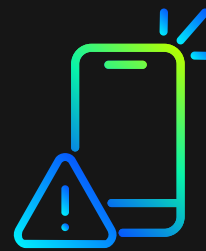




Getting Started Guide

Voice Traffic Filter



**Spam
Blocker**
Powered By Mutare

Voice Traffic Filter Overview

Voice Traffic Filter (VTF) is a configurable call filtering and network security application for your voice channel. When VTF is implemented, calls to the enterprise can be filtered through a series of analytic steps including a dynamic database of known spam, scam, and robocall numbers, STIR/SHAKEN scoring data, as well as an organization-specific set of rules that can be applied to incoming calls.

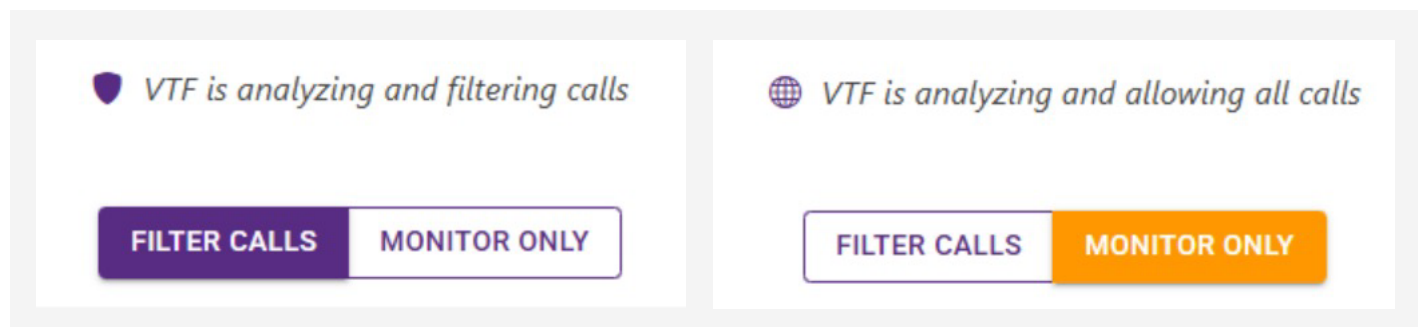
Any flagged call can be immediately dropped or redirected by enterprise policy without ringing through, sparing users the time and disruption of calls and notifications from unwanted callers and protecting those users and the voice network from potential criminal intrusions.

Welcome to Voice Traffic Filter

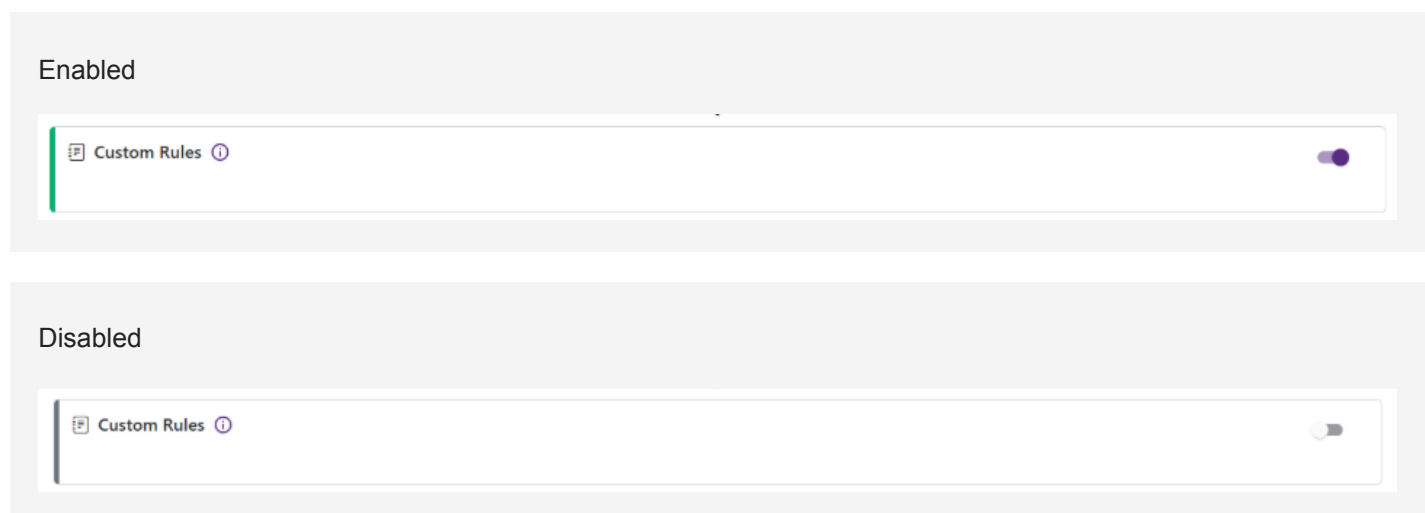
Now that you've successfully logged in, we'll take you on a short tour. This should take 15-20 minutes. This tour will guide you through all features and give you some hands-on experience with managing your voice traffic and understanding what the caller experiences based on your filter criteria.

Configuration Page

From the top of the page, you can toggle VTF between FILTER CALLS to take action on calls after being analyzed, or MONITOR ONLY to just analyze calls. If the filter status is MONITOR ONLY, all calls are Allowed, no matter the results of the analysis.



Below the toggle, each of the four layers of protection can be enabled or disabled within each section. If enabled, you'll see a green line indicating as such on the left-hand side of the layer section. If disabled, it will be indicated by a grey line on the left-hand side.



Custom Rules

Spam Blocker, powered by Mutare recommends leaving this feature Enabled so that you can create Custom Rules for callers and callees.

STIR/SHAKEN

Configure how Voice Traffic Filter handles the STIR/SHAKEN data in your system with the provided tools. Note that you may need to communicate with your carrier to receive STIR/SHAKEN parameters in your SIP traffic. STIR/SHAKEN number validation is sent via the P-Asserted-Identity header in SIP signaling. The 'verstat' tel URI parameter in the SIP INVITE can be parsed to have one of the first three values. If desired, an action can be selected for each of the three results. In addition, an action can be selected when receiving a call with no 'verstat' tel URI parameter.

STIR/SHAKEN ⓘ

TN-Validation-Passed

Action
No action

TN-Validation-Failed

Action
No action

No-TN-Validation

Action
CAPTCHA, drop failures

No verification status

Action
No action



TIP

Spam Blocker, powered by Mutare recommends that you send calls with a TN-Validation-Failed to CAPTCHA and drop failures. Calls that fail validation usually are from unreliable parties.

Proprietary Dynamic Database (PDD)

The PDD is a continuously evolving hard line of defense against known spam, scam, and vishing attack campaigns. It taps into multiple worldwide resources dedicated to tracking and verifying tens of millions of numbers related to nuisance and nefarious call activity.

When enabled:

- Incoming calls are checked against multiple databases
- A configurable action of applied if the number is flagged

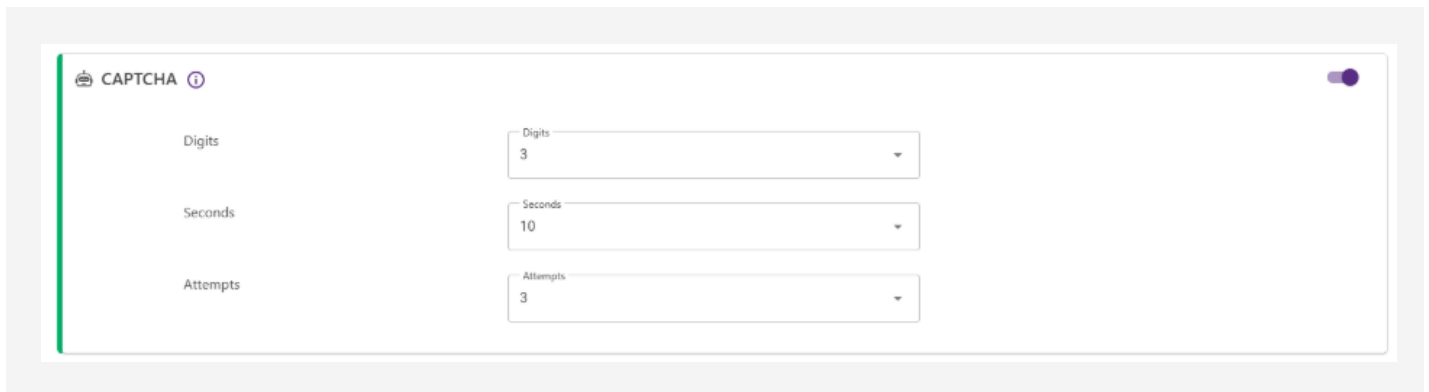


TIP

- Start out with a do-no-harm approach and set your PDD to one of the CAPTCHA actions.
- Enable PDD in early deployment to benefit from continuously updated threat intelligence.

CAPTCHA

The Voice CAPTCHA helps differentiate bots from human callers and reduces the risk of blocking legitimate traffic.



CAPTCHA ⓘ

Digits: 3

Seconds: 10

Attempts: 3



TIP

Spam Blocker, powered by Mutare recommends configuring your CAPTCHA with the following settings:

- Digits – Set this to 2 or 3. One is too easy for bots; more than three is a nuisance for real callers.
- Seconds – Set this to 10. This gives humans enough time to respond.
- Attempts – Set this to 2 or 3.

Exercise It!

Here are some exercises to get you familiar with using VTF.

From the Call Activity page:

- Start out by calling one of your phone numbers
- Refresh the page, you should see your call appear near the top of the Call Details area. Look for your caller ID. Note the Action that was taken on your call.

Head to the Custom Rules page:

- Now let's add a rule!
 - Use your phone number as the "From"
 - The number you called as the "To"
 - Select Drop as the Action

Go back to the Call Activity page:

- Call that phone number again.
- The call should Drop. Note that if in Monitor Mode the call should show that it would've been dropped.
- Refresh to see the call details, showing that your call was dropped due to a Custom Rule.

Go back to the Custom Rules page:

- Click the pencil icon to Edit the rule and change the Action to CAPTCHA-Drop and save.

Go back to the Call Activity page:

- Call the phone number again. When prompted to enter digits by the CAPTCHA, enter them correctly.
- Refresh the page to see the updated results
- Call the phone number again. When prompted to enter digits by the CAPTCHA, enter them incorrectly. Repeat until the call is dropped.
- Refresh the page to see the updated results

Go back to the Custom Rules page:

- Click the trashcan icon to Delete the rule

Go back to the Call Activity page:

- Call the phone number again.
- Ensure that the call is Allowed.
- Refresh the page to see the updated results.

This walkthrough provides you with some guidance on the features of your Voice Traffic Filter. You are in control. Check back weekly during the first month of use so that you can see the trends. Feel free to utilize the Custom Rules to add Rules for blocking, routing, or allowing callers as needed. Check the Call Activity page to see how each call is handled.

Support

- Escalate access issues to your Tenant Administrator
- Contact CallTower Support for any filtering anomalies at support@calltower.com
- Be sure to include Tenant name, timeframe, and examples