calltower

VTF Admin Guide

Voice Traffic Filter

Spam Blocker
Powered By Mutare

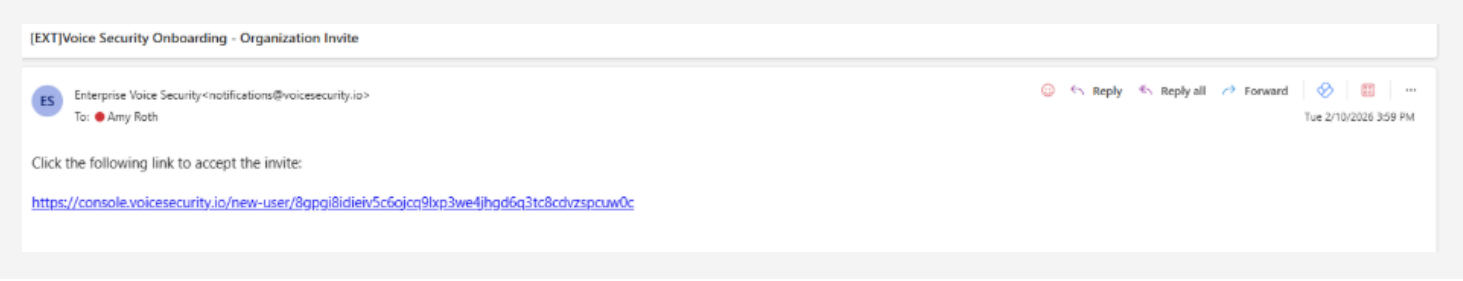
Voice Traffic Filter Overview

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.

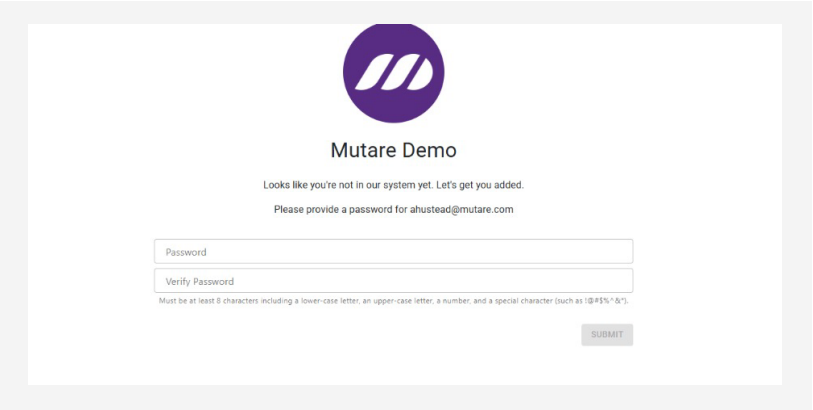
Any flagged call can be immediately dropped or redirected by enterprise policy without ringing through, sparing users the time and disruption of calls and notifications from unwanted callers and protecting those users and the voice network from potential criminal intrusions.

Invitation

To get started, users will receive an email invitation like the one below.



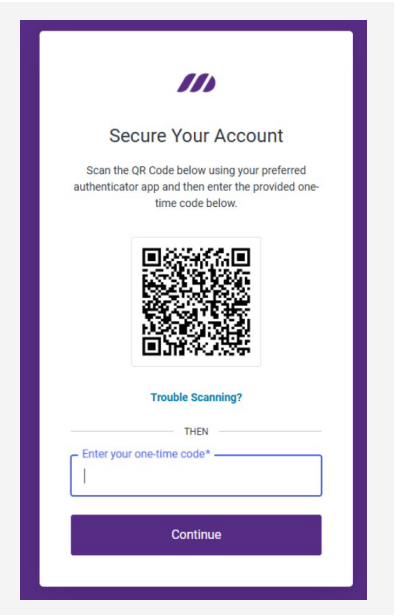
Clicking the link within the email will take the new user to the registration page in the Console where they will set their password.

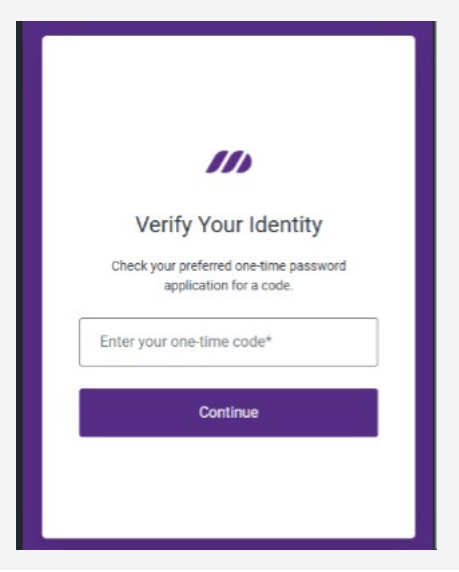


The user will be prompted for Mult-Factor Authentication (MFA) after logging in with a username and password.

Setting up MFA

You should see a QR code to scan within your Authenticator app





The user then enters the one-time code shown in the Authenticator app via the login page

The user should now be able to click to login. If there are any issues, please contact your Administrator.

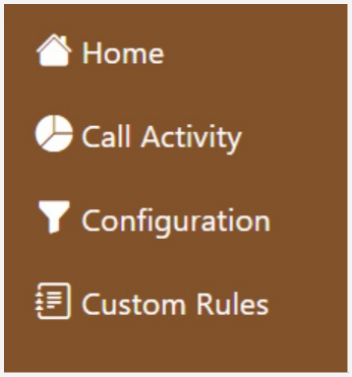
Note Existing Console users will not have to go through the above registration process when being invited to a new Tenant. Rather, they will see the new Tenant from the Tenant picker dropdown.

The Console

You have quick access to the navigation menu, your Profile, Tenant Picker, and Feedback from any page in the Console.

- Your Profile allows you to change the time zone and language and can be accessed from all pages of the Console.
- If you have access to more than one Tenant, you can access them from the Tenant Picker dropdown.
- Clicking the Feedback icon opens a pop-up that enables you to submit feedback to Spam Blocker, powered by Mutare and let us know what we can do to improve your experience.

The Navigation Menu is on the left side of the page:



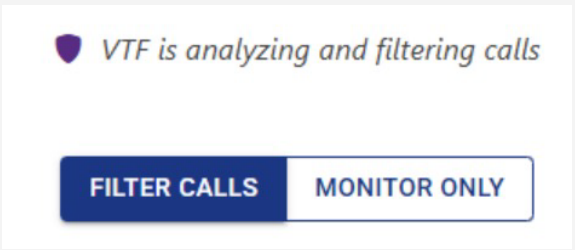
Configuration

The Configuration page defines how Voice Traffic Filter analyzes and acts on inbound calls.

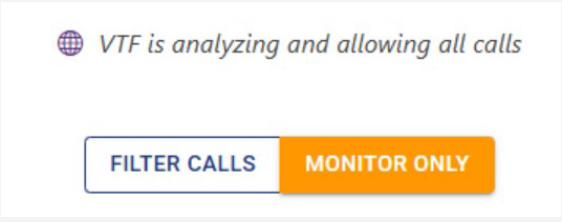
Filter Mode

There are two filter modes in VTF:

FILTER CALLS – Actively applies actions based on call analysis.



MONITOR ONLY – All calls are allowed regardless of analysis results. The call is still analyzed and shows what would have happened.



TIP

Start new deployments in MONITOR ONLY mode to get an understanding of your traffic patterns before enforcing actions.

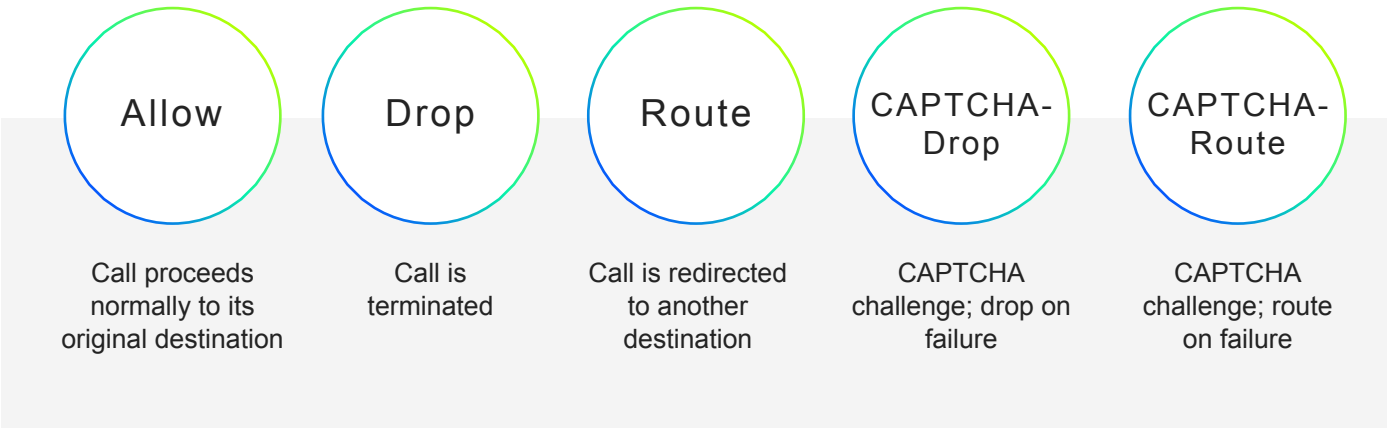
Analysis Priority Order

Incoming calls are analyzed in the following order:

1. Custom Rules
2. STIR/SHAKEN
3. Proprietary Dynamic Database

Call Actions

For each filtering layer, you can define an action:



Custom Rules

Custom Rules allows you to explicitly define how calls should be handled based on calling and called numbers. These rules take precedence over other filtering layers when enabled.

Rules Matching Logic

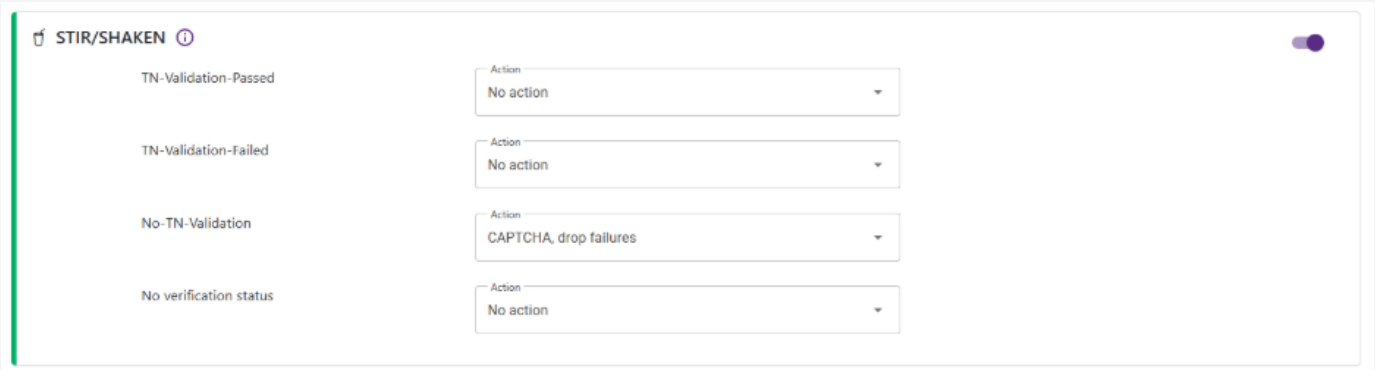
Custom Rules compare:

- Calling Number
- Calling Number

If a match is found, the associated action is applied. If no match is found, analysis continues to the next filtering layer.

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.



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:

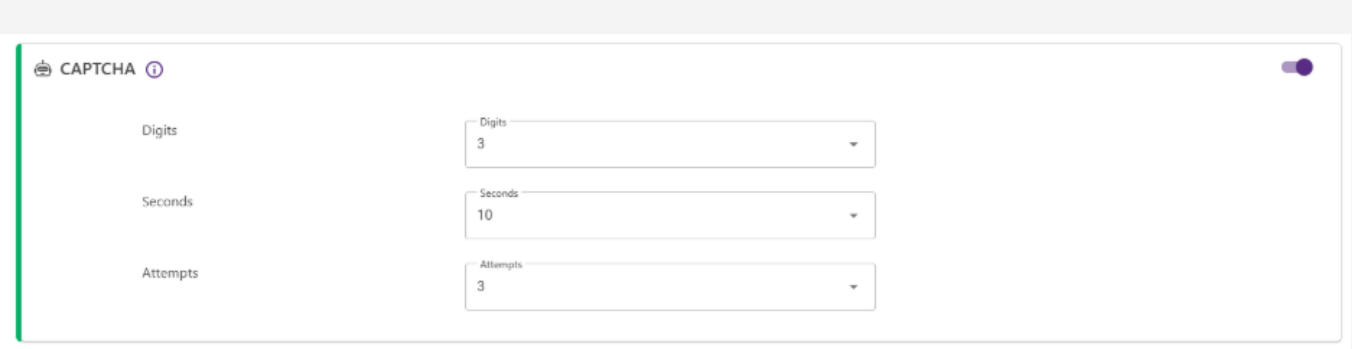
- Incoming calls are checked against multiple databases
- A configurable action of applied if the number is flagged

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. The Voice CAPTCHA answers the call and challenges the caller to enter a series of random digits.



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.

Call Activity

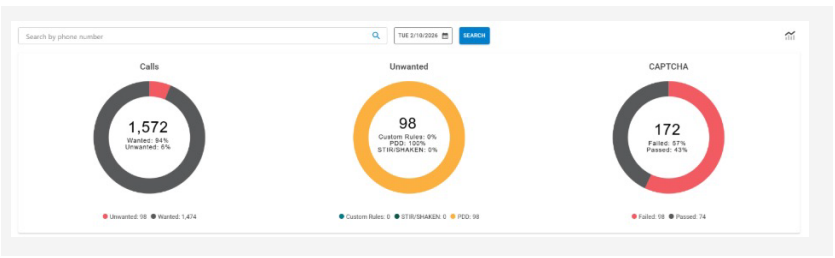
Provides visibility to all inbound traffic and filtering decisions.

From the top of the page, you can:

- Filter results by phone number or date range (the page loads with today's calls)
- Show/hide the donut charts

Dashboard Visualizations

The top section displays three donut charts:



Calls

Total calls, with a breakdown of Wanted and Unwanted calls analyzed by VTF

Unwanted Calls

Breakdown of Unwanted calls by filtering layer:

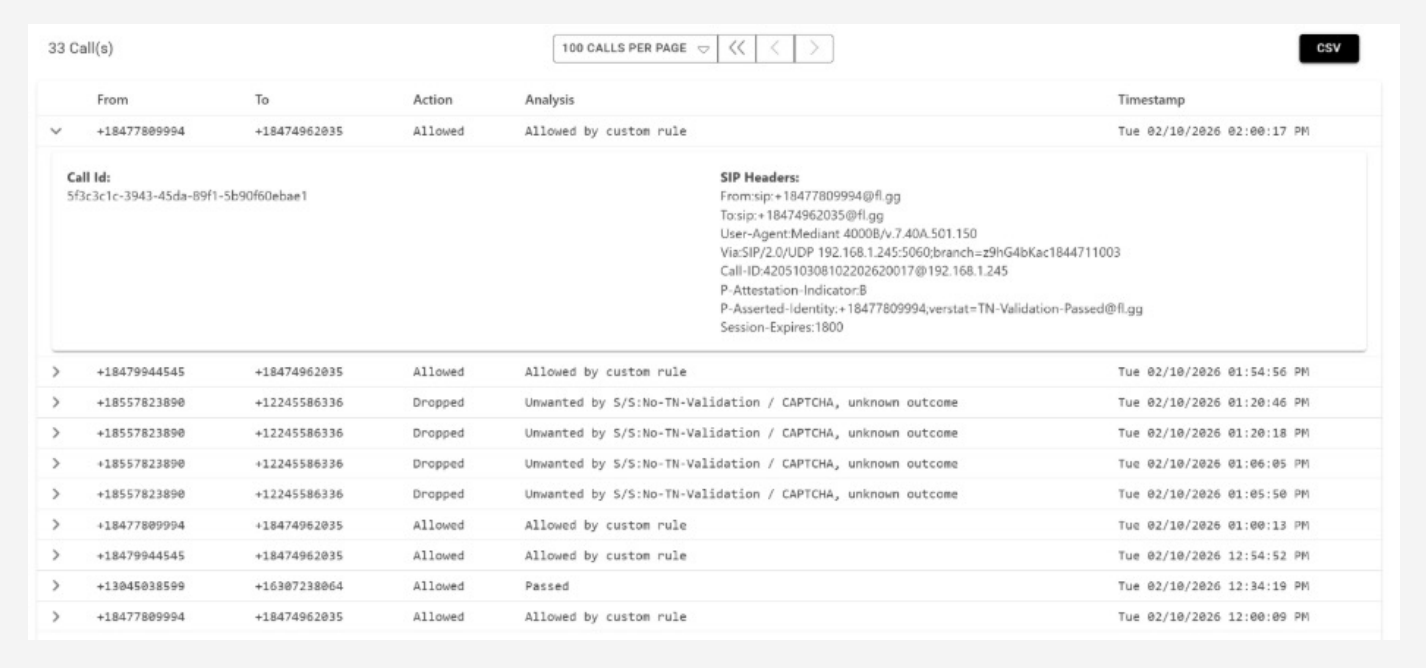
1. Custom Rules
2. STIR/SHAKEN
3. Proprietary Dynamic Database

CAPTCHA

The number of calls that passed or failed the Voice CAPTCHA

Call Details

The lower section displays detailed call records, sorted by most recent. Shows the Action taken and analysis performed. Expand the row to view full call details



TIP

Review call details regularly during onboarding to validate that filtering rules are behaving as expected before enabling more aggressive actions. Look for spikes in your traffic. Identify repeat offenders or patterns. This early oversight helps you to fine tune policies confidently and defensibly.

Mutare Support

For platform issues, contact support@calltower.com. Include tenant name, ID, timeframe, and examples.