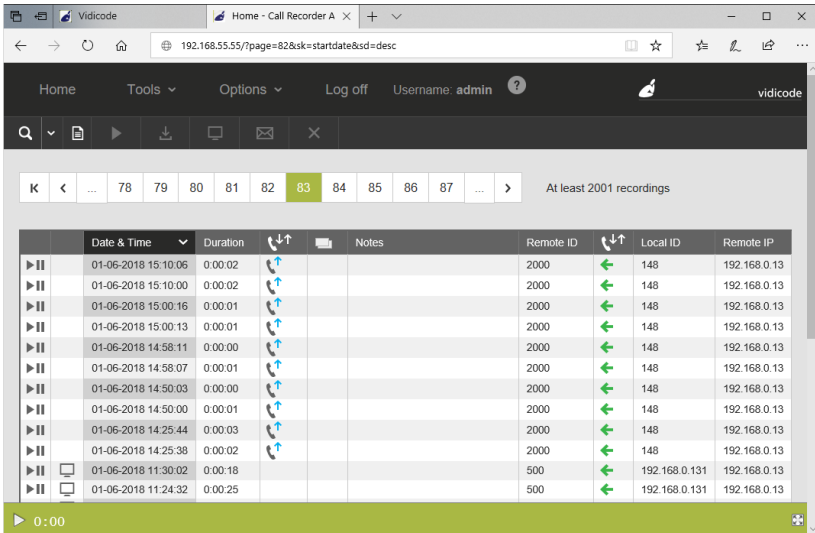
Personal Settings button on the main screen
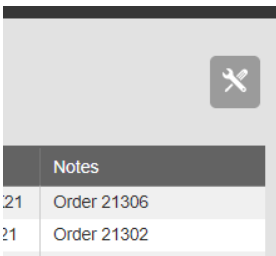
With the Personal Settings button a user can configure his own Home Screen layout, by selecting the **visible columns** from a dropdown menu. This dropdown menu contains a list of columns the user is allowed to see. The contents of this dropdown menu is determined by the general Visible Columns setting from the Display settings.

For this button to show, it is needed that the option "Users can change personal settings" is enabled. This option is found at Options → System settings → System.

4.1   Searching

To search for a recording with certain properties, click **Home** and then the Search button (magnifying glass). You can search for calls in a time

range, a remote or local telephone number or name, and containing specific text in its notes. When searching in text fields, the use of the wildcards * and ? are supported. This allows for the following searches:

Search text	Search for exact match	Result
15	No	telephone numbers that contain "15" anywhere
15	Yes	telephone number "15"
15*	Yes or No	telephone numbers that start with "15"
*15	Yes or No	telephone numbers that end on "15"
1??	Yes	telephone numbers of length three, that start with "1"

To save a query for later reuse, click Save Query, and type a name. Saved queries are shared between all users, and can be accessed by clicking on the small arrow on the right on the Search button. A query can be deleted by pressing the Delete key while the query is highlighted in this menu. You need the Edit Notes permission on all calls in order to add or delete a query.

To cancel the search click the **Cancel** button.

Note: this search function can be used to delete multiple calls. Enable the "Delete recordings" permission and the "Delete multiple calls" permission.

Click on the magnifying glass and perform a search query. Search for the recordings you want to delete.

Click on the List button and select "Delete all calls resulting from search query."

4.2 Exporting the call listing

Click on **Home**. Next to the search button, there is a List button, which gives access to the possibility to export the call listing to CSV format.

List button to export the call listing

Note: when granted the required permissions, you can use the List button to delete multiple calls.

4.3 Access to the recordings

4.3.1 Playback

Click on **Home** to reach the call listing. A recorded call in the call listing can be played back by clicking on the Play symbol in the first column of the table, or by selecting the call, and clicking the "Play" button. Depending on the browser and the settings, playback might be inside the browser or external.

External playback:
The recording might be downloaded to a temporary location on your computer and played back by your default audio player. To prevent this for users that do not have the download permission, enable the system setting "Playback permission allows playback only inside the browser".

Playback inside the browser:

If playback is inside the browser, you will see a media player at the bottom of the Apresa web page. This can be used to pause, and to move to another playing position. If playback is inside the browser, then annotations can be added and displayed in the web interface (see next section)

To playback screen or video recordings, enable the "Special properties of the call" column in the Display Settings. Calls that have a screen recording will show a screen icon. Clicking on this screen icon to play the video.
The video playback can be a multi-screen or a multi-participant recording. Double click on one of the screens to maximize it.
Video recordings based on MP4 can played back in a modern browser. MP4 recordings are made by Apresa Client PRO and the Teams Recording Bot.
Video recordings based on WMV can only be played inside the browser using Internet Explorer (using Media Player). WMV recordings are made by Apresa Client (standard).

4.3.2 Add annotations to a call

Click on **Home** to reach the call listing. If playback is inside the browser, then annotations can be added and displayed in the web interface.

To add an annotation, right-click on the time bar, and choose Add annotation. The annotation will be assigned the first available letter (A, B, C), and it will be placed at the specified time position on the time bar of the media player. The notes of an annotation are displayed when the mouse hovers over the marker. Searching for notes also searches for the notes of the annotations. An existing annotation can edited, moved, or deleted, by right-clicking on it, provided the user has the Edit notes permission.

4.3.3 Download recordings

Click on **Home** to reach the call listing. If you have the Download permission, then it is possible to download single recordings, or multiple recordings in .zip package.

4.3.4 Send a recording by E-mail

Click on **Home** to reach the call listing. When an email address is configured for your user account, it is possible to have the system email the recorded call to you, by clicking the "E-mail" button.

  E-mail button

A confirmation will show up in the Apresa web interface
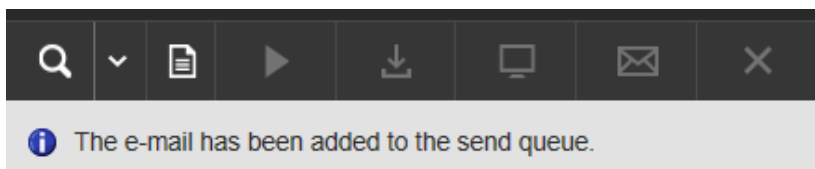
The email has been sent by Apresa. It will show up in your mailbox with the source address your System administrator has specified (Options – System settings – E-mail tab – Source address) with the attached recording.
In the e-mail the search criteria for the recording are stated. The name of the recording contains the date and time of day.

4.3.5 Delete recordings

Click on **Home** to reach the call listing. If you have the "Delete recordings" permission, a call can be deleted by first selecting it and then clicking the Delete button.

⚠️   If the Recycle Bin is enabled in the options, deleted calls are moved to the recycle bin. Otherwise, they are deleted permanently.

4.3.6 Delete all calls resulting from search query

From the menu accessed by the list button, it is possible to delete all calls that result from a search query that you have the 'Delete recordings' for. If no search query has been specified, all calls for which you have the 'Delete recordings' permission will be deleted. This option itself is only available if you have the global 'Delete multiple calls' permission.

See also: [delete multiple calls](#).

4.3.7 Reassigning recordings to another tenant

In a multi-tenancy setup, if the option "Allow administrators to reassign recordings to another tenant" is enabled in the System settings, an administrator can click the Edit icon button, select "Assign recording to another Tenant", and then choose the new tenant for the selected recordings. To see the result, enable the Tenant column. You can enable it in the display settings.

4.3.8 Encrypting or decrypting call content

When call encryption for a tenant is enabled, the tenant administrator can permanently encrypt any previously recorded call that was not encrypted.

For encrypting an unencrypted call, first select them in the call listing. Then select the encrypt call content option from the edit menu. After encryption, the call can only be listened to by providing the password.

The tenant administrator can also permanently decrypt a call. First select an encrypted call in the call listing. Then select the decrypt call content option from the edit menu. After providing the password, this will store the decrypted call on the server. After decryption, the call can be listened to by anyone with the appropriate permissions, without providing the decryption password.

4.4 User data associated with recorded calls

4.4.1 Category
A category can be assigned to each recorded call. This is displayed in the call listing as a colored box (red, blue, etc.). When clicking on it, another color (category) can be selected, if the user has the "Edit notes" permission. Categories can be given names in the System settings.

4.4.2 Notes

To each recorded call, a note can be attached. To fill in a note, click inside the Notes column, type the note, and press OK. To edit a note, the "Edit notes" permission is needed.

		Date & Time	⌄	Duration	☎↓↑	🗨	Notes		Remote ID	☎↓↑	Local ID
▶❚❚		22-06-2018 10:10:53		0:00:44	☎↓						614750143
▶❚❚		22-06-2018 10:08:56		0:00:34	☎↓						31700234654
▶❚❚		22-06-2018 10:07:40		0:00:13	☎↓						393618401164
▶❚❚		22-06-2018 10:06:07		0:00:18	☎↓						448123704834
▶❚❚		22-06-2018 10:01:02		0:00:20	☎↓		OK	Cancel			31649027194
▶❚❚		22-06-2018 09:59:09		0:01:08	☎↓						31386910386

4.5   Telephone numbers and associated names

It is possible to fill in the names of the external and internal callers in the call listing. To attach a name to a telephone number, click inside the "Name of remote" or "Name of local" column, and type the name. To edit names, the "Edit names" permission is needed. Names can also be changed in the Contact List.

4.6   Call direction

The call direction can have four different values:

Incoming
The call was initiated by the remote party.

Outgoing
The call was initiated by the local party.

Internal
The call was between two local parties. The one who initiated the call, is found in the local columns, the one who received the call is found in the remote columns. Note: The remote columns actually contain a local party in this case.

Unknown
This happens when the system can detect audio data only, but no call signaling.

If the "Caller/receiver columns" option (Display Settings) is enabled, the caller columns always contain the one who initiated the call. For call

direction detection configuration, see the related options on the **VoIP** tab in the **System options**.

A second call direction column can be enabled. In the Display settings, this column is called Direction (2). This column displays the call direction as an arrow, from the initiator to the receiver.

The columns displayed in the call listing can be configured in the **Display Settings** page of the Options menu.

5   How to use various recording features

This topic describes how to enable or use various features.

By default, do not record calls. Decide during a call whether to store the complete call.

- Enable store on demand, either for the whole system in the Recording settings, or for some User accounts.
- in System settings, Dial code tab, specify a dial code (e.g. #9), and as action choose "Store this call"

Then during a call, press the configured dial code (e.g. #9) to have the recording stored. Otherwise, it will be deleted.

Do not record a part of a call, by default record

- in Recording settings, enable "Silence on demand"
- in System settings, Dial code tab, specify a dial code (e.g. #9), and as action choose "Start silence"
- do the same for "Stop silence"

During a call, use the defined dial codes to start and stop the silencing.

Record a part of a call, by default do not record

- in Recording settings, enable "Recording on demand", either for all, or for a set of telephone numbers
- in System settings, Dial code tab, specify a dial code (e.g. #9), and as action choose "Start recording"
- do the same for "Stop recording"

During a call, use the defined dial codes to start and stop recording. Each part will be stored as a separate recording.

Stop or delete a recording on demand

- in Recording settings, enable Delete on demand (e.g. for All)
- in System settings, Dial code tab, specify a dial code (e.g. #9), and as action choose "Delete"

During a call, press the defined dial code to stop and delete the recording.

Temporarily stopping screen recording

Use silence on demand.

Remarks about dial code detection in general

- Normally, only dial codes from the local side are processed (see System settings, VoIP tab, Dial code action).

Using CSTA for active recording

At the PBX:

- Enable CSTA
- Create a dedicated SIP phone for the Apresa
- For Unify OpenScape Voice:
    - Enable the Silent Monitoring Agent subscriber feature for each phone that must be recorded.
    - Enable the Silent Monitoring Supervisor subscriber feature for the Apresa phone.

At the Apresa:

- Access Tools, VoIP service, and configure the VoIP Service with the SIP phone settings created earlier, and configure it to accept calls.
- In Options, Recording settings, configure the CSTA phones to monitor.
- In Options, System settings, Network tab, configure the CSTA type, and other CSTA settings.

6   Multi-tenancy

Multi-tenancy is a set of features for having multiple tenants simultaneously use the same installation. The recordings of tenants are logically separated. Tenants can have a number of separate options applied to their data. Other options are applied globally to the whole system.

How to setup multi-tenancy

Options → System settings → System

To use multi-tenancy, in menu Options, open the System settings, System tab, and enable "Multi-Tenancy".
A Tenant is a special user group that has the Tenant option enabled.

Options → Tenants

A new tenant can be created in menu Options, Tenants, Add. (This is the same as adding a new user group, and checking the *Tenant* checkbox for that user group. Make a 'regular' user group a Tenant by checking its *Tenant* checkbox.)

Options → Tenants

Users can be added to a tenant, in the same way as for regular user groups. Users that are member of a tenant group or any of its subgroups, are seen as belonging to this tenant. These users can have one or more user phones (telephone numbers or IDs).

How recordings are assigned to a tenant
If the local (or remote) party of a call matches with one of the user phones, it is assigned to the tenant to which this user belongs. The usual user access control options are applied when matching a call (such as "Usage of SIP ID as identification"). A recording is never assigned to more than one tenant *). If no tenant user phone matches, then the recording is not assigned to any tenant.

> *) the Duplication setting allows tenants to have a private copy of a recording, when a call is recorded between two tenants of the same system. See [Recording Settings](#).

If the option "User access based on Local ID" is enabled, or the option "Assign recording to tenant when call starts" is enabled, recordings are assigned to a tenant (or no tenant), as soon as the call starts. Otherwise the call is assigned at the end of the call, which means that call would not be visible to a tenant user during the call in Active Calls or in the Apresa Client.

Once a recording is assigned to a tenant, it remains assigned to this tenant, even if the user phones of the tenant are changed.

Access to recordings by tenants
Tenant-users can only access recordings that belong to its tenant, even if the user has been given global permission to all recordings.

Tenant options

Options → Tenants

To set specific options for a Tenant, open the Tenants page (Options menu), and Edit the Tenant.

Limitations
Multi-tenancy is not applied to all types of recordings:

Types of recordings	Multi-Tenancy applied
VoIP recordings, and other recordings made using the network	Yes

V-Tap recordings	Yes
Recordings made with a recording card (ISDN, Analog, Digital TDM)	No
Recordings imported from other Vidicode call recorders (using FTP)	No
Recordings imported from another Apresa server	Yes
Recordings imported from Araña	Yes

Note: When using Multi-Tenancy, do not give tenants access to the Contact List, Name of remote, and Name of local fields. Otherwise tenants could see the contacts and names filled in by another tenant. The contact list is a global list, shared by all tenants, so to ensure data separation, do not give tenants access to it.

7 Permissions

Permission are defined at the level of user groups or users. A useful set of default permissions is defined at the Organization level. These permissions apply recursively to all groups in the organization. (see Defining groups and permissions).

7.1 Call access permissions

The following call-related permissions are possible:

Permission	Description

View listing	The list of calls can be viewed.
Playback recordings	Playback of audio recordings of calls is possible.* (excluding screen recordings)
Playback screen recordings	Playback of screen recordings, using Internet Explorer (see also Home)
Download recordings	Call recordings can be downloaded, also multiple at once. Playback of recordings (including screen recording playback) is possible.
Delete recordings	Call recordings can be deleted. Note: the "Delete multiple calls" permission is also needed to delete multiple calls using the search filter.
Edit notes	Notes attached to a call recording can be edited.

*) The handling of playback compared to download is dependent on browser configuration. Playback inside the browser is possible with modern browsers and MP3 encoding, and with Internet Explorer and the Windows Media Player ActiveX. In other situations, the file might be downloaded to a temporary location, and played back from there. See also the System setting "Playback permission allows playback only inside the browser".

The permission applies only to calls of the user or group that is filled in. As a special feature, instead of a specific user or group, it is possible to give permission to calls of users depending on to whom the permission is given:

- **special: itself:** The permission specifies what a user may do with its own recorded calls.
- **special: its own group:** The permission specifies what a user may do with recorded calls from people in his group.
- **special: subgroups of its own group:** The permission specified what a user may do with recorded calls from people in subgroup of his

own group. For example, a manager may access calls from the group he manages.

It is also possible to give a global permission:

- **special: Everyone:** The permission specifies what a user may do with any recorded call

7.2 User account editing permission

Permission	Description
Edit user accounts	When granting this permission, you can specify which user account or which group of user accounts may be edited. A) If **special: Everyone** is specified, then access to all users and groups is granted, except the administrator accounts. All permissions can be set, except the administrator permission. The list of managed phones can be edited. B) If a group is specified, then the user accounts in that group can be edited and deleted, and new users in that group can be added. The group itself cannot be edited. C) If a user is specified, then the user account of that user can be edited. B,C) Users can be moved to another managed group. Permissions can be granted, but only if the manager has this permission himself. A new phone can be added to the list of user phones, but only if it is in the managed phones list of the manager (taking into account wildcards).

7.3   System access permissions

The following system-related permissions are available:

Permission	Description
Tenant Administrator: Audit Trail	Retrieve the audit trail of the users of the tenant (the tenant group of which this user is also a member).
Tenant Administrator: Export recordings	Enable/disable and configure the time schedule of the export of recordings of the tenant (the tenant group of which this user is also a member). The system administrator needs to do configuration of the export destination beforehand (on the command line).
Tenant administrator: Call encryption	This option allows a tenant to set up a password-protected per tenant call encryption.
Web Client	The user can access the web client. In case a user has only this permission or this permission in combination with the edit notes permission, only the web client can be reached and all other pages are blocked, and after logging in the user will immediately be redirected to the web client.
Live Dashboard	The user can access the Live Dashboard using the Tools menu. It provides a configurable selection of live data and statistics.
Access to contact list	The list of external and internal telephone numbers and their names can be viewed. The contact list is system-wide or per tenant.
Edit names	Names attached to a telephone number can be edited. Names are stored in the contact list, which system-wide or per tenant.
Add recordings (API)	This permission can be used by a mobile app or another remote application to upload recordings into the database for this user.

View system info, reset alarm	The system information page can be viewed (which shows the system health status), and resettable alarms can be reset.
Manage user sub-accounts	The user can create new user accounts, but with the restriction that only phones can be added to these account that are also part of his own account. These new user accounts can be managed (edited/deleted) by this user. This can be useful in a multi-tenant situation. New user accounts are created in the same group as the manager. Note: Consider using the "Edit user accounts" permission instead.
Edit recording filters	The recording filters on the Recording settings page can be edited.
Edit configuration (Administrator)	The complete configuration of Apresa can be edited, including user accounts and system settings. This makes the user a full administrator.
Level 2 administrator	Allows access to the following pages: Contact list, Export/import recordings to/from another Apresa, Diagnostics, Users, User groups, Tenants.
Level 3 administrator	Allows access to the following pages: Users, User groups, Tenants.
Delete multiple calls	Allows for the deletion of multiple calls at once with a search filter. In addition, it is still required to have the 'Delete recordings' permission before a call can be deleted via this option.

Lower level administrators are prevented from editing higher level administrator accounts, or assigning higher level permissions.

8   Apresa Client

8.1   Apresa Client Introduction

This chapter is about the Apresa Client, a client for Vidicode Call Recorder Apresa. Apresa Client is PC software that can be used to do screen recording, start and stop recordings, make notes, and perform other actions on active calls. The Apresa Client communicates with the Apresa server machine. It is intended to be used by users or agents that have a telephone that is recorded by the Apresa server. You can use Apresa Client for Free Seating.
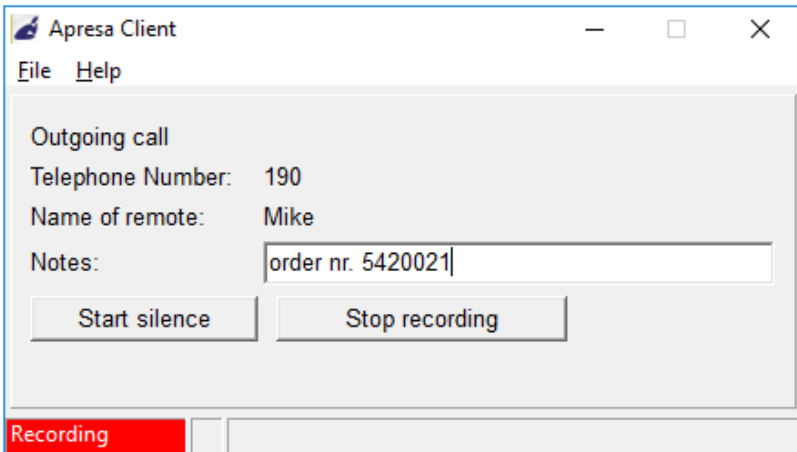
8.1.1   Configuration in the Apresa web interface

Options → Users

For users to use Apresa Client, they must have an enabled Apresa account. To create a user account, open the Apresa web interface and log in as administrator, and move the users screen. When creating the new account, also specify the telephone, or telephones that belong to the user. Calls that involve these telephones, are reported to the Apresa Client, to trigger, for example, screen recording.

8.1.2   Screen recording

Apresa Client for Windows → File → Options → Screen

To enable screen recording, the "Screen recording" option must be enabled in the Options of the Apresa Client. Screen recording starts when a call is initiated or received, and stops when the call stops. The screen recording is then uploaded to the Apresa server. You can download the screen recording of a call in the **Home** tab of the Apresa web interface. Select a call and click on the 'Download screen recording'

 button.

Options → Recording settings

Note: In the call listing of the Apresa web interface, you will easily see which recordings have screen recordings attached to them, if you enable the Visible Column "Special properties of the recording" in the Recording Settings.

Differences between video file formats
Apresa Client creates screen recordings in wmv format. Apresa Client Professional is able to create screen recordings in mp4 format. You can download wmv and mp4 files and watch them on you PC.
Note that wmv files are playable in Internet Explorer, while mp4 files are playable in modern browsers like Chrome, Firefox and Edge.

8.1.3   Blank a Part of a Screen Recording

Options → Recording settings

In the Recording settings of the Option menu, turn on Silence on Demand.

Apresa Client for Windows → File → Options → Hotkey

- Click on the Start Silence edit box and press a key, for example, F6.
- Click on the Stop Silence edit box and press a key, for example, F7.
- Start the call
- Before you are about to view privacy sensitive information, e.g. somebody's home address, press the "Start Silence" key you have chosen.
- Press the "Stop Silence" key you have chosen to continue the screen recording.

- End the conversation

Result: there will be a screen recording, with a blank part in it.

8.1.4   Adding notes during a call

Edit the notes field to add a note to the call.

8.1.5   Closing the Apresa Client

Go to the Apresa Client (in Windows). When you click on the close button ⊠ of the main screen, the main screen will close, but the application will be remain active in the background. To close the application completely, right-click on the Apresa Client icon in the system tray, and choose Exit.

8.2   Apresa Client Menu

File
- Account: Set the username and password for logon to Apresa. This screen can be reached also when the options screen is locked with a password.
- Options: Change the configuration.
- Licensing: Only available in the Professional version for managing the license
- Log Files: Opens in explorer the directory that contains the log files
- Exit: Closes the application

Help

- Contents: Opens the inline manual.
- Check for update: Checks for updates online. Updates can be installed here too.
- About: Show version information.

8.3   Apresa Client Options

Apresa Client for Windows → File → Options

To open the options screen of the Apresa Client, choose Options from

the File menu or click on the ⚒ button.

8.3.1   Apresa Client: account settings

Apresa Client for Windows → File → Options → Account
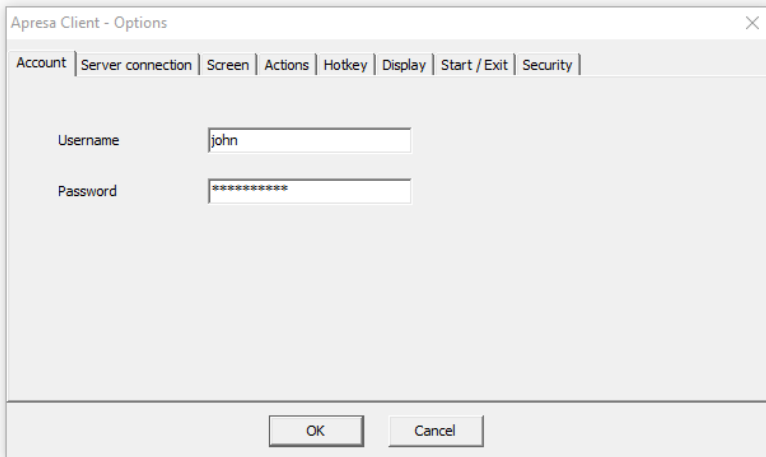
On the account tab, input your Apresa username and password.

8.3.2   Apresa Client: server connection with Apresa

Apresa Client for Windows → File → Options → Server Connection

Apresa Server IP address: The IP address or IP name of the Apresa server. If a non-default port is used, add a colon and the port number, for example: 1.2.3.4:9000

Secured HTTPS connection: When this option is enabled, Apresa Client will communicate with Apresa using the HTTPS protocol. For this to work, it is needed that HTTPS is also enabled and configured on the Apresa server.

8.3.3   Apresa Client: Screen

Apresa Client for Windows → File → Options → Screen

Screen recording: If this option is enabled, a recording of what is visible on the screen will be made during a call, and uploaded to the Apresa server afterwards.

Standard: The standard screen recording method is available by default. Recordings are in WMV format.

Advanced: The advanced screen recording method is available only in the Professional version. Recordings are made in MP4 format. A higher capture framerate might be possible.

FPS: The number of frames per second of the screen recording. A higher value gives a better quality video, but requires more CPU power and disk space.

Continue recording after end of call: The screen recording will continue until the specified number of seconds have elapsed, or until a new call starts.

Merge audio and screen recording: Merge the audio recording, as provided by the Apresa server, with the screen recording. This option is enabled by default. The merging process takes place after completion of the call, and uses much CPU power.

Record multiple monitors in one row: If multiple monitors are recorded, record all the monitors simultaneously in one (wide) row, in one file. For the advanced screen recording method, this is always done. Otherwise, monitors are recorded separately and stored in separate files, and combined together in a compressed zip file.

Screens to record: If the PC has more than one monitor, choose here which monitors should be recorded. The monitors are recorded separately, and the separate screen recordings are uploaded to the server in a combined .zip file. *Known problem:* The mouse cursor is not captured correctly in a multi-monitor setup.

Extra settings for the Advanced screen recording method:

Show mouse clicks: Mouse clicks are visually shown in the screen recording using a colored circle.

GPU acceleration: This can improve the fluency and speed of the capture and lower main CPU usage (enabled by default). Disable in case of incompatibility.

8.3.4   Apresa Client: Actions

Apresa Client for Windows → File → Options → Actions
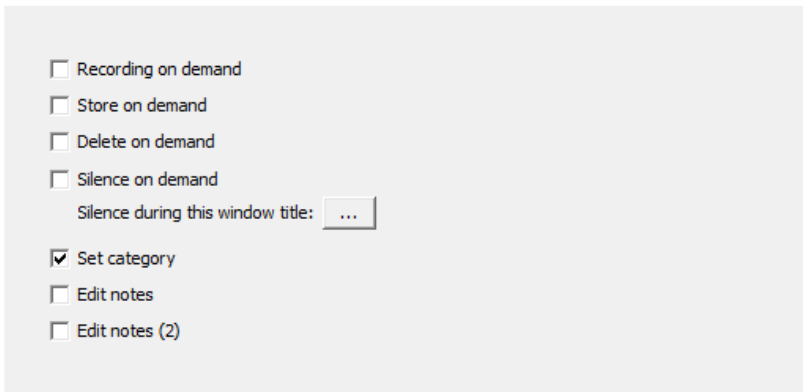
Recording on demand: Shows a button "Start recording" to start recording of a call "on demand" at the click of the button. For this to work, "Recording on demand" must be enabled for the local telephone number or channel.

Store on demand: If this option is enabled, a button "Store this call" is displayed in the main screen. When this button is pressed, the current call will be stored. This option is only relevant when the option "Store on demand" is enabled in the Recording options on the Apresa Server.

Silence on demand: If this option is enabled, a part of the recording of a call can be silenced by pressing the "Start silence" button during the call. To start recording audio again, press the "Stop silence" button. When portion of a call is silenced, the screen recording will be blanked out as well. This option only works if "Silence on demand" is enabled in the Recording options on the Apresa Server.

Silence during this window title: Click the [...] button to define the window titles to scan for. If an application window is found that contains the specified text in its title, silencing will be activated automatically. Screen recording is also blacked-out when silencing. The window title of browsers usually contain the title of the web page that is visited.
It is possible to let it scan for multiple window titles. If one of them is present, silencing is activated. When none are present anymore, silencing will again be deactivated automatically.

Manually enter the window title in the text box, or choose from one of the currently detected window titles (click the small drop-down arrow button). Then press Add to add the window title to the list of items to scan for.

To edit an existing item, select it, edit it using the text box, then press the Edit button.

To delete an item, select it, then press Delete.

When the configuration is correct, press OK.

Set category: If this option is enabled, a call can be assigned to a category. Categories are defined on the Apresa server (Options, System settings, Category tab).

Edit notes: If this option is enabled, notes can entered during a call and saved. The user must have the permission to edit the Notes field.

Edit notes (2): The same for the secondary notes field.

8.3.5   Hotkey

Start recording	Ctrl + Shift + F7
Stop recording	Ctrl + Shift + F8
Start silence	Ctrl + Shift + Alt + S
Stop silence	Ctrl + Shift + Alt + S
Delete	Ctrl + Alt + D
Store this call	None

Hotkeys are keyboard shortcut combinations to do an action (such as starting the recording), even when the program is in the system tray, and you are working in another application. The shortcuts can use Ctrl, Alt, and Shift, and a combination of those, plus another key on the keyboard, for example: Ctrl + Shift + X. Single keys are not accepted as hotkey. When using only the Shift key, only the function keys (F..) are accepted. When a hotkey is defined, the key combination might have no longer any effect in other applications, so choose carefully to avoid conflicts (for example, don't define Ctrl + S as hotkey). To define a hotkey, place the cursor in the edit box, and then press the key combination. To remove a hotkey, press Backspace. It is allowed to reuse a key combination for multiple purposes, for example, it is allowed to have one key combination for both starting and stopping the recording.

8.3.6 Display
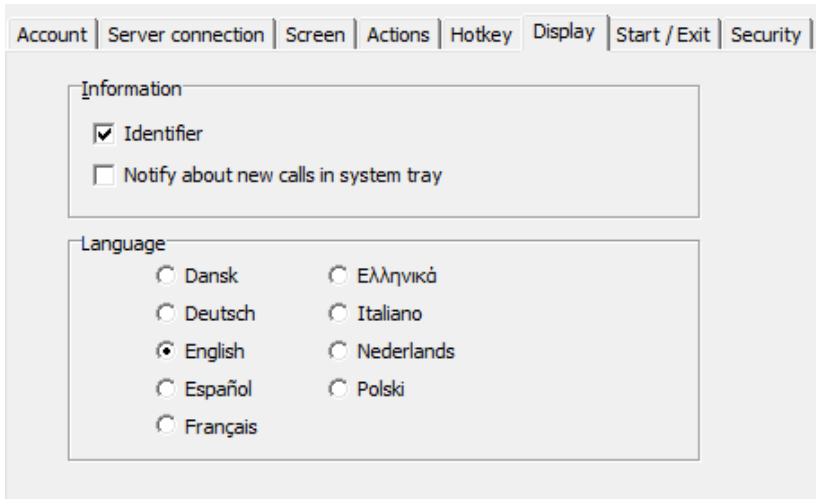
Information:

- Identifier: Displays a unique identifier (ID) of the call, that can be used later to lookup the call in the web interface.
- Notify about new calls in system tray: If the program is active in the system tray (main window closed), and a new call is detected, this is shown in a notification message. Clicking the message opens the main window.

Language:

- The interface language can be chosen here: Danish, German, English, Spanish, French, Greek, Italian, Dutch or Polish.

8.3.7   Start / Exit
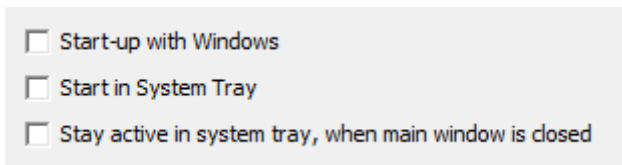
Start-up with Windows: Start the program at logon in Windows.
Start-up in System Tray: Start the application in the system tray (the lower right area in Windows).

Stay active in system tray, when main window is closed: When this option is on, the software will move to the system tray and continue to record calls, when the main window is closed. To completely close the software, right-click on the system tray icon, and select Exit, or choose File, Exit from the main menu.

8.3.8   Security

Password for options: The specified password must be entered before this settings screen is opened.

8.4   Apresa Client Licensing

Move a license to another PC
On the old PC, start the software, choose Menu, Licensing.
Then click the Deactivate button.
The uninstall program will also attempt to deactivate.
Then Activate the key on the new PC.

Offline activation
Perform normal license activation. When the program detects it
Cannot reach the server, it will display information for offline activation.
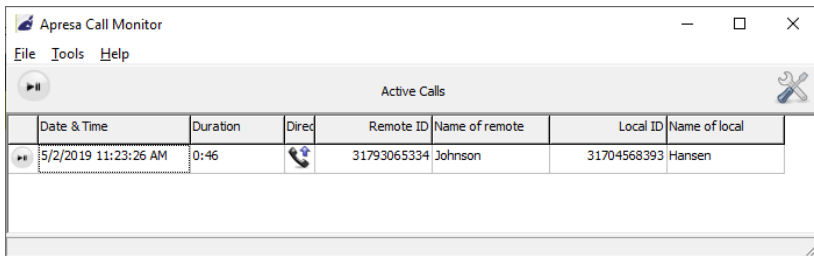
8.5   Apresa Client: free seating

The user chooses a seat to work from. With Apresa Client, running on the PC of this seat, he logs on to the Apresa with his username and password. See Free Seating for more information.

9   Apresa Call Monitor

The Apresa Call Monitor is a client for the Call Recorder Apresa from Vidicode. Apresa Call Monitor is PC software that provides the possibility to listen to currently active calls in near real-time. The Apresa Call Monitor is PC software that communicates with the Apresa server machine to get its data.

9.1   Call Monitoring

Options → Recording settings → Call monitoring

Initial server configuration
To do call monitoring, this option must be enabled on the Apresa Server. Call monitoring uses resources of the Apresa server, and for this reason, it is not enabled by default. To enable call monitoring:

1. Open the Apresa web interface and log in as administrator.
2. Open the Options menu, and choose Recording settings.
3. There, enable the option Call monitoring.
4. Click Apply, and let the recording component restart

Call monitoring
In the main screen, the list of active calls is displayed. This list is updated automatically when new calls arrive or stop. The same permission rules that apply in the Apresa web interface, also apply to the Call Monitor client. In other words, to monitor a call, you must have permission to playback the call.

In the screen above, there is one call active, an internal call from John (300) to Mike (149).

To start monitoring a specific call, do one of the following:
- double-click on the call
- or click the play button in the first column of the call
- or select the call, and press the play button at the top left of the window

The call that is currently monitor (played back), has the following symbol in the first column: audio

To stop monitoring a call:
- press the play/pause button at the top left of the window
- or start the monitoring of another call

9.2   Apresa Call Monitor Options

Open the options screen, click on the button with the   symbol.

Apresa Call Monitor → 🛠 → Account

Account
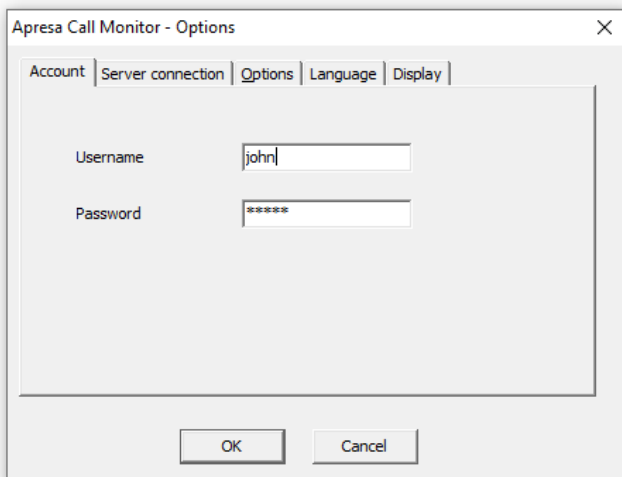
On the account tab, input your Apresa username and password.

Server connection

Apresa Server IP address: The IP address or IP name of the Apresa server. If a non-default port is used, add a colon and the port number, for example: 1.2.3.4:9000
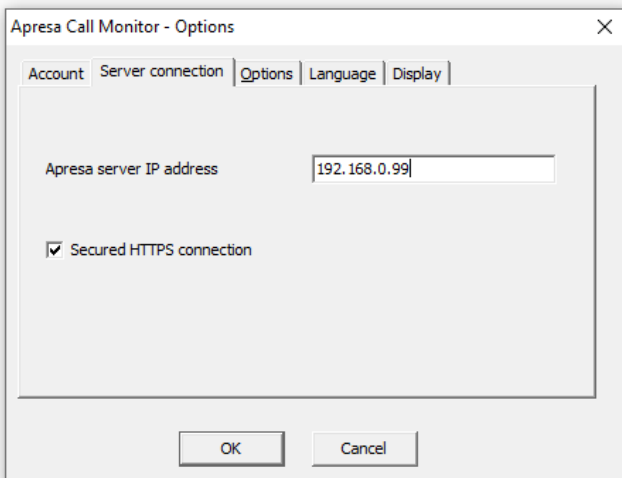
Secured HTTPS connection: When this option is enabled, Apresa Client will communicate with Apresa using the HTTPS protocol. For this to work, it is needed that HTTPS is also enabled and configured on the Apresa server.

Options
Automatically starting monitoring when a new call starts: When a new call starts, call monitoring for that call is started automatically if call monitoring is not yet active.

Language
The interface language can be chosen in the Language tab.

Display
Here you can choose which columns should be visible in the Apresa Call monitor.
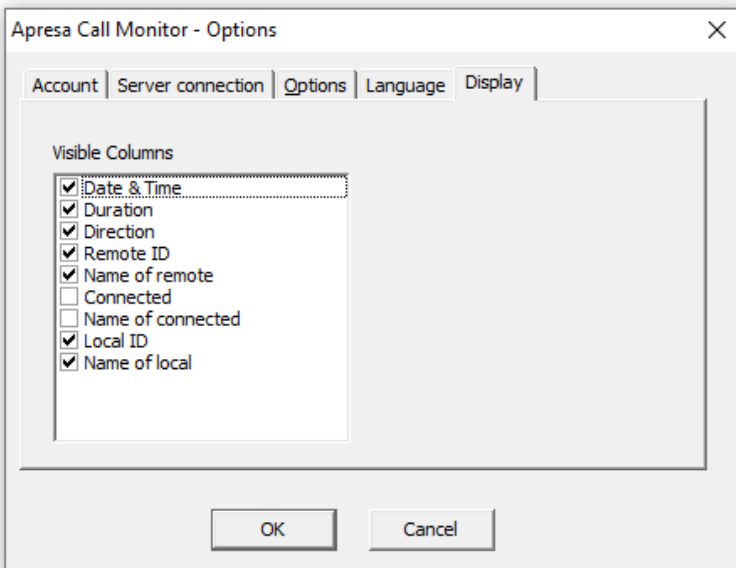
10 Free Seating

There are many reasons why it is important to know which employee has made a certain telephone call. When your company uses free-seating, you might need to do some extra configuration.

The Apresa will try to detect which user makes a phone call, and store this information in the Apresa database.

10.1 No free seating: the telephone has one user

If a telephone has one user, fill in the telephone number in the settings page of the user. The calls made with this telephone will be assigned to the user.

10.2 Free seating: the telephone has more than one user

When a company uses free-seating, employees don't have a fixed seat. For example, a seat consists of a PC and a telephone. The other employees work during other shifts or they have chosen other seats to work from.

10.2.1 When you don't need the Seats Configuration
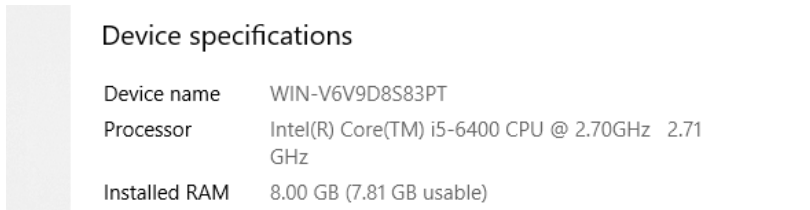
The Apresa will try to detect the user from the protocol data, for example when a user has his own unique telephone number, or when the Apresa can detect the log in of the user. Fill in the unique telephone number in the settings page of the user. You'll find the telephone number in the call listing of the Apresa, when this telephone made at least one call.

10.2.2 When you need the Seats Configuration

If the Apresa can't assign a call to a user in the ways described above, you might want to use the Seats Configuration.

The Seats Configuration only works if you install the Apresa Client for Windows on the PC of a seat. First make sure the Apresa Client works without the Seats Configuration. Then continue.
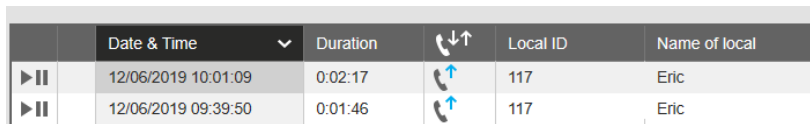
Find the exact name of the PC in the Windows Settings.

Find the caller ID of the phone in the Home Screen of the Apresa. In this example the local ID is "117", but in many cases it is a MAC address.

Go to Users of the Options menu and click on a user. Click the "Edit" button and click on the link to the Seats Configuration. Assign a telephone to a PC there. Fill in the exact name of the Windows PC (for example "WIN-V6V9D8S83PT"), and fill in a number that identifies the telephone. This can be:
● a channel number (non-VoIP)
● a caller ID (VoIP)

In this example PC "WIN-V6V9D8S83PT" and telephone "117" make up a seat. Fill in all seats, on separate lines, that you want to make available. Please note the extra comma.

The following CSV format is expected.
Name of the PC,ChannelNumber,Caller ID
Specify either a channel number (non-VoIP), or a caller ID (VoIP). Show
example

Seats configuration

WIN-V6V9D8S83PT,,117

Save   ✕ Cancel

Turn on "User account for free-seating" for every user that will use free seating.

The configuration is completed.

The user chooses a seat to work from. With Apresa Client, running on the PC of this seat, he logs on to the Apresa with his username and password. Apresa Client will send the name of the PC (e.g. "WIN-V6V9D8S83PT") and the user name (e.g. "Eric") to Apresa. In the Seats Configuration "WIN-V6V9D8S83PT" and "117" make a seat. Therefore Apresa will assign calls made by telephone "117" to "Eric". This way Apresa is able to assign telephone calls to a user.

11 Apresa License activation

11.1 Apresa Base Key License Activation

The Apresa Base Key License is essential for the system to work.

If you bought the Apresa "Software Only" version, install the Apresa on a server (or virtual server) and then activate the base key license. This license key starts with 42. Select compatibility mode licensing if this is a reinstallation on the same hardware and you want to reuse existing keys that were activated on an older version of Apresa, or on a new version with activated compatibility mode.

Open a browser on a pc.
Go to the web interface of the Apresa, for example 192.168.55.55.
Login with your username and password.
You will only see the "Software activation" link if your base key license is not activated yet. Click on this link.
Enter the license key.
Copy (with Ctrl+C) the activation request code.
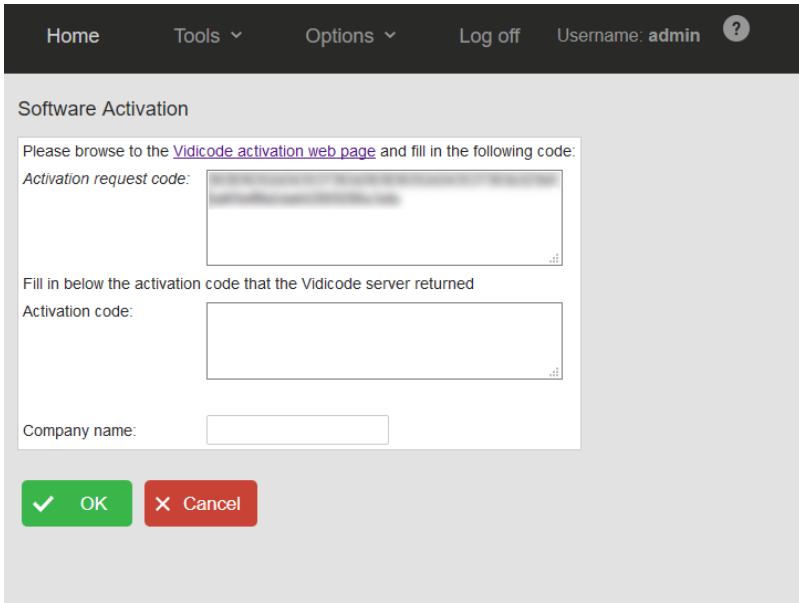
Click on the link "Vidicode activation web page"
(You can also reach the Activation web page if you browse to
www.vidicode.com/activation)
The webpage "Apresa System Activation" has two boxes to fill in.

Apresa System Activation

Activation request code: [   ]

Company name: [   ]

[Send activation request]

Paste (with Ctrl+V) the activation request code into the input box
named "Activation Request Code"
Fill in "Company name" and press "Send activation request".
The same webpage will show you the activation code.
Copy (Ctrl+C) the activation code.
In your browser, return to the web interface of the Apresa

Paste (Ctrl+V) into the input box "Activation code".
Enter "Company name" and press ok.
The activation of the base software of the Apresa is completed.

After the base license is activated, the system will have a software serial number assigned, and you can start adding additional licenses for recording channels, and for software updates.

11.2 Apresa Channel License Activation

Vidicode offers, among others, the following licenses to record telephone calls:
- 1 VoIP channel license
- 5 VoIP channel license
- 10 VoIP channel license
- 1 Analog channel license
- 8 Analog channel license
- 1 TDM channel license
- 8 TDM channel license
- 6 ISDN E1/T1 channel license

- 1 External device recording license

Go to the **Options** menu and click on **System Settings**. Go to the **System** tab of the System Settings page. To activate the license, click on the link *Activate new channels license*.

System	Alarm	Schedule	Network	VoIP	Dial code	E-mail	Category

Software serial number:		80321
System name:		
License key:		Activate new channels license

This will send you to the following page on www.vidicode.com:

Apresa Channel License Activation

License key:		
Software serial number:	80321	(8xxxx)
E-mail address:		

Send data

Fill in the license key and an e-mail address. Click **Send data**. Another license key will be displayed:

Apresa Channel License Activation

License key:

9015-9015-9015-9015

To complete the activation:

- Open the Apresa web interface
- Log on as administrator
- Open the Options menu, and choose System settings
- Copy the license key from this page, and paste it into the Apresa web interface, in the License key input box
- Press Apply.

Activate another license key

Go to the **System** tab of the **System Settings** page and fill in this license key .

Click the **Apply** button to confirm.
The activation of the channel license is completed.

11.3 Agent Evaluation License Activation

Go to the **Options** menu and click on **System Settings**. Go to the **System** tab of the System Settings page. To activate the license, click on the link *Activate new channels license*.

Activating the Agent Evaluation License works the same as activating a Channel License. See Apresa Channel License Activation and follow those instructions to complete the activation.

11.4 Apresa S & U License Activation

By installing the S&U-license, you are assured of support and free upgrades for your Apresa call recorder system. The first year of the S&U-license comes free of charge with every new Apresa system delivered.

> *Note: It is recommended to activate the channel licenses first.*

Your dealer will contact you when the validity of the S&U-license is about to expire, so action can be taken in time to renew the S&U-license. S&U-licenses are available with a 1-year or 3- year validity period.

Needless to say, but the operability of Apresa as a reliable and functional machine is NOT compromised in any way by an expired S&U-license. Only the ability to upgrade the Apresa-base-software and support from the Vidicode customer support dept. is no longer available.

KEEP YOUR APRESA LICENSE FORMS SAFE

You may need these in the future if you want to re-install the software, recording channels, etc. for whatever reason.

START OF THE INSTALLATION OF THE S&U-LICENSE

To install the S&U-license follow the steps listed below:

• Open the Apresa web server interface, log on as administrator;
• Click on System Settings from the Options menu;

System	Alarm	Schedule	Network	VoIP	Dial code	E-mail	Category

Software serial number:	80582	
System name:		
License key:		Activate new channels license
Number of channels:	260	
G.729 decoding channels:	6	
RT-Audio decoding channels:	0	
External phones:	10	Configure
Software updates until:	26-05-2021	Renew service license

• Click on "Renew Service License" , you will be redirected to the Vidicode License Server;

Apresa Service License Activation

License key:	
Software serial number:	80582
System description:	260 x VoIP, 6 x G.729, 10 x Mobile, Agent Evaluation
Customer company name:	
Dealer company name:	
E-mail address:	

Send data

• Enter the S&U-license key (with dashes), customer company name, dealer company name;

• Enter your e-mail address; (used for renewal notification)

• Copy the generated license key, and paste it to the "License key" input box of the Apresa web interface;

System	Alarm	Schedule	Network	VoIP	Dial code	E-mail	Category

Software serial number:	80321
System name:	
License key:	Activate new channels license

• Press apply;

The activation of the S&U license is completed.

• Check the "Software updates until" field this must show the new expiry date.

G.729 decoding channels:	6	
RT-Audio decoding channels:	0	
External phones:	10	Configure
Software updates until:	26-05-2022	Renew service license

11.5 External Phone License Activation

External phone license activation is discussed in a separate chapter in this manual.

12 External phone recordings configuration

How to set up the upload of **mobile phone** recordings to Apresa.

Vidicode V-Upload is an app available on the Google Play Store. The app supports upload to Apresa from call recorder applications on your mobile phone, including: Total Recall, ACR Call Recorder, Xiaomi's built-in recorder, Zoiper, and MizuDroid.

On the server side, you will need the following:

12.1 External phones licenses

Options → System Settings → System

How to set up the upload of mobile phone recordings to Apresa.

On the server side, you will need the following:

- External phones licenses (1 per mobile phone)

You'll need one External phones license per mobile phone.

Go to the **System** tab of the **System Settings** page. To activate the license, click on the link *Activate new channels license*.

This will send you to the following page:

Apresa Channel License Activation

License key:

Software serial number: 80321 (8xxxx)

E-mail address:

[Send data]

Fill in the External Phone Recording license key and an e-mail address. Click **Send data**. Another license key will be displayed:

Apresa Channel License Activation

License key:

9015-9015-9015-9015

To complete the activation:

- Open the Apresa web interface
- Log on as administrator
- Open the Options menu, and choose System settings
- Copy the license key from this page, and paste it into the Apresa web interface, in the License key input box
- Press Apply.

Activate another license key

Go to the **System** tab of the **System Settings** page and fill in this license key .

System	Alarm	Schedule	Network	VoIP	Dial code	E-mail	Categ

Software serial number: 80321

System name:

License key: 9015-9015-9015-9015

Click the **Apply** button to confirm. After the activation of the first external phone license, the Options menu has a new option: **External phones**.
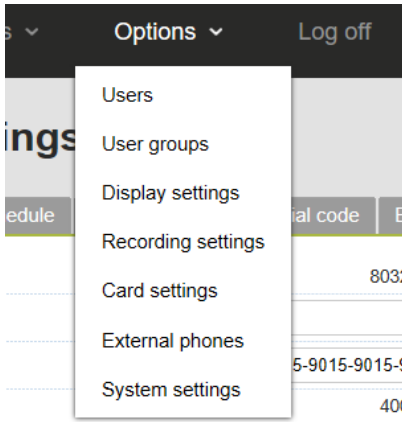
Go to the External phones page via the menu, or click **Configure** next to External phones on the **System** tab of the **System Settings**.

12.2 External phones configuration

Options → External phones

The number of external phones is limited by the license count. You can specify here from which external phones recordings will be accepted.

The external phones are identified by their phone number (this will become the Local ID in the call listing), or in the case of mobile phones possibly their IMEI number.

Input the telephone numbers one per line. For mobile phones, optionally add a comma, and specify the IMEI. Use one line per device.

Example:
43-904265-647083-1 , +43732204034
43-954305-737086-5 , +43732204038

Alternatively, this list can be linked to the users of a group. Select the group, and select which property of the users to use to fill this list. In this case, the list is not edited manually, but filled in automatically.

The user needs to have "Add recordings (API)" permission. See the picture below.
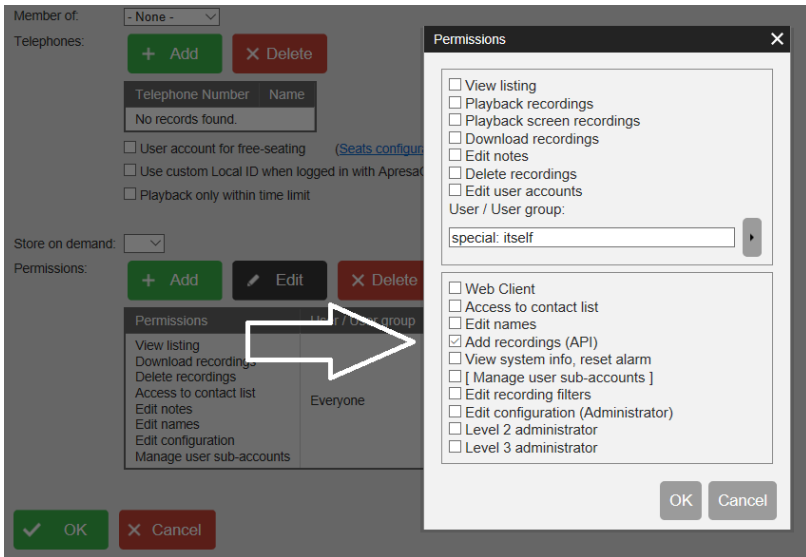
The user needs to have the Local ID as one of its Phones.

Make sure the Apresa server is properly secured (updated with Debian security patches, use https not http).

The Vidicode V-Upload mobile phone app supports upload to Apresa.

On the mobile side, use the same user account credentials for uploading.

13 Data Encryption

13.1 Encryption of the communication

Tools → System → Encryption → Create a certificate
Options → System settings → Network

Apresa can provide a secure HTTPS web interface, to prevent that web pages or downloaded recordings are intercepted by a third party. HTTPS can be enabled on the Network tab in the System settings, after a certificate has been enabled on the Encryption page.

> Remote-access to the Apresa system shell, when enabled, is possible using the SSH protocol, which is an encrypted protocol.

13.1.1 HTTPS for encryption of the communication

Tools → System → Encryption → Create a certificate
Tools → Certificates → Create a certificate
Options → System settings → Network

Encryption of the communication between Apresa and the user of the web interface can be established using HTTPS. There are a number of ways to create a certificate.

- Let Apresa create a self-signed certificate.
- Use a certificate from Let's Encrypt CA.
- Generate a certificate sign request to obtain a signed certificate from another CA. Upload this certificate to Apresa.
- Uploading a certificate to Apresa.

13.1.2 HTTPS - the certificate is self-signed by Apresa

Choose **Certificates** from the Tools menu.
In the Certificates tab, click the Add button.
Fill in Name, Days valid and IP Name or IP Address.

Create a certificate

Name:	ApresaCert
Days valid:	365
IP Name or IP Address:	apresa.company.com

Other fields are optional. Click on the Advanced checkbox for advanced options. After filling in this form, click Ok. You will see the following page:

Certificate

Name:	ApresaCert	
Common name:	apresa.company.com	
Trusted:	☐	
Private key:	✔	
Web server access to the private key:	☐	(SAML)
Show certificate information:	☐	
Used for:	**Used for**	
	HTTPS (System settings)	

The Certificate has been created. To enable HTTPS, go to Options, System Settings, Network tab. Choose **Browser protocol** "HTTP + HTTPS" or "HTTPS". Choose the certificate that has been created from the dropdown list of **HTTPS Certificate**. In this case "ApresaCert (apresa.company.com)".

NTP server address:	0.pool.ntp.org	Test
Browser protocol:	HTTP + HTTPS ⌄	
HTTPS Certificate:	ApresaCert (apresa.company. ⌄	Certificates
Azure	☐	

At the bottom of the page, click **Apply**. This completes setting up HTTPS.

Use HTTPS instead of HTTP to visit the Apresa web interface. Note that when a self signed certificate is used, warnings may be generated or the certificate may be rejected entirely. See Creating a self signed certificate in this document for more details.

13.1.3 HTTPS - the certificate is from Let's Encrypt CA

Tools → Certificates → Let's Encrypt → Register

Choose **Certificates** from the Tools menu.
In the Certificates tab, click the **Let's Encrypt** button. Click on **Register**.
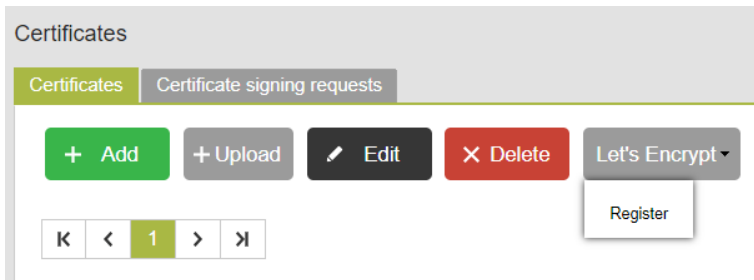
Register:
Before a certificate can be requested, it is required that an account is created at Let's Encrypt and that their subscriber agreement is accepted. The E-mail address provided here will be used by Let's Encrypt to notify you when a certificate is about to expire.

See Let's encrypt certificates in this document for more information.

After the certificate is created, enable HTTPS as follows. Go to Options, System Settings, Network tab. Choose **Browser protocol** "HTTP + HTTPS" or "HTTPS". Choose the certificate that has been created from the dropdown list of **HTTPS Certificate**.

13.1.4 HTTPS – the certificate is from another CA

Tools → Certificates → Certificate Signing requests

Take the following steps to enable HTTPS using a certificate from another Certificate Authority (CA):
- Generate in Apresa a Certificate Signing request.
- Download the Certificate Signing request.
- Send the Certificate Signing request to the CA.
The CA responds by sending a signed certificate.
- Upload the signed certificate to Apresa.
- Adjust the network settings: Browser protocol and HTTPS Certificate.

Generate in Apresa a Certificate Signing request
Choose Certificates from the Tools menu, and click on the Certificate Signing requests tab. See Certificate signing request in this document for details.

Download the Certificate Signing request
Choose Certificates from the Tools menu. Click on the Certificate signing request. Click on Edit. Click on Download the Certificate Signing request.

Send the Certificate Signing request to the CA
You can send the download certificate signing request to the CA.

Upload the signed certificated sent by the CA to Apresa
Choose Certificates from the Tools menu. Click on Upload. See Upload a certificate in this document for details.

Adjust the Network settings
After the certificate is uploaded, enable HTTPS as follows.. Go to Options, System Settings, Network tab. Choose **Browser protocol** "HTTP + HTTPS" or "HTTPS". Choose the certificate that has been created from the dropdown list of **HTTPS Certificate**.

13.1.5 HTTPS – Upload a certificate

It is possible to upload a certificate to Apresa.

Choose Certificates from the Tools menu. Click on Upload. See Upload a certificate in this document for details.

After the certificate is uploaded, enable HTTPS as follows. Go to Options, System Settings, Network tab. Choose **Browser protocol** "HTTP + HTTPS" or "HTTPS". Choose the certificate that has been created from the dropdown list of **HTTPS Certificate**.

NTP server address:	0.pool.ntp.org	Test
Browser protocol:	HTTP + HTTPS	
HTTPS Certificate:	ApresaCert (apresa.company.	Certificates
Azure	☐	

13.2 Encryption of the stored data

13.2.1 Full disk encryption

Full disk encryption can be chosen **during installation**, and it will encrypt everything on the hard disk except the boot sector. Full disk encryption cannot be disabled or enabled later on. During reboot, it requires that a pass phrase is entered with a keyboard (connected directly to the system), in order to unlock and start the system. If the pass phrase is lost, it is impossible to recover the data, or even to start the system.

When data is accessed using the web interface, the data is sent in decrypted form. In order to secure this communication, consider using HTTPS (see above). When data is exported using backup, the data is also sent in decrypted form. You can secure this communication with HTTPS.

13.2.2 System-Wide encryption of call content

Tools → System → Encryption → Encryption of call content

As an alternative to full disk encryption, the call content of recorded calls can be encrypted. This option can be switched on and off in the

web interface. When enabled the call content of **new calls** will be encrypted. Call meta data, such as the start and stop time, and the telephone numbers, will not be encrypted. Only the audio (or video) content of calls will be encrypted.

Encryption of new calls

Call content encryption can be enabled on the [Encryption page](#). You can choose a pass phrase there. You will be asked to restart the recording component to let the changes to take effect.

Prevent playback and download of encrypted calls

When the Apresa system is rebooted, the recording of calls will continue, and the web interface will be available, but playback will be impossible. In other words, decryption of the call content will be unavailable, for security reasons. In order to enable playback (decryption), the pass phrase must be entered. In the web interface, there will be a warning displayed, that this must be done. The pass phrase can be entered using the web interface. This pass phrase is used by the system to unlock the playback possibility. This is a one-time procedure, for as long as the Apresa system remains switched on. As long as it is on, playback will continue to be possible, until the next reboot.

When data is accessed using the web interface, the data is sent in decrypted form. This way you can playback audio files in your browser or download unencrypted, playable audio files from the Apresa. In order to secure this communication, consider using HTTPS (see above).

When data is exported using backup, the encrypted call content will be stored at the backup location in encrypted form. That is in unaltered form.

13.2.3 Per-tenant encryption of call content

Tools → Call encryption

Call content encryption can also be applied per-tenant separately. This feature works very differently compared to the system-wide call encryption described above. For tenant call encryption, the decryption of call content happens in the web browser of the user that wants to play or download the recording. To play or download an encrypted call, a password is required. Each tenant can set its own password. The password itself is never sent to Apresa and no decryption is happening

on Apresa for playback. Once a call has been encrypted, nobody without the password is able to decrypt the calls. This also includes system administrators. If the password is lost, it is not possible to retrieve the calls.

The tenant call encryption feature allows for the encryption of the recordings of a tenant. Only the call contents are encrypted. Call meta data, such as telephone numbers, is not encrypted.

Tenant call encryption can be configured on the tenant call encryption page by a tenant administrator who has the following permission:

Tenant administrator: Call encryption

This permission allows a tenant to set up a password-protected per tenant call encryption. This is done at Tools → Call encryption.

For playback and downloading of tenant encrypted calls, a modern browser is required. The following browsers are known to work:
- Firefox
- Chrome
- Chromium-based Microsoft Edge
- Safari
Internet Explorer will not work.

Enabling tenant call encryption brings a few limitations
- HTTPS is required. Playback, downloading or changing the encryption settings cannot be done over plain HTTP.
- Screen recordings and card recordings are currently not encrypted with this method.
- Encrypted calls that are exported to another Apresa will not be usable there.
- For backup purposes it is important to note that recordings are stored in an encrypted format that is not self-contained. Restoration of these calls to a playable state will always require a copy of the database as well.

14 Active Directory

14.1 Possibilities

● Log on to Apresa with Active Directory

For every user, you can select log-on method LDAP (Active Directory). When the user logs on, Apresa checks username and password remotely on the Active Directory server. If it matches, the user is allowed access to the Apresa.

● Import a user group from Active Directory

Apresa can import a user group from Active Directory, and then continue to update the Apresa group by synchronization with the Active Directory user group(s).

The username is used as identification. Name, email address, and telephone number are imported and updated from AD. The password is not imported, but checked during log-on. When automatic synchronization is on, changes that are made in Active Directory will be applied automatically to the user group in Apresa.

14.2 Enable LDAP log on method for a user

Options → System settings → Network
Options → Users

● Go to the network tab in the System settings. Scroll to "AD server address (LDAP)". Click on the Add button. This opens a window.

Fill in the AD server address, AD user domain and LDAP Domain.

- **AD server address (LDAP):** The IP address or IP name of the Active Directory or LDAP server, on which to check username and password during log on, for the users for which this is enabled. Multiple servers can be added. For example:

  dc1.company.com

- **AD user domain:** The Active Directory (Windows) domain name to use, when checking a username. Users are logged in using DOMAIN\username. For example:
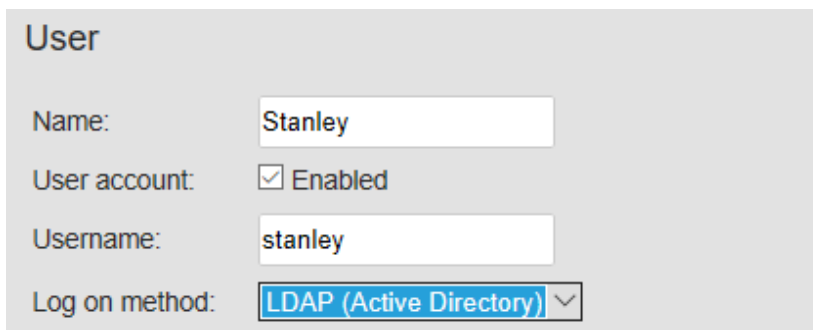
  COMPANY

- **LDAP Domain:** The distinguished name of the organization. For example:

  company.com

In this example, the connection string used by the Apresa will be: LDAP://dc1.company.com/CN=COMPANY,DC=company,DC=com

- After filling in the fields, click on Ok. This applies the settings and closes the window.

- Go to the Users page via the Options menu.

- Select a user and click on the Edit button. Choose LDAP (Active Directory) as Log on Method.

When the log on method LDAP (AD) is selected, and the user logs on, the username and password are checked remotely on the Active Directory or LDAP server. If it matches, the user is allowed access to the Apresa. This means that you do not have to define the password in the Apresa, only the user name. The AD server address and AD user domain that is used during log on, is read from the Network settings.

14.3 Import an Active Directory Group to Apresa

Options → System settings → Network
Options → User groups

- Go to the network tab in the System settings. Scroll to "AD server address (LDAP)". Click on the Add button. This opens a window.

Fill in the five fields.

- **AD server address (LDAP):** The IP address or IP name of the Active Directory or LDAP server, on which to check username and password during log on, for the users for which this is enabled. Multiple servers can be added. For example:

    dc1.company.com

- **AD user domain:** The Active Directory (Windows) domain name to use, when checking a username. Users are logged in using DOMAIN\username. For example:

    COMPANY

- **LDAP Domain:** The distinguished name of the organization. For example:

    company.com

When browsing for groups, the LDAP search query would then search within DC=company,DC=com. In the Group settings, if you link a group to AD, you can specify an LDAP group which resides below the LDAP Domain specified here.

- **LDAP User:** The LDAP user account to be used when searching the Active Directory for user groups, and importing the user details. For example:

administrator

- **LDAP Password:** The password of the LDAP User.

In this example, the connection string used by the Apresa will be:
LDAP://dc1.company.com/CN=COMPANY,DC=company,DC=com

- After filling in the fields, click on Ok. This applies the settings and closes the window.

- Fill in the settings in the Network tab of the Options menu.

Return to the Network tab.

- Fill in the **LDAP Synchronisation Interval**.

If the synchronization interval is set to zero or empty, the synchronization is not performed. When automatic synchronization is on, changes that are made in Active Directory will be applied automatically to the user group in Apresa.

- Check the Advanced settings checkbox in the top right corner.

- Optionally, fill in **UPN as Username (LDAP)**. If this setting is enabled, when importing users from AD, the Universal Principal Name (UPN) is used as username. UPN uses email address format (user@domain).

- At **LDAP telephones** of the Network tab, specify which data fields the Apresa should import from AD.

LDAP telephones:	General phone number ∨
	E-mail ∨
	- ∨

- Go to User groups of the Options menu.

- Click on a user group and click on the Edit button.

- Click the import button of the **LDAP group** setting. This shows the LDAP Groups window. Select an AD server address (LDAP) from the

list and click ok. This setting is only visible if an AD server is configured in the System settings (Network tab).

Apresa does not import group structures from Active Directory, but places the imported users in one Apresa group.

When a group is linked to Active Directory, it is not possible to manually add or remove users to or from that group.

For the import from AD to work, the following options need to be set in the system settings, Network tab: AD server address, AD user domain, LDAP Domain, LDAP User, LDAP Password, and LDAP Synchronisation Interval.

15 Using ADFS for sign-on

If ADFS is used for logging on, Apresa users don't have to fill in their passwords in the log-on screen of Apresa. Instead, Apresa redirects the browser of the user to the website of ADFS. If the user has an active session, the user is redirected back immediately. If the user has no active session, the user needs to input username and password. After verification, the user is redirected back to Apresa. In this redirect, there is a message for Apresa which tells Apresa the verified identity of the user.

15.1 Configuration of ADFS

This section assumes the use of Windows Server 2019 with ADFS 5.0.

- Start the AD FS Management application
- Select Relying Party Trust, and choose Add Relying Party Trust

  - Select Claims aware
  - Select the option to enter data manually
  - Display name: Apresa (or choose something else)
  - Configure certificate: Click Browse and select the certificate from Apresa (rename the certificate file from .crt to .cer if needed).
  - Enable support for the SAML 2.0 WebSSO protocol
  - As Relying party SAML service URL, type the URL at which Apresa is accessed. The URL needs to start with https://
  - As Relying party trust identifier, fill in the SAML identifier of Apresa, which "Apresa-SN", where SN is the serial number of Apresa, and then click Add.
  - The other settings could be kept at their defaults for now.

- The new relying party trust is now created. The Claim Issuance Policy editor is automatically opened, or otherwise, right-click on the newly created item, and choose Edit Claim Issuance Policy. Apresa accepts the claim types Name ID, UPN, and Name, for identification of the user (its username).

  To generate a UPN claim on this ADFS server using Active Directory:

  - Click Add Rule

- Select Send LDAP Attributes as Claims
- Claim rule name: LDAP claim (or choose something else)
- As Attribute Store, select Active Directory
- As LDAP Attribute, select User-Principal-Name
- As Outgoing Claim Type, select UPN

If you are receiving a UPN claim from another source and only need to pass it through:

- Click Add Rule
- Select Pass Through or Filter an Incoming Claim
- Claim rule name: UPN pass through (or choose something else)
- Incoming claim type: UPN
- Select Pass through all claim values

- Right-click on they Relying Party Trust "Apresa", and choose Properties.
  - Move to the Endpoints tab
    - Click Add SAML
    - Select SAML Logout
    - As Trusted URL, type the URL at which Apresa is accessed. The URL needs to start with https:// . After successful log on, the user will be directed back to this URL.
    - As the Response URL, type the same URL, but add /sso-logout.php at the end, for example: https://1.2.3.4/sso-logout.php

  - Move to the Signature tab
    - Click Add, and select the certificate from Apresa

15.2 Configuration of Apresa

15.2.1 User configuration

Options → Users

- A user account in Apresa should exist with a username that is equal to the claimed UPN (or other supported claim type), and the log on method should be set to SAML (ADFS).

Options → User groups

- An ADFS server (External logon service) can be selected on the group level. If LDAP import is enabled, then newly created users are set to log on using ADFS automatically. Otherwise, the logon method of the user must be set to ADFS manually on the user page.

15.2.2 Certificates

Tools → Certificates

- Menu Tools, Certificates.
- Upload the ADFS Signing certificate of the ADFS server
- Create a new certificate to identify Apresa. Edit the newly created certificate, and enable Web server access to the private key.

15.2.3 System configuration

Options → System settings → Network

- In the Options, System settings, Network tab, enable the option **Logon using external party**.
- Fill in the Apresa access URL (the URL needs to start with https://) that users use to access Apresa.
- Apresa certificate: Select the certificate that will be used by Apresa to sign SAML messages sent to ADFS. (created in the previous step)
- Click Add to configure a connection to a ADFS server.
- Name: The name can be freely chosen.
- Technology: SAML
- Entity ID: of the ADFS server. Usual format: http://somedomain.com/adfs/services/trust
- Certificate: of the ADFS server. It will be used to verify the identity of the ADFS server when connecting to it. (Selected the ADFS Signing certificate imported previously)
- Sign-on URL: Usual format: https://somedomain.com/adfs/ls/
- External sign-off: Enable this option if you want to perform an ADFS sign-off when the user logs out.
- Sign-off URL: Usual format: https://somedomain.com/adfs/ls/

16 Apresa API

Integration with other software is possible with the Apresa API. Using the API, you can send HTTPS requests to Apresa to perform certain actions. The requests will always contain a password or authentication code to allow access.

You can use the API to let Apresa perform actions on recordings, such as: starting, stopping, storing, and deleting. This way your software can use Apresa's recording features like "Storing on demand" and "Deleting on demand". You can also request for a list of Active Calls and edit properties of the call, like the notes field.

Detailed information on the Apresa API syntax is available in a separate document.

Example

IP address of Apresa: 192.168.0.9
username=eric
password=abc

Request:
https://192.168.0.9/client.php?username=eric&password=abc&info=AllActiveCalls

Reply:
RequestedInfo: AllActiveCalls Know: 536(31793065334,0) List:
[{id:536,remoteid:"20190502_120309_o0005",startdate:1556791389,
remote:"31793065334",local:"31704568393",connected:"",lname:"Hansen",rname:"Johnson",cname:"",remote2:"192.168.0.9",local2:"192.168.0.30",direction:1,linenr:0}] ServerTime: 1556791392

---

17 Transcription tasks

Options → System settings → Network

Configure the transcription feature on the Network tab of the System settings. For audio transcription to work, an account at *VoiceCrunch* is needed. This online service will analyse the audio and create text. It will send the text to Apresa, where it will appear in a special transcription field of the recording. Transcription fields of recordings are searchable in the Apresa web interface.

Options → System settings → Network → Transcription tasks link

The Transcription tasks page can be reached from the System settings, Network tab, by clicking the Transcription tasks link.
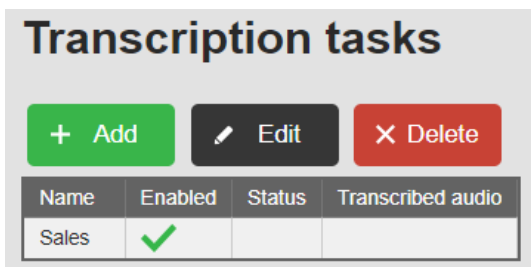
On this page you can configure which calls should be transcribed. To add a new transcription task, click the Add button.

Name: Input a name to identify this task (can be chosen freely)
Enabled: For disabled tasks, no further calls will be added to the transcription queue.
Maximum audio duration to process: Input the maximum number of audio minutes to transcribe for this task. The idea is to set a limit to the resources used for transcription. If not filled in, no limit is applied.
Filter: A number of filters can be defined to narrow down what calls should be transcribed.
Telephone number or ID: Only calls that involve the specified telephone numbers are transcribed. Multiple telephone numbers can be specified comma separated and can include the wild cards * and ?, similar to the regular search feature on the Home screen.

Date: Specify the date range of calls that must be transcribed. If no date range is specified, calls are transcribed regardless of their date.
Duration: Optionally specify a minimum and maximum duration. Calls with a duration outside this range are not transcribed for this task.

As long as a transcription task is enabled, the system will continue to check if new calls match the filter. Calls that match are added to the transcription queue. They are processed by the transcription provider, and the resulting transcription is stored when ready. The process of transcription can take a long time depending on the duration of the audio, and if many other calls are in the queue.

Changes that are made to transcription tasks apply only to calls that are not yet added to the queue. The existing transcription queue remains unmodified.

Options → Display settings → Visible columns

Make sure the column **Special properties of the recording** is visible on the Home screen. See Display settings.

18   Solving Problems for Passive Recording

18.1 Turn on "Collect information about all calls"

Go to: *Options → System settings → VoIP settings → Collect information about all calls*. Select "Active Calls" and Click "Apply".
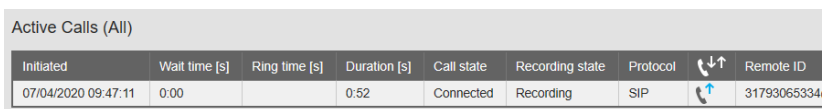
The page "Active Calls (All)" is now enabled. This page is meant for solving recording problems. **Disable it after diagnosis, because it consumes resources.**

Go to: *Tools → Active Calls (All)*

The Active Calls (All) page shows live information about calls even before they are connected (while ringing), and also about calls that are not recorded.

18.2 VoIP problem: the Apresa is not recording

- Is it passive or active recording? Active recording (CSTA etc.) is not discussed in this chapter.
- Check if anything is seen in:
  - Active Calls (All) (from the Tools menu, when enabled)
  - Active Calls (from the Tools menu)
  - the Home screen (main call listing)

Active Calls (All)

Initiated	Wait time [s]	Ring time [s]	Duration [s]	Call state	Recording state	Protocol	↓↑	Remote ID
07/04/2020 09:47:11	0:00		0:52	Connected	Recording	SIP	↑	31793065334(

Picture: Tools → Active Calls (All)

Picture: Tools → Active Calls

Picture: Home, main call listing

18.3 No calls are seen in Active Calls (All)

Tools → Active Calls (All)

- Log in as admin with full permission.
- Enable "Options → System settings → VoIP settings → Collect information about all calls" to be able to reach the Active Calls (All) page.
- Check if the port-mirroring (also known as SPAN) is configured correctly in the network.
- Examine: Options menu → System settings page → VoIP tab → VoIP network. For testing, try the option "All".
- Examine: Options menu → Recording settings → Addresses to record. For testing, try the option "Record everything". If this helps, have look at the values you entered here. Did you enter IP or MAC addresses? Are they entered correctly?

Addresses to record ✕

Place each IP address, IP name, or MAC address on a separate line
192.168.0.2
d8-8a-c9-30-7e-ce
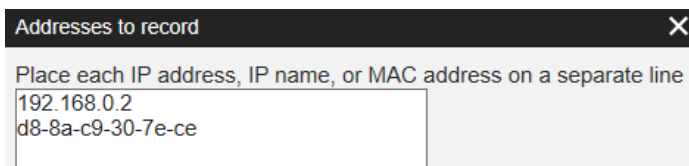
18.4 Calls are seen in Active Calls (All), but not in Home screen.

Tools → Active Calls (All)

> *Note:* A recording appears in the Home screen after the recording is completed, but for this to work you need to enable "Automatically refresh list of calls" from the Options menu, Display settings. (Or you have to manually refresh the Home page.)

The Active Calls (All) page shows you the **Recording state** of the current call(s).

Active Calls (All)

Initiated	Wait time [s]	Ring time [s]	Duration [s]	Call state	Recording state	Protocol	↳↑	Remote ID
07/04/2020 18:34:32	0:00		0:31	Connected	Outside filter	SIP	↳↑	317930653340

The following **Recording states** are possible:

- **Recording state: Waiting for audio stream / connection.**

There might be a problem with the audio stream or with the connection.

Audio stream problems (Waiting for audio stream / connection)
It is possible that Apresa receives SIP (call signaling data), without receiving RTP (audio stream). For example, this happens in the following case:

> **Example of an audio stream problem:**
> **When SIP and RTP follow different routes in the network**
>
> Assume Apresa receives data using port-mirroring from/to
> the PBX, and SIP communication between telephones is
> sent via the PBX, but RTP communication is sent directly
> from phone to phone, not via the PBX.
> In this case Apresa receives SIP, but doesn't receive RTP
> (audio). Then the call is not recorded.

You can make a network trace in Apresa and open it in Wireshark to see
if there's RTP present or not. Apresa cannot record a VoIP call without
receiving RTP. See VoIP tracing.

Connection problems (Waiting for audio stream / connection)
See: Options → System settings → VoIP→ Start recording when
connected.

Start recording when connected:	☐	(SIP)

If "Start recording when connected" is enabled, Apresa starts recording
only after the call has been answered. For some protocols (non-SIP)
Apresa might not be able to detect when a call has been answered. In
this case, disable the option "Start recording when connected" to let it
start recording.

- **Recording state: Outside filter**: Examine the recording filters (SIP
  filter and telephone number filters). See Options menu → Recording
  settings.

Active Calls (All)

Initiated	Wait time [s]	Ring time [s]	Duration [s]	Call state	Recording state	Protocol	↕↑	Remote ID
07/04/2020 18:34:32	0:00		0:31	Connected	Outside filter	SIP	↵↑	31793065334(

In this example, the Protocol is SIP. In that case you have to examine at
the SIP filter. See the picture below.

SIP Filter:	Only record calls that match the filter ▾	(VoIP SIP)
	✎ Edit 1180	
Telephone number filter:	No filter ▾	(VoIP HFA / H.323 / Avaya)

- **Recording state: Recording on demand:** Examine the setting: Options menu, Recording settings, Recording on demand. The "Recording state" is "Recording on demand". Nothing is recorded (yet). The "Recording state" changes to "Recording" when a recording starts. Turn it off for testing.

Active Calls (All)

Initiated	Wait time [s]	Ring time [s]	Duration [s]	Call state	Recording state	Protocol	↓↑	Remote ID
08/04/2020 09:48:12	0:01		0:52	Connected	Recording on demand	SIP	↑	317930653334@

- **Recording state: License overflow:** Check VoIP licenses in Options menu, System settings, System tab. See Apresa Channel License Activation.

- **Recording state: Deleted:** This is used for the "Delete on demand" function. Go to Options, Recording settings to turn it off for testing.

Active Calls (All)

Initiated	Wait time [s]	Ring time [s]	Duration [s]	Call state	Recording state	Protocol	↓↑	Remote ID
08/04/2020 16:38:55	0:00		0:32	Connected	Deleted	SIP	↑	317930653334@

- **Recording state: Waiting for audio level:** Examine Options → Recording settings → Audio Detection. When enabled, Apresa starts a recording when the "Audio level threshold" reaches a certain level (in dB). Turn this off for testing.

Active Calls (All)

Initiated	Wait time [s]	Ring time [s]	Duration [s]	Call state	Recording state	Protocol	↓↑	Remote ID
08/04/2020 21:14:50	0:00		0:24	Connected	Waiting for audio level	SIP	↑	317930653334@

Audio detection   All ▾   (VoIP)

Audio level threshold: 30   dB (0 - 40)   (VoIP)

- **Recording state: Outside schedule:** Examine Options → System settings → Schedule.

Active Calls (All)								
Initiated	Wait time [s]	Ring time [s]	Duration [s]	Call state	Recording state	Protocol	↓↑	Remote ID
08/04/2020 16:26:44	0:00		1:48	Connected	Outside schedule	SIP	↑	31793065334(

For testing, check the box of the current day and remove the start and stop times from the edit boxes.

Monday:	☑
Start time: (1)	
Stop time: (1)	
Start time: (2)	
Stop time: (2)	

- **Recording state: Direction filter:**

Examine if the call direction filter is applied and correct this when needed.

- **Recording state: Recording:**

  - Store on Demand. Examine the setting: Options menu, Recording settings, Store on demand. The "Recording state" is "Recording", because Store-on-demand commands by the user are processed after the recording has finished.

Active Calls (All)								
Initiated	Wait time [s]	Ring time [s]	Duration [s]	Call state	Recording state	Protocol	↓↑	Remote ID
07/04/2020 09:47:11	0:00		0:52	Connected	Recording	SIP	↑	31793065334(

  - Store on Demand for a user. Check if store on demand is enabled *for a user* in the User account screens. See: Options menu, Users. Select the User and click Edit.

- Minimal recording duration. Examine the setting: Options menu, Recording settings, Minimal recording duration. The "Recording state" is "Recording", because Minimal-duration checks are performed after the recording has finished.

Active Calls (All)								
Initiated	Wait time [s]	Ring time [s]	Duration [s]	Call state	Recording state	Protocol	↶↓↑	Remote ID
07/04/2020 09:47:11	0:00		0:52	Connected	Recording	SIP	↶↑	31793065334

- Check if you enabled the recording of incoming, outgoing, or local calls. Enable all three for testing. They are found in the Options menu, Recording settings.

Record incoming calls:	☑
Record outgoing calls:	☑
Record local calls:	☑

The "Recording state" is "Recording", because these three settings are checked after the recording has finished.

Important: the detection of the call direction might be wrong or absent, in which case filtering on the call direction can lead to calls not being recorded, while they should be recorded. See Call direction.

Active Calls (All)								
Initiated	Wait time [s]	Ring time [s]	Duration [s]	Call state	Recording state	Protocol	↶↓↑	Remote ID
07/04/2020 09:47:11	0:00		0:52	Connected	Recording	SIP	↶↑	31793065334

> *See the separate description below on how to perform a network trace and collect log files.*

18.5 Calls are seen in the Home screen but not playable (.mcf)

- The audio might use an unsupported or unlicensed audio codec.

18.6 VoIP problem: Detected phone numbers are incorrect

IP addresses are shown as both Local and Remote ID
This means Apresa sees audio streams (RTP), but not the call signaling.
- Check if a protocol setting is needed: Which protocol / PBX is it? For Siemens, Avaya, Ericson Mx-One, Nortel, Megaco H.248, Nortel UNIStim, Xpert, Samwin: enable the specific setting in System settings, VoIP tab.
- Check if call signaling is also port-mirrored (ask your network manager)
- Check if call signaling is not encrypted (ask your PBX manager)

IP addresses are shown as Local ID (Remote ID is OK)
- For some protocols, detection of a Local phone number is not supported
- For some protocols, it might be needed to reboot/restart/replug/relogin the phone
- Ensure all local phones are within the range specified in the Local IP addresses settings

18.7 VoIP problem: Direction is missing or incorrect, or Local/Remote ID swapped

- Enable Local and Remote IP address in Display settings

- Check Local ID and Remote ID of recorded calls, to see which one is actually the local / remote side, from that we know which IP addresses are local/remote
- Correct the Local IP addresses setting (System settings, VoIP tab). It only effects new calls.
- If an IP address is not consistently Local/Remote, don't specify it.
- In some cases the option "SIP INVITE determines IP addresses" might be needed or give better result.

From Options menu, System settings, VoIP settings.

Local IP Addresses: This setting is used to determine whether an IP address corresponds to a local phone (extension). It is also used for detecting of the direction of a call (incoming, outgoing, or internal). A singular IP address or an IP address range can be specified. To specify multiple IP addresses or ranges, separate them by a comma. An IP range must be specified in the CIDR notation. For example: 192.168.0.0/24 means that the first 24 bits are fixed, and the last 8 bits may vary, which means that, in this example, all IP addresses that start with 192.168.0. would be considered local.
Remote IP Addresses: In a VoIP call, there are two IP addresses that communicate. If one of them is in the Remote IP Address range, the other is consider local. The format is the same as for Local IP Addresses.

- When IP addresses cannot be used to determine direction (which is rare), use the setting "Local telephone numbers" (advanced VoIP setting) to use the phone numbers instead. To do this, go to the VoIP tab of the System settings and check the Advanced settings checkbox to see the advanced options.

18.8 VoIP problem: Dial codes (0-9 *#) are not recognized

- Dial codes are accepted only from the local extension side by default (System settings, VoIP tab, Dial code action).
- Check if the Local/Remote sides are correct and not swapped (see previous how to correct)

- In System settings, VoIP, set VoIP recording module to Default.

18.9 VoIP problem: Only the external partner is recorded

When only the external partner is recorded, this is possibly caused by incomplete port-mirroring of the RTP-stream (one side only). To make sure if incomplete port-mirroring is the cause of the problem, you can make a network trace, which will show it perfectly.

18.10 VoIP tracing

18.10.1 How to create a network trace

To help you solve a problem, the Vidicode team might ask you to send them a network trace. This is how to do it.

1. Log in as administrator (admin) in the web interface
2. Open the **Tools** menu, select **System**
3. Click the **"Enable"** button next to Network trace
4. Perform the specific action that was handled incorrectly by Apresa.
(For example, if the problem was that incoming calls have no caller ID, then make an incoming call.)
5. Click the **"Disable"** button next to Network trace
6. Click **"Download Log Files"**
7. The filename is for example Apresa_logs_20180621_100000.tgz. Please verify if the downloaded file contains the .pcap trace file inside (Optional step)
8. If there are other situations that must be traced, then go back to step three. Each trace must be downloaded, before proceeding to the next trace.
9. Send the files to Vidicode including a description of what was recorded in the trace. If the files are less than 20 MB, you could use email to send them to support@vidicode.com.
Larger files could be transferred using this dropbox request:
https://www.dropbox.com/request/76ri413lO0pGZdcfqley
Otherwise, another way of transferring the files must be arranged, for example transferring the file with TeamViewer when logged in.

18.10.2 How to inspect and verify a network trace

You can inspect the trace yourself.

- Use 7zip to open the tgz file. There is a separate pcap file per network interface.
- Extract the pcap and open it in Wireshark.
- For some protocols (at least SIP and H.323), it is possible to see the calls in **Wireshark**. In the **Telephony** menu, choose **VoIP calls**. This shows the list of calls, but even then, Wireshark does not always show phone number information. For example for Avaya H.323, Apresa can detect phone numbers, Wireshark cannot.
- Select a call, click the Flow button (or the Flow Sequence button)
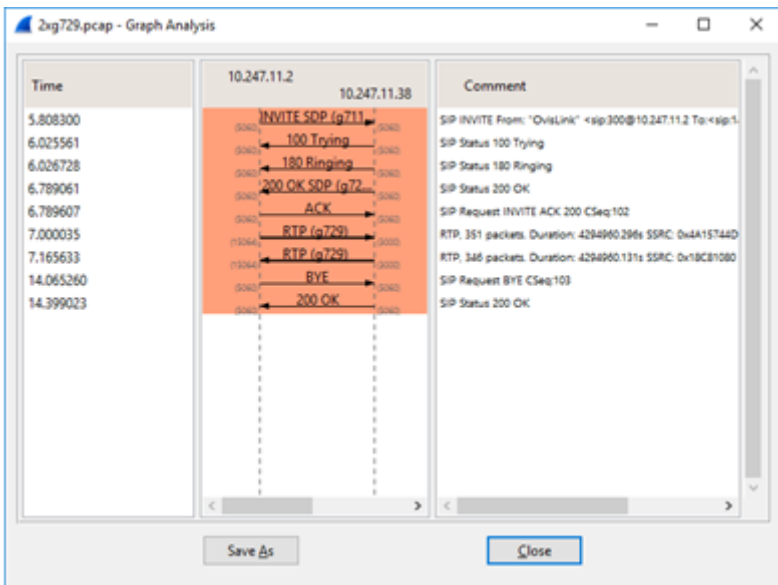
- There should be call signaling in both directions, and RTP (audio) in both directions. It shows the used codec (G.711 / G.729).
- To see if there is any traffic from an IP address: In the main screen of Wireshark, in the display filter, type:
  `ip.addr==192.168.0.20` (for example)
- To see if traffic there is any SIP traffic, in the display filter, type:
  `sip` (it shows then only SIP packets), and for H.323 packets, type:
  `h225`
- HFA is on TCP port 4060. Encrypted HFA is on TCP port 4061.

- To check for encrypted SIP, type: `tcp.port==5061` (encrypted SIP cannot be recorded)
- For Aastra, SIP calls are expected without phone number info
- For Alcatel, display filter: `udp.port==32000 or udp.port==32512` (or in some cases, it might be plain SIP)
- For Avaya IP Office, H.323 calls are expected without phone number info
- For Nortel UNIStim, display filter: `udp.port==5100`
- For Panasonic, display filter: `mgcp`
- For Samwin, display filter: `tcp.port==81`
- For Xpert, display filter: `tcp.port==9000`

19 The Tools menu

19.1 Contact List

Tools → Contact List

The Contact list page can be reached from the **Tools** menu, when the user has the "Access Contact list" permission.

The contact list is system-wide or per-tenant. The contact list contains all internal and external callers whose calls have been recorded. It is possible to edit this list, provided you have the "Edit names" permission.

Identifier 153 is a local caller named "Tessa". Calls in the Home listing will show "Tessa" in the *Name of Local* column. You can edit this name and specify if 153 is a local or remote caller.

If identification is based on the full SIP ID (user@host), then the contact list will also show full SIP IDs.

Import from a CSV file

To import data into the contact list from a CSV file, click the Import button. On the next page, upload the CSV file that contains the data. The CSV file is expected to have the following format: (example)
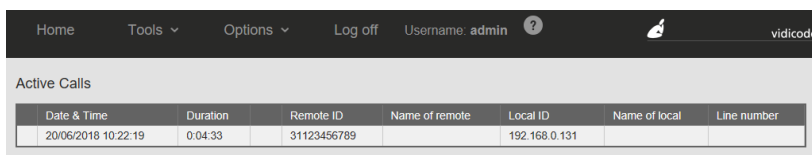
Telephone number, Name, IsLocal
200, Sales, 1
+3320102010, J. Williams, 0
LINE#5,Name of line five,1

The first line is assumed to contain a header, and is skipped. The LINE# syntax is used to reference a line used by card recording, followed by the line number. The IsLocal column is optional. The contact will be assumed to be remote if nothing is specified. The CSV file is assumed to use UTF-8 encoding. A verification screen is displayed that shows what data will be imported. The CSV import can be used to edit existing records, or create new entries, but not for deleting records.

19.2 Active Calls

Tools → Active Calls

The Active Calls page can be reached from the **Tools** menu. On this page, calls that are recorded, and calls that could be recorded potentially (on demand) are listed. The page updates automatically, showing the new current list of active calls. It only shows calls for which the current user has the View listing permission (directly, or indirectly as administrator).

Active calls of VoIP type, can be played back in the web interface only after they have finished. Then, they will be listed in the main call listing. For near real-time playback (monitoring) of current active calls, use the Apresa Call Monitor instead.

19.3 Active Calls (All)

Tools → Active Calls (All)

This page is available if the VoIP option "Collect information about all calls" is set to collect information about active calls. Go to: Options → System settings → VoIP settings → Collect information about all calls. Select "Active Calls" and Click "Apply". It is only accessible for administrators.

The Active Calls page displays information about all active calls that are detected on the network.

Active Calls (All)								
Initiated	Wait time [s]	Ring time [s]	Duration [s]	Call state	Recording state	Protocol	↓↑	Remote ID
07/04/2020 09:47:11	0:00		0:52	Connected	Recording	SIP	↑	31793065334

This page does not show information about calls that are recorded using PCI recording cards. Calls that are not recorded are also listed, and the reason why they are not recorded is indicated, for diagnostic purposes. For the SIP protocol, it also displays calls that are ringing, but not connected yet.

If the Local and Remote fields are empty during the ringing phase, this could be solved by enabling the option "SIP INVITE determines IP addresses".

The VoIP option "Collect information about all calls" takes resources and is disabled by default. Therefore the Active Calls (All) menu option is disabled by default also.

The Active Calls (All) page is only available for an administrator.

See also: Solving Problems for Passive Recording

19.4 Live Dashboard

Tools → Live Dashboard

This page shows a configurable selection of live data and statistics. The configuration can be different for each user. The data is updated automatically. Data is shown about active calls and finished calls of today. The data is filtered based on the access permissions of the user.
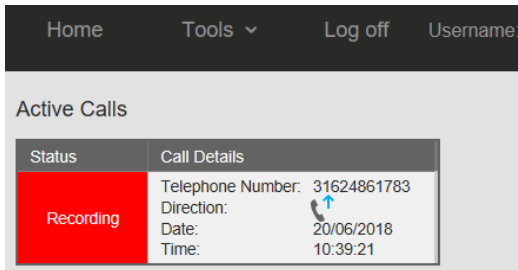
19.5 Web Client

Tools → Web Client

Via the web client, users can perform actions on active calls. To access this page, the user must have the web client permission. You'll find the Web Client in the **Tools** menu.

Active Calls

In this table, currently active calls are listed. This table will update automatically. For calls to appear, they need to involve telephone numbers or SIP ids that are listed under the telephones section on the user page of the logged in user.

Action

Perform an action on the call. Availability of these actions is controlled via the recording settings (Options menu). In this example, Silence on demand is turned on.

Availability for a certain user is controlled via the user page of the user. Under Permissions, grant the user Web Client permission. After doing this, click on the *Web Client Settings* button and enable the required boxes for that user. This is essential for the user to see the buttons on his or her Web Client page, to perform actions.
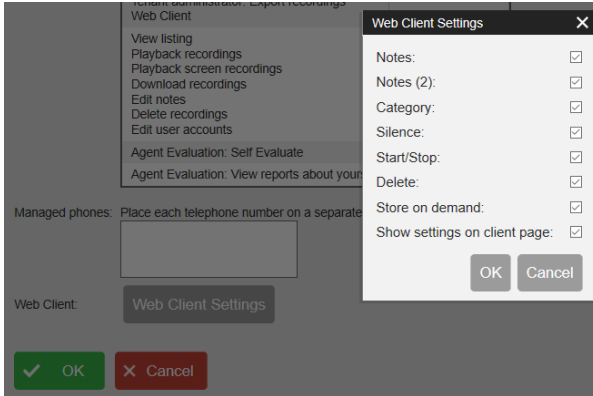
Available actions are:

Start Silence/Stop silence: Starts the silence on call that is being recorded or starts the sound again on a call that is being silenced.
Start/Stop Recording: Starts recording a call that is not being recorded or stop the recording of a call that is being recorded.
Delete: Delete the call and erase the recording
Store this call: Store a call when the recording has finished

Status:
Shows the status of the call:

White: Call is not recorded
Red: Call is recorded
Blue: Call is silenced

Category, Notes and Notes (2):

Edit the category of a call and the notes fields. These are subject to the edit notes permission. These fields are available while the call is recorded.
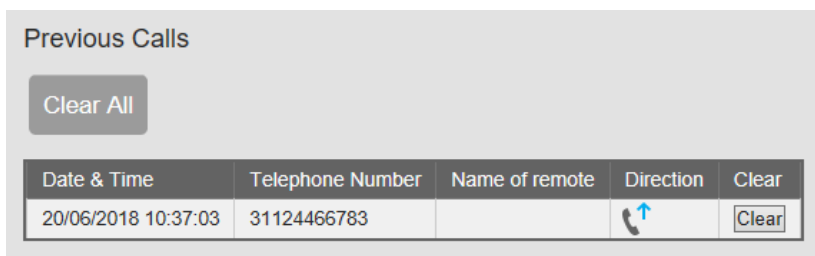
Call Details:
Shows information about the active call

Previous Calls:
Any finished and recorded calls are moved to this table. From this table, the category and notes can be edited.
Calls can be cleared from this table individually with the clear button or all at once with the Clear All button. This will not delete the recording, it is only removed from this web client view. The view is also cleared when the page is reloaded.

Web Client Settings
Using the Web Client Settings, you can hide elements from the user interface. Click the button of Web Client Settings to see if all elements are turned on for the user. Turn off all elements the user should not see. These Web Client Settings can be defined on group level via the user group page or on user level via the user page and optionally the web client page itself.
Note that the Web Client Settings only apply to the user interface itself. For the underlying actions to succeed, the proper permissions and recording settings are still required.

The web client user interface settings are:

Notes: Show the editor for the first notes field
Notes (2): Show the editor for the second notes field
Category: Show the category editor
Silence: Show the button for starting and stopping silence for calls that have silence on demand enabled.

Start/Stop: Show the button starting and stopping a recording for calls with recording on demand enabled.
Delete: Show the button to completely delete a call for which delete on demand is enabled.
Store on demand: Show the button to store a call for which store on demand in enabled.

The group level settings have the following extra options:

Apply to subgroups: When this option is enabled for a group, the webclient settings will also be applied for members of a subgroup of this group.
Otherwise they will only be applied to members of this group.

Allow settings to be overridden in subgroup: If this option is also enabled in combination with the "Apply to subgroups" option, the web client settings for specific subgroups can be overridden.

Allow settings to be overridden for group members: If this option is enabled, the web client settings can optionally be overridden for specific users.
Other members of this group will continue using the group defined web client settings.

The group level settings and user level settings via the user page have the following extra option:

Show settings on client page: If enabled, the web client settings can be changed from the web client page itself.
Otherwise the settings will be hidden, so that only users with permissions to edit users and user groups can change the settings.

19.6 Statistics

Tools → Statistics

The **Statistics** page can be reached from the **Tools** menu.

The following statistics are available:

- **Number of calls:** a time line of the number of calls in subsequent periods

- **Time of day:** the number of calls at different hours of the day (e.g. between 7 AM and 8 AM)

- **Local caller:** the number of calls (incoming, outgoing or internal) by local callers (employees). Sorted to show the most frequent callers at the top of the list.

- **Local caller - details:** For each local caller (extension / employee), it shows per day the following: Number of calls during that day, total call duration, average call duration, the time of the first and last call. The report describes one week or one month. The Total row shows the data for all employees. Note: Internal calls will be counted double in this total, because two employees were at the phone.

- **Remote caller:** the number of calls (incoming, outgoing or internal) by remote callers. Sorted to show the most frequent callers at the top of the list.

- **Call duration:** a histogram of the duration of calls (for example: how many calls were shorter than 10 seconds), or alternatively, a time line of the average duration of calls in subsequent periods

- **Not recorded calls:** the number of calls that were not recorded because the channel license limit was reached. (This statistic is only available for administrators)

- **Maximum number of simultaneous calls:** The highest number of calls that were ever simultaneously active in a particular time period (a day). Calls that were not recorded because of the channel license limit, are included. But calls that are outside of the recording filter, are not included.

Number of Calls			
per year	⊞	📈	📊
per month	⊞	📈	📊
per week	⊞	📈	📊

Time of Day			
	⊞		📊

Local caller			
	⊞		◕

Local caller - Details			
Month	⊞		
Week	⊞		

Remote caller			
	⊞		◕

Call Duration			
histogram	⊞		📊
per year	⊞	📈	📈
per month	⊞	📈	📈
per week	⊞	📈	📈

Wait time before answer			
histogram	⊞		📊
per year	⊞	📈	📈
per month	⊞	📈	📈
per week	⊞	📈	📈

Not recorded calls			
Time of Day	⊞		📊

Maximum number of simultaneous calls			
per day	⊞		

To filter the statistics to a certain time range or other characteristics, click the Filter button. The filter functionality is similar to the Search function on the main page.

Click the Filter button if you are satisfied with the parameters, or click Cancel your query if you want to start over.

The statistics are automatically filtered based on the access rights of the user that is logged in. Most statistics make a distinction between incoming, outgoing, and internal calls. Most statistics are available in tables and charts. Tables can be exported to CSV for import in spreadsheet software.
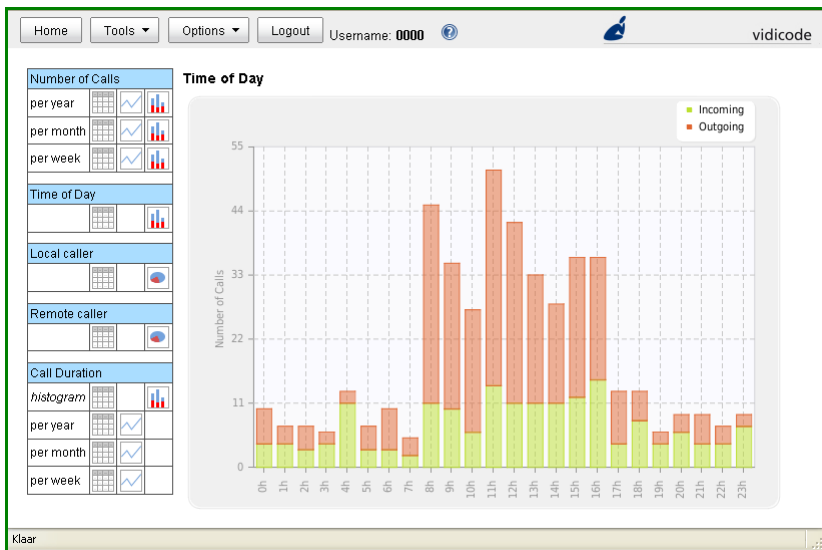
Hover over points in the graph to view their exact value. Items in the legend can be clicked to enable or disable them on the graph. For browsers that do not display the graphs properly, compatibility mode can be enabled in the Display settings.

19.7 Recycle Bin

Tools → Recycle Bin

The Recycle Bin can be reached from the **Tools** menu, when the user has any Delete permission.

Note: To turn on the Recycle Bin, go to Options, System Settings, System tab. Check the Recycle Bin box and click Apply.

Th Recycle Bin page has similar functionality, compared to the main call listing.

On this page, it is possible to delete calls permanently, or to restore calls, if you have the Delete permission on those calls.

• To delete a call permanently, that resides in the Recycle Bin, select the call(s), and then click the delete ❌ button. This action cannot be reversed.

• To restore a call from the recycle bin, to move it back to the main call listing, select the call(s), and then click the edit-undo ↩ button.

From the list button, it is also possible to restore or delete all calls that result from a search query. To use these options, the global 'Delete multiple calls' permission is required and the 'Delete recordings' permission is required for each individual call that you try to restore or delete with these options.

19.8 Agent Evaluation

19.8.1 Introduction

Tools → Agent Evaluation

Agent Evaluation monitors the performance of an agent. Using Call Evaluation, you can assign as score to each call. This will determine the overall score of an agent.

The **Agent Evaluation** add-on is activated with a separate **license key**. To reach this add-on, open the **Tools** menu, and choose **Agent Evaluation**.

Preparation
To give access to this add-on to users that are not administrators, special Permissions must be defined.

Agent Evaluation is about evaluating agents. The Agent Evaluation add-on requires that for each agent, a user is defined, with its phones. This is needed for the system to know to which agent a particular call belongs. The user accounts of these users do not have to be enabled. It will still work, even if the user accounts are disabled.

19.8.2 Agent Evaluation Permissions

Access to the Agent Evaluation module by a user is controlled by user permissions. To change permissions, open the <u>Users</u> or <u>Groups</u> page. The following levels of access are available:

None: No access
Report: The user can view all the reports (tables, charts, for all user agents, and projects)
Evaluate: The user can evaluate calls, and view all the reports
Manage: Access to all parts, can view and edit calls and schedules of any supervisor.
Supervisor: Access to all parts, except that users who have this permission are limited to viewing calls added to projects by themselves or by their schedules. Supervisors can also only add and evaluate calls from agents that are in the same group or in a subgroup.
Schedule: Allows supervisors to edit their own schedules.
Self Evaluate: Allows agents to view and evaluate their own calls, but not edit any evaluations done by supervisors.
View reports about yourself: Allows agents to view evaluation reports about themselves, but not edit these reports or view reports about other agents.

19.8.3 Dashboard

Tools → Agent Evaluation → Dashboard

The dashboard of the Agent Evaluation module shows supervisors and managers statistical information about agents. It also allows for this information to be printed, and exported to PDF if a PDF printer (such as Microsoft Print to PDF in Windows 10) is available on the PC of the user.

- When viewing the dashboard, information can be filtered by project and/or agent. To do this, double click a project or agent.
- To print or export to pdf, press Export Page. The printing dialog will be opened. To export as pdf, select the pdf printer if available.
- Graphs can be changed to show data from the past Year, Month, Week, or Day by selecting any of these options in the boxes below them.

19.8.4 Evaluation Forms

Tools → Agent Evaluation → Evaluation Forms

The Agent Evaluation module uses Evaluation Forms.

An Evaluation Form is essentially a list of **questions** that must be answered for each call during evaluation. A question could be, for example, "Did the agent answer the call politely?" Answers to this question have to be selected from a pre-defined set of answers, for example: Good, Avg., Poor. Such as list of possible answers is called an **Answer Type**. When defining an Evaluation Form, for each question, an answer type can be selected from the list of available answer types. It is possible to define your own Answer Types. Some questions are **not always applicable**. This means they can be answered with N/A, and in that case, they will be left out of the score calculation. Each question can be assigned a **weight**, which determines the importance of the question in the final score that will be awarded to the call. Questions can be organized in sections, by adding headers to the list of questions. To do so, add a question, and choose "- Header -" as the Answer Type.

An example Evaluation Form with 5 questions, and 3 sections.

Adding a new question

19.8.5 Answer Types

You can define your own answer types to use in the evaluation forms of the Agent Evaluation module.

To define you own answer types, click the "Define Answer Types" button in the Evaluation Forms screen, and then click Add. The following format must be used:

Answer1=Score1\Answer2=Score2 etc.

For example:

Good=2\Avg.=1\Poor=0

This means that the answer "Good" will give the maximum score to the agent, Avg. (average) half of the score, and Poor will award no points. The scores that are assigned to the answers here, such as the score 2 for "Good", are only relative scores. They are always scaled to the same proportion, and after that, the weight of the question is applied. This means the definition "Good=2\Avg.=1\Poor=0" and the definition "Good=4\Avg.=2\Poor=0" are equivalent. To give separate weights to questions, use instead the weight property of the question itself.

To export answer types, select the answer types you wish to export and press the export button. A file will then be downloaded that contains the selected answer types. To export all answer types, do not select any answer types and press export. All answer types will then be selected and downloaded to a file.

19.8.6 Projects

Tools → Agent Evaluation → Projects

The Agent Evaluation module features **Projects**.

The calls that are to be evaluated are organized into **Projects**. Each project uses one Evaluation Form. When a project is created, it contains no calls. Calls that belong to the project, and are to be evaluated, can be added to the project in the **Call selection** screen. After a call has been added to a project, a user with that permission to evaluate calls, can select the call and evaluate it.

19.8.7 Schedules

Tools → Agent Evaluation → Schedules

Schedules can add calls to projects based on a set of parameters. They can be set to run daily, weekly or monthly, and when run will add calls to projects based on a preset filter.

Calls added by these schedules can only be viewed by the Supervisor assigned to the schedule, or Managers.

Schedules also have a feature called "Moving Schedule". This feature allows the schedule to move in time. Suppose you have a filter set to add calls made yesterday to a project, and you have set this schedule to run daily. When "Moving Schedule" is enabled and the schedule is run, the filter will be changed to select calls from a day later. So for instance if the filter is set to add calls from April 7th 2021, it will now add calls from April 8th 2021. When the schedule is set to weekly it will move the schedule by a week. And a month for monthly.

Per Telephone number of ID: Instead of adding X calls to the project, this option will make the schedule add X calls to the project for every item in the field "Telephone number or ID".

19.8.8 Evaluation of a call

Tools → Agent Evaluation → Call Evaluation

By evaluating a call, indirectly, the performance of the agent that has done the call, is evaluated. Before a call can be evaluated, a user must be added for the agent that is evaluated (see: Introduction).

First select a project for which you want to evaluate calls, in the drop-down box at the top. Then, select a call, and click Evaluate, or double-click on the call.

Alternatively, users with the supervisor permission can right click calls on the main page to pull up a context menu. This menu will show all available projects and allows a user to quickly add a call and go to the evaluation page.

In the screen that opens, the following information is presented:
- Date and time of the call
- The agent that performed the call
- The direction of the call (incoming or outgoing)
- The duration of the call

- The preliminary or final score

Click the right arrow button to playback the recording of the call. Click on the button with the monitor image to playback or download the screen recording.

Note for screen recordings: Playback in a browser of wmv files is only available in Internet Explorer. Use Apresa Client Professional to create mp4 screen recordings, which are playable in a modern browser like Chrome and Edge.

Answer the questions to evaluate the call. For each question, choose one of the answers. Choose N/A if the question is not applicable. The evaluation is not taken into account if not for all questions an option has been selected. The evaluator can fill in additional Notes about the call or the agent, as necessary, in the Notes field, and for each question separately. When all questions have been answered, the final score is displayed at the top.

Click Save to store the evaluation of the call.

19.8.9 Reports

Tools → Agent Evaluation

To view and export reports, a user must be administrator or have the Agent Evaluation Report permission.

The following reports are available:

Project Reports

This report presents the scores **per project**. The data in this report can be filtered on a particular agent. It is possible to view the total score, or zoom in on the individual questions, by selecting one of the evaluation forms. It is possible to zoom in further for the details per call (Evaluated Calls Report).

Agent Reports

This report presents the scores **per agent**. The data in this report can be filtered on a particular project. It is possible to view the total score, or zoom in on the individual questions, by selecting one of the evaluation

forms. It is possible to zoom in further for the details per call (Evaluated Calls Report).

Evaluated Calls Report

This report presents the call evaluation data **per evaluated call**. The data in this report can be filtered on a particular project, and agent. The score data in this report can also be viewed graphically in a line or bar chart. These charts can show, for example, how the performance of an agent has progressed over time.

The report data in tables can be exported to CSV format, for import in spreadsheet software, or other compatible software. The CSV file is stored in UTF-8 encoding, using the comma (,) a separator, and the double quotation mark (") as field start and end marker.

Example screen with a bar chart of the score:
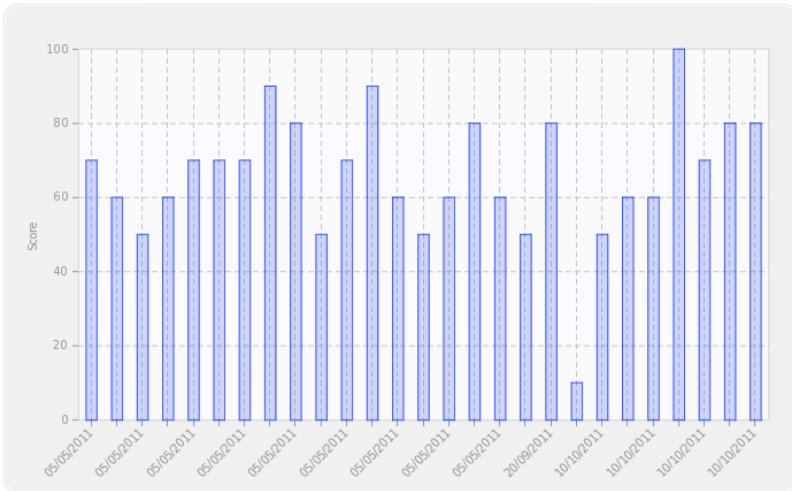
19.9 VoIP Service

Tools → VoIP Service

You can find the VoIP Service in the **Tools** menu.

The VoIP Service allows the Apresa to function as a SIP phone, SIP server, or SIP proxy. It can accept multiple SIP calls simultaneously, and forward calls based on rules. This functionality can be used for:
• MoReSo (mobile recording)
• Cisco Dual Stream Active Recording
• Playback of a notification into the call

VoIP Service: This is the main switch that enables or disables this feature. If this setting is switched off, then no VoIP service is performed
Restart service: This is only needed in special situations, when the basic settings are changed. It causes active calls, that flow through Apresa, to be dropped. (See also **Apply**)

General

Delayed SDP offer: This option is related to a detail of the SIP protocol. It must be enabled for Cisco Dual Stream Recording.
Reject duplicated calls: Incoming calls with the same caller and receiver as an existing active call, are rejected. To let this option take effect, restart the VoIP service.
Accept SIP registrations: Enables other SIP phones or entities to register at Apresa. Details are configured under SIP Registrator.
NAT Address: Sets the IP address the VoIP services advertises for RTP connections. If left empty the local IP address will be used. This option can be used if the Apresa is behind a NAT and the local IP address can not be used. If may also be required add the local to public IP mapping in the system settings for recording to succeed.
SIPREC: Enables handling of incoming SIPREC call data. Enabling this option also adds an additional SIP registration option (see below). SIPREC requires VoIP Service version 1.9.6.3. In addition, it might be needed to configure the external telephony system to send SIPREC data to Apresa.
Determine direction: This SIPREC option can be used in combination with specifying local numbers on the system settings page under the VoIP setting to determine call direction. For this to work, the SIPREC client needs to provide the participant data in a predictable order. If one of the participants is detected as local and the other remote, this setting controls which participant is seen as the caller and which as the callee to determine if the call is incoming or outgoing. If the recording client does not provide the participants in a predictable manner, setting this option to disabled will mark the calls with unknown direction.

Protocol

With these options, transport protocols for SIP can be enabled. The local port on which the VoIP service expects the protocol can also be adjusted. The options are UDP, TCP and TLS. SIP over TLS is encrypted. As TLS uses TCP, the TLS and TCP local port must not be the same if both are enabled.

TLS provides the following extra options:

Certificate: For the VoIP service to accept encrypted calls, a certificate is necessary. Certificates can be created or uploaded via on the certificates page. The list of all certificates that may be used for setting up the encrypted TLS connection for SIP calls. One may be selected here.

Verify certificates: When this option is enabled and a certificate is received from a TLS peer, the certificate is checked for its validity. This requires that the certificate is trusted. For outgoing TLS connections, this also requires that there is a subject alternative name in the certificate that matches the domain name that was contacted. This option will mainly apply for outgoing calls, but if a client sends a client certificate, this will be checked as well.

Record: Enable yes if encrypted calls must be recorded. Compatibility mode uses the recording method from older versions. It is not recommended for new installations and must not be used in combination with SIPREC.

If you enable TLS, also enable the Secure RTP option, otherwise the audio stream is not encrypted.

Codecs

Select the audio codecs to be enabled or disabled for the VoIP service. Only the enabled codecs will be accepted or offered for use in a SIP call. All the listed codecs can be recorded by Apresa, but not all listed codecs can be used by the VoIP service to send audio. This is not a problem if the VoIP service only needs to accept calls, and when it does not need to send any audio.
The VoIP Service needs to be able to send audio when inserting a notification message or when forwarding a call when it stays in the loop.

In this case it is important that the selected codec is supported by the VoIP Service for sending audio. G.711, G.722, iLBC, and Opus audio can be sent, G.729 audio cannot be sent (but it can be received).

RTP

Minimum port and Maximum port: These settings control the range of UDP ports that the VoIP service will try to allocate for RTP sessions.
Secure RTP: This option will enable the use of encrypted RTP. This option should be used in combination with the TLS protocol for SIP.
SAVP: When this option is set, the VoIP service will generate SIP offers with the RTP/SAVP profile set when SRTP is on for outgoing calls or when the delayed SDP option is enabled. This may be required for interoperability. This setting only works when SRTP is enabled as well.

Last calls: This table provides a list of the calls that were handled by the VoIP service, and which rules was applied to them. This is useful when setting up and verifying rules.

SIP Line 1 / SIP Line 2: The VoIP service can communicate with possibly two SIP destinations (for example a SIP trunk, a SIP PBX, or a SIP phone).
IP name or IP address: The IP name or IP address of the SIP server.
SIP REGISTER: If enabled, Apresa will try to register itself with the specified username and password. This might be needed when communicating with a SIP PBX or SIP trunk.
Username: This will usually correspond to the telephone number of Apresa.
Password: The password used during SIP registration.
Domain: Apresa will register itself with username@domain. When left empty, the IP name or IP address of the SIP server, which is specified above, will be used as domain.
Local IP: This setting only needs to be set if a non-standard local port is defined (not 5060), and if the main IP address of Apresa should not be used as originating IP address. In that case, fill in the local IP address that should be used.
Local port: Fill in if Apresa needs to register itself on a non-standard local port (not 5060). This could be needed to avoid conflicts with other use of port 5060.
Registration interval: The SIP registration interval in seconds. When left empty, Apresa can use the default SIP registration interval, or the one advocated by the SIP server.
Local IP address in messages (NAT): If Apresa is communicating to a server in another network, it can be needed to specify the local IP

address that Apresa must specify in SIP messages. If left empty, this will be determined automatically.
Protocol: Controls over which protocol the registration is made.

SIP Registrar: This section is available if the "Accept SIP registrations" option is enabled.
Username: The telephone number of the other entity that registers at Apresa
Password: The password that the other entity must provide to register at Apresa as this telephone number
To route calls to a registered telephone, use the Forward call action, and select Registered phone.

SIPREC: This section is available if the SIPREC option is enabled. Enable SIP REGISTER if Apresa needs to register itself as a SIPREC recording server. This is not needed for all SIPREC implementations.

Actions Rules: When an incoming call arrives, the system will verify if the call satisfies the conditions of rule 1. If so, then action of rule 1 is performed. Otherwise, the system will verify if the call satisfies the conditions of rule 2. If so, then the action of rule 2 is performed. Otherwise, the system will verify if the call satisfies the conditions of rule 3. And so on. Because at least one action rule has to be performed, the last rule has the condition "Always".

Condition:
- **Always:** The selected action will be performed unconditionally.
- **Check source telephone number:** The condition is satisfied if the telephone number of the initiator of the call matches any of the specified telephone numbers. Multiple telephone numbers can be specified separately, or using the wild cards * and ?, meaning * = any number of digits, ? = one digit.
- **Check destination telephone number:** The condition is satisfied if the telephone number of the receiver of the call matches any of the specified telephone numbers. Again the same wildcards are allowed.

Action: There are the following possible actions:
- **Reject call:** This causes the call to be terminated.
- **Accept call:** The call is answered. The system will keep the call active, until the remote side ends the call.
  - o Play test tone: Enable this option to let the system playback test tone into the call. Otherwise, the system will remain silent. If the option "None" is chosen, it will not even send RTP packets; this can cause a time-out error on some systems.

- **Forward call:** The call is forwarded to one of the two SIP lines (defined earlier). When forwarding, there are the following options:
    - o **Forward destination:** The SIP line to which to forward the call, or alternatively forward to registered phones (see SIP Registrar)
    - o **Protocol:** Controls over which transport protocol the SIP is forwarded. Original will use the same protocols for the incoming and outgoing call.
    - o **Destination phone number:**
        - ▪ **Original:** the destination telephone number is not changed, except that an optional dialing prefix can be removed from and/or added to the start of the phone number. This causes the system to behave like a SIP proxy.
        - ▪ **Read phone number:** This is for use with the MoReSo sim-chip.
        - ▪ **Fixed:** the call is forwarded to the custom fixed telephone number that is filled in
    - o **Source phone number conversion:** When forwarding a call to another SIP line, it might be needed or desirable to change what is reported as the telephone number of the originator of the call. This might be needed because the SIP line is a SIP trunk that allows only some source telephone numbers. Or secondly, it might be desirable, because it allows the final receiver of the call to see the right call-back number. The conversion table has the following format: Original number=New number. On the left hand side, in the original number, it is allowed to use * to match any phone number.
    - o **Stay in loop:** When Apresa stays in the loop, this means all audio of the call must continue to flow through it, and bringing down Apresa, will cause the active calls to be dropped. When this option, "stay in the loop", is disabled, an attempt is made to stay out of the loop, but this is not guaranteed.
    - o **Use username for caller:** When forwarding to a SIP line, it will use the username of the SIP line registration as the source telephone number.
- **Play notification message:** An audio message will be played back into the call, and then the system will proceed with the next action. Click the Upload button to upload an audio file that contains the audio message that must be used as notification message. The audio file will be converted to an internal format for playback. If the audio file cannot be converted, first convert the audio file to a supported format (for example PCM .wav format).
    - o **Send notification to:** This option decides if the notification message will be heard by the caller or the receiver of the call.

- **Selection menu:** This allows the caller to make a choice using dial codes 0-9 or * or #. Upload an audio message to be played. Select the rule to jump to when a dial code is pressed by the caller. If no actionable dial code is pressed for the specified timeout period, then the timeout action will be performed. Without a timeout, the software will wait until the caller makes a choice or hangs up. The timeout can also be used to trigger repeat of the audio message, by selecting itself as the timeout action.
- **Store this call:** This signals to the recording component that the recording of the call must be stored, when store on demand is enabled.
- **Start recording:** This signals to the recording component that recording of the call must start, when recording on demand is enabled.
- **Delete:** This signals to the recording component that the recording of the call must be deleted. This also works when the Delete on demand option is switched off in the Recording settings.

Apply: New action rules and conditions can be applied without restarting, by clicking the Apply button. Active calls will not be dropped.

Example: store when permission to record is granted
Goal of the example: Ask permission to store the call, and only then store the call.

Rule 2 of the example is:

2.	Condition:	Always	⌄
	Action:	Selection menu	⌄
	Notification message:	Upload	
		Action	
	Dial code 0	None	⌄
	Dial code 1	Rule 3	⌄

Upload an audio file with the following content: "If you grant permission to record this call, please press 1."

Rule 3 of the example is:

19.10   Certificates

Tools → Certificates

To reach this page, open the **Tools** menu, and click **Certificates**. Via this page, certificates can be managed on the Apresa. The certificates are used for authentication and setting up encrypted connections with other network entities.

> Note: The chapter HTTPS for encryption of the communication shows which steps to take to enable HTTPS.

This page shows a list of all the certificates managed via the web interface. It indicates for which certificates a private key is available and which certificates are trusted.

Select a certificate and click Edit to view or download it, and edit its name and whether it is trusted.

For a certificate to be used for setting up a secured connection in which the Apresa functions as the server the private key of the certificate is necessary. An example is the HTTPS protocol to secure the communication with the web interface.

If the Apresa functions as the client and wants to connect to another server via an encrypted connection, the other server will present its own certificate. If this certificate is not issued by a recognized certificate authority, the Apresa may reject the certificate and the connection will not be made. Certificates can be imported and set to trusted, so that the Apresa can recognize the certificate and complete the encrypted connection. An example where this may be necessary is if LDAP synchronization is done via the secured LDAPS protocol.

There are a number of ways of creating certificates in the Apresa:
• creating a new self signed certificate
• uploading an existing certificate
• creating a certificate signing request. Together with such a request, a private key is generated on the Apresa. This request can be downloaded and send to a certificate authority for creating a signed certificate. The resulting certificate can then be uploaded to the Apresa. With this method, the private key will not have to leave the Apresa server.
• using Let's Encrypt

Note: for HTTPS to work, it must be enabled in the Network settings.

19.10.1   Edit Certificates

Tools → Certificates → Edit

Select a certificate and click **Edit**. On this page individual certificate information is shown.

Name: The name of the certificate in the certificates page. It can be edited here. It is only used for reference and not part of the certificate.
Common name: The common name of the subject in the certificate
Trusted: Toggles if the certificate is added to the list of trusted certificates of Apresa.
Private key: Shows if a private key is available for this certificate. A private key is needed by the web server for doing HTTPS, and for the VoIP Service for doing SIP over TLS.
Web server access to the private key: This option should normally be disabled. It needs to be enabled if the certificate will be used for ADFS (SAML).
Show certificate information: This will output all contents of the certificate
Show intermediate certificate information: This will output all contents of all intermediate certificates.
Used for: This will show what the certificate is currently used for. Double clicking on the entries will redirect to the page where this can be managed.

Download
Here the certificate and possibly the intermediate certificates can be downloaded from the Apresa.

Let's Encrypt

These options are exclusive to certificates obtained from Let's Encrypt.

Revoke: This will make a request to Let's Encrypt to revoke this certificate. Revoked certificates can still be used, but may be rejected by other applications if they check the revocation status of the certificate at Let's Encrypt.

Renew now: This will immediately try to renew the certificate, regardless of when it expires.

19.10.2   Creating a self signed certificate

Tools → Certificates → Add

Click on Certificates in the Tools menu. Click on Add. Via this page, a self-signed certificate can be created.

Name: This value is shown on the certificates page to identify a certificate in the database. It has no meaning for the created certificate itself.

Days valid: Specify for how many days the certificate is valid.

IP Name or IP Address: This is the hostname for which the certificate will be valid. It will be used for the Common Name in the subject of the certificate.

The following optional properties can also be added to the certificate subject of the certificate.

- Country Code
- State or Province name
- Locality or City
- Organization
- Organizational unit
- E-Mail address

Additionally, multiple subject alternative names for the host can be specified. These are alternative names for which the certificate is valid. Currently three different types of subject alternative names can be added via the web interface:

- **DNS:** Specifies a DNS domain name. If the Apresa has multiple different IP names, they can all be specified as a DNS name.
- **IP:** Specifies an IP address. Adding a IP address name, will also make the certificate valid if the Apresa is approached directly via its IP address.
- **URI:** Specifies a uniform resource indicator, like a SIP URI.

Empty alternative names will not be included in the certificate.

The option "Copy common name to subject alternative name" is on by default and will copy the Common Name (filled in as IP Name or IP Address) to the subject alternative names. If this is not desired, this option may be unchecked.

Note that when a self signed certificate is used, warnings may be generated or the certificate may be rejected entirely. For example, if a self signed certificate is used for an HTTPS connection, browsers will warn about this. To get around these issues, the certificate would have to be imported by the clients that are connecting to the Apresa. Alternatively, a certificate issued by a trusted certificate authority can be uploaded to the Apresa instead.

Note: If you have manually configured lighttpd to use a custom certificate on the command line, this configuration might be overwritten or create a conflict, when configuring HTTPS certificates in the web interface.

Advanced settings

Enabling this checkbox will show more options for including certificate extensions. The default selection should suffice for most applications, but if desired adjustment to these extensions can be made here. Note that for a certificate signing request that while the extensions may be included, it is up to the certificate authority to decide if these extensions should be copied back into the signing certificate.

Common to all extensions

Critical: Marks the extensions as critical. If an extension is marked as critical and an application does not understand the extension, the certificate must be rejected. If the extension is not marked as critical, it can be ignored

Basic Constraints

Include: Include this extension in the certificate
CA certificate: Enable if the certificate is a certificate authority certificate.
Path length: If the certificate is a CA certificate, the path length indicates the maximum number of CAs that can appear below this one in a certificate chain

Key usage

Indicates for what purposes the public key of contained in the certificate may be used. If no key usage is selected, this extension will be omitted.

Extended key usage

Further refines the key usage extensions. If no extended key usage is selected, this extension will be omitted.

Secret Key:

Key type: This setting controls which type of keypair is generated for the certificate. By default, a keypair based on the RSA algorithm is generated. On Debian 10 elliptic curve keypairs can also be generated.
RSA bits: The length of the RSA key. The default length is 2048 and should be sufficient. The key length can be increased if desired, but this will require a higher computational cost.
Curve type: Which elliptic curve should be used to generate an elliptic curve keypair.

> Note: The chapter <u>HTTPS for encryption of the communication</u> shows which steps to take to enable HTTPS.

19.10.3   Upload a certificate

Tools → Certificates → Upload

Click on Certificates in the Tools menu. Click on Upload. Via this page an existing certificate can be uploaded.

Name: Name for the certificate that is shown on the certificates page. It has no meaning for the certificate itself.

Trusted: Set if the uploaded certificate should be added to the list of trusted certificates

Upload: In this section the certificate itself can be selected. All certificates must be uploaded in the PEM format. There are two ways to upload: either selecting the file containing the certificate, or by directly copy and pasting the contents of the certificate file.

Certificate: This is the certificate itself. The certificate should have the form:

-----BEGIN CERTIFICATE-----
[Certificate]
-----END CERTIFICATE-----

Private key: In case the certificate will be used by the Apresa to set up encrypted connections or authenticate itself, a private key is necessary. The private key should have the form:

-----BEGIN RSA PRIVATE KEY-----
[KEY]
-----END RSA PRIVATE KEY-----

or

-----BEGIN PRIVATE KEY-----
[KEY]
-----END PRIVATE KEY-----

Intermediate Certificate: If a certificate has been obtained from a certificate authority, the intermediate certificate with which the certificate has been signed, may also have been included. It may be necessary for the intermediate certificate to be send along with the certificate when establishing an encrypted connection. Uploading this intermediate certificate here, ensures that the Apresa can do this.
As it is possible for there to be more than one intermediate certificate, this option will accept multiple certificates bundled in one file. All certificates should be delimited with:

-----BEGIN CERTIFICATE-----
[Certificate]

-----END CERTIFICATE-----

Note: The chapter HTTPS for encryption of the communication shows which steps to take to enable HTTPS.

19.10.4 Certificate signing request

Tools → Certificates → Certificate Signing requests

Click on Certificates in the Tools menu. Click on Certificate Signing requests.

Via this page, a certificate signing request can be created. A certificate signing request can then be send to a certificate authority to obtain a signed certificate. The finalized certificate can then be uploaded to the Apresa. This means the private key will be generated and will remain on the Apresa.

Name: This value is shown on the certificates page to identify a signing request in the database. It has no meaning for the created signing request itself.

IP Name or IP Address: This is the hostname for which the certificate will be valid. It will be used for the Common Name in the subject of the certificate.

The following optional properties can also be added to the certificate subject of the certificate.

- Country Code
- State or Province name
- Locality or City
- Organization
- Organizational unit
- E-Mail address

Additionally, multiple subject alternative names for the host can be specified. These are alternative names for which the certificate is valid.

Currently three different types of subject alternative names can be added via the web interface:

- **DNS:** Specifies a DNS domain name. If the Apresa has multiple different IP names, they can all be specified as a DNS name.
- **IP:** Specifies an IP address. Adding an IP address will also make the certificate valid if the Apresa is approached directly via its IP address.
- **URI:** Specifies a uniform resource indicator, like a SIP URI.

Empty alternative names will not be included in the certificate.
The option "Copy common name to subject alternative name" is on by default and will copy the Common Name (filled in as IP Name or IP Address) to the subject alternative names. If this is not desired, this option may be unchecked.

Note that when a self-signed certificate is used, warnings may be generated, or the certificate may be rejected entirely. For example, if a self-signed certificate is used for an HTTPS connection, browsers will warn about this. To get around these issues, the certificate would have to be imported by the clients that are connecting to the Apresa. Alternatively, a certificate issued by a trusted certificate authority can be uploaded to the Apresa instead.

Note: If you have manually configured lighttpd to use a custom certificate on the command line, this configuration might be overwritten or create a conflict, when configuring HTTPS certificates in the web interface.

Advanced settings

Enabling this checkbox will show more options for including certificate extensions. The default selection should suffice for most applications, but if desired adjustment to these extensions can be made here. Note that for a certificate signing request that while the extensions may be included, it is up to the certificate authority to decide if these extensions should be copied back into the signing certificate.

Common to all extensions

Critical: Marks the extensions as critical. If an extension is marked as critical and an application does not understand the extension, the certificate must be rejected. If the extension is not marked as critical, it can be ignored

---

Basic Constraints

Include: Include this extension in the certificate
CA certificate: Enable if the certificate is a certificate authority certificate.
Path length: If the certificate is a CA certificate, the path length indicates the maximum number of CAs that can appear below this one in a certificate chain

Key usage

Indicates for what purposes the public key of contained in the certificate may be used. If no key usage is selected, this extension will be omitted.

Extended key usage

Further refines the key usage extensions. If no extended key usage is selected, this extension will be omitted.

Private Key:

Key type: This setting controls which type of keypair is generated for the certificate. By default, a keypair based on the RSA algorithm is generated. On Debian 10 elliptic curve keypairs can also be generated.

RSA bits: The length of the RSA key. The default length is 2048 and should be sufficient. The key length can be increased if desired, but this will require a higher computational cost.

Curve type: Which elliptic curve should be used to generate an elliptic curve keypair.

Note: The chapter HTTPS for encryption of the communication shows which steps to take to enable HTTPS.

19.10.5   Let's Encrypt certificates

Let's Encrypt is a service to acquire a free certificate that will automatically be trusted by any reasonably modern browser. To obtain a Let's Encrypt certificate, it is required that Let's Encrypt can verify that you control the domain for which you are requesting the certificate. This means that the Apresa must be reachable via the Internet with this domain name.

Register:
Before a certificate can be requested, it is required that an account is created at Let's Encrypt and that their subscriber agreement is accepted. The E-mail address provided here will be used by Let's Encrypt to notify you when a certificate is about to expire.

Get certificate:
Use this option to obtain a Let's Encrypt certificate after registering.

Name: The name by which the certificate is identified in the Apresa database. It has no meaning to the certificate itself.
Key type: Which type of keypair is generated for the certificate. Keypair generation based on the RSA algorithm is the default. On Debian 10 based systems keypairs based on elliptic curves can also be generated.
RSA bits: The length of the RSA key. The default length is 2048 and should be sufficient. The key length can be increased if desired, but this will require a higher computational cost.
Curve type: Which elliptic curve should be used to generate an elliptic curve keypair.

Domain names:
Here domain names can be added for which Let's Encrypt will try to issue a certificate. Let's Encrypt will check if you control all domain names provided here, so the Apresa must be reachable over the internet by all domain names provided here. It this is not the case the issuing of the certificate will fail. Note that neither wildcard certificates nor IP addresses are not supported.

Update E-mail:
Use this option to update the E-mail address of the Let's Encrypt account.

Deactivate account:
This will deactivate the registered Let's Encrypt account. This means this account can no longer be used to request or revoke certificates. Note that is still possible to revoke certificates with their private key instead.

Deactivating the account is not reversible. Once deactivated, a new account must be created.

Automatic renewal:
Certificates issued by Let's Encrypt are valid for 90 days, so must be renewed regularly. When automatic renewal is enabled, the Apresa will try to automatically renew certificates that will expire in 30 days. When certificates are renewed or fail to renew in this manner, an E-mail will be sent to the administrator E-mail address or addresses.

Alarms for expiring certificates

When a certificate expires, it will generally not be accepted anymore and must be replaced. Otherwise, possible service interruption can occur. Via these settings, alarms can be generated on the system information page for certificates that are expired are about to expire so that an appropriate action may be undertaken.

Generate alarms for certificates with private key: Enabling this setting will generate alarms for expiring certificates for which the private key is also available.

Generate alarms for certificates without private key: Enabling this setting will generate alarms for expiring certificates for which no private key is available.

Generate alarms when certificates expire in x days: This setting controls how long before a certificate expires an alarm is generated.

> Note: The chapter HTTPS for encryption of the communication shows which steps to take to enable HTTPS.

19.11 Export & Import

19.11.1 Backup

Tools → System → Backup

The Backup page can be reached from the System page, which can be reached from the Tools menu by administrators.

Backup destination
Apresa can backup the call database with all recordings to another network drive, to a local disk, or (advanced) to a location on its own file system.

Type:
Choose the Type from the **dropdown** menu: Network drive, Directory (mounted disk), Directory, Local Disk, or SFTP.

Backup to a Network drive:

Windows Domain Name: The domain name where the destination network drive is located.
Username/Password: Fill in the login details if authentication is required to write to the network drive.
Server name: The Windows server name or the IP address of the server of the network drive.
Network share name: The Windows name of the network backup drive.
Backup directory: The subdirectory on the network drive where Apresa must write the backup.

Backup to a Directory (mounted disk):

Backup to the specified Linux directory. The directory must be a reference to a local or remote disk (it must be a mount point). The mount point could be created by the user using the system shell.
Backup directory: This is the Linux directory path at the Apresa server, where the backup must be written.

Backup to a Directory:

This method allows the backup to be written to an arbitrary directory, even when it is not a mount point. Use with care. Writing the backup to an unsuitable directory, for example a directory that is located on the main disk partition, can fill up disk space, and cause system malfunction.

Backup to a Local disk:

Local disk: This selection box lists the detected (USB) disks and partitions.
Backup directory: The subdirectory into which to write the backup (optional).

Backup using SFTP:

Server name: The SFTP server name or IP address. If the SFTP server is not running on standard port 22, add a colon and the port number. For example: sftp.company.com:2022
Log on method:
- Username/Password: Fill in the credentials for accessing the SFTP server. Export and restore backup currently only supports this type of log-on method.
- Key-based authentication: In this case the password does not need to be filled in, but the username needs to be specified. The key of Apresa will be used. Click on the arrow button to view it. You will need to add this key at the SFTP server to allow access. It is currently not possible to use a custom key.
Backup directory: The directory at the SFTP server where to write the backup. This can be a relative path from the home directory of the user, or an absolute path. Example: /data/apresa/backup

When accessing a new SFTP server for the first time, an entry will be added to the known hosts file. If the server changes without changing the server name, the connection will be blocked. This is to avoid man-in-the-middle attacks. Manually changing the known hosts file is then needed to allow connections to the changed server.

Data to backup
You can specify a time range that must be backed up. Recordings that have a start date in this time range are backed up, others are skipped. The database is always copied in its entirety.

Select what data to backup:
- Database & Recordings: This option is for creating a backup of all data.
- Database: The database contains the Apresa settings and configuration, and meta-data about the calls, but not the recordings itself.

Retention period
Delete database backup older than ... days: If backup is run daily, a new database file (apresadb....sql.gz) is created on the backup each day. Specify the number of days after which these database backup files must be deleted by the system, or leave it empty, to keep all files.
Delete calls older than ... from backup: Recordings that are older than the specified number of days are deleted permanently from the backup. Meta-data in the backup is not effected by this setting, because it is in

the database backup files (see previous option). This option is only available if the system option "Retain information about calls in the backup" has been enabled and used to keep information about the calls in the backup.

When to backup
You can specify the time of the day when the backup must be run. When the update frequency is set to "Once", the backup will be run only once and then stop. Otherwise, the backup will be updated periodically, for example, once every week.

Diagnostics
When the backup fails, a diagnostic message is displayed for the administrator, when logged in (after refreshing the page), and if email is configured, it is also sent by email. The email status is also part of the health status page.

- Could not resolve address for X: Name or service not known
The lookup of the IP address for the name failed. Use the IP address instead, as "Server name".

- Unable to find suitable address
The IP address is incorrect or unreachable

- E(2): No such file or directory
The subdirectory is incorrect

- E(6): No such device or address
The Network share name does not exist

- E(13): Permission denied
Incorrect user name or password

- E(16) Mount is denied because the NTFS volume is already exclusively opened
The disk is already mounted. Unmount it first. Or point to the existing mount point, using the option "Directory (mounted)"

- E(20): Not a directory
The main directory is incorrect

- Protocol negotiation failed: NT_STATUS_CONNECTION_RESET
This could be due to a SMB version mismatch.

19.11.2 Retain information about calls in the backup

System → System Settings → Retain information about calls in the backup → Configure

This page can be reached from the System settings, clicking Configure next to the option "Retain information about calls in the backup".

Description of the relevant option in the System settings:

> **Retain information about calls in the backup:** Store the meta-data of calls in the backup, even after they are deleted from the main storage, until they are deleted from the backup archive by the system. This option is needed for quickly performing actions on the backup (for deleting tenant data from the backup, and for applying a retention period on calls in the backup).
> When disabling this option, information about the calls in the backup is no longer retained (the information is deleted). After enabling this option, calls that are newly written to the backup, are registered (information about it is remembered). To fill the registry with information about calls that were copied to the backup before this option was enabled, click Configure.

Number of Records: This is the number of calls in the backup that the system has retained information about.

To add information about existing calls in the backup, click **Browse**, and select a backup database that exists in the backup directory, and then click **Import**. This will only work if the backup is configured and access to it is working. The import process will take time. The page will reload automatically until the process is completed. It is possible to do other things, while it is busy importing.
The process described above of importing existing information from backup databases is not needed if the option "Retain information about calls in the backup" has been enabled for the whole time that backup was performed.

After importing one or backups, it can be preferable to let the system recalculate the Tenant backup statistics.

19.11.3 Restore backup

Tools → Export & Import → Restore backup

The Restore backup page can be reached from the Export & Import page, which can be reached from the Tools menu by administrators.

Apresa can put back the content of a previously made backup.

The options on the Restore page are similar to those on the Backup page. Additional options:

Filename of database backup: The date of the backup is normally included in the filename, for example apresa20110201.sql.gz is the backup of on the 1st of February 2011. In this way, you can choose to restore the system to the state on a specific date. Use the Browse... button to avoid mistakes in entering the filename, and to verify that the other settings, such as the backup directory, have been set correctly.

Restore method: There are two restore methods:
- **Restore calls:** Only the recordings are restored from the backup. Recordings are added (no recordings are deleted).
- **Full restore:** This action will **ERASE** the current data on the Apresa, and replace it with the content of the backup. This includes the recordings, settings, and licensing.

The restore action is performed at once.

19.11.4   Export to other Apresa servers

Tools → Export & Import → Export to Apresa server

Recordings from an Apresa can be exported to another Apresa.

The protocol that is used is *SFTP*, which means the transmission is secured. The *public* key authentication mechanism is used. This means no password needs to be shared between the two recorders, only the public key of the sending Apresa.

Configuration of the *sending* Apresa
The Apresa can send recordings to another Apresa. To configure this feature, in the **Tools** menu, select **Export & Import**, then click the **Export** button. This will take you to the screen called **Export recordings to another Apresa server**.
To add an export target, click the **Add** button.
- **Enabled:** If an export target is not enabled, it is not processed

- **Description:** This description will be used to refer to this export target, for example in error reports
- **IP Name of IP Address:** The connection address of the Apresa to which the recordings must be sent
- **Filter:** When the filter is empty, all recordings will be exported. Otherwise, only the recordings of the phones of the specified user or group are exported.
- **Restart from the beginning:** Enable this option, to start again exporting from the first and oldest record.

In this same screen, the **public key** of this Apresa can be viewed. We will need this information to configure the receiving Apresa to accept our recordings.

Configuration of the *receiving* Apresa
To allow another Apresa to upload recordings to our Apresa, this has to be specifically allowed first. To do so, in the **Tools** menu, select **Export & Import**, then click the Import button. Then click the **Add** button.
- **Name:** A descriptive name to remember which server we have given permission
- **Public key:** The public key of the Apresa that will be allowed to connect and upload recordings. The key starts with ssh-rsa.

For this feature to work, it is needed that the **Remote shell** is enabled in the **System settings**. Options → System settings → System → Remote shell. For safety, it is essential that the default password is changed.

19.11.5   Export recordings to network drive

Tools → Export & Import → Export to network drive

The Apresa can export its recordings to a network drive. This option is found in Export & Import of the **Tools** menu. This functionality is similar to Backup, but it has the following differences:
- The call information is stored as an XML file
- The data cannot be loaded back into the Apresa. If this is important, use Backup instead.
- The files are stored in the root of the export directory, not in subdirectories.

Export recordings: There are three options: Never, At request, Always. "At request" means that the recording is only exported if marked as such during the call using the Apresa API.

From: Use this option to reset the export to the beginning, or to let it export only new recordings (skip any in between), when that is needed.
Filter: Only export recordings of the selected group, that is, if the telephone number of the call matches with the telephone number of one of the users in the selected group.
Filename: Optionally specify a custom file name formatting used in the export.
Export XML: If enabled, information about the call (telephone number etc.) will be stored in an XML file, alongside the recording files. The XML file has the same file name as the recording, except another extension.
Include custom directory information in XML: This will write the specified directory, together with the filename, in the XML file.
Verify telephone number: This is a custom feature, not intended for general use (by default it is off).
Export screen recordings: If disabled, then the screen recordings will not be exported.
Delay export if no screen recording is yet available: This will delay the export of recordings for which the screen recording is not yet uploaded by Apresa Client. If the screen recording is not available after 60 seconds, the recording is exported without.
Delay export: This will delay export of recordings until the number of specified minutes after the end of the call. In the mean time, the notes or category of the recording could be edited, and this will be reflected in the delayed export.

The export destination options are described on the Backup page.

Special options not needed for normal use
Include custom directory information in XML: If enabled, the XML data will contain a tag with this custom directory information, followed by the wave file name. For example C:\data\20140424_145959_o9413.wav. The underlined text (C:\data\) is the text that should be entered in this option to get this effect.
Verify telephone number.

XML Format
Inside the <callinfo> tag, the following tags can be present:

startdate	date and time of the start of the recording (the call), in the format: YYYY-MM-DD hh:mm:ss
start_ms	start time milliseconds portion (not always available)

duration	the duration of the recording in seconds
duration_ms	duration milliseconds portion (not always available)
local / remote / caller / receiver	detected phone numbers
local_name / etc.	the associated name of the detected phone number
direction	0=incoming, 1=outgoing, 2=internal (both sides local), 3=external (both sides external)
category	the number of the category
notes/notes2	primary and secondary notes of the recording
data	custom data added using the API
id	ID of the recording (unique within the recorder)
recording	file name of the audio recording
location	the custom directory information plus the file name

19.11.6 Import from another recorder

Tools → Export & Import → Import from other recorder

Apresa can import recordings made on other Vidicode call recorders. This option is found in Export & Import of the **Tools** menu. For example, recordings made on an analog/digital CR Single, Call Recorder PRI, Call Recorder ISDN, CR Quarto, CR Octo, etc. can be easily imported. The import is based on FTP.

Table column	Explanation
Enabled	Yes/No. Import is enabled/disabled.
Description	Free text field.
IP Name or IP address	IP address (or name) from the recorder to import from.
Username	Username to login (password is on the "Edit" page)
Error status	Status of the connection with the Recorder. For instance: "Ok", "Logon NOK", "No file-list", etc.
Date of last imported call	If "Restart from date" isn't used, the system will use this to search for newer files.

Extra fields in the Edit recorder dialog:

Fields	Explanation
Password	Password to login
Define new password	If you enable this option you can define a new password
Import every (minutes)	The interval the system will try to import new recordings.
From date	The first date to start importing recordings
Restart from date	Enable the "From Date" importing of recordings. This setting will be automatically disabled after the import.

If there is an error during the import, Apresa will start the next import round beginning with the failing file. The "Import every (minutes)" setting also defines the interval between retries after a failure. It makes sense to set the "Import every (minutes)" setting to a low value, when you want to import a large amount of recordings.

The audio files that are stored on the recorders are imported into Apresa without converting into another codec. Audio files that use the G.723 codec can be converted to MP3 and played back inline on Debian 8 and 9 (on older Debian 8 systems, it might require the libav-tools update). On other systems, the files cannot be converted to MP3, which means inline playback is not possible. To listen to the audio, the audio file can be downloaded, and could be played back using VidiPlayer.

19.11.7   Import from Araña

Tools → Export & Import → Import from Araña

Araña is a Vidicode product that runs on a Windows PC or server, and can maintain an archive of recordings imported from other Vidicode call recorders.

To import an Araña database, the archive can be read from a network share, or from a connected USB disk. The configuration options to read the Araña archive are similar to those on the **Backup** page.

Click on Enable to start the import action. Refresh the page to see the progress.

Multi-tenancy is applied to the new recordings during import, based on the current configuration.

The audio files are imported into Apresa without converting into another codec. Audio files that use the G.723 codec can be converted to MP3 and played back inline on Debian 8 and 9 (on older Debian 8 systems, it might require the libav-tools update). On other systems, the files cannot be converted to MP3, which means inline playback is not possible. To listen to the audio, the audio file can be downloaded, and could be played back using VidiPlayer.

19.11.8   Configuration management

Tools → Export & Import → Configuration management

This option is found in Export & Import of the **Tools** menu. Use this option to save and restore the configuration (settings) of Apresa.

Saving the configuration will only save the settings, not the recordings. To make a backup of the configuration and the recordings, see [Backup](#).

Restoring the configuration will replace the existing settings. This action cannot be undone, unless you have first saved a copy of the configuration. Restart might be needed to apply all the new settings.

When restoring the configuration, you can choose if the network configuration should be restored or not.

19.12   System

Tools → System

The System page can be reached from the Tools menu by administrators.

At the top of the page, the current version of Apresa is displayed.

19.12.1   Software update

Tools → System → Software Update

In the update screen you can perform Apresa updates, and configure updates for the Debian operating system.

Apresa updates

Apresa updates are provided during the service period. If the service period has expired, the service period can be extended using a service license key (in the system settings).

Apresa can check for updates online, or you can manually download an update, and upload it to Apresa.

• **Online-update:** To check for an update online, click the "Check for Update" button. Apresa will need internet access for this to work. A description of the update will be displayed. To execute the update, press the Download button. The update will be downloaded from the Vidicode server and then installed.

• **Upload:** If you have an update file available, with this option you can manually upload it to the Apresa server. Apresa will not need internet connection in this case. After it is uploaded, the update will be installed. The perform a regular update using the official channel, the update file and change log can be retrieved from the Vidicode server manually.

Debian operation system updates

Debian security updates are provided by the Debian community during the long term support period. When this period has expired for a particular Debian version, security updates are no longer provided.

Automatic security updates: This displays if Apresa is configured to install security updates. In addition, a number of prerequisites needs to be satisfied for updates to be installed:

• Required Debian packages for unattended updates. These can be installed by enabling the Install checkbox.
• Online connection. Apresa needs to have outbound internet access.
• A supported Debian version (long term support period)
• The Debian package system needs to be in a good consistent state. Installing incompatible or broken packages can result in the system no longer being able to update automatically.

Frequency update check: Apresa can check daily for new security updates. In addition, if you want to run the update check immediately, enable the Run now checkbox. Running a security update can take 5 minutes or more, depending on how many packages need to be upgraded.

If anything was upgraded, a confirmation email is sent to the administrator email address.
During upgrade, there can be an interruption of the functionality of the recorder, for example when the database engine needs to be restarted after upgrade.

Server for installing Debian software: This server is not used for security updates, but for installing additional software. Input a nearby server from the mirror list, or alternatively for Debian 9 http://deb.debian.org/debian/ could be used.
Notice: Generally it is not recommended to install additional software, because it could interfere with the normal operation of the recorder.
This server can be used when installing the Debian packages needed for unattended security upgrades.

19.12.2 Encryption

Tools → System → Encryption

The Encryption page can be reached from the System page, which can be reached from the Tools menu by administrators.

- **HTTPS**

Apresa can provide a secure web interface, to prevent that web pages or downloaded recordings are intercepted by a third party. To enable a secured web interface, a certificate must be created first. Apresa can use an existing certificate and private key, or it can create a self-signed certificate based on the contact information that you fill in. After the certificate has been created, the Browser protocol must be set to HTTP + HTTPS (or HTTPS only), on the Network tab in the System settings, and the certificate selected there. When first accessing the Apresa web interface using HTTPS, the browser will present a warning if the certificate is self-signed. Browsers usually have an option to add a security exception for a specific certificate.

- **Encryption of call content**

To enable call content encryption, click the Enabled checkbox, and fill in a pass phrase in the Password field. It is important to remember this pass phrase, in order not to lose access to the data.
It is possible to change the pass phrase. Click "Define new password", and fill in a new pass phrase. This new pass phrase will be required to unlock both new and earlier encrypted calls of this system.

See also: Data Encryption.

19.12.3   Backup

Tools → System

Backup:
To backup the **call database**.
See: Backup from the Export & Import chapter.
Restore backup:
To restore the backup of the **call database**.
See: Restore backup from the Export & Import chapter.
Configuration management:
To backup the Apresa settings.
See: [Configuration management](#) from the Export & Import section.

19.12.4   Audit Trail

Tools → System → Audit Trail

Enable the audit trail to collect information about actions performed by users on the Apresa system.

The audit trail can be enabled in the System settings. On the System tab, enable the Audit Trail option. The audit trail can be stored in files or in the database, or in both.

Logs created for tenants can be viewed by a (non-tenant) administrator. Tenant administrators can access their own audit trail log, and the audit trail logs of their users.

View
To view the audit trail, open the Tools menu, choose System, and then click the Audit Trail button. The audit trail files or database will be shown depending on what interface has been chosen in the system settings.

The contents of the Audit Trail
The audit trail contains actions performed on data or system actions. If the option "Include data views in Audit Trail" is enabled, then also viewing of data and search parameters are logged in the audit trail.
- Date and time when the action was performed

- IP address from which the action was performed if the action was done using the web interface
- User that performed the action. Actions that were triggered using a telephony dial code action might not have an associated user
- A description of the action that was performed

File-based audit trail
Per user, a file can be downloaded which contains a log of actions performed by this user.

Database audit trail
A list of audit trail entries are displayed. It is possible to search for entries within a certain date or time range, that belong to a specific user, or that contain the specified text in its description.
The user field can be empty if the action was not associated with a user (when done through DTMF), or the user account was deleted in the mean time.

List of included actions
The following actions (among other things) are logged in the audit trail:

- Log in / log out
- Playback/download (active) call
- Edit notes / annotations / category of a call
- Delete call

- Backup: configure/start, stop, restore
- Configure export recordings
- Free-seating configuration
- Set time
- Unlock decryption/playback key
- Create self-signed HTTPS certificate
- Factory reset / removing of licenses

- System restart / halt
- Network restart
- Recording component restart

- Trace on/off
- Download log files
- Card log files: download, delete

- User groups: add/edit/delete

- Users: add/edit/delete
- Import/export users from/to CSV
- User changing their own password

- Install card driver
- System update: internet/file

- Change card setting
- Change telephony settings
- Change display settings
- Change recording setting
- Change system setting

19.12.5   System actions

Tools → System

Restart network: Restarts the ethernet network interfaces.
Restart recording component: Restarts the VoIP and Card recording components. Hold the shift key to remove the cache of the VoIP engine during restart. The cache might contain information on where agents are logged in.
Restart system: The complete Apresa system will shut down, and then reboot.
Shutdown system: The complete Apresa system will shut down, and remain switched off.

Install driver: Use this if a recording card is added to an existing Apresa system without cards.

19.12.6   Date & time

Tools → System → Set System Time
Tools → System → Set system date & time

The current local Apresa system date and time is displayed here. It is recommended to let the time be adjusted automatically using NTP (See Network tab of System settings). If NTP is not used, or if the time is too far off, the date and time can be set here manually. As a first thing when configuring an Apresa system, the time zone should be set correctly. This is required for NTP to work properly.

19.12.7 Diagnostics

Tools → System

Download Log Files: Downloads a package of recent log files, plus the most recent network trace. Usually this is sufficient for analysis.
Download Extended Log Files: Downloads a larger set of log files, including operating system level log files, plus the most recent network trace.
Network trace: The network trace records all data that is seen by the first and second ethernet ports. This can be used to diagnose a problem with VoIP call recording. Note: Only one network trace is kept on the system. Making a new traces, removes the previous trace. Downloading a trace, removes the trace from the Apresa. To make multiple traces, download the log files after each trace.
By default, tracing is limited to a certain maximum number of packets. If this limit is reached, the trace stops automatically. To trace without this limitation, click on the right part of the Enable button, and choose "Unlimited trace".
Archive log files: These contain:
- Detailed card recording log files if enabled in the settings (System settings, System, Detailed logging of card recording). This applies to analog, TDM, and ISDN recording.
- Log files that were automatically archived when an error occurred if enabled in the settings (System settings, Alarm, Collect log files on error)
System information: Displays a range of detailed information, including the detected health state.

System Information

Server time:	2018-06-18 10:45:39
Local time:	2018-06-18 10:45:39
Software serial number:	1234567
Apresa version:	9.0.0.0
VoIP channels:	0
G.729 channels:	0
RTA channels:	0
Digital TDM channels:	0
Analog channels:	0
ISDN PRI channels:	0
Add-ons:	Agent Evaluation
Linux Distribution:	Unknown
Kernel version:	Unknown
Hard disks:	Disk sda: 931 GB Disk sdb: 931 GB
Software RAID:	RAID1
Hardware RAID:	Not used
Card driver:	Driver not installed
Recording cards:	Digital TDM card S/N 123456 with 16 channels configured for Ericsson MxOne Analog card S/N 654321 with 8 channels
MAC addresses:	

System health

Measured quantity	Value	Status
Power Supply		OK
Temperature of hard disk sda	40 °C	OK
Temperature of hard disk sdb	38 °C	OK
Temperature of CPU Core 1	41 °C	OK
Temperature of CPU Core 2	33 °C	OK
Voltage Vcore	1.27 V	OK
Voltage in1	0.75 V	OK
Voltage AVCC	3.31 V	OK
Voltage VCC	3.31 V	OK
Voltage in4	1.86 V	OK
Voltage in5	1.3 V	OK
Voltage in6	1.47 V	OK
Voltage 3VSB	3.3 V	OK
Voltage Vbat	3.18 V	OK
Speed of fan 1	2220 RPM	OK
Speed of fan 2	1318 RPM	OK

At the bottom of the System information page, the following buttons are shown:
- Reset resettable alarms
- Simulate a system error
- Network status

19.12.8   Network

Tools → System → System Information → Network status

This page lists the open network ports, currently active connections, and the firewall status.

This page can be reached as follows as an administrator:
- Menu Tools > System
- System Information (at the bottom of the page)
- Network status (at the bottom of the page)

Network ports
The port number and program name gives an indication of the purpose of the connection. The port number in the Local Address column is displayed after the colon (IP:PORT).
• Port 80 or 443 is used by the web interface and API, and accessed by a web browser or the Apresa Client.
• Port 22 is used for SSH, which is used for remote shell access (putty), and incoming connections when receiving recordings from another Apresa.
• Port 5060 or port 5061 is used by the VoIP Service if enabled (SIP protocol).
• Port 2016 is for incoming V-Tap connections.
• Port 123 is used for NTP (time synchronization)
• Port 9004 is used for connections with the Apresa Lync Plugin (Skype for Business)

Services
• lighttpd is the web server
• snmpd implements SNMP alerts and status information (menu Options > System settings > Alarm)
• yate handles incoming SIP calls (menu Tools > VoIP Service)
• mono handles the connections for Skype for Business on port 9004 (menu Options > System settings > VoIP > Apresa network service).
• avahi-daemon performs mDNS/zeroconf local network services
• ntpd performs time synchronization

Firewall
Included in the Debian repository is the firewall called Uncomplicated Firewall, abbreviated as ufw. See:
https://wiki.debian.org/Uncomplicated%20Firewall%20%28ufw%29
If it is not yet installed, it can be installed on the command line using apt-get. Its status is displayed on this page. See the documentation of ufw for details about enabling and configuring the firewall. Be careful to not lock yourself out of the web interface and remote system shell, or block essential services of the recorder.

19.13   Tenant call encryption

Tools → System → Call encryption

The Call encryption page allows the configuration of per-tenant call encryption, and can be reached from the Tools menu by a user with Tenant administrator: Call encryption permission. To reach this page and

configure call encryption for a certain tenant, this user needs to be a
[member](#) of the tenant.

19.13.1 Enabling / disabling call encryption

To enable the call encryption, click the enable box and fill in the
password twice and click apply. Any new recordings will be encrypted
after the recording has finished. To disable the call encryption, uncheck
the enable box and click apply. Any new calls will no longer be
encrypted. Previously recorded calls will remain encrypted and will still
require the password.

19.13.2 Changing the password

To change the password after it has been set, click the define new
password checkbox. Then provide the old password and the new
password twice. Changing the password in this manner, changes the
password of all previously encrypted calls as well. The old password can
then no longer be used to play these calls.

19.13.3 Resetting the password

If the password is ever lost, the password can be reset by clicking the
reset button. Any new recordings will no longer be encrypted until call
encryption is re-enabled again with a new password. Old recordings will
remain encrypted and the old password will still be required after for
playback or downloading of the recordings. If the call encryption is later
re-enabled with a new password after a password has been reset, this
new password will not apply to the old recordings.

20 The Options menu

The Options menu has nine sub menu's, which are visible to the user according to the permissions he has. The Administrator has all permissions and can add, edit and delete Users, User groups, Display settings, Recording settings and System settings

Menu buttons on the main screen
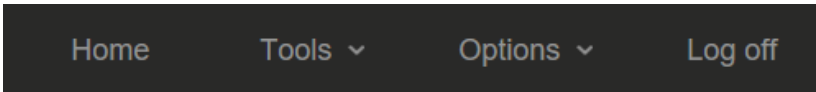
20.1 Personal settings

Options → Personal settings

The Personal Settings page can be reached from the Options menu. This menu option is only available when the system setting "Users can change personal settings" is enabled.

Password: Users can change their password, except if password verification is performed externally, through LDAP / AD or ADFS.
Display language: Users can also choose a custom display language.

20.2 Users

Options → Users

The users page can be reached from the Options menu by administrators. Administrators can manage the user list.

Name	User account	Username	Telephones	Member of
Administrator	✔	admin	0	
Alwin	✔	alwin	1	Organization, Support
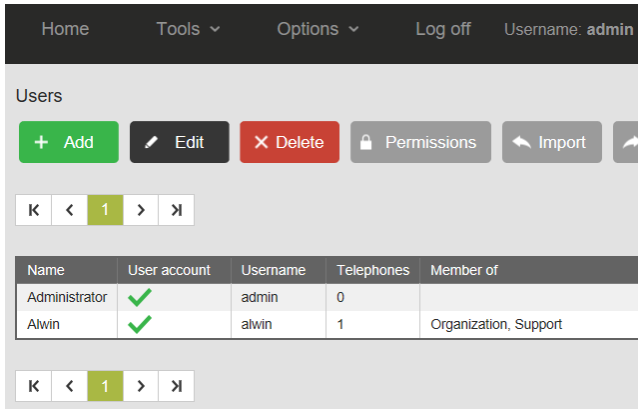
To create a new user account, click the Add button. In the next page, you can enter the details of the new user account. In the same way, an existing user account can be edited.

Name: This is the display name of the user. This can be different from the username (see below).

User account: The user account can be enabled or disabled. Only enabled user accounts can be used to log in.
Username: This is used by the user to log in.
Password: The password for the user account. You can generate the password automatically or fill it in yourself. The password must satisfy the requirements as specified on the system-settings page. If the new password is automatically generated it is also sent to the user by e-mail. If you let the system generate a password automatically, an email address of the user must be specified.

Log on method: The default log on method (Local verification) means that the password is verified by Apresa internally, based on the configured password.

When the log on method LDAP (AD) is selected, and the user logs on, the username and password are checked remotely on the Active Directory or LDAP server. If it matches, the user is allowed access to the Apresa. This means that you do not have to define the password in the Apresa, only the user name. The AD server address and AD user domain that is used during log on, is read from the Network settings. See chapter Active Directory on how to configure this.

If the method to Logon using external party is selected, the browser of the user is redirected to the website of the configured identity provider (ADFS or Microsoft online) to sign in, and then redirected back to Apresa. See also the "Logon using external party" option in the Network settings, and the "External logon service" option on the User Group page.

E-mail: The e-mail address of the user.

Group membership: A user can be part of one group (or more groups). All permissions of the group apply to the user also.

Telephones: A list of telephone numbers, SIP IDs, or TDM channels, that belong to the user. Usually, the IDs entered here should match the Local ID (or Remote ID) as displayed in the main call listing. An exception is when the setting "Usage of SIP ID as identification" is set to a non-standard value.

User account for free-seating: If enabled, this account will be usable for Apresa Client only. When logged in using the Apresa Client, calls will be filtered based on the name of the PC where the client is running. All channels or phone numbers that the user can possible use, should be added to the list of Telephones (above). Only the telephones that are present at the PC, according to the Seats configuration (defined in a separate screen), are monitored by Apresa Client. Each PC (called a seat) can have one or more telephones (a TDM channel or a VoIP phone number) associated with it. See Free Seating.

Use custom Local ID when logged in with Apresa Client: When enabled, the Local ID of calls will be changed to the Name of the logged-in user. This can be used in combination with the setting "User account for free-seating".

Playback only within time limit: This is a custom feature to allow access only to calls that were made within a certain time span.

If enabled, calls older than 30 minutes compared to the latest call and calls made before the last login are not accessible for that user.

Store on demand: Switches "Store on demand" to either on or off for calls with the specified telephones. When "Store on demand" is on, no calls will be stored, except those that are marked to be stored using a dial code action (See: VoIP settings) or using Apresa Client. If this option

is not specified here at the user level, the default setting specified in the Recording settings is used.

Permissions: These are personal permissions, in addition to the 'inherited' permission that the user has, because of group membership. It is recommended to use personal permissions only in exceptional situations. See [Defining groups and permissions](#).

Managed telephones: This is relevant for users that have a non-global "Edit user account" permission. The managed telephones setting specifies which phone number this manager may add to user accounts. The use of wildcards is supported: * (matches digits or text of any length), and ? (matches a single digit or character). For example, if 15? is specified, this means the manager may add the phones 150, or 151 (etc.) to user accounts, but not 160. This prevents a manager from giving himself access to calls that he should not have access to.

Web Client: Display settings for the web client can be changed here for users that have the web client permission. The last option in this menu hides these settings on the web client page itself, so that users are prevented from changing the settings there.

Calculated properties
Inherited permissions: These permissions are given to the user because of group membership. This permission list cannot be edited directly on this page. To edit these permission, edit the mentioned group.

To view a list of all calculated permissions for a specific user, select that user in the user list, and click the **Permissions** button.

Legacy properties
Manager: The manager is the user that created this account as a sub-account. This can be useful in a multi-tenant situation. The manager is not a full administrator, but has the "Manage user sub-accounts" permission.

20.3 User groups

Options → User groups

See also [Defining groups and permissions](#).

The **User groups page** can be reached from the Options menu by administrators. On the user groups page, all user groups are listed. Administrators can manage this list.

To create a new user group, click the **Add** button. In the next page, you can enter the details of the new user group. In the same way, an existing user group can be edited.

To delete a normal group, select the group, and press the Delete button. The users in the group will not be deleted.

To remove a Tenant from the system, select the group that represents the Tenant, and then press the "Delete tenant data" button. This will delete all associated recordings, user accounts, and sub-groups. This action cannot be reversed. *Remark:* a tenant cannot be removed unless you change the tenant into a normal group by clicking "Edit" and unchecking the Tenant checkbox.

For each user group, the following properties are stored:

Name: The name of the group

Higher level group: User groups are organized in a hierarchical tree. When selecting a higher level group, the current group will become a subgroup of that group. If this option is disabled afterwards, the group will no longer be a tenant, and its recordings will be unassigned from it.

Tenant: When enabled, different settings can be applied to users and recordings that belong to this group, for multi-tenancy. This setting is available only if Multi-Tenancy is enabled in the System settings.

User group

Name: West

Higher level group: Organization

Tenant: ☑

| Options | Schedule | Statistics |

Options:

Minimal recording duration:	5	seconds
Disk Usage:	0.0	MB
Maximum Disk Usage:	2000	MB
Delete calls older than ...:	50	days
Delete calls older than ... from backup:	50	days
Maximum number of channels:	10	(VoIP)

Available features for tenant:

Recording on demand: ☐

Silence on demand: ☐

Members: ➕ Add ✕ Delete

Member
No records found.

✏ Import ✕ Delete

LDAP group:

Permissions: ➕ Add ✏ Edit ✕ Delete

Permissions	User / User group	For whom is the permission
Level 2 administrator		This group and its subgroups

✔ OK ✕ Cancel

Options

Options of a Tenant:

Minimal recording duration: Recorded calls that are shorter than the specified duration, will be discarded. This setting takes precedence over the global setting in the Recording settings.
Maximum Disk Usage: When disk usage of the tenant reaches the maximum, old recordings of the tenant will be deleted automatically. Whether the listing in the database is also removed depends on the System setting "Remove auto-deleted recordings from the call listing".
Delete calls older than ...: Calls that belong to this tenant and that are older than the specified number of days are deleted permanently from the hard disk. The global auto-delete setting (System settings) is applied in addition to this setting.
Delete calls older than ... from backup: Calls belong to this tenant and that are older than the specified number of days are deleted permanently from the backup. The global auto-delete setting for the backup is applied in addition to this setting. This option is only available if the system option "Retain information about calls in the backup" has been enabled and used to keep information about the calls in the backup.
Maximum number of channels (VoIP): This defines the maximum number of VoIP calls of this tenant that are recorded simultaneously. This can be used to prevent one tenant from using all the available VoIP channel licenses.
The following **features** can be enabled/disabled:
- Recording on demand
- Silence on demand
When disabled, this means it cannot be enabled for a user that belongs to this tenant. This is only relevant if in the Recording settings, the particular setting is set to "Defined at user level".

Schedule

Schedule of a Tenant:

The recording schedule of the tenant can be defined here. See also the global recording schedule in the System settings, Schedule tab.

Statistics

Statistics of a Tenant:

Recordings: The number of recordings that belong to this tenant, that are stored in the main storage.
Disk Usage: The combined file size of these recordings.
Backup Recordings: The number of recordings that belong to this tenant, that were stored on backup.
Backup Disk Usage: The combined file size of these recordings.

Other properties of a user group:

Members: The users that are member of this group. Press Add or Delete to add or delete group members. Users that are member of the group automatically have all the permissions that are assigned to the group.

LDAP group: For importing users of a group from Active Directory. This setting is only visible if an AD server is configured in the System settings (Network tab). When automatic synchronization is on, changes that are made in Active Directory will be applied automatically to the user group in Apresa. The username is used as identification. The name, email address, and telephone number are imported and updated from AD. The password is not imported, but checked during log-on. When a group is linked to Active Directory, it is not possible to manually add or remove users to or from that group. For the import from AD to work, the following options need to be set in the system settings, Network tab: AD server address, AD user domain, LDAP Domain, LDAP User, LDAP Password, and LDAP Synchronisation Interval. See chapter Active Directory on how to configure this.

Azure AD user group: For importing users of a group in Azure AD. This setting is only available if one or more Azure apps are configured in Apresa in the System settings (Network tab). The group is synchronized at once, and then synchronized with the same frequency as configure for LDAP (LDAP Synchronisation interval). When a group is linked to Azure AD, it is not possible to manually add or remove users to or from that group. The password is not imported. To allow login, also select the corresponding External logon service below.

External logon service: Select the external logon service for use by users in this group. In addition, this has the effect of enabling the SAML (ADFS) logon method for users that are created during LDAP import. See Using ADFS for sign-on.

Samwin User group: For importing users of a group from Samwin. This setting is only visible if the Samwin User group option is enabled in the

System settings (Network tab). Changes in Samwin are applied automatically to Apresa during the next synchronization.

Require multiple users to login: Users in this group will only get access to Apresa after two (or the specified number) of them logon. It works as follows. After the first user logs on, Apresa will present again the logon page for logging in as the second user. Only after the required number of users have logged in, access to the Apresa web interface is granted. Both usernames will be shown in the top bar where normally the single username is shown, and mentioned in the audit trail. The permissions of the first user that has logged on will be applied during the session.

Permissions: Permissions of a group apply to all members of the group. Optionally they can also be applied to members of subgroups (recursively).

The user and group list can be export to or imported from a CSV file.

20.4 Tenants

Options → Tenants

The Tenants page can be reached from the Options menu by administrators, if Multi-Tenancy is enabled in the system settings.

The Tenants page lists all groups for which the Tenant option is enabled.

Name: This is the name of the tenant, which equals the name of Tenant user group.

Other Tenant settings are explained on the User groups page.

To **add** a tenant, click Add. To **edit** the settings of a tenant, select a tenant and click Edit. Actually editing or adding of a tenant is done on the user group page, where tenant specific settings can be set, or features can be enabled.

To **delete** a tenant and its data, select a tenant, then click **Delete tenant data**. This will delete the tenant group, and associated recordings and user accounts. The system first asks for a confirmation before doing this destructive action. Optionally (by default enabled), tenant data is also deleted from backup. This means tenant data is removed from the

database backups, and the tenant recording files are deleted. For safety, a copy of the original databases is kept on the backup disk with the prefix OLD_. If needed, these files can be removed manually.

Other actions

Assign recordings to tenant: All recordings that are not yet assigned to any tenant, will be evaluated and possibly be assigned to a tenant. In the normal situation, only new recordings are assigned to a tenant. Recordings that are already assigned to a tenant, will not be reevaluated, and will not be moved to another tenant, even if the user phones in the tenant group are changed.

Export tenant data to backup: This exports call data of the selected tenant to a directory of the backup disk. This is intended to be used when a tenant leaves the system. The main database, and the various databases on the backup disk, will be scanned for recordings of the tenant. The audio files of the recordings, together with the call meta data in CSV format, is exported to a subdirectory of the backup directory. This is a background action that can take a long time. To monitor the progress, visit or refresh the Tenants page.

Recalculate statistics: (Local disk): This recalculates how many recordings are stored for each tenant in the main archive, and how much disk space is used. (Backup): This recalculates how many recordings are stored for each tenant in the backup, and how much disk space is used. This option is only available if information is retained about the backup (a setting). The statistics are shown on a Tenant page on the Statistics tab. The statistics can have an effect on functionality, when a maximum disk space is defined for a Tenant.

20.5 Export recordings

Options → Export recordings

This menu item is only visible for users that have the permission: "Tenant administrator: Export recordings". This user must be a member of the tenant. It allows the tenant administrator to enable and configure the time schedule of the export.

If you get the error that the "Export destination is not configured", then contact the system administrator to perform this configuration.

20.6 User list import and export

Options → Users → Export
Options → Users → Import
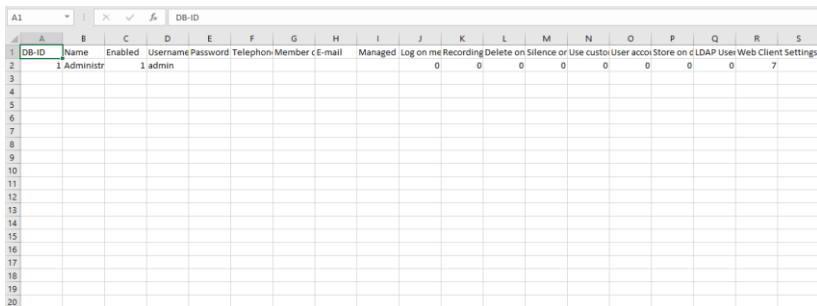
To allow quick data entry, it is possible to import the user account list from an external CSV file. This section will describe how to do this.

● Select Users in the Options menu, to move to the Users page

First, we export the user list.

● Click the Export button

This will prompt the download of a file that contains the user list (users.csv). This file will serve as a reference of the format that Apresa expects when importing a user list from CSV. The CSV file can be opened in spreadsheet software (for example Excel, and OpenOffice.org). Make sure that the comma is used as the separator character, and all columns are interpreted as text. Using the spreadsheet software, you can edit existing user account data, and add new user accounts by adding new rows of data.

users.csv in Excel

For new user accounts, the DB-ID column must be left blank. In the telephones column, the telephone numbers of the user are enumerated, separated by commas. In the "Member of" column, the groups of which the user is a member are enumerated, separated by commas. The changes that you make can be imported back into Apresa, as follows:

● Click the Import button, in the Users screen.

- Input the filename with CSV data, and press the Upload button.

To result of the import will be presented for verification. If any errors are detected (such as a reference to an unknown group), then these errors must be corrected first in the file, before the data can be imported.

- Press the Import button

The user list import is completed.

User group list import and export works similar.

Web client column

The web client settings column controls the display settings of the web client for the user. To edit this refer to the table below. In this table each setting gets a number. Select the numbers of the settings that need to be enabled and, add them together and input this number in the column. E.g. to enable editing of notes, notes(2) and category use 7 (= 1 + 2 + 4)

Edit notes	1
Edit notes(2)	2
Edit categories	4
Set silence	8

Start/Stop	16
Delete	32
Store on demand	64
Editing settings on web client page	128

20.7 Display settings

Options → Display settings

The Display Settings page can be reached from the Options menu by administrators. These display settings apply to all user accounts.

Language: Choose the language that must be used by Apresa. If a text is not available in the chosen language, English is used instead.

Date format: The date and time format is used in the call listing and at other places. Optionally, milliseconds of the start time and duration can be displayed in the main call listing (VoIP only).

Number of calls per page: Specifies how many calls are displayed per page in the main call listing (Home).

Automatically refresh list of calls: If enabled, new calls or notes made by co-workers will show up in the main call listing automatically. The data will be refreshed periodically depending on the specified **update interval**. The data will not be refreshed when an edit screen is open.

Direct playback (MP3): If enabled, playback will be inside the web page using HTML5. This is only possible for MP3 encoding (See Recording settings). Direct playback is a requirement for viewing and editing annotations.

Playback compatibility mode: If disabled, the waveform of a recording will be shown when you are playing it in a browser.

Convert to MP3 for playback: If enabled, the recording will be converted to MP3 format for playback (leaving the original unmodified). This is to allow direct playback inside the browser, using other browsers than Internet Explorer.

Convert to MP3 for download: If enabled, the recording will be converted to MP3 format for download (leaving the original unmodified).

Direct playback in Internet Explorer: If enabled, playback in Internet Explorer will be inside the web page using an embedded Windows Media Player ActiveX control.

Charts compatibility mode: If enabled, graph types that are more compatible with old browsers will be used (images).

File name of downloaded recordings: By the default downloaded .wav files use the Identifier (%i) as file name. For example: 20130225_155815_o481.wav. This Identifier includes the date and time, but no other information. To specify the file name for downloaded files, the following tags can be used:

Tag	Meaning
%i	Identifier
%d	Date

%t	Time
%L	Name of local
%l	Local ID (Telephone number)
%R	Name of remote
%r	Remote ID (Telephone number)
%C	Name of connected
%c	Connected (ISDN PRI, telephone number)
%b	Line number
%>	Direction
%A	Category name
%a	Category number

The file names on the Apresa itself and in backup, remain unmodified.

Email button: If this option is enabled, then an email button is shown on the call listing pages, to let a user email a recordings to itself, if the user has an email address.

Only show annotations by web users: Hide annotations added by the API. This can be useful if displaying too many API annotations cannot be handled by the browser.

Caller/receiver columns: If this option is enabled, caller and receiver columns are displayed, instead of remote and local columns. This might be preferable when internal calls are recorded, because otherwise local numbers would be displayed in the remote column.

Visible columns: Choose which columns must be displayed in the call listing. For the secondary notes columns, a custom label can be specified (for example: Invoice number).

Headers of visible columns in the call listing

Date & Time ∨	Duration	☎↓↑	▭	Notes		Remote ID	Name of remote

Visible columns

Column	Description
Play button	A play button to playback the recording, as alternative for the play button at the top. See direct playback options.
Special properties of the recording	This column displays information about the recording using icons: • If a screen recording is

	available. Clicking on the icon will playback the screen recording if supported. • If the recording is encrypted (lock icon) • If the audio failed to convert (codec problem) • If the recording was auto-deleted (retention period) • If it was a missed call • If the call was not recorded because the channel license limit was reached (see option in system settings) • If an audio transcription of the recording is available. Clicking on the icon will open the transcription.
Date & Time	The start date and time of the call (recording)
Duration	The duration of the call (recording)
Wait time before answer	The duration the phone was ringing until it was answered (if this could be determined)
Direction	Incoming (if remote side initiated), Outgoing (if local side initiated), Internal (both sides are internal, the local side is the initiator), External (no icon, both sides are external, the Local ID is the initiator)
Category	A color-coded category with a configurable label (See System settings)
Notes	Notes filled in by the user
Notes (2) ... Notes (5)	Additional notes fields. These can be given a custom label.
Remote ID (Telephone Number)	The telephone number (or ID or IP address) of the remote side of the call. Or if the call was internal, the remote side was the receiver of the call.

Name of remote	The name associated with the remote party in the Contact List. This could be filled in by a user, or it might be pre-filled by the recorder based on detected data.
Connected (Telephone Number)	For ISDN, this it the telephone number that is signaled when the call is answered. It can be a more detailed phone number of the destination of the call. For most other protocols, this field is not used.
Name of connected	The name associated with the connected phone number in the Contact List.*
Direction (2)	An arrow pointing from the initiator to the receiver of the call, for when Local and Remote ID fields are enabled.
Local ID (Telephone Number)	The telephone number (or ID or IP address) of the local side of the call. Or if the call was internal, the local side was the initiator of the call.
Name of local	The name associated with the local party in the Contact List.* This could be filled in by a user, or it might be pre-filled by the recorder based on detected data.
Remote IP	The IP address of the remote party.
Local IP	The IP address of the local party.
Tenant	In case of multi-tenancy, the Tenant to which this is call is assigned (which Tenant has access to this call).
Checksum	A calculated hash checksum of the recording, if enabled in the System settings.
Identifier	A unique identifier of the recording.
Recorder Name	Name of the recorder on which the call was originally recorded.

*) The fields containing Names use either the system-wide Contact List, or the per-tenant Contact List.

20.8 Recording settings

Options → Recording settings

The Recording Settings page can be reached from the Options menu by administrators.

Recording settings

Audio file encoding:	MP3 (compressed)	
Encoding quality:	Standard	(MP3)
Encoding mode:	Constant bitrate	(MP3)
Bitrate:	16 kbps	(MP3)
Addresses to record:	Record everything	(VoIP)
SIP Filter:	No filter	(VoIP SIP)
SIP Filter Incoming call:	No filter	(VoIP SIP)
SIP Filter Outgoing call:	No filter	(VoIP SIP)
Telephone number filter:	No filter	(VoIP HFA / H.323 / Avaya)
Telephone number filter:	No filter	(VoIP other)
Telephone number filter:	No filter	(Digital TDM / Analog / ISDN PRI)
Duplication:	Off	(VoIP SIP)
Recording on demand:	Off	(VoIP / ISDN PRI)
Delete on demand:	All	
Silence on demand:	Off	(VoIP)
Audio detection	Off	(VoIP)
Side of the call to record:	Both	
Record incoming calls:	☑	
Record outgoing calls:	☑	
Record local calls:	☑	
Do not mark calls as internal:	☐	(Digital TDM / Analog / ISDN PRI)
Do not store calls with missing telephone number:	☐	(Digital TDM / Analog)
Store on demand:	☐	
Minimal recording duration:	5	[seconds]
Call monitoring:	☑	

✔ Apply   ✗ Cancel

Audio file encoding: By default, audio files are stored using the GSM compression. It provides a good balance between sound quality and disk space requirements. For higher sound quality, it is possible to choose the G.711 codec instead. Audio files made with the GSM or G.711 codec can be played back on almost all PCs. For VoIP recordings, it is also possible to store data in G.711 stereo format. The local and remote side are then split in separate channels.

MP3 encoding settings: These options can be used to change the quality settings of the MP3 encoder.
- Encoding quality: General quality setting of the MP3 encoder. The higher the quality setting used, the higher the computational cost the MP3 encoding will be.
- Encoding mode: Two encoding modes are available, CBR (constant bitrate) and VBR (variable bitrate). MP3 files encoded with a constant bitrate are generally better supported by MP3 players and will have a predictable file size. But it may also result in file sizes that are higher. MP3 files encoded in VBR mode will have varying bitrates throughout a recording depending on the encoded audio. This can result in a better audio quality to file size ratio. But the file size becomes unpredictable and some MP3 players do not handle VBR as well as CBR.
- Bitrate: CBR only. A higher bitrate can result in higher audio quality, but at the cost of larger file sizes.
- Variable bitrate quality: VBR only. Increasing this value will result in a higher average bitrate. This can improve audio quality, but at the cost of larger file sizes.

Addresses to record: By default, Apresa will record calls from all connected VoIP phones. With this option, you can specify which VoIP phones should be recorded. Please note that the maximum number of simultaneously recorded calls is limited by the number of licensed channels. Phones that must be recorded can be specified using IP addresses, IP names, and MAC addresses. MAC addresses should be in the format: 11:22:33:44:55:66 or in the format: 11-22-33-44-55-66. Alternatively, a PCAP filter can be specified directly. If the PCAP filter is invalid, then no filter is applied. External documentation about the PCAP filter is found at http://www.tcpdump.org/manpages/pcap-filter.7.html.

SIP Filter: The following options are available:
- **No filter:** All SIP calls are recorded (unless disable by another feature). This is the default.
- **Only record calls that match the filter:** When this option is chosen, the SIP name or SIP id (telephone number) of the initiator and receiver of each VoIP call is checked if it is equal to one of the items in the filter. If neither the sender nor the receiver is found in the SIP filter, the VoIP call is not recorded. When editing the filter list, click Generate to use the list of user phones as starting point. If you would want this to happen automatically, see the option "All user phones" below.
- **Only record calls that do not match the filter:** This means that calls involving telephone numbers in the list, are not recorded.

- **All user phones:** Only SIP calls involving telephones of users will be recorded. When a change is made to the user list, this is automatically reflected in the SIP Filter in real-time without restarting.

Note: When the SIP filter is enabled, calls for which the protocol is not recognized, will not be recorded. This is similar to when the option "Only record RTP in calls" is enabled.

SIP Filter Incoming call: Incoming SIP calls are recorded only when they are allowed by this filter and the main SIP filter.
SIP Filter Outgoing call: Outgoing SIP calls are recorded only when they are allowed by this filter and the main SIP filter.
The same options are available as for the main SIP filter. These two SIP filters (in/out) are currently only available for the Default recording engine, not for Snip.

Telephone number filter: There are three separate telephone number filters, for H.323 based protocols, for other VoIP non-SIP protocols, and for ISDN PRI. These filters can be used to limit recording to specific local telephone numbers, or to exclude specific local telephone numbers from recording.

Instead of specifying telephone numbers one by one, it is possible to specify a range of numbers to be recorded. For example to record all numbers in the range from 3914100 to 3914199, specify: 3914100 - 3914199. The required format for number ranges is: First number space - space last number. The first and last number must have the same number of digits.
Alternatively, it is also possible use the * star sign at the front or at the end (not in the middle), to match with any number of characters at the front or end of the telephone number. For example, +33* will match any phone number that starts with +33, and another example, *1020 will match any phone number that ends on 1020.

Duplication: The purpose of this setting is to allow tenants to have a private copy of a recording, when a call is recorded between two tenants of the same system. The duplication recording will have local and remote swapped, as follows:

	Direction	Remote ID	Local ID	Tenant
1. Original recording	Incoming	0444001	0333001	A

2. Duplicated recording	Outgoing	0333001	0444001	B

The duplication feature has these options:
- Off: Duplication is not performed.
- All: Duplication is applied to all recordings.
- Only that match the filter: A recording will be duplicated if both parties of the call (local and remote) are in the list.
- Calls between tenants: Duplicate only when tenants call each other. This is the recommended setting to use.

The two recordings are treated in the system as separate calls. Actions such as delete on demand, are applied to the recordings separately, so it could be one is deleted, while the other continues. The duplicated recordings require extra channel licenses, and use additional processing power and storage capacity. Duplication is only available for VoIP.

CSTA Telephone numbers: This option is applicable only if CSTA is enabled in the System settings, CSTA Type. The listed telephones are monitored using CSTA, to detect when a new call starts, and to detect the call details of the call. If CSTA Active mode is on, a conference call is setup to the recorder. If there is a SIP filter, the monitored telephone numbers should also be part of the SIP filter, to let the calls be recorded. This setting is applied to the recording engine with a delay of about 15 seconds.

For each monitored CSTA phone, additional parameters can be specified, separated by a semicolon (;). The required format is:

Telephone number to monitor;IP address;Alternative telephone number

- The telephone number to monitor must always be specified.
- The IP address parameter is only relevant in CSTA Passive (Internal) mode.
- The alternative telephone number needs to be specified if the communicated telephone number in CSTA events or during the SIP conference call is different from the telephone number to monitor. For example, it might be that the monitored telephone number is 2040, while the alternative telephone number is +43308572040.

CSTA VDN Telephone numbers: If VDN's are used, for instance in call center environments, you can specify them here. For accurate resolving of the external number it is necessary that all the VDN's between the

external number and the answering device are specified. This setting is only applicable for Avaya DMCC.

CSTA Called Telephone numbers: Only applicable to Mitel Mx-One. Only calls that have a matching called phone number that match the filter, are recorded using CSTA (active).

Recording on demand: This setting is applied after the previous filters have been applied. If this setting is off, the software will function unmodified as usual. If this setting is set to All, then all VoIP calls are recorded only on request. If the setting is set to "Only that match the filter", then the calls with the specified telephone numbers are recorded only on request. If a call is recorded only on request, this means it is initially not recorded, but it will be recorded, when the command to start recording is given. Initially, it will be listed in the Active Call list, and the Active Call (All) list, but not recorded. See the picture below.

Active Calls (All)

Initiated	Wait time [s]	Ring time [s]	Duration [s]	Call state	Recording state	Protocol	↓↑	Remote ID
08/04/2020 09:48:12	0:01		0:52	Connected	Recording on demand	SIP	↗	3179306533

Recording can be started from the Apresa Client or with a recognized Dial code (dial code action start and stop). If the setting is set to "Defined at the user level", then when editing a user, recording on demand can be enabled or disabled for that user. When the recording starts, the recording state changes to "Recording".

Active Calls (All)

Initiated	Wait time [s]	Ring time [s]	Duration [s]	Call state	Recording state	Protocol	↓↑	Remote ID
08/04/2020 10:05:50	0:00		3:06	Connected	Recording	SIP	↗	3179306533

Note: For Analog and Digital TDM, there is a line-based setting in the Card settings.

Delete on demand: When enabled, a recording can be stopped and erased by using dial code actions. This feature can be enabled for all, or only for a set or range of telephone numbers, or defined at the user level. To specify a line number of card recording, use a hash sign followed by the channel number, for example #5.

Silence on demand: When enabled, a part of the recording can be silenced by using dial code actions or using Apresa Client. Silencing also stops the screen recording (if any). For VoIP, a list of phone numbers can

be specified for which silencing is available. For card recording (TDM, Analog, ISDN), it is either on or off for all.

Audio detection: When enabled, VoIP calls will be recorded only once the audio level is above the specified threshold. The recording is stopped when the audio level falls below the threshold and this continues for the amount of time specified in the silence time-out setting. Recording can be started and stopped multiple times during a call. This setting does not apply to non-VoIP calls.

Record incoming/outgoing/local calls: Before using these options, make sure the direction is correctly detected by Apresa, by checking in the Call Listing. See also the Local IP Addresses setting in the System settings, VoIP tab.

Do not mark calls as internal: This option only applies to non-VoIP protocols. If enabled, calls are marked as incoming or outgoing, but never as internal.

Do not store calls with missing telephone number: When this option is enabled, calls that lack a remote number will not be stored and not be included in the call listing.

Store on demand: When enabled, no calls will be stored, except those that are marked to be stored using a dial code action (*See: Dial code actions*) or using Apresa Client. This global can be overruled on a per-user basis.

Minimal recording duration: Recorded calls that are shorter than the specified duration, will be discarded.

Call monitoring: If this option is enabled, the Apresa Call Monitoring software (PC software) can be used to listen to active calls in near real-time (a few seconds delay).

When you click the **Apply** button, the settings are applied immediately if possible. Otherwise, the system will ask for your permission to restart the recording component, in order to apply the new settings. Restarting the recording component will usually have the effect of losing the recording of currently active calls.

20.9 Card settings

Options → Card settings

The Card Settings page can be reached from the Options menu by administrators. This page is not available in VoIP-only systems.

This page lists the recording cards that are inserted in the Apresa. These cards provide recording of digital TDM calls, as well as for analog telephony.

Column	Description
Serial number	The serial number of the recording card (not of Apresa)
Present	A green check mark is shown if the card is present. A red cross means that the card is not present or unusable.
Card type	The exact card type of the recording card.
Card type	Whether it is a Digital TDM or Analog recording card.
Channels	The number of channels on the card that are usable for recording. Between brackets the first and last line number is displayed. These line numbers are used in the rest of the Apresa system.
PBX manufacturer	This applies to digital TDM cards only. The PBX manufacturer and model must be set to

PBX model	the PBX model that is used, for each card separately. After you have edited this property, the recording component must be restarted.

Names can be assigned to line numbers of the recording cards. This is done in the [Contact List](#). These names will be used to populate the "Name of local" column in the main call listing.

To edit the settings of a recording card, select the card, and click the **Edit** button.
To edit *per channel* settings of a recording card, click instead the **Edit (per channel)** button.

Settings for digital TDM

Select the PBX Manufacturer and PBX Model that most closely matches your PBX, if not instructed otherwise by Vidicode. Apresa uses knowledge of the protocol used by the PBX to detect the start and end of the calls.

Event codes: This allows for custom event codes to be used for detecting ringing events, and call start/stop events.

Start condition: This is an option to switch on a special customization, for detecting the start/end of a call.

Audio detection: If this option is enabled, in addition to the PBX-specific protocol events, also the audio level is monitored to detect the start and end of a call. Normally, this option should not be enabled.

> **Sensitivity:** Lower this value if the Apresa starts a recording when no call is busy. If calls are split in multiple parts, it might help to increase this value, or to increase the silence time-out.
> **Silence time-out:** If the line is silent (below the audio level threshold), for this amount of time, then the recording is stopped, except when there is another indication that a call is active.

DTMF: If this option is enabled, the audio is analysed for DTMF tones, and these will be interpreted as dial codes. It makes no distinction between the local and remote side. For some PBX, pressed digits keys are recognized without DTMF analysis, and in that case, this DTMF option should be disabled, otherwise double digits will be detected.

Store metadata of missed calls: Stores entries in the database for unanswered calls (only applicable to: ISDN BRI)

Amplification: The local and remote side can be amplified separately with a maximum of 6 x 3 dB = 18 dB.

The following settings can be set *per channel*:

Phone type: For some PBX types, there is support for special type of phones (e.g. system console phones).

Check line status: When enabled, the line status will be checked, and if a problem is found, this will treated as a system error. It checks if the channel is offline (line disconnected / phone unavailable), and if there

are signal interpretation errors (this can indicate a signal quality problem).

Recording on demand: If this setting is off, the software will function unmodified as usual. If this setting is switched on, then the calls on the channel are recorded only on request. If a call is recorded only on request, this means it is initially not recorded, but it will be recorded, when the command to start recording is given. Initially, it will be listed in the active call list, but not recorded. Recording can be started from the Apresa Client or with a recognized Dial code (dial code action start and stop).

Check on recording inactivity: Let this channel be monitored for inactivity (See System settings, Alarm).

> **Recording inactivity (per channel):** If there are no recordings on this channel during this specified time duration (inside the specified activity periods in the System settings), it is treated as an error. If this field is left empty, the value from the System settings is used.

Loud voice detection: If enabled, the system will check if the audio level is above the **sound level threshold** (dB), during a specified **duration**. *Note: the dB values are not an absolute, but a relative measure. If there is difficulty selecting an appropriate level, it might be helpful to use the* **Channel status** *monitor functionality.*
If loud talking is detected, the following is done:
- The call is marked with the category 1 (color red). To give this category a name, use System settings, Category.
- An email is sent to the administrator email address with the details of the call (date & time, number, channel, etc.)

Channel status: The channel status monitor displays the detected audio level (but only if loud voice detection is on, and a call is active) for the selected channel.

Settings for analog recording cards

To edit the settings for one specific channel, select the channel, and press Edit. It is also possible to edit the settings of multiple channels at once. To change the settings for all channels at once, click Select All, and then press Edit.

Setting	Description

Start condition	Choose what will trigger the start of a recording. None: No recordings will be made on this channel. Off-hook: The recording will start as soon as it detects off-hook (voltage is below the off-hook threshold), and stops when it detects on-hook. Audio level: The recording will start when it detects the audio level is above the audio level threshold, and stop when it is below the threshold for as long as the silence time-out. Always: Recording will start at once. Use together with the Split long recordings option.
Off-hook threshold	Voltage level to distinguish between on-hook and off-hook For example: 28 (Volt)
Sensitivity	This value controls which audio level will cause the recording to start. The value corresponds to the following voltages: 1 750 mV 9 70 mV 2 550 mV 10 50 mV 3 350 mV 11 35 mV 4 300 mV 12 28 mV 5 250 mV 13 20 mV 6 175 mV 14 15 mV 7 100 mV 15 10 mV 8 85 mV 16 8 mV
Silence time-out	If the line is silent (below the audio level threshold), for this amount of time, then the recording is stopped.
Amplification	Apply a constant amplification to the recorded audio. The value must be between -6 and 6. Multiply the value with 3 dB to get the audio amplification that will be applied.
Automatic Gain Control (AGC)	If enabled, audio is amplified automatically.

Recording on demand	If this setting is off, the software will function unmodified as usual. If this setting is switched on, then the calls on the channel are recorded only on request. If a call is recorded only on request, this means it is initially not recorded, but it will be recorded, when the command to start recording is given. Initially, it will be listed in the active call list, but not recorded. Recording can be started from the Apresa Client or with a recognized Dial code (dial code action start and stop).
Check on recording inactivity	Let this channel be monitored for inactivity (See System settings, Alarm)
Recording inactivity (per channel)	If there are no recordings on this channel during this specified time duration (inside the specified activity periods in the System settings), it is treated as an error. If this field is left empty, the value from the System settings is used.
Loud voice detection	If enabled, the system will check if the audio level is above the sound level threshold (dB), during a specified duration. Note: the dB values are not an absolute, but a relative measure. If there is difficulty selecting an appropriate level, it is probably helpful to use the Channel status monitor functionality. If loud talking is detected, the following is done: - The call is marked with the category 1 (color red). To give this category a name, use System settings, Category. - An email is sent to the administrator email address with the details of the call (date & time, number, channel, etc.)
Split long recordings	If enabled, recordings are split automatically when they are active longer than the specified maximum duration.

Channel status: The channel status monitor displays the detected voltage level. If loud voice detection is on, and a call is active, it also displayed the detected audio level.

Settings for ISDN PRI

Setting	Description
Swap local and remote side of the call	The Local and Remote ID will be swapped. The direction (IN/OUT) will be reversed as well. The same effect could be created by swapping the receive and transmit lines in the ISDN cable.

20.10   External phones

Options → External phones

After the activation of the first external phone (mobile) license, the Options menu has a new option: External phones.

On this page, the Apresa can configured to receive recordings from mobile devices.

The number of external phones is limited by the license count. You can specify here from which external phones recordings will be accepted. The external phones are identified by their phone number (this will become the Local ID in the call listing), or in the case of mobile phones possibly their IMEI number.

Input the telephone numbers one per line. For mobile phones, optionally add a comma, and specify the IMEI. Use one line per device. Example:

43-904265-647083-1 , +43732204034
43-954305-737086-5 , +43732204038

Alternatively, this list can be linked to the users of a group. Select the group, and select which property of the users to use to fill this list. In this case, the list is not edited manually, but filled in automatically.

See [Mobile phone recordings configuration](#) in this manual for more information.

20.11 System settings

Options → System settings

The System Settings page can be reached from the Options menu by administrators. It contains the following tabs:

- System
- Alarm
- Schedule
- Network
- VoIP
- Dial code
- E-mail
- Category

System settings

| System | Alarm | Schedule | Network | VoIP | Dial code | E-mail | Category |

Software serial number:	1234567
License key:	[_____] Activate new channels license
VoIP channels:	0
G.729 decoding channels:	0
RT-Audio decoding channels:	0
Digital TDM channels:	0
Analog channels:	0
ISDN PRI Channels:	0
Software updates until:	14.06.2016 Renew service license
Remote shell:	☐
API authorization code:	••••••••• ☐ Define new password
Maximum number of logged in users:	100
Maximum number of webserver connections:	
Session idle time-out:	100 [minutes]
Maximum session duration:	720 [minutes]
Calculate checksum:	SHA-1 ▾
Delete calls older than ...:	900 [days]
Remove auto-deleted recordings from the call listing:	☐
Load auto-deleted recordings from backup:	☐
Recycle Bin:	☑
Users can change personal settings:	☑
Password:	☐
Recovery when password has been forgotten:	☐
Minimum password length:	
Strong passwords required:	☐
User must change password:	☑
Renew password after:	[days]
Password history:	passwords
Duration of user account block:	[seconds]
Multi-tenancy:	☑
Duplicate names allowed:	☐
A user is member of only one group:	☐
A phone belongs to only one user:	☐
User access based on Local ID:	☐
Mask last digits of Remote ID:	digits
Playback permission allows playback only inside the browser:	☑
Unofficial updates allowed:	☐
Audit Trail:	☑
Manual is available for:	Everyone ▾
Statistics are available for:	Users ▾
Digital TDM Detailed Logging:	☐ (TDM)
Manually edit configuration file of card recording:	☐ (TDM)
Line name in file name:	☐ (TDM)
Export recordings	⚙ Configure

[✔ Apply] [✖ Cancel]

When the Advanced settings are hidden, check the Advanced settings checkbox to see them.

20.11.1   System

Options → System settings → System

System name: The system name is displayed in the web interface in the top bar, and included in the subject of system emails.

License key: The license key determines the number of licensed channels. If the number of simultaneous calls exceeds the number of licensed channels, calls will be lost. To add new recording or decoding channels, click on the link "Activate new channels license", fill in the license key that you have received on purchase. The system will reply with a new license key. Input this license key in the License key input box in the Apresa web interface, and press Apply.

VoIP channels: The number of licensed VoIP channels. This is the maximum number of simultaneous VoIP recordings that can be made.

RT-Audio decoding channels: The number of simultaneous calls that can be decoded from RT-Audio codec.

Digital TDM channels: The maximum number of simultaneous digital TDM recordings that can be made (Synway DST or SHR card).

Analog channels: The maximum number of simultaneous analog recordings that can be made (Synway ATP card).

ISDN PRI Channels: The maximum number of simultaneous ISDN PRI recordings that can be made (Synway DTP card).

External phones: The number external phones, identified by a Local ID (or IMEI), that can be imported from an external source using the API. Click Configure to configure the External phones.

Software updates until: The date after which the service period of providing Apresa software updates will end. To extend the service period, click Renew service license, and use the S&U license code that was provided on purchase. OS-level updates are not affected by this date, but depend on long term support schedule of Debian.

Remote shell: When this option is enabled, you can connect remotely to the Apresa system to open a remote shell using a SSH client, provided the Apresa system is reachable, and the network traffic is not blocked. The first time you enable this option, you will be prompted to specify a new password. It is essential for safety that you input a new password. For more information, see the Apresa manual.

API authorization code: Password of the Apresa API (for more information, see the Apresa API documentation)

Maximum number of logged in users: The maximum number of users that can be logged in on the Apresa web interface. Use this setting to prevent too much server load.

Maximum number of web server connections: This number must be at least equal to the number of ApresaClient instances that are running at the same time, because each ApresaClient (PC software) keeps one connection open constantly. In addition to this number, about 4 extra connections are needed for normal use of the web interface. It is recommended to keep this setting low, because higher numbers will use extra memory and CPU time.

Session idle time-out: Users are logged out automatically when not active during the specified time period.

Maximum session duration: Users are logged out automatically when they are logged in longer than the specified time period.

Calculate checksum: For verification that a recording has not been altered, Apresa can calculate a checksum. This checksum can be made visible in a column of the call listing (For enabling this column, see Display settings). Apresa supports the MD5, SHA-1, and SHA-2 (256 or 512 bit) methods for calculating a checksum.

Delete calls older than ...: Calls that are older than the specified number of days are deleted permanently from the hard disk. This function is also called auto-delete. When the input box is left empty, auto-delete is off. (See also the retention period settings on the backup page.)

Independent of this setting, to ensure the system can continue to create new recordings at the maximum supported rate, the system will always perform auto-deletion of old recordings when the disk space falls too low (below 2 GB or below 25% whatever is less).

> **Remove auto-deleted recordings from the call listing:** If this option is disabled, call information is retained in the call listing. This is required for the next option (load from backup) to work.
> **Keep auto-deleted evaluated calls in call listing:** If this option is enabled, meta data of calls that were added to an Agent Evaluation project for evaluation, are preserved when the recording is auto-deleted. This is an exception to rule described in the previous option.
> **Load auto-deleted recordings from backup:** If this option is enabled, and a recording is auto-deleted, but not removed from the call listing, then a user can select the call for playback, and then the system will attempt to load this recording from the backup location.

Delete screen recordings older than ...: Screen recordings that are older than the specified number of days are deleted permanently from the hard disk (not from the backup). This options is applied in addition to the other auto-delete options. This option only has an effect if it is set to a lower value than the general auto-delete option.

Delete transcriptions older than ...: Transcriptions that are older than the specified number of days are deleted permanently from the hard disk (not from the backup). This options is applied in addition to the other auto-delete options.

Note: Auto-delete actions are applied in addition to each other, this means that each action possibly causes more to be deleted, never less.

Delete from main archive when deleting from backup: If this option is enabled, the same retention period that is applied to the backup (globally or per tenant) is also applied to the main archive. The meta-

_____

data of the calls will also be deleted from the main archive call listing, even if the option "Remove auto-deleted recordings from the call listing" is disabled. The idea behind this is as follows. Usually, the retention period of the main archive will be shorter than that of the backup. For example, a tenant could have a retention period in the main archive of one month, but keep meta-data in the call listing, and enable the option to load recordings on-demand from the backup. The tenant could have a retention period of one year in the backup. At that point, recordings are deleted from the backup, and meta-data of the calls are deleted from the main archive. Loading from backup would not be possible anymore anyway. The recordings itself were already gone from the main archive then, because of the shorter retention period, so only meta-data is deleted.

Retain information about calls in the backup: Store the meta-data of calls in the backup, even after they are deleted from the main storage, until they are deleted from the backup archive by the system. This option is needed for quickly performing actions on the backup (for deleting tenant data from the backup, and for applying a retention period on calls in the backup).

When disabling this option, information about the calls in the backup is no longer retained (the information is deleted). After enabling this option, calls that are newly written to the backup, are registered (information about it is remembered). To fill the registry with information about calls that were copied to the backup before this option was enabled, click Configure.

Prevent recovery of deleted data: If enabled, recordings data that is deleted is first overwritten with pseudo-random data multiple times, to prevent recovery of the original content. The data erasure procedure takes time, depending on the size of the deleted data. When this option is off, which is the default, recording files are simply unlinked, and recovery might be possible with special tools.

Notes: Because of file system journaling, caching, and possibly other factors, it cannot be guaranteed to absolutely prevent recovery in all cases. This option is not applied to the meta data in the database. It is also not applied during a complete system reset.

Recycle Bin: If enabled, calls are moved to the Recycle Bin when they are deleted. On the Recycle Bin page you can restore the calls, or remove them permanently.

Users can change personal settings: When enabled, users can choose a custom display language. Users will be able to change their password, except if this is disabled in the (advanced) option below, or if password verification is performed through LDAP/AD.

Recovery when password has been forgotten: If enabled, then users can request a new password to be delivered to them by email.

Minimum password length: The minimum length of the new password.
Strong passwords required: If enabled, the password must contain an upper case letter, a lower case letter, and a number.
User must change password: If enabled, the user must change his/her new password on first log-on, after a new one had been issued by email.
Renew password after: The maximum number of days the user can use his password. After this time period, the user must change his password.
Password history: This determines the number of unique new passwords a user must use before an old password can be reused.
Duration of user account block: This is the time (in seconds) an user account is blocked after 5 wrong password attempts.
Multi-Tenancy: Enable multi-tenancy to have separate settings per group that uses the recording system. Recordings are assigned to exactly one tenant (or no tenant), depending on whether the phone of the call is a phone of a user that is a member of the tenant group.

> **Assign recording to tenant when call starts:** If this setting is enabled, or if "User access based on Local ID" is enabled, then a recording will be assigned to a tenant, if one matches, as soon as the recording starts. Otherwise, the recording will be assigned to a tenant when the recording ends.
>
> **Exclude disabled user accounts when determining the phone numbers that belong to a tenant:** Calls are assigned to a tenant if the involved phone number matches with a telephone of a user account that is a member of the tenant group. If this option is enabled, then only enabled user accounts are checked for a match.
>
> **Allow administrators to reassign recordings to another tenant:** Allow an administrator to move existing recordings to another tenant. In the main call listing screen, an administrator can then click the Edit icon button, select "Assign recording to another Tenant", then choose the new tenant for the selected recordings.
>
> **Contact list per tenant:** When enabled, each tenant has a separate contact list. The contact list contains the names that are associated with a phone number.

Duplicate names allowed: Two or more user accounts with the same name are allowed to exist, if this option is enabled.
A user is member of only group: When adding users to a group, only users that are not yet part of any group are available for selection.
A phone belongs to only one user: A phone can be added to only one user. A phone is identified by phone number (VoIP), or line number (analog/TDM).
User access based on Local ID: Users have access to calls made by one or more telephones (identified by a telephone number, or a SIP IDs, etc.). If

this setting is enabled, the system will check the Local ID, but not the Remote ID, to determine if the user has access to the call.

Mask last digits of Remote ID: If enabled, the last few digits of the Remote ID will be replaced by an X in the call database.

Playback permission allows playback only inside the browser: The system will try to prevent downloading of recordings, while still allowing inline playback inside the browser. Since playback always requires some form of file data transfer, it cannot be fully guaranteed that no download will happen. But under normal circumstances, a user that has no download permission will not be able to download recordings, not even to the temporary directory, regardless of the browser setup.

Unofficial updates allowed: When enabled, this allows the installation of updates that are not from the official manufacturer. Otherwise, the signature of the update will be validated before installation.

Allow temporary unencrypted storage on disk of active calls: If this option is not enabled, active calls are recorded first in memory, and then stored encrypted when finished. This is the default. When this option enabled, active calls are recorded on disk, and then encrypted when finished. This can prevent an out of memory situation when there are long active calls. This option only applies if call content encryption is active.

Audit Trail: (Files) When enabled, audit files are created that log each significant action of users, such as playback of a recording.

Audit Trail: (Database) When enabled, entries are created in the database that log each significant action of users.

It is possible to enable both the file and database audit trail, but usually you would want to enable one of both. The database audit trail has more features. The audit trail can be accessed using, Tools, System, Audit Trail.

> **Remove audit trail entries older than: (Database)** Audit trail entries that are stored in the database that are older than the specified days are permanently removed.
>
> **Web interface: (Audit Trail)** When viewing the audit trail, select to show either the audit files or the audit database. Both could contain different data, depending on whether they were enabled during different periods.
>
> **Include data views in Audit Trail:** If enabled, viewing data (such as viewing the call listing), and searching for data, is also logged in the audit trail.

Manual is available for: Choose here for whom the included online manual will be available: for everyone (that includes non logged-in users), users (that are logged in), or only for administrators.

List of active calls is accessible for: Choose if the active calls list page can be viewed by all users, or only by administrators (including level 2 but excluding level 3 administrators).

Statistics are available for: Choose here who can access the statistics page. Regardless of this setting, statistics are filtered by user access rights.

Detailed logging of card recording: This option is intended for when there is a problem with card recording.

> **Delete log files older than ...:** Detailed card recording log files that are older than the specified number of days are deleted permanently from the hard disk. When the input box is left empty, auto-delete is off.

Manually edit configure file of card recording: Enable this option for full control over the configuration file used for card recording. Otherwise this file would be edited automatically by the application software, based on the supplied settings.

Line name in file name: A TDM specific feature to include the line name into the used filename.

Export recordings: Backup recordings to a network drive.

20.11.2 Alarm

Options → System settings → Alarm

Recording file checking: Checks every recording file for integrity (header, length, etc.). If a problem is detected, it will be treated as a system error.

Check on recording inactivity: Checks if recordings are made during the specified time periods that are configured below. If inactivity is detected for a too long duration, this is treated as a system error.

Day of the week: The days of the week that recording activity is to be expected, by default this all days.

Start/stop time: This specifies the time periods during which recording activity is expected. It is possible to specify one or two such time periods (for example two periods excluding lunch time).

Maximum call duration: A recording (call) that is longer than the specified duration, is treated as a system error. Otherwise, an endless recording might prevent recording inactivity to be detected. This setting is only effective if inactivity detection is enabled.

Recording inactivity (system-wide): If there are no recordings anywhere in the system (including imported recordings) during this specified time duration (inside the specified activity periods), it is treated as an error.

Recording inactivity (Apresa): If there are no recordings made by Apresa (excluding imported recordings) during this specified time duration (inside the specified activity periods), it is treated as an error.

Recording inactivity (other recorders): If there are no recordings during this specified time duration (inside the specified activity periods) imported by FTP from another recorder, whose inactivity check is enabled, then it is treated as an error.

Recording inactivity (per channel): If there are no recordings on a channel that is enabled to be checked for inactivity, during this specified time duration (inside the specified activity periods), it is treated as an error. It is only effective if it is enabled for the particular channel in the card settings. It is available for analog and digital TDM channels.

Notify administrator if channel license limit is reached: If enabled, an email will be sent if a recording was not started because the channel license limit was reached.

Maximum number of simultaneous calls: This value is specified as a percentage of the available licensed VoIP channels. The default value is 100 (%), which means that the system alarm is activated when the number of active calls exceeds the number of licenses, which means some active calls will not be recorded. It is also possible to let the alarm start earlier, to prevent loosing recordings at all. For example, a value of 90 means the alarm will be activated when more than 90% of the available channel licenses are in use.

Collect log files on error: When an error occurs in the recording engine and it has to close, log files are automatically collected if this option is enabled. The log files can later be downloaded from the logs archive (Tools, System, Archive log files).

> **Number of collected log packages to keep:** Specify how many log packages, that were created automatically on error, should be preserved. Suppose this number is 5, this means that the latest 5 log packages are kept. This will give information about the last 5 errors that occurred.

SNMP Configuration: *Manual:* The SNMP configuration file can be edited manually with this option in case extra configuration is desired that is not available via the web interface. With this setting active the configuration file will not be overwritten by the web interface. *Web interface:* The SNMP configuration can be changed via the web interface. Note that any manual edits to the SNMP configuration file can be overwritten by the web interface with this setting active.

Remote access to SNMP: Enable access from remote using the SNMP protocol.

Enable SNMPv2: Enable access via the SNMPv2 protocol. SNMPv2 is unencrypted and unauthenticated.

SNMP community: This is similar to a user name, used for access control. It must match the SNMP configuration of the client. It is possible to configure multiple SNMP communities by providing them as a comma-separated list.

SNMP trap community: This community will be attached to generated traps. If left empty, the first SNMP community is used instead.

SNMP access IP range: The IP address or range from which to allow access. To allow access from all IP addresses, use: 0.0.0.0/0. For a range, set to 0 those parts that are free. For example, use: 192.168.5.0/24 instead of 192.168.5.34/24.

Receiver of SNMP alarm message (traps): The IP address or DNS name to receive SNMP trap events. SNMP trap events are alarm or other notifications, that are sent from the Apresa server to the SNMP client. There can be a 5 to 10 minute delay between the actual event and the trap. The trap events can be send to multiple destinations by providing several IP addresses as a comma-separated list. Every IP address will receive a copy of the trap. Note that this setting only works with single IP addresses and not with IP ranges.

Enable SNMPv3: Enable access via the SNMPv3 protocol. SNMPv3 can be encrypted and authenticated. Via the web interface a single user can be created that use the User-based Security model (USM) of SNMPv3. Authentication and encryption will be required for this user. Alarm messages/traps can also be send via this user. More complex SNMPv3 configurations must be done manually.

Username (SNMPv3): The username for the SNMPv3 user.

Password (SNMPv3): The password for the SNMPv3 user. The minimum password length is 8 characters.

Authentication protocol (SNMPv3): The authencation protocol used for the SNMPv3 user. It is recommended to leave this as SHA unless otherwise required.

Encryption protocol (SNMPv3): The encryption protocol used for the SNMPv3 user. It is recommended to leave this as AES unless otherwise required.

Receiver of SNMP alarm message (traps) (SNMPv3): The IP address or DNS-name of the receiver of the SNMPv3 trap events. Can be a comma separated list to send the trap events to multiple destinations. The trap receiver(s) must also be configured with the username, password. Sometimes the engine ID must be configured on the receiving end as well, depending on the SNMP application that must receive the traps (see below).

Engine ID (SNMPv3): Read-only field that will be populated once a SNMPv3 user has been configured. The user at the trap receiver(s) must sometimes be configured with this engine ID before the SNMP application will process SNMPv3 traps.

Stop VoIP service if VoIP recording component fails: The VoIP service is stopped when a failure is detected in the operation of the VoIP engine. The VoIP service is often used for active recording.

Check for card recording driver errors: If enabled, the status of the card recording driver is checked, and if a known error condition is detected in it, this is detected as a system error, and the recording component is restarted automatically.

Teams Bot Check: If enabled, the system will periodically check if the Teams bot is up and running. The Teams Bot is run in Azure and is used to record MS Teams calls.

Teams Bot Server address: The URL at which the bot can be reached, for example: https://bot.company.com

Teams Bot Password: The administrator password of the bot, that is also usable in the control panel of the bot (configured in service.auth in the configuration xml file of the bot).

20.11.3   Schedule

Options → System settings → Schedule

When recording is not scheduled, no calls are recorded at all, when it is scheduled, recording is performed according to the other specified filters (if any).

Day of the week: The days of the week that recording activity is to be expected, by default this is all days: 1234567, with 1 being Sunday. Use 23456 to exclude the weekend.

Start/stop time: This specifies the time periods during which recording is scheduled. It is possible to specify one or two such time periods (for example two periods excluding lunch time).

Wednesday:	☑
Start time: (1)	7:00
Stop time: (1)	12:00
Start time: (2)	12:30
Stop time: (2)	21:30

20.11.4   Network

Options → System settings → Network

Configure: The network settings can be configured using the web interface, or manually (on the command line). If the network settings are configured using the web interface, it will write to the files: /etc/network/interfaces , /etc/resolv.conf , /etc/hostname . Otherwise it will leave these files untouched, and the existing configuration will remain.

DHCP: When enabled, the Apresa server will try to acquire an IP address automatically using DHCP.

IP Address, IP Subnet Mask, IP Gateway Address: These settings usually do not need to be filled in when using DHCP. When not using DHCP, they must be filled in manually.

DNS Server Address: IP address of the Domain Name Server

IP Name: The IP name that the Apresa server must have

NTP server address: Apresa can synchronize its clock with an NTP time server. After applying the settings, press the Test button to check the current status. You can fill in up to 4 addresses (advanced). To use the standard pool from the internet, use:

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org
3.pool.ntp.org

If you are using a local NTP server, the standard NTP server provided by Windows client platforms (Windows XP, Windows 10) have known problems that prevent the NTP client on Linux from synchronizing with it. To solve this, it can help to install a standard conforming NTP server on it (see https://www.meinbergglobal.com/english/sw/ntp.htm for example), or switch to using another NTP server.

If an NTP server is advertised using DHCP, it is used instead of the value in this setting.

Browser protocol: The default browser protocol is HTTP, and it is unencrypted. HTTPS, on the other hand, is encrypted. Before enabling HTTPS, a certificate must be created on the Encryption page.

Certificate: This list contains all available certificates that may be used for the HTTPS protocol. One of them may be selected here.

Web server port (HTTPS): By default, HTTPS is server on port 443. This port number can be changed here.

Configure second ethernet port: It is usually not needed to configure the second port, even when using the second ethernet port for mirroring. When needed, it is possible to assign a static IP address, or a dynamic one using DHCP. This might be needed when using the Apresa network service (VoIP tab) to receive information from the Apresa Lync Plugin on a Lync Server.

Azure: This is for importing users from a security group and single sign-on using Azure AD. The Application ID (also called Client ID) refers to

the App registration in Azure AD and has the format 00000000-0000-0000-0000-000000000000. The Tenant ID has the same format, and refers the company that the users are part of. It is also called the Directory ID in Azure. The password refers to the client secret. Select the AD fields to use for populating the list of telephones when importing users.

You can refer to an Azure app where defining an external logon service.

AD server address (LDAP): The IP address or IP name of the Active Directory server (LDAP), on which to check username and password during log on, for the users for which this is enabled. Multiple servers can be added. See chapter [Active Directory](#) on how to configure this.

> **AD user domain:** The Active Directory (Windows) domain name to use, when checking a username. Users are logged in using DOMAIN\username.
>
> **LDAP Domain:** The distinguished name of the organization. For example: company.com. When browsing for groups, the LDAP search query would then search within DC=company,DC=com. In the Group settings, if you link a group to AD, you can specify an LDAP group which resides below the LDAP Domain specified here.
>
> **LDAP User:** The LDAP user account to be used when searching the Active Directory for user groups, and importing the user details.
>
> **LDAP Password:** The password of the LDAP User.

UPN as Username (LDAP): If this setting is enabled, when importing users from AD, the Universal Principal Name (UPN) is used as username. UPN uses email address format (user@domain).

LDAP telephones: Specify which fields in Active Directory to use when importing user phones. More than one field can be specified.

LDAP Synchronisation Interval: The user groups that are configured to be imported from AD, will be synchronized periodically according the specified interval. If the synchronization interval is set to zero or empty, the synchronization is not performed.

Logon using external party: Enable this option to allow users to log on using an ADFS server, or another type of SAML Identity Provider. This will apply to users for which the logon method of their user account is set to use SAML (ADFS). See [Using ADFS for sign-on](#).

Access URL of Apresa: Fill in the web address that users use in their browser to access Apresa. The address needs to start with https://.

Logon procedure: This setting determines what happens when only one ADFS is defined in the system.

- **Ask for username:** Depending on the username, and the logon method of this user, the user will be redirected to ADFS, or prompted for the password for local (or LDAP) logon.

- **Show login button:** The user will be redirected to the configured ADFS after clicking the button. This can be used for additional clarity about where they are logging in, and reduces the chance of redirect loops in case of a failure.
- **Redirect immediately:** The user will be redirected immediately to the configured ADFS for log on.

In the case the user is not asked for a username, a local logon is still possible by appending ?nosso to the URL (nosso= No single sign-on), for example: https://1.2.3.4/?nosso . When there are multiple ADFS servers configured, the user is always asked first for a username, to determine to which ADFS to redirect.

If you are using a customized logon page that is not updated for this new feature, the logon page might to not show properly.

Certificate of Apresa: Select the certificate that will be used by Apresa to sign SAML messages sent to ADFS. Also import this certificate into ADFS to let it trust messages from Apresa. A certificate can be generated on the Certificates page.

One or more external logon services (ADFS servers) can be configured. For each external logon service, the following options apply:

- **Name:** The name can be freely chosen, and has no effect on the sign-on procedure.
- **Technology:** This can ADFS (SAML), or Azure AD (OAuth)

For ADFS (SAML), the following settings apply:

- **Entity ID:** of the ADFS server. Usual format: http://somedomain.com/adfs/services/trust
- **Certificate:** of the ADFS server. It will be used to verify the identity of the ADFS server when connecting to it. A certificate can be imported on the Certificates page.
- **Sign-on URL:** Usual format: https://somedomain.com/adfs/ls/
- **External sign-off:** Enable this option if you want to perform an ADFS sign-off when the user logs out.
- **Sign-off URL:** Usual format: https://somedomain.com/adfs/ls/

For Azure AD (OAuth), the following settings apply:

- **External sign-off:** Enable this option to close the session at Azure AD when logging out
- **Azure app:** Select one of the available Azure apps. See the Azure app setting.

For more information see <u>Using ADFS for sign-on</u>.

Samwin User group: Enables group synchronization with a remote Samwin installation. In addition it is needed, to specify the Samwin group on the <u>User group</u> page.

Server address: IP address and optionally the port of where the Samwin database can be reached.

Database: The database name on the Samwin server.

Username/Password: The database login credentials for the Samwin server.

Synchronization Interval: The groups that are configured to be imported from Samwin will be synchronized periodically according to the specified interval.

CSTA Type: Select the PBX type to which to connect, using CSTA. Options are for example: Unify OpenScape 4000, Unify OpenScape Business, Unify OpenScape Voice, Avaya, Avaya DMCC, Mitel 400 Series, Mitel Mx-One, Panasonic, Mitel MiVoice Business (OIG), and Mitel (Aastra) 5000.

Active: When enabled, CSTA is used to setup a conference call to the recorder, which makes port-mirroring unnecessary. The VoIP service needs to be configured to answer this call, except for Avaya DMCC. Port-mirroring is then not needed. When active is disabled, CSTA is used to improve the call meta data (telephone numbers and direction).

CSTA Passive Mode: There are three modes:
- **Telephone Based:** This applies to certain Unify phones that can initiate a SIP call to a recorder.
- **Mirror (Internal):** In this setup, VoIP data is recorded on the inside using port-mirroring (also known as SPAN). The telephone numbers are corrected or improved by CSTA. It requires knowledge of the IP address of the monitored phones.
- **Mirror (External):** In this setup, VoIP data is recorded on a SIP trunk using port-mirroring (SPAN). The local telephone number is corrected or improved by CSTA.

CSTA Username/Password: Login credentials to be used for the CSTA connection.

CSTA server name: The CSTA server IP name or address. The main IP address of the PBX might be different from the IP address of the CSTA server.

CSTA server port: The port number for CSTA at the CSTA server.

CSTA Switch Name: This setting is needed for connecting to the Avaya PBX.

CSTA Apresa Telephones: This is the phone number at which this recorder is reachable. For Avaya DMCC, this can be a range of phone numbers. (This is only applicable to active recording.)

CSTA Apresa Telephones Password: The password to use when logging in the recorder phones specified above.

Apresa Local IP: The IP address of Apresa to use when using Avaya DMCC. When left blank, the first IP address of Apresa will be used.

CSTA Media Server: Specify, in case of OpenScape Voice and active recording, if a Media-Server/ONS number must be used.
CSTA Conference Number: If a Media Server is used, specify the ONS number here (just for OpenScape Voice).
CSTA Silent Monitoring: Enable this feature if you want Silent Active recording. This option is especially for the OpenScape HiPath 4000.
CSTA RCG Number: If you enabled the above option, you have to specify the Route Control Group to be used. This number must also be configured in the PBX. OpenScape HiPath 4000 only.
CSTA Do not record: All numbers in this list will never be recorded. You can specify the numbers separated with commas, like: 100,200,300, as a range, like: 100-120 or you can use a wildcard, like 58*.
CSTA Clear Conference after: Specify the number of seconds before ending a conference call that was made by CSTA in active mode with OpenScape 4000. If left empty or set to zero, then the conference call is not stopped artificially. If this setting is enabled, the CSTA conference call is made only if the corresponding setting on the "Recording settings" page ("Record incoming calls", "Record outgoing calls", "Record local calls") is enabled. This setting is intended to be used when the CSTA conference call is used only for making an announcement, and not for recording. In that case, specify a duration that is larger than that of the announcement. When the announcement has played, the conference call serves no purpose anymore and can be cleared.
CSTA Devices Multi-Controllable: Specifies whether multiple sessions can control the device. Only for Avaya DMCC. Default is false.
CSTA Record trigger text: The UserData field (UUI field) can be used to control recording. With the option "Record only these calls", only calls with this trigger text are recorded. With the option "Keep these calls with store on demand", the trigger text will cause the recording to be kept if store on demand is enabled. This setting only applies to Avaya DMCC.
CSTA Stereo recording: This option only applies to Avaya DMCC. If enabled, stereo recordings are made, with a separate channel for the local phone that is to be recorded, and a separate channel for the other side of the call. This option only works if the audio file encoding is set to a stereo format in the Recording settings. Recording in stereo requires double the amount of recorder telephone numbers (see CSTA Apresa Telephones), because two separate recorder connections will be made for each recorded call. This also affects the number of licenses needed from Avaya.
CSTA Apply SIP filter on outgoing calls: If enabled, the SIP filter rules will be applied to the dialed phone number as detected by CSTA for outgoing calls. Sometimes the phone number detected using CSTA contains an additional dialing prefix (for example a zero), compared to

the telephone number detected on the SIP trunk. This could be matched on in the SIP filter. This setting applies only to Mitel 400.

CSTA Local ID: This setting determines if the Agent ID (when detected) will be stored as Local ID in the call database.

CSTA Connected Column: There are three options here: "None" (the connected column is empty), "Agent ID" (the column is always used for the agent ID) or "Dialed number", this is the number the external party originally dialed. The default is "Agent ID".

CSTA Status: This shows the current CSTA status.

Note: Also set the CSTA Telephone numbers to be monitored in the Recording settings.

V-Tap: Enable this option to let Apresa accept data from V-Tap devices.

V-Tap Tunnel port number: The TCP port at which the Apresa server will listen for connections from V-Tap devices (by default 2016). If Apresa is connected to the Internet using a router, it might be needed to configure port-forwarding for this port at the router. The same port number must be specified at the V-Tap device.

V-Tap Data separation: Enable this option when V-Taps are installed in possibly more than one network. When data separation is enabled, data from each V-Tap is processed separately and independently. This is the default option. This is essential for data integrity when V-Taps are installed in multiple networks, and data is sent to one central Apresa server. If data separation is disabled, data of all the V-Taps are processed with the assumption that they occurred in the same network. This can be needed if V-Taps are used to stream live mirrored network data from various points in the same network and data of a single call might come from multiple sources and needs to be combined to form a complete recording.

Accept only known V-Taps: When this option is enabled, only V-Taps with a MAC address configured in the table below will be accepted. Any other V-Tap with an unknown MAC address will be disconnected.

Accept only encrypted V-Tap connections: When this option is enabled, only V-Taps that encrypt the connection will be accepted. Any V-Taps that tries to send data unencrypted will be disconnected.

Store V-Tap recordings in received format: This option applies to V-Tap Analog, BRI and PRI, but not to V-Tap VoIP. If enabled, the recordings will be stored in Apresa unmodified, as they were created on the V-Tap Analog, BRI or PRI. If this option is disabled, the recordings will be stored in Apresa as configured in the Recording settings.

Generate an alarm if V-Tap disconnects cleanly: If this option is on, a connected V-Tap disconnecting will always generate an alarm. If this option is off, a V-Tap disconnecting via a regular disconnect request will

not generate an alarm. All other disconnects that result from an error will still generate alarms.

V-Tap extended alarms: V-Taps can send extended error information about themselves to the Apresa. If this option is on, alarms are generated based on this information. If this option is off, this information is not used. Disconnects will generate alarms regardless of this setting.

V-Tap Encryption password:

> **Default:** This encryption password is used for decrypting the data received from the V-Tap, when no device-specific encryption password is specified in the table below. The same encryption password must be specified at the V-Tap device.

> Multiple V-Taps that are connected to the same Apresa, can each have a separate password. V-Tap devices are identified by their MAC address. The MAC address must be entered as 12 characters (without colons). V-Taps can also be assigned to a tenant. Any call received via such a V-Tap will be assigned to this tenant. This will take precedence over any other tenant assignment configurations. Optionally a V-Tap can be given a name as well. This name is used to refer to the V-Tap on the status page and in alarm messages instead of its MAC address.

Always generate an alarm when a V-Tap in the table is not connected: Turning this option on will always generate a system alarm when a V-Tap configured in the table above is disconnected. Otherwise an alarm is only generated when a V-Tap disconnects after a first connect after a restart of the recording service.

ShoreTel Database: Integration with ShoreTel call info database, to get active call information. This needs to be combined with port-mirroring of the RTP audio streams to create recordings. On the ShoreTel Director server, the TrkHlpSvc service needs to be enabled. Consider disabling the option MGCP in Apresa to disable interpretation of port-mirrored call signaling and only use database information.

> > **Server address:** IP address of the ShoreTel server containing the MySQL database with telephony info.
> > **Server Port:** The port number at which the MySQL server can be reached.
> > **Username/Password:** The MySQL database login credentials (that is allowed access to the relevant database tables containing the call information)
> > **Database: (1)** The name of the database containing the heapportstatus and heaptrunkstatus tables.
> > **Database: (2)** The name of the database containing the ports table. This is optional, but is needed to detect the IP addresses of remote soft phones.

Salesforce: Integration with Salesforce.

> **Authentication domain:** Normally this should be "login.salesforce.com" (or "test.salesforce.com" in case of sandbox environment).
>
> **Username/Password:** Credentials of the Salesforce account to be used by Apresa
>
> **Add call records:** If enabled, a (completed) task of type call will be created in Salesforce on a matching Contact or Lead. Currently the following custom fields of a task are required to exist:
>
> • Call_Recording_Link: This will contain a link back to this server to playback the recording
>
> • Completed_Date: This will be set to the date and time of the end of the call
>
> **Apresa URL:** This is the URL that will be used when generating the link to the call recording. For example: https://recorder.company.com or http://192.168.1.2 .
>
> **Call type:** The call type of the generated call record in Salesforce.

Client connector: When many instances of Apresa Client (PC software) connect to this server, this option can help to reduce load on the server.

Toshiba SMDR: Turns on support for Toshiba SMDR. These records can be used to improve local phone numbers.
Toshiba SMDR Port: The port on which Apresa should receive the Toshiba SMDR data. The default port is 1109.
Toshiba IP Addresses: IP address from which Toshiba SMDR data is expected to be received from. This is an optional setting. The IP Addresses are only used for health monitoring and to generate alarms when a connection from one of these addresses closes.

Transcription: Select a transcription provider (VoiceCrunch) to use for converting audio into searchable text.
- For a good result, the audio storage codec should be set to **G.711 Stereo** (Recording settings, Audio file encoding).
- The Debian package for PHP curl (php-curl), and the package containing trusted CA certificates (ca-certificates) need to be installed.

Server address: Input the URL of the transcription service (including https://). Recordings will be sent to this address for transcription, based on the defined transcription tasks.
API token: Input the VoiceCrunch API token

store data as: Select in which field (column) new transcriptions must be stored
Transcription tasks: Click this link to go to the page where you can define which calls should be transcribed.

The following setting enables a special custom feature that is not intended for general use.
Import Tenants from Mitel Telepo: Import tenants with their users and telephone numbers from the Mitel system. This import happens once every 24 hours.

      Mitel IP Name or IP Address: Name or IP address of the management node. Once the Mitel IP Name or IP Address field has been set, an Import button will appear. Clicking on it, will immediately start a background task to import the tenants.

      Mitel Token: Token for a ticket used to authenticate an external application

      Mitel Secret: Secret for the same ticket as the token used to authenticate an external application

      Mitel Higher level group: Any tenants imported from the Mitel Telepo will have this group as their higher level group

20.11.5   VoIP settings

Options → System settings → VoIP settings

VoIP network: Select on which network ports the recorder must listen for VoIP traffic.
- *All:* The recorder listens for VoIP traffic on all detected network ports, up to 8 maximum.
- *On the "Phone" network socket:* The recorder listens for VoIP traffic on the second network port (marked as "Phone" on default hardware), and any additional ports (up to 8 maximum), but excluding the first port (marked "PC" or "LAN" on default hardware).
- *[All + Internal]:* The recorder will listen for VoIP traffic on all detected network ports, and it addition, it will listen for VoIP traffic inside the recorder (the loopback virtual interface). Normally this option should not be chosen.
- *None:* The recorder does not listen for VoIP traffic on any device.

Check for faults: When enabled, the ethernet connection to the VoIP network will be checked (cable present or not, dropped packets), and included in the system health state.

Restarting recording component: When a time is filled in, the system will restart the recording component if no calls are busy at that moment, each day. If a call is busy, it is rechecked a number of times, and if there are still active calls, then the recording component is not restarted. Use the format HH:MM. Example: 02:30

VoIP recording module: The Default option can handle all the supported protocols. The Snip option can handle more load on multi-core systems, but supports only the SIP protocol. The Snip option lacks support for much of the special options, but it does support the following:

- in the System settings VoIP: SIP port, Local/Remote IP addresses, Local telephone numbers, Dial code action, Split long recordings
- in the Recording settings: Audio file encoding, Addresses to record, SIP Filter, Recording/delete/silence/store on demand, Record inc./outg./local calls, Call monitoring
- under Tools: Encryption of call content

Database link: This setting is normally set to Internal. This setting determines if the VoIP recording engine communicates with the database through an internal link, or through the web server (external).

PF_RING: Enables an advanced kernel driver, that reduces packet drop when under high load. It requires Debian 7 or higher to operate.

ERSPAN without header: Enable this option if you need to capture ERSPAN data that lacks the normal header.

IP address of PBX: The IP address of the VoIP telephone system. This usually not needs to be filled in. It is currently only used in combination with the next setting.

Do not record SIP calls that start at the PBX: When both the traffic to and from the PBX is seen by Apresa, this will result in double recordings in some situations. To prevent this, this option can be enabled.

SIP port: Comma-separated list of SIP ports (UDP/TCP).

- For the Default module: If nothing valid is specified, all ports are checked for SIP data.
- For the Optimized module: If nothing is specified, only port 5060 is checked for SIP data.

SIP INVITE determines IP addresses: If enabled, the IP addresses of the SIP invite, and not of the RTP, will be used to determine the direction of the call (incoming/outgoing).

Local IP Addresses: This setting is used to determine whether an IP address corresponds to a local phone (extension). It is also used for detecting of the direction of a call (incoming, outgoing, or internal). A singular IP address or an IP address range can be specified. To specify multiple IP addresses or ranges, separate them by a comma. An IP range must be specified in the CIDR notation. For example: 192.168.0.0/24 means that the first 24 bits are fixed, and the last 8 bits may vary, which

means that, in this example, all IP addresses that start with 192.168.0. would be considered local.

Remote IP Addresses: In a VoIP call, there are two IP addresses that communicate. If one of them is in the Remote IP Address range, the other is consider local. The format is the same as for Local IP Addresses.

Local telephone numbers: This is a comma separated list of telephone numbers that are local. This setting is useful if it cannot be determined whether a call party is a local entity, based on IP address alone. Instead specifying telephone numbers one by one, it is possible to specify a range of numbers. For example to specify all numbers in the range from 3914100 to 3914199, specify: 3914100 - 3914199. The required format for number ranges is: First number space - space last number. The first and last number must have the same number of digits.

MAC address as Local ID: When this option is enabled, the MAC address will be used as the identifier for local telephones. A name can be attached to the identifier.

Name as Local/Remote ID: In the VoIP protocols SIP and SCCP, a name is sometimes communicated. This option specifies when Apresa must use this name as identifier.

Usage of SIP ID as identification: SIP IDs are usually of the form number@host, for example 152@192.168.0.43. The default option specifies that only the part before the @ (usually the number) will be used for telephone identification (user access).

Option	ID that will be used for telephone identification	
	for example SIP ID 152@192.168.0.43	for example john@company.com
Only use first part of SIP ID	152	john
Use full SIP ID for identification	152@192.168.0.43	john@company.com
Use full SIP ID except last number	152@192.168.0	john@company
Use first part of SIP ID if it is a telephone number	152	john@company.com

This can be useful in a multi-tenant environment. For example, the local number 140@1.2.3.4 can belong to tenant 1, while 140@4.5.6.7 can be long to tenant 2.

This option does not influence whether or not the full SIP ID is displayed in the main call listing.

Use P-Asserted-Identity as identifier (Caller): If enabled, the P-Asserted-Identity SIP header field will be used, instead of the From field, to identify the calling party.

Use P-Asserted-Identity as identifier (Receiver): If enabled, the P-Asserted-Identity SIP header field will be used, instead of the To field, to identify the receiving party.

If the P-Asserted-Identity field contains only an IP address, or a similar unusable identifier is detected, then the field will not be used, even if the setting is enabled.

SIP data field: Input a (custom) SIP field that must be extracted from the SIP data, and select in which field the extracted data must be stored in the database.

From secondary call legs, only use the Receiver ID: If enabled, the first call leg will determine the ID of the caller, while the last call leg will determine the ID of the receiver.

Split recording when telephone number changes: If enabled, recordings are split when the telephone number of one of the call participants changes during a call. It is applied in the following circumstances: During a special SIP call transfer, during a SIP identity change, during a Cisco SCCP telephone number change, and during an change of remote ID of a Xpert call. If the option is disabled, the original telephone number is preserved, and the whole call is stored is one recording.

SIP REFER: When enabled, detects a special type of SIP transfer that uses REFER messages. Without this option, the caller ID would not be detected correctly.

Start recording when connected: When enabled, for the supported protocols, no recording will be made of the call setup period. The recording will exclude the time during which the phone was ringing. The recording starts when the connection is established.

Dialing prefix for outgoing calls: The digit or digits that must be dialed first when making an external call. Only set this option if remote numbers in outgoing calls contain an extra digit (or digits) at the start compared to remote numbers in incoming calls. The dialing prefix will be removed from the number in the call listing, and the call will be marked as outgoing.

Phone number prefixes to remove: This can be used to remove unwanted text from the front of the telephone number (for example the + sign). Multiple prefixes can be specified separated with a comma. This applies only to the SIP and the Cisco SCCP protocol.

Phone number suffixes to remove: This can be used to remove unwanted text from the end of the telephone number. The star (*) sign can be used at the end of the suffix to match any number of characters.

It can be used to remove everything from the telephone number after and including a certain character sequence. Multiple suffices can be specified separated with a comma. This applies only to the SIP and the Cisco SCCP protocol. For a SIP ID of user@host, the suffix is applied only to the user part.

Detect phone number between parentheses: If the detected ID of the caller or receiver contains an ID between parentheses (round brackets), then the ID between the parentheses is used.

Audio stream can belong to multiple calls: When there are two SIP sessions, but only one audio stream, both SIP sessions will recorded if this option is enabled. Actions such as filtering can be performed on them separately. When the two SIP sessions are two legs of the same call, this option can lead to calls being recorded twice. Alternatively, if this option is disabled (which is the default currently), only one of the two sessions would be recorded.

Recording on demand is never applied to other phones in the SIP filter: Normally, a call is recorded on demand if one or both parties are in the recording on demand list. When this option is enabled, however, if one party is not in the recording on demand list, but it is in the SIP filter, then it is not recorded on demand, even when the other party is in the recording on demand list.

Unpreferred SIP IDs: When there are two SIP sessions, and only one audio stream, preference will not be given to those SIP sessions whose telephone numbers (or IDs) are mentioned here (comma separated). For Lync/S4B, if a phone number is communicated in the Referred-By SIP field, this will replace an unpreferred SIP ID.

Dial code action: This option determined when VoIP dial code commands (DTMF / digit press) are performed:

- *Local caller:* Dial code commands are performed only when they come from an IP address that is local (see the setting Local IP Addresses).
- *Only that match the filter:* Dial code commands are performed only they come from a phone that is in the recording filter.
- *All:* Dial code commands are performed always.
- *Tenant:* The dial code is performed only if coming from a phone of the tenant to which this call would be assigned.

Call pickup dial code: When a pickup dial code is specified (for example **), Apresa will attempt to detect such calls, and correct the remote number and direction, such that instead of, for example, **100, you see the real remote number. Apresa can only detect call pickup when it is started by dialing the call pickup dial code, followed by the extension. So if the dial code is **, and the extension is 100, then **100 is dialed. This feature is only available for the SIP protocol.

Alternatively, if the pickup code matches the complete phone number, for example, the destination phone number is "**333" and the pickup code is also "**333", then the direction is set to incoming, and no other changes are made. The actual phone number might be detectable using the "Use P-Asserted-Identity as identifier (Receiver)" setting.

Handle call legs separately: When a SIP call is forwarded with the same CallId through multiple hosts, each connection is handled as a separate call if this option is enabled. Otherwise, it is handled as a single call.

Use SIP tags for detecting end of call: This option is used for complex scenarios with multiple call legs. The SIP tags of some SIP fields are used to detect if all call legs are ended, or if the call continues. It is not recommended to switch this option on, unless necessary.

Detect Aastra Numbers: Enables detection of dialed telephone numbers when using an Aastra PBX.

H.323: Enable this option for Siemens HFA, Aastra / Ericsson Mx-One, and Avaya IP Office.

> **Avaya IP Office:** This option, together with the H.323 option, must be enabled for Avaya IP Office.
>
> **Local ID Detection (Avaya):** Sets the method that will be used to detect the Local ID for the Avaya protocol.

Avaya Stimulus: Enable this option for the SIP-based Avaya protocol used by IP Office.

> **Store on demand trigger text:** If the specified text is detected on the phone display, then the call is stored, if store on demand is enabled. This option is for use with the Avaya SIP-based Stimulus protocol.

Detect queue number: If enabled, it will attempt to detect the queue number and place it in the Connected telephone number field (without the @host part). This option is intended for use with Avaya IP Office SIP.

Cisco Active Recording direction detection: When using Cisco Dual Stream Active Recording, the direction of the call (incoming or outgoing), is detected based on the zero prefix of the remote telephone number. This zero prefix is removed from the telephone number, before display in the call listing.

innovaphone: When using innovaphone PBX, and conferencing in calls to the Apresa VoIP Service, enable this option to detect the remote ID and direction of the main call.

Megaco / H.248: This option enables support for the Megaco protocol (also known as H.248).

MGCP: This is option enables support for the MGCP protocol, which is used by Panasonic and ShoreTel.

Nortel UNIStim: This option enables support for the Nortel Unified Networks IP Stimulus protocol.

- **Local ID:** This option determines if the Local ID will be the detected telephone number, or the name (if available). (for Unistim)

Stop trigger texts (Alcatel): When one of the texts is found on the phone display, the recording is stopped and deleted. Multiple trigger texts can be specified separated by a comma.

OpenScape Xpert: This option enables support for recording the Unify OpenScape Xpert trading system. Recording also needs to be enabled and configured in the OpenScape Xpert System Manager.

> **Xpert Master Turret:** The recorder will connect to this device to receive call meta data. To connect to multiple devices, use a comma separated list of IP addresses.
>
> **Xpert Local ID / Connected:** These two settings determine which data items will be used to fill in the Local ID and Connected column in the database. This setting only effects new calls. Options:
>
> - Line Name (Example: 5320). This is usually a line number. A turret can dial out and receive calls on multiple lines.
> - Line Name (Example: 2.6.1/3.8). The identifier (ID) of the line.
> - Username. This is the configuration name that is selected during log on.
> - Device. The identifier of the device.
> - Conference ID. This is the ID of the line conference, that is the same for all lines participating in the same conference on the same turret. It can have a different value on another turret.

SIPREC OpenScape Xpert: This options enables support for recording via the SIPREC protocol received from the OpenScape Xpert system. For this setting to work, it is also required that the VoIP Service is activated and configured for SIPREC. The OpenScape Xpert system also provides additional Xpert specific data about the recorded calls. This data can also be stored in the database. The following options control which information is stored where.

SIPREC Xpert Caller ID: This setting controls which data item is used to fill in the local, remote and connected caller ID columns in the database if the selected data option is available. The connected ID is only used when a conference is recorded.

Unique to this setting:

- Original. This uses the original number. In case a different selected data item is not available, this is also used.

SIPREC Xpert Data/SIPREC Xpert Notes: This setting controls which data item is stored in one of the notes (editable) or data (non-editable) columns in the database.

Unique to this setting:

- None. This leaves the column empty.

The following options are shared between both settings:

- Line Name. Line label of the affected Xpert Client.
- Line ID. The identifier (ID) of the line.
- Node Address. Xpert specific client ID.
- Agent Name. Profile name of the affected Xpert client.
- Device Type.
- Display Name. Mapping of the relevant Xpert Client (resolved by local telephone book or the display name coming from the SIP PBX)

The following data fields are available for SPM recording. There are up to four lines on each SPM panel that are assigned to a channel from 1 to 4.

These settings control how the data pertaining to the channels is stored in the database.

- SPM Channels. This stores all data from all channels in this field. The data is prefixed with the channel number and type.
- SPM Channel 1-4. This stores all data from this specific channel in this field. The data is prefixed with the type.
- SPM Line IDs. This stores the Line IDs from all channels in this field. The data is prefixed with the channel number.
- SPM Line ID 1-4. This stores the Line ID from this specific channel in this field.
- SPM Line Names. This stores the Line Names from all channels in this field. The data is prefix with the channel number
- SPM Line Name 1-4. This stores the Line Name from this specific channel in this field.
- SPM Caller Numbers. This stores the Caller Number from all channels in this field. The data is prefixed with the channel number.
- SPM Caller Number 1-4. This stores the Caller Number from this specific channel in this field.
- SPM Called Numbers. This stores the Called Numbers from all channels in this field. The data is prefixed with the channel number.
- SPM Called Number 1-4. This stores the Called Number from this channel in this field.

SIPREC Broadworks: Turns on support for Broadworks SIPREC extension data. Use the SIPREC Broadworks Data and SIPREC Broadworks Notes options to store the extra Broadworks data in the database notes or data fields. The following extra extension data is available:

- External tracking ID: Identifier for all recordings. Can be shared by multiple recordings if they were split due to call transfers.

- Service Provider ID: The identifier for the name of the service provider or enterprise to which the user requesting recording belongs.
- Group ID: The identifier of the group to which the user requesting recording belongs
- User ID: The identifier of the users for which the call is being recorded
- Call ID: The SIP call ID for the call being recorded
- - Calling Party number: Phone number of extension that identifies the calling party
- Called Party number: The called party number after translations.
- Dialed digits: The digits dialed by the subscriber. Only available for outgoing calls.
- Redirection information: Information if a recorded call is redirected/transferred. Includes the phone number of extension of the redirected from party, the phone number or extensions of the redirected to party and potentially a new external tracking ID.

SIPREC Broadworks ignore store on demand: Broadworks extends the SIPREC protocol with a store on demand function. By default this extension will be detected if SIPREC broadworks support is turned on. If no store trigger is received during the recording, the recording will be discarded afterwards. Enabling this option will disable this functionality so that the recording will always be stored.

Mitel MiNet: This option enables support for the MiNet protocol used by MiVoice Office and Mitel IP phones.

Samwin: This option enables support for the protocol used by Samwin, a call center product.

> **Local ID:** This option determines if the Local ID will be the detected telephone number, or the UserID (if available). (for Samwin)

SIP NEC: This option enables support for the SIP NEC protocol.

SIP log-on detection: (Broadsoft) This option enables log-on agent detection for the hotelling function of Broadsoft.

SIP log-on detection: (Telephone number) This option enables log-on detection based on a telephone number that is dialed by the agent to log on or off.

- **Log on:** Specify the telephone number that is dialed to log on. The agent id is expected to be dialed after this code.
- **Log off:** Specify the telephone number that is dialed to log off.

Speakerbus: Enables integration with Speakerbus iSeries, using CDR data to detect phone numbers.

Port number: Apresa will accept TCP connections on the configured port, and interpret the received CDR Speakerbus data.

Apresa network service: This option needs to be enabled to record Microsoft Lync calls. It also requires that the Apresa Lync Plugin (ALP) is installed at the Lync server.

Filter Known Video: Enabling this option will filter out the RTP that is a known video codec used by Skype for Business. This will stop pure video sessions to show up as an unplayable recording in the calls database.

ALP IP addresses: The IP addresses on which the Apresa Lync Plugin will be installed and that will connect to this Apresa. This is used only for health monitoring. If connection to one of the ALP addresses is lost, this is regarded as a system error.

RTP over TCP: Checking this option allows for the recording of RTP audio streams that are sent over TCP instead of the usual UDP. This is very uncommon, but can occur with Skype for Business.

NAT Mapping: In case of a static NAT mapping between a public IP address and a private IP address, it may be possible that the public IP address is signaled, while the Apresa receives the RTP stream on the private IP address. In such situations, calls may not be properly recorded, because signaled information cannot be properly associated with the RTP streams, since the IP addresses differ. Using this option, a mapping can be made known to the Apresa, so that it can be used during call recording. Every mapping should be put on a new line with the form: <public IP address>=<private IP address>

Only record RTP in calls: RTP is the protocol used to transport audio between two parties over the network. RTP is used in call protocols such as SIP and H.323. If this option is enabled, and if no call signaling has been detected that is related to a detected RTP stream, then the RTP stream will not be recorded. Otherwise, it will be recorded, and the stream will be added to the call database with IP addresses as identification, without telephone numbers.

Amplification: The amplification of the VoIP audio data during recording. Use a positive value to increase the volume, or a negative value to decrease the volume.

Split long recordings: If a recording continues longer than the specified duration (in minutes), the recording is closed, and a new recording is started.

Maximum silence gap to include: When there is a gap in the audio stream of a call, and this gap is larger than the specified number of seconds, then this gap is removed from the recording, and a beep is inserted instead. If not filled in, the default value is 10 seconds.

Insert tone at time jumps: A beep sound is inserted into the recording at the point where a gap was removed from the audio stream (a discontinuity in the RTP time stamps).
Collect information about all calls: This enables live information about calls even before they are connected (while ringing), and also about calls that are not recorded. It will enable a new menu item in the Tools menu called Active Calls (All).
Only enable when needed, because otherwise it uses resources unnecessarily.
Store metadata of missed calls: If enabled, missed calls are included in the call listing. This applies only to new calls.
Store metadata of calls over channel limit: If enabled, calls that were not recorded because of the channel license limit, are included in the call listing. This applies only to new calls.

20.11.6   Dial code actions

Options → System settings → Dial code actions

Dial code, dial code action: An action can be assigned to a dial code. For example, it can be configured that dialing *11 during a call, will cause Apresa to email you the recording of the current call, when finished. To do so, fill in *11 as the dial code, and select "E-mail current recording" as the dial code action.
For Cisco SCCP, speed dial buttons are represented as code S (for the first speed dial button), and T, U, V, W, X, Y, Z (for additional speed dial buttons).
Apresa is not always able to detect dial codes. In that case, dial code actions cannot be used. Apresa Client (PC software) or the Web Client might be used instead to perform call actions.
- The dial code actions **"E-mail current recording"** and **"E-mail previous recording"** require that there is a user account with an email address filled in and a telephone that matches the local or remote party of the call. It will email the current or previous recording of this user.
- The dial code action **"Store this call"** is relevant when the option "Store on demand" is enabled in the Recording settings.
- The dial code action **"Start silence"** will silence the recording from that point in time, until the **"Stop silence"** dial code action is performed, but only if "Silence on demand" is enabled in the Recording settings.
- The dial code action **"Start recording"** will start the recording of a call that is configured to be recorded on demand, but is currently not yet recorded. The recording will continue until the end of the call, or until the **"Stop recording"** dial code action is performed.

- The dial code action **"Delete"** will stop the recording of the current call and delete it, and will not start recording again for this call. The dial code action **"Delete and restart"** will stop and delete the current VoIP recording, but start a new recording afterwards for the same call. If recording on demand is on, it will add an item to the active calls without actually recording yet. The "Delete and restart" option is currently available only for VoIP. These two dial code actions are only possible for phones for which Delete on demand is enabled in the [Recording settings](#).
- The dial code action **"Add annotation"** will add a marker at the specified time during the call. Annotations are displayed on the time line during inline playback.
See also the "Dial code action" setting in the VoIP tab.

20.11.7 E-mail

Options → System settings → E-mail

E-mail address of administrator: This email address will be used for sending system messages about the status of the system. The second email address also receives a copy of these messages.
E-mail address (Loud voice detection): This email address will be used for sending messages when the system has detected a loud voice in the call. If not defined, then the message will be sent to the administrator.
Source e-mail address: This email address will be used as the default sender address of e-mails that Apresa sends.
Send e-mail report periodically: This option specifies how often Apresa must report its status to the administrator by email.
E-mail report time: This option specifies at which time of the Apresa reports its status by email.

Report schedules: These schedules define when and which report will be sent by email. These report schedules are configured on a separate page. These are independent of the status email defined in the previous setting.

Report Schedules

Options → System settings → E-mail → Report Schedules → Configure

This page can be reached from the System settings, Email tab, by an administrator. Here you can configure when and which reports

---

> will be sent by email.
>
> Currently only one type of report is available:
> * Calls per user: This will list all users in the system, and how many of their calls were recorded.
>
> The reports will be sent automatically during the night, after the selected time period has past. To preview a report without sending it by email, click the View button. To generate and send the selected report by email now, click Perform Now.
> Reports are always generated about the previous time period that has finished. So for example, when the time period "Week" is selected, the report will be about the previous week. When "Day" is selected, the report will be about yesterday. The name of the report is included for reference in the report. The report is sent to the specified email address. Multiple email addresses can be specified comma separated.

Email recordings to: Automatically email all recordings to either a fixed email address, or to the associated user.

Method to send email: *SMTP relay server:* Apresa sends the email to this relay server using SMTP, based on the parameters specified below. *Direction connection:* Apresa itself looks up the MX record for the destination email address using DNS, then connects directly to this server using SMTP.
SMTP server address: The IP address or the IP name of the SMTP relay server that Apresa may use to send email.
SMTP user name/password: These parameters must be filled in when authentication is required by the SMTP server.
SMTP encryption: For additional security, Apresa can use SSL or TLS to communicate with the SMTP server, provided that the SMTP server supports the protocol.
SMTP port number: The port number that is used to communicate with the SMTP server (default: 25).

Email templates: Select one of the email templates, click Configure, and then fill in the subject and content of the email. The tags displayed on the right (such as <USR>) will be replaced by their values if available when the email is sent. The following email templates can be defined:
* New password: This email template is used when a new password is defined on the User page by an administrator, and the option "Send e-mail to user" is enabled.

- Verification Code: This email template is used for the Verification Code if the option "Log on Verification Code" is enabled.

20.11.8 Category

Options → System settings → Category

A category can be assigned to each recorded call. This can be done in main call listing. The names of the categories can be entered here. To choose a custom color for a category, click on the colored box, and select a new color.

20.11.9 Apply changes

Options → System settings

To save changes, click the Apply button. If a component needs to be restarted to apply the new settings, you will be asked for permission first. Some settings can be applied without restarting.

21   System Shell

Normally you will not need the system shell. Only use it when you are aware of what you are doing. In rare cases it is used for maintenance purposes, and there is documentation available for customers about how to access it. Be careful with this.

Warning: Using the system shell, it is possible to destroy all recorded calls, or cause the system to stop functioning.

If you want to use the remote shell, go to the System settings of the Apresa and check "Remote Shell" to enable it. You will be prompted for a new password. It is recommended to leave the remote shell option disabled when it is not needed.

22 GNU General Public License.

Some portions of the device software are covered by the GNU General Public License. The source code of these portions will be provided upon request for a charge of no more than the cost of physically performing the source distribution under the terms of Sections 1 and 2 of the GPL License *) on a medium customarily used for software interchange.

If you want to receive the source code, contact Vidicode:

Ecosoft B.V. / Vidicode
Blauw-roodlaan 140
2718 SK Zoetermeer
The Netherlands
Tel: +31 793471000
Fax: +31 793618092
E-mail info@vidicode.com

*) The GPL License can be found on the Application CD that comes with your Call Recorder Apresa, in the folder **License.**