SoniControl User Documentation

SoniControl is a novel technology for the recognition and masking of acoustic tracking information. The technology helps end-users to protect their privacy. Technologies like Google Nearby and Silverpush build upon ultrasonic sounds to exchange information. More and more of our devices communicate via this inaudible communication channel. Every device with a microphone and a speaker is able to send and receive ultrasonic information. The user is usually not aware of this inaudible and hidden data transfer. To overcome this gap SoniControl detects ultrasonic activity, notifies the user and blocks the information on demand. Thereby, we want to raise the awareness for this novel technology.

The project SoniControl is funded by Netidee (www.netidee.at) and is a project at the Media Computing Group at the Institute for Creative\Media/Technologies at Sankt Pölten University of Applied Sciences (mc.fhstp.ac.at). The project website of the SoniControl project with all published results and resources can be found here: sonicontrol.fhstp.ac.at. The SoniControl App is released under GNU General Public License version 3.0 (fsf.org/). You can download it on the Google Play Store.

License

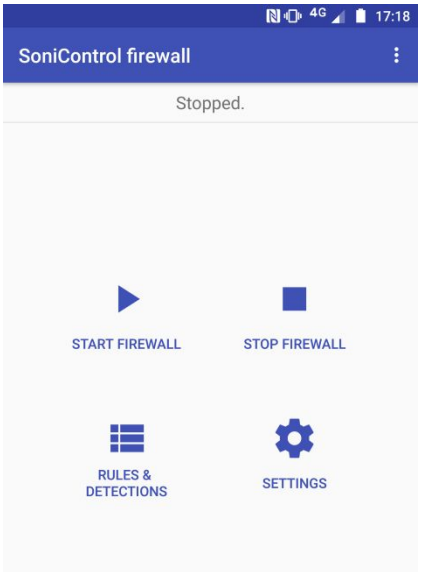
Permissions and Privacy Statement

To work properly, SoniControl requires the *microphone permission* to scan for ultrasound communication. You can also use the microphone as a blocking option. If you want to use location-based functionalities, the *location permission* will also be needed.

- We use the microphone to capture sound, but process only the ultrasonic part, we remove everything under 17kHz.
- Sounds are analyzed in real time on the phone.
- Detections are stored locally in a JSON file, including the time, the type of technology detected by our algorithm, the decision, whether the sound source shall be blocked in future or not and the location of the detection (if location access is permitted by the user). The user can delete this file at any time via the "settings" menu.

- If allowed, we check the users' location regularly in order to automatically block or allow signals when they enter an area covered by a firewall rule (e.g. where they previously detected ultrasonic communications and decided to block it in future).
- The Internet permission is required to display the geographic map background and to share detections with the community. This permission is classified by Google/Android as uncritical (protection_normal). Therefore it is not shown in the permission overview of the app's detail information. No data is uploaded without the user opting in. Sharing is done on demand, when the user checks "Share detection", or automatically if an "always" firewall rule is met and the user opted in for sharing detections by default (from the "settings" menu). If the users share their detections, the time, technology detected, blocking decision, the location information (if allowed by the user) and a short audio sample of the detection (everything under 17kHz is removed), will be uploaded to the SoniControl server. No user ID is stored, and thus the data is anonymous.
- If allowed, the geolocation is used to center the map on your position.

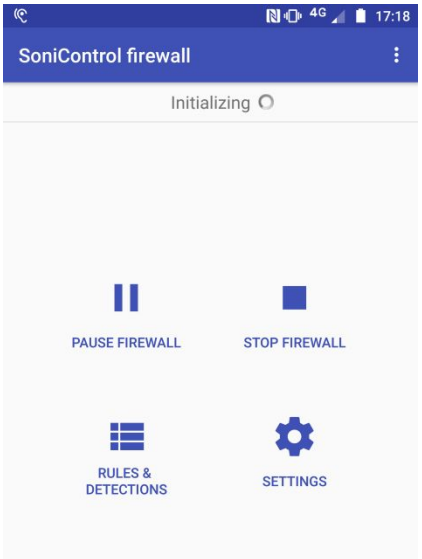
Starting the firewall



When you open the application, there are four buttons for "Start/Pause", "Stop", "Rules & Detections" and "Settings". A notification symbol indicates when the firewall service is present in the background. On start it is not yet shown as the firewall is “Stopped”.

When you click on "Start firewall", the app starts to scan the ultrasonic range and the notification symbol appears / changes to a normal ear. The app needs about 10s to initialize the detection system (learning the "normal" background noise).

Pausing the firewall



When the firewall is scanning for ultrasound, you can tap on the “Pause” button to pause the process. You can then restart without having to wait for the firewall to initialize. This is useful, e.g. if you like to use ultrasound for some time (pairing a device, or sending some information) and then activate the firewall again.
When the app blocks ultrasounds, you can also tap on “Pause” to stop this process. Tapping on Start again will then restart scanning normally. You can see if the firewall

is scanning or blocking via the status text, the notification and its symbol. This symbol will be changed back to the “On hold” one, after hitting the Pause button.

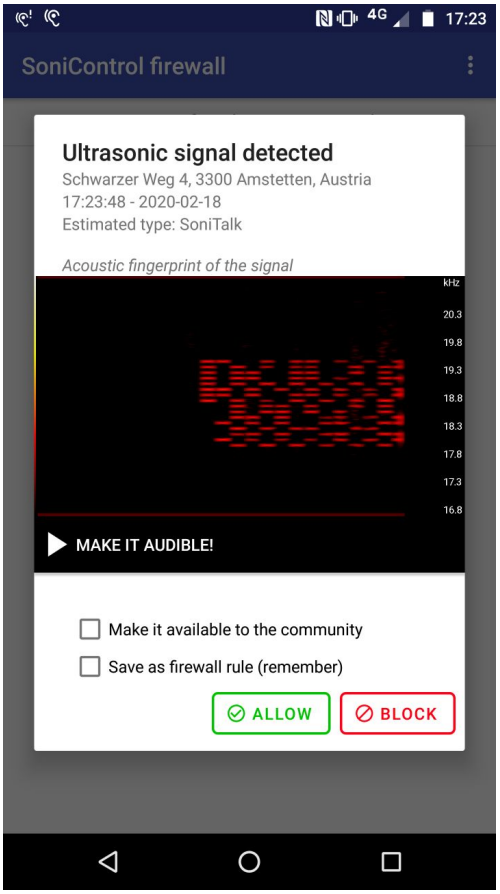
Stopping the firewall

When you tap the Stop button in the app, all processes will be closed, all resources will be released, and no background task will run anymore, so the notification can be canceled. When tapping the Start button again, the scanner will need to be initialized again.

On ultrasonic signal detection

When an ultrasonic signal is detected, an alert dialog appears, showing the location and time of the detection, as well as several diagnostics features:

- The signal’s estimated type is shown (or “unknown” if it could not be recognized)
- The acoustic fingerprint (spectrogram) of the signal is visualized
- The user can press on “Make it audible” to listen to a hearable pitch-shifted version of the ultrasonic signal.



The dialog offers the user with two main options to deal with the detected signal:

- **Block**: depending on your settings, your smartphone will block the signal using one of the two possible methods:
  - Either the same frequency range as the signal will be sent from your smartphone’s speaker to “jam” it, or
  - if the microphone is available and you checked the setting “use microphone to block”, the app takes the access to the microphone, effectively keeping other apps from recording.
- **Allow:** ignore the signal. This is useful, e.g. if you like to use ultrasound at this place for some time (pairing a device, or sending some information). In this case you also probably want to pause the firewall until you are done using ultrasound. If you want to always allow this type of signal at this place, check the option “Save it as a firewall rule (remember)”.

Additionally, two checkboxes give “long-term” options regarding the signal for the user to :

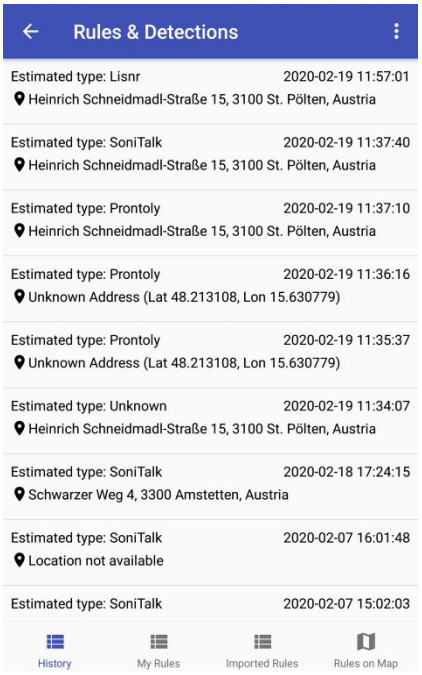
- “**Make it available to the community**” which shares the detection with the community, making it possible for other users to import this detection as a firewall rule in their app (blacklist / whitelist). When this option is checked, the detection is uploaded anonymously to the SoniControl server. No data is uploaded without the user opting in. The sharing process happens on demand, when the user checks “Share detection”, or has opted in for sharing in the settings menu. The shared data consists of the location information (if allowed by the user), the detection time, the estimated detected signal type, the blocking decision and a short audio sample of the detection. This audio sample only consists of the inaudible information above 17kHz, so no speech etc. is included.
- “**Save it as a firewall rule (remember)**” which stores the detection locally in a JSON file. This means we can later *automatically block or allow* the signal when detecting it at this place again (this decision can be changed in the “Rules & Detections” activity). Not saving a signal/location as a rule allows you to get notified again on detection, e.g. to check how often you detect a signal, or how big its range is.

If the signal was allowed, the detection starts again and the notification symbol changes back to the normal ear.
If the signal was blocked, the blocking process starts and the notification symbol changes to the ear with a little speaker.

Rules & Detections

The "Rules & Detections" activity is split in four tabs:

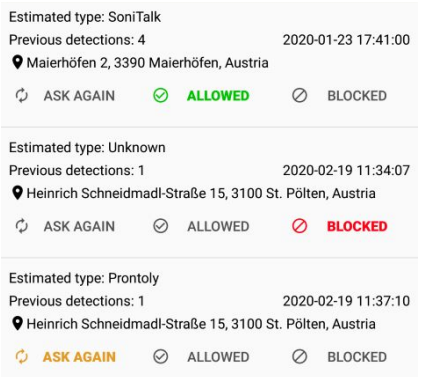
History



The “History” tab shows all ultrasonic signals detected so far (unless the user deleted one or more of them). The following information is shown:

- On the top left, the “**Estimated type**” indicates the signal’s technology provider, if recognized (otherwise “Unknown”)
- On the right side, the **date and time** when the signal was detected
- On the bottom, the **address** where the signal was detected if location was allowed, available, and if an address match was found. If no match could be found (or if there was no internet access), “Unknown address” is shown with the GPS coordinates next to it. If location was not allowed or not available, “Location not available” is displayed.

My Rules



The “My Rules” tab shows firewall rules, that is, ultrasonic detections for which the “Save it as a firewall rule (remember)” checkbox was checked in the detection alert dialog. Additionally to the content present in the “History” tab, it indicates the amount of “**Previous detections**” of this signal’s type at this place and the current **rule status**, which can be one of “Ask again”, “Allowed”, or “Blocked”, meaning that next time this signal’s type is detected at this place, the firewall should ask the user again to take a decision, respectively allow or block automatically the signal.

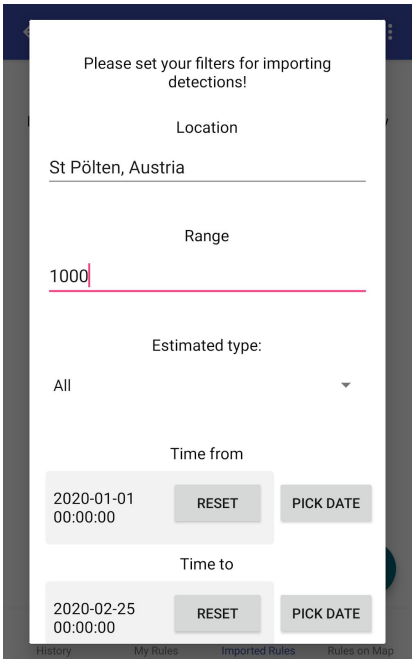
You can change the rule status by tapping on the corresponding button. You can delete a rule by pressing longer on it.

Imported Rules

The “Imported Rules” tab allows users to import firewall rules that were shared by other users by checking the “Make it available to the community” checkbox in the detection alert dialog.

Similarly to antivirus’ blacklists, this allows users to download a set of rules to preemptively block specific signals in their area.

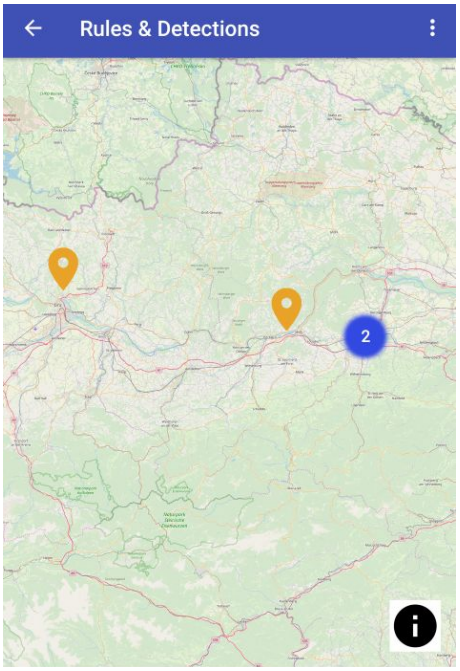
The layout of the items is the same as in the “My Rules” tab.



The import dialog offers five fields to filter detections to import.

- The chosen **location** will be the center for the geographic filter, working together with the **range** that indicates the radius in meters around this central location.
- The signal **type** to import can be selected.
- A timespan can be defined by entering a start and/or end **dates**.
- If a field is not filled in, all uploaded detections matching the other criteria (if no filter is set, all detections) will be downloaded. The default date for the start is the launch date of the firewall and the default end date is the current date.

Rules on Map



The “Rules on Map” tab offers a geographical view of the Rules stored in the “My Rules” and “Imported Rules” tabs. It does NOT show the history, nor detections from other people (unless you imported them).

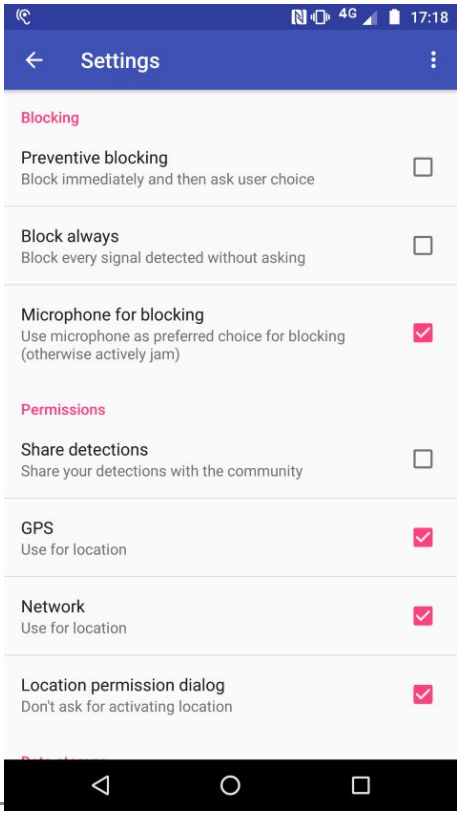
The color of the markers stands for the rule status:

- Red markers will always be blocked
- Green markers will always be allowed
- Orange markers will trigger the detection alert dialog asking again for a decision on the next detection of the corresponding signal at this place.

If you tap on a marker, a circle will appear whose size represents the signal strength. The radius of the circle is NOT representing the distance reached by the signal.

Further, blue circle icons represent clusters of detections (detections that are too close to each other to be shown separately). When you zoom in, the cluster will split into single markers.

Settings



The settings are split in five sections:

Blocking

- “**Preventive blocking**”, gives the opportunity to block as soon as a signal is detected (before the alert asks the user what to do with the signal).
- "**Block always**", blocks every signal detected without asking the user.
- “**Microphone for blocking**”, Use the microphone as preferred choice for blocking (otherwise actively jam).

Permissions

- "**Share detections**", sets the checkbox to share your detections with the community to true by default. You can always change your choice in the alert dialog.
- "**GPS - Use for location**" and
- "**Network - Use for location**" are both ways to give or not access to the location service. When both are disabled, you cannot save Firewall rules to automatically block or allow signals.
- "**Location permission dialog**" - "Don't ask for activating location", if checked, the alert asking you to activate the location hardware setting will not be shown.

Data storage

- "**Save detections in JSON file**", gives the user the opportunity to opt-out from saving any data. When both this is checked, you cannot save Firewall rules to automatically block or allow signals.
- "**Clear detections of JSON file**", deletes the file storing Firewall Rules and Detections.

Advanced settings - Detection

- "**Advanced diagnostics**", notifies of detection after signal end (more accurate recognition, but the detection is triggered later).
- "**Location radius**", indicates how far a signal should still be blocked.

Advanced settings - Jammer (active blocking)

These settings focus on the behavior of the blocking process:

- "**Pulse duration**", decides how long a single pulse during the jamming process is.
- "**Pause duration**", decides how long a pause between two pulses should be.
- "**Bandwidth**", how broad one jamming signal is (in Hz).
- "**Blocking duration**", how long the app will block before it checks the location and distance to the detected signals location again.

Reset settings

- "**Reset all settings to default**", will reset all settings to the default state.