

**WMC** | GLOBAL

**WMC** | GLOBAL

WORLDWIDE BRAND AND CUSTOMER PROTECTION AT SCALE



# MOBILE FEEDBACK LOOP API DOCUMENTATION

V2.0 08.07.2024

# TABLE OF CONTENTS

<a href="#">GETTING STARTED WITH MOBILE FEEDBACK LOOP</a>	<a href="#">2</a>
<a href="#">MOBILE FEEDBACK LOOP TICKET SUBMISSION WORKFLOW</a>	<a href="#">4</a>
<a href="#">MOBILE FEEDBACK LOOP SUBMISSION TEMPLATE</a>	<a href="#">9</a>
<a href="#">MOBILE FEEDBACK LOOP API CURL COMMAND EXAMPLES</a>	<a href="#">11</a>

# GETTING STARTED WITH MOBILE FEEDBACK LOOP

Mobile Feedback Loop (MFL) synchronizes abuse desk reporting with WMC Global specialists trained to investigate potential smishing, vishing, and malicious robocalls that implicate a phone number. WMC Global investigates fraudulent phone numbers through its relationships with Network Operators, Number Registries, and Regulators, actioning phone numbers where malicious activity is evident.



**BASE URL:** <https://wmcglobalsupport.zendesk.com/api/v2>

WMC Global provides MFL as part of its anti-phishing services. MFL employs the Zendesk v2 API to automatically create tickets via integration within customer service platforms to coordinate investigations with threat analysts.

..



## DOCUMENT STATUS

This document supports the implementation of the Zendesk v2.0 API for Mobile Feedback Loop. The API and documentation are subject to change.

REFERENCE	URL
Zendesk v2 API documentation	<a href="https://developer.zendesk.com/rest_api/docs/support/introduction">https://developer.zendesk.com/rest_api/docs/support/introduction</a>
API key method for authentication	<a href="https://developer.zendesk.com/api-reference/introduction/security-and-auth/#api-token">https://developer.zendesk.com/api-reference/introduction/security-and-auth/#api-token</a>
Request Ticketing API	<a href="https://developer.zendesk.com/rest_api/docs/support/requests">https://developer.zendesk.com/rest_api/docs/support/requests</a>

# MOBILE FEEDBACK LOOP TICKET SUBMISSION WORKFLOW

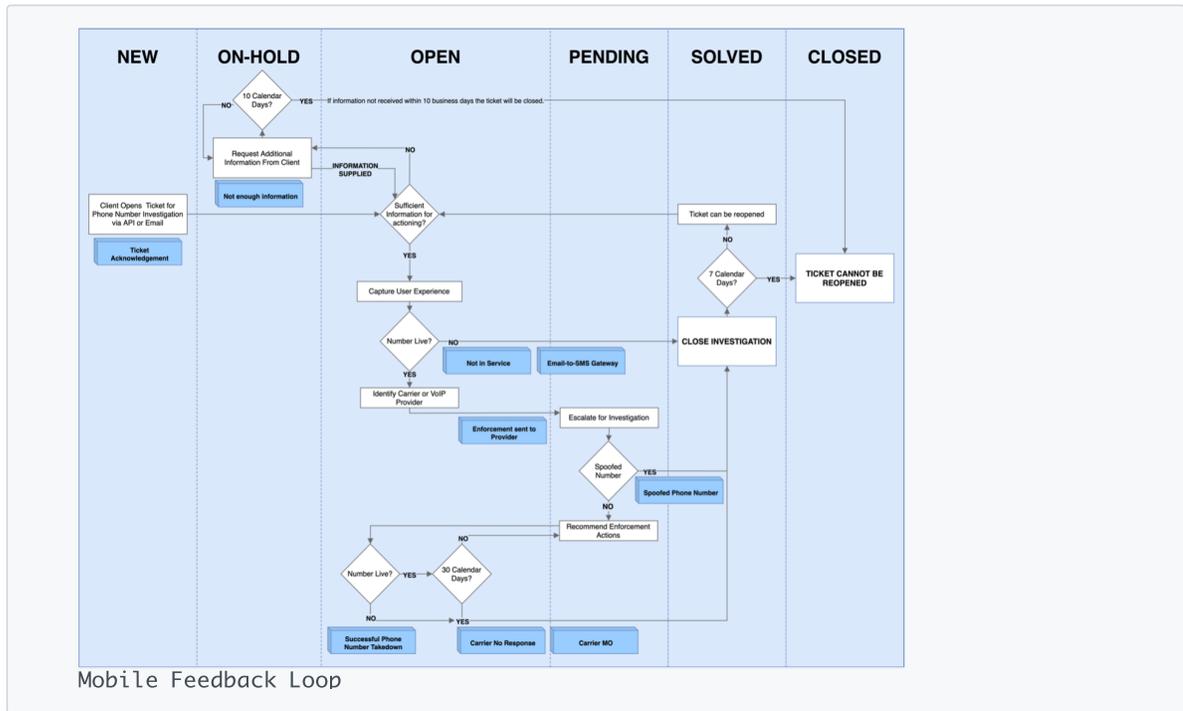
---

## 1. CREDENTIALS

Supply a **corporate email address** for your organization. WMC Global will provide an API Token to access [wmcglobalsupport.zendesk.com](https://wmcglobalsupport.zendesk.com) for your organization's tickets.

## 2. TICKET STATUSES AND RESOLUTIONS

STATUS	DESCRIPTION
<b>NEW</b>	The ticket has yet to be actioned by WMC Global.
<b>OPEN</b>	The ticket is either in the initial investigation stage -or- has already been enforced by the phone number provider and the response is awaiting WMC Global's review.
<b>PENDING</b>	The ticket has been enforced. WMC Global is awaiting further action from the phone number provider.
<b>ON-HOLD</b>	The ticket has insufficient information to continue the investigation. WMC Global will request additional information. When an <b>ON-HOLD</b> ticket receives the requested information, the status moves to <b>OPEN</b> to restart the investigation. If the information is not supplied by the customer within 10 business days, the ticket is automatically closed.
<b>SOLVED</b>	WMC Global has concluded its investigation and has relayed its findings and any associated enforcement actions. The ticket may be re-opened while in this stage.
<b>CLOSED</b>	WMC Global has concluded its investigation and has relayed its findings and any associated takedown actions. The ticket cannot be re-opened. Replies to the ticket will open a new ticket.



Mobile Feedback Loop Workflow

COMMUNICATION	DESCRIPTION
<b>DOWN AT INTERCEPT</b>	The phone number was not live at the time it was called, and no further action can be taken.
<b>SPOOFED PHONE NUMBER</b>	The phone number was confirmed to be spoofed and no further action can be taken.
<b>EMAIL-TO-SMS GATEWAY</b>	The phone number submitted for investigation is a carrier email-to-SMS gateway number and no further action can be taken.
<b>TIER-1 CARRIER</b>	The phone number provided is a mobile-originating, Tier-1 carrier-owned phone number. As such, the phone number is ineligible for takedown but may be eligible for blocking in carrier systems. Recommended blocking and filtering actions have been provided to the carriers.
<b>CARRIER NO RESPONSE</b>	Multiple enforcement attempts over a 5-day period were made, but no response was received from the phone number provider.

<b>SUCCESSFUL PHONE NUMBER TAKEDOWN</b>	The phone number is disconnected, suspended, or otherwise taken offline.
<b>OUT OF SCOPE</b>	The phone number provided is not enforceable under the MFL contract. If you have questions about contract scope, please reach out to your Customer Success Manager.
<b>TICKET ACKNOWLEDGEMENT</b>	An email confirmation that the request has been received with the ticket information.
<b>NOT ENOUGH INFORMATION</b>	In order to process the request more information is required. The status will remain in ON-HOLD until additional information has been supplied.
<b>ENFORCEMENT SENT TO PROVIDER</b>	Initial enforcement has been sent to the associated phone number provider
<b>FALSE POSITIVE</b>	This phone number is a legitimate business line and/or performing legitimate business actions.

### 3. RAISING AND UPDATING AN INCIDENT TICKET

Follow the instructions below. The API will return the Ticket ID. This value is referred to as **id** in the ZenDesk API Documentation.

#### 3.1 Incident Ticket Content

After logging in with the API Token provided, a new Incident Ticket can be created using **Create Request** as documented in the [Zendesk Requests API](#).

The `subject` field should be completed with the name of your organization and the nature of the request. You may include your own reference number, if desired, at the beginning of the subject line.



#### EXAMPLE

[Optional Reference Number] [Company Name] Phishing on [Phone Number]

The **Create Request** should be completed as follows:

FIELD	DESCRIPTION
<b>REPORTED PHONE NUMBER</b>	Phone Number to be investigated. Must be only one per Incident Ticket.
<b>FULL MESSAGE TEXT (For Smishing)</b>	Provide if available for SMS-delivered phishing
<b>USER EXPERIENCE</b>	Mandatory for all investigations, as this tells us the type of abuse experienced and guides enforcement actions.
<b>DATE ATTACK OCCURRED</b>	Provide if available.
<b>REQUESTER</b>	Enter the email address for which the AP key was issued. (see section 1.1 above)

## 3.2 Updating an Incident Ticket

To provide more information on an Incident, use the **Update Request** feature of the API. The **Update Request** functionality adds a comment with your additional information to the ticket. It will not change the original submission.

## 3.3 Creating a New Incident Ticket that refers to a Closed Incident

Once a ticket is closed, it cannot be reopened. New requests can reference the closed ticket for additional follow-up. Reference 3.1 Incident Ticket Content (above) and include the `via_followup_source_id` parameter to specify the closed ticket.

# 4. RETRIEVING INCIDENT TICKET INFORMATION

## 4.1 Retrieve a Specific Incident Ticket

If you know the Incident Ticket ID provided when it was created (see 3.1 above), it can be retrieved using the search string value `query=99999999`.

## 4.2 Retrieve Multiple Incident Tickets

Retrieve multiple Incident Tickets using the Search API by forming search strings that are conditional on specific fields, such as `Status`, or search for a particular term, such as `telephone number` or `name`. You will need to specify the query type as a ticket.



### EXAMPLE

To find tickets created on a specific day, you would search  
`query=created:2020-07-07 type:ticket`

## 4.3 More Information Needed

To ensure you respond to incidents where a ticket is On-Hold status, regularly use the Search API with the search `query=type:ticket status:on-hold` to identify which Incident Tickets require additional information.

## 5. API TESTING

When submitting testing tickets via the API that you don't want investigated, please note "TEST" in the subject line. They will be deleted to prevent impacting monthly reporting.

# MOBILE FEEDBACK LOOP SUBMISSION TEMPLATE

---

## WHAT IS REQUIRED FOR ENFORCEMENT?

1. There must be evidence provided that the submitted phone number has been engaging in malicious activities that are infringing on the client's brand
2. There must be a valid ten-digit US phone number
3. There must only be one phone number per investigation
4. The submitted number must not be a safe-listed number, such as a valid business line, etc.

## SUBJECT LINE TEMPLATE:

[Company Name] Investigation: [phone Number]

## EMAIL BODY TEMPLATE:

Reported Phone Number:  
Date Attack Occurred:  
User Experience:  
Full Message Text (for Smishing):  
Customer Phone Carrier or Phone Number (if available):  
Attach a screenshot of all text message interactions that occur (if available)

### SUBJECT EXAMPLE

My Company Inc. Investigation: 000-000-0000

### BODY EXAMPLE

**Reported Phone Number:** 000-000-0000

**Date Attack Occurred:** 2/2/2022

**User Experience:** The customer received a text message claiming to be from My Company Inc. It offered them a prize to fill out a form with their account username and password. Once complete they received a text asking them to send the message to their friends.

**Full Message Text (for Smishing):** This is My c0mpany Inc. Fill out your information to win a prize!  
hxxps://pr.iz.esInc.tk

**Customer Phone Carrier or Phone Number (if available):** Customer's number is 111-111-1111

# MOBILE FEEDBACK LOOP API CURL COMMAND EXAMPLES

## CURL TO UPLOAD A FILE

cURL

```
https://wmcglobalsupport1654275478.zendesk.com/api/v2/uploads?filename=test_file_1.txt --
data-binary @test_file_1.txt -H "Content-Type: application/binary" -v -u
software.qa@wmcglobal.com/token:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX0 -X POST
```

In the above request you need to do the following:

- Edit the **file name**, e.g., filename=Zendesk\_test\_file.txt
- Edit the **file path**, e.g., filename=test=file.txt
- Edit to include your **email address** and **API key**, e.g., [test@wmcglobal.com](mailto:test@wmcglobal.com)/token:XXX0

The above request will return an upload token, e.g.,

"token": "IGbFePbgGHaULCm3Tq4z0eXxx", this token can be included as part of the request when creating or updating a ticket.

## CURL TO CREATE A TICKET

cURL

```
https://wmcglobalsupport1654275478.zendesk.com/api/v2/requests.json -d '{"request":
{"subject": " [Optional Reference Number, e.g., 123] [Company Name, e.g., XYZ Inc.]
Phishing on [Phone Number/URL, e.g., 123-456-7890]", "comment": {"html_body": "<p>Reported
Phone Number: [e.g., 123-456-7890]</p>
<p>Date Attack Occurred: [e.g. YYYY-MM-DD]</p><p>User Experience: [e.g., This is a
description of the user experience]</p><p>Full Message Text (for Smishing): [e.g., This is
the full text message]</p>
<p>Customer Phone Carrier and Number (if available): [e.g., AT&T 123-456-
7890]</p>}}}' -v -u
software.qa@wmcglobal.com/token:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX0 -X POST -H
"Content-Type: application/json"
```

In the above request, you need to do the following:

- Edit the subject, e.g., "subject": "Ref#123 XYZ Inc. Phishing on 123-456-7890"
- Edit the **body**, replacing the brackets and example text with the actual data, e.g.,

cURL

```
"html_body": "<p>Reported Phone Number: 123-456-7890</p><p>Date Attack Occurred: 2022-06-05</p><p>User Experience: This is a description of the user experience</p><p>Full Message Text (for Smishing): This is the full text message</p><p>Customer Phone Carrier and Number (if available): AT&T 123-456-7890<p>"
```

- Edit to include your **email address** and **API key**, e.g.,  
test@wmcglobal.com/token:XXXXXXXXXXxXXXXXXxxx0XXXXXXXXXxxXXxxXXxX0

## CREATE TICKET WITH A FILE ATTACHMENT

cURL

```
curl https://wmcglobalsupport1654275478.zendesk.com/api/v2/requests.json -d '{"request": {"subject": " [Optional Reference Number, e.g., 123] [Company Name, e.g., XYZ Inc.] Phishing on [Phone Number/URL, e.g., 123-456-7890]", "comment": {"html_body": "<p>Reported Phone Number: [e.g., 123-456-7890]</p><p>Date Attack Occurred: [e.g. YYYY-MM-DD]</p><p>User Experience: [e.g., This is a description of the user experience]</p><p>Full Message Text (for Smishing): [e.g., This is the full text message]</p><p>Customer Phone Carrier and Number (if available): [e.g., AT&T 123-456-7890]</p>", "uploads": [{"lbP6iuJHf0kr1jvI9Fw0x7KUJ"}]}}' -v -u software.qa@wmcglobal.com/token:XXXXXXXXXXxXXXXXXxxx0XXXXXXXXXxxXXxxXXxX0 -X POST -H "Content-Type: application/json"
```



### ATTACHING EVIDENCE TO FILES

To include a file in a ticket, you will first need to upload the file using the `/uploads` API endpoint and then “attach” the file to the ticket request.

In the above request, you need to do the following:

- Edit the **subject**, e.g., "subject": "Ref#123 XYZ Inc. Phishing on 123-456-7890"
- Edit the **body**, replacing the brackets and example text with the actual data, e.g.,

cURL

```
"html_body": "<p>Reported Phone Number: 123-456-7890</p><p>Date Attack Occurred: 2022-06-05</p><p>User Experience: This is a description of the user experience</p><p>Full Message Text (for Smishing): This is the full text message</p><p>Customer Phone Carrier and Number (if available): AT&T 123-456-7890<p>"
```

- Edit the **upload token**, e.g., "uploads": ["1bP6iuJHf0kr1jvI9Fw0x7xxx"]
- In this instance, the brackets are part of the request structure and should remain. Only the alphanumeric value in the quotes should be replaced.
- Edit to include your **email address** and **API key**, e.g.,  
test@wmcglobal.com/token:XXXXXXXXXXxXXXXXxxxx0XXXXXXXXXxxXXXXXXxXxX0
- The above created request will return a request id, e.g., "id": "29". This id can be used to add additional comments to a ticket via the update request; see below.

## UPDATE TICKET WITH A FILE

cURL

```
curl https://wmcglobalsupport1654275478.zendesk.com/api/v2/requests/30.json -d '{"request": {"comment": {"html_body": "<p>Adding a file to this ticket.</p><p>Please see attached.<p>"}, "uploads": ["6Xojm9eXtrDBGRC9beGR6i0db"]}}' -v -u software.qa@wmcglobal.com/token:XXXXXXXXXXxXXXXXxxxx0XXXXXXXXXxxXXXXXXxXxX0 -X PUT -H "Content-Type: application/json"
```

In the above request, you need to do the following:

- Edit the **ticket id**, e.g., /29.json
- Edit the **body**, e.g., "html\_body": "<p>Adding a file to this ticket.</p><p>Please see attached.<p>"

- Edit the **upload token**, e.g., "uploads": ["1bP6iuJHf0kr1jvI9Fw0x7XXX"]
- In this instance, the brackets are part of the request structure and should remain. Only the alphanumeric value in the quotes should be replaced.
- Edit to include your **email address** and **API key**, e.g.,  
test@wmcglobal.com/token:XXXXXXXXXXxXXXXxXXXXxXXXX0XXXXXXXXXxxXXXXXX  
xxX0