

# MANUALE PIRACY SHIELD

## VERSIONE PER SEGNALATORI





## Sommario

1. Introduzione.....	4
2. Processo di accreditamento.....	5
3. Accesso alla VPN .....	6
Collegamento VPN site-to-site per l’accesso all’infrastruttura della piattaforma Piracy Shield ospitata in Microsoft Azure Cloud .....	6
Configurazione del dispositivo VPN on-premises .....	7
Creazione e verifica della connessione VPN site-to-site su Azure .....	8
4. Raggiungimento piattaforma.....	9
5. Sicurezza.....	10
Sistema di autenticazione .....	10
Processo di Autenticazione .....	10
Primo accesso .....	10
Access Token .....	10
Refresh Token.....	11
Limitazioni .....	12
Rate limit.....	11
Whitelist.....	15
6. Generale.....	17
Cosa è un Ticket? .....	17
Cosa è un Ticket Item? .....	18
7. Ciclo di vita del ticket .....	20
8. Utilizzo.....	23
9. SLA.....	24
10. Manuale operativo - Interfaccia .....	25
Autenticazione .....	25
Login.....	25
Logout .....	26
Ticket.....	27
Creazione di un nuovo ticket .....	27
Visualizza la lista dei DDA.....	29
Visualizzare tutti i ticket della propria utenza.....	29
Visualizzare un singolo ticket.....	31



Rimozione del singolo ticket entro 75 secondi .....	33
Creazione di un ticket errore .....	36
Caricamento della prova .....	37
Visualizzare tutti i dati presenti nella whitelist della propria utenza.....	40
Rimuovere dati dalla whitelist .....	41
11. API.....	42
Autenticazione .....	42
Login.....	42
Refresh .....	44
Logout .....	45
Ticket.....	46
Creazione di un nuovo ticket .....	46
Preleva la lista DDA .....	48
Preleva un singolo DDA.....	49
Preleva un singolo ticket.....	50
Preleva tutti i ticket presenti nella propria utenza .....	52
Rimozione del singolo ticket entro 75 secondi .....	54
Creazione del ticket errore .....	55
Caricare la prova di un ticket .....	57
Visualizzare dati del pacchetto prova caricato per un ticket .....	60
Ping .....	60
Whitelist.....	53
Inserire un dato in whitelist.....	53
Visualizzare tutti i dati presenti nella whitelist .....	54
Rimuovere dati dalla whitelist .....	55



# 1. Introduzione

Benvenuto

---



Il presente manuale fornisce informazioni dettagliate su come interagire con l'interfaccia web e con i punti di accesso delle API per utilizzare le funzionalità della piattaforma PIRACY SHIELD.

Si prega di notare che questa documentazione è da considerarsi confidenziale e sarà soggetta ad ulteriori aggiornamenti.

## 2. Processo di accreditamento

### Procedura di accreditamento per i Segnalatori

---

L'accesso alla piattaforma Piracy Shield, per le attività di live blocking, necessita di una procedura di registrazione e di accreditamento da parte dei Segnalatori.

Di seguito, le istruzioni per l'accREDITAMENTO:

1. Accedere al [portale di accreditamento](#) e cliccare sul link "Entra con SPID".
2. Selezionare il proprio provider SPID e inserire le proprie credenziali.
3. Cliccare sul link "Accreditamento per ISP per piattaforma Privacy Shield".
4. Compilare il modulo con le informazioni richieste.
5. Inviare il modulo e attendere la conferma dell'accREDITAMENTO via PEC.
6. Al termine della procedura, una volta accREDITATI, accedendo nuovamente al Portale dei servizi AGCOM, si potrà scaricare, cliccando sull'apposito link, il documento con le informazioni necessarie per predisporre l'accesso alla piattaforma Piracy Shield.



## **3. Accesso alla VPN**

---

Per raggiungere la piattaforma Piracy Shield, per ogni Segnalatore sarà predisposto un collegamento VPN site-to-site tra l'infrastruttura Microsoft Azure Cloud, che ospita la piattaforma di live blocking, e l'infrastruttura del Segnalatore dalla quale avranno origine le interrogazioni.

Collegamento VPN site-to-site per l'accesso all'infrastruttura della piattaforma Piracy Shield ospitata in Microsoft Azure Cloud

---

---

Istruzioni per la configurazione del dispositivo on-premises. Configurare il dispositivo VPN on-premises per stabilire una connessione VPN site-to-site con Microsoft Azure, seguendo questi passaggi:

## Configurazione del dispositivo VPN on-premises

Le connessioni site-to-site richiedono un dispositivo VPN compatibile con Azure configurato correttamente. Per configurare il dispositivo VPN, è necessario utilizzare gli stessi valori della chiave condivisa, dell'indirizzo IP pubblico e dello spazio degli indirizzi IP che si sono usati per creare il gateway di rete locale su Azure.

Per facilitare la configurazione del dispositivo VPN on-premises, Agcom invierà, ad ogni Segnalatore, cifrato, un modulo con la richiesta delle seguenti Informazioni:

- Nome del dispositivo VPN
- Modello del dispositivo VPN
- Indirizzo IP pubblico del dispositivo VPN
- Spazio degli indirizzi IP della rete on-premises
- Chiave condivisa per la connessione VPN
- Indirizzo IP del gateway VPN su Azure
- Spazio degli indirizzi IP della rete virtuale su Azure

Per informazioni sui dispositivi VPN compatibili e sulla loro configurazione, è possibile consultare la seguente guida: [About VPN devices for connections - Azure VPN Gateway](#).

## Creazione e verifica della connessione VPN site-to-site su Azure

Una volta ricevuto il suddetto modulo, l'ISP dovrà configurare il proprio dispositivo VPN on-premises e restituire ad Agcom il modulo compilato con i parametri utilizzati per la configurazione.

Alla ricezione del modulo compilato, Agcom configurerà l'endpoint VPN nell'infrastruttura di Piracy Shield e predisporrà i test di collaudo del collegamento da effettuarsi in collaborazione con l'ISP.

Completato il test di collaudo, avendo verificato che la connessione sia attiva e funzionante e che consenta l'accesso alle interfacce di Piracy Shield, l'attività di configurazione VPN si considererà completata.

Per approfondimenti si rimanda alla seguente guida: [Create a site-to-site VPN connection in the Azure Portal](#).



## 4. Raggiungimento piattaforma

---

A seguito dell'accesso alla VPN la piattaforma sarà raggiungibile tramite la seguente modalità:

- interfaccia web agli indirizzi:
  - Ambiente di test <https://psp01-dev.agcom.it>
  - Ambiente di produzione <https://psp01.agcom.it>
  
- Accesso diretto delle API attraverso gli indirizzi:
  - Ambiente di test <https://psp01-dev.agcom.it/api>
  - Ambiente di produzione <https://psp01.agcom.it/api>

## 5. Sicurezza

### Sistema di autenticazione

#### Processo di Autenticazione

---

Il sistema di autenticazione implementato prevede l'utilizzo di token JWT (JSON Web Tokens) per garantire un accesso maggiormente sicuro ed affidabile.

Le due tipologie utilizzate sono: access token e refresh token. Questi due tipi di token distinti svolgono ruoli complementari all'interno del processo di autenticazione e autorizzazione degli utenti.

#### Primo accesso

Il processo di autenticazione inizia quando un utente effettua il primo accesso alla piattaforma. Per iniziare, l'utente fornisce le proprie credenziali di accesso, ovvero l'username e la password, attraverso un modulo di login. Successivamente queste informazioni vengono verificate e, se valide, consentiranno di ricevere un access token e un refresh token.

#### Access Token

---

---

Questo token viene utilizzato per autenticare l'utente durante la sua sessione attiva e garantire che abbia l'autorizzazione necessaria per accedere alle risorse o eseguire azioni specifiche. La durata dell'access token è generalmente breve, per migliorare la sicurezza del sistema.

L'access token deve essere incluso in ogni richiesta API che richiede autenticazione e autorizzazione. Questo avviene utilizzando il meccanismo comunemente noto come "Bearer Token" (RFC 6750). Quando un utente autenticato desidera accedere a una risorsa protetta o eseguire un'azione, l'access token viene inserito nell'intestazione dell'autorizzazione della richiesta HTTP. Il formato dell'intestazione sarà simile a questo:

Authorization: Bearer <ACCESS\_TOKEN>

La durata massima di validità di un access token è di 1 ora.

## Refresh Token

---

Questo token è necessario per la generazione periodica di un access token qualora quest'ultimo fosse scaduto. A differenza degli access token, i refresh token hanno una durata estesa, consentendo agli utenti di rimanere autenticati senza dover effettuare nuovamente l'accesso frequentemente.

Il processo di rinnovo di un access token inizia quando un access token scade. In tal caso, tramite API, sarà possibile inviare una richiesta per ottenere un nuovo access token utilizzando il refresh token associato.



Qualora anche il refresh token fosse scaduto, l'utente dovrà effettuare nuovamente l'accesso fornendo le sue credenziali.

La durata massima di validità di un refresh token è di 7 giorni.

## Limitazioni

### **Rate limit**

Per garantire un utilizzo equo e mantenere prestazioni ottimali della piattaforma abbiamo implementato dei limiti di frequenza (Rate Limit). I limiti di frequenza definiscono il numero massimo di richieste che possono essere effettuate alla piattaforma entro un determinato intervallo di tempo.

Questi limiti sono progettati per prevenire abusi, proteggere le risorse di sistema e garantire un'esperienza coerente per tutti gli utenti.

Dettagli sulle limitazioni di frequenza:

- Il limite di frequenza si applica globalmente a tutti gli endpoint dell'API nel sistema.
- I limiti di frequenza dovranno essere impostati e coordinati in base al numero di utenti che utilizzeranno la piattaforma.

Quando si supera il limite di frequenza (Rate Limit), si riceverà una risposta con il codice di stato HTTP 429 e un messaggio di errore che indica il superamento del numero consentito di richieste.

Il limite attuale è di: 1000 richieste in 1 secondo.

Per evitare di superare il limite di frequenza, si consiglia di implementare adeguati meccanismi di throttling o batching delle richieste nella propria applicazione.

È importante notare che i limiti di frequenza possono essere soggetti a modifiche e potrebbero variare in futuro.

## **Interruzione temporanea del servizio per abuso**

Come dettagliato nel capitolo precedente, al fine di garantire un utilizzo corretto ed efficiente della piattaforma, sono state implementate delle modalità di sicurezza su determinati endpoint, che prevedono un ban temporaneo del proprio indirizzo IP.

Di seguito i moduli correntemente attivi:

- Modulo anti brute-force: prevede il ban temporaneo per continue richieste di login, al superamento dei parametri indicati di seguito:
  - o Richieste massime: 50 nell'arco di 1 minuto di tempo
  - o Durata ban: 15 secondi

Questi parametri potranno essere soggetti a cambiamenti durante il tempo.

## Whitelist

La whitelist potrà essere popolata con:

FQDN

IPv4

IPv6

CIDR IPv4

CIDR IPv6

Per ogni FQDN dovrà essere associato il Registrar di riferimento.

Per ogni indirizzo IP o blocco CIDR dovrà essere associato un Autonomous System Number (ASN) di riferimento.

Tutti gli elementi inseriti saranno considerati esclusivamente per i ticket successivi.  
La whitelist non avrà un'efficacia retroattiva.

## Segnalazione e risoluzione problematiche

---

Per ricevere assistenza e /o segnalare eventuali problematiche di natura tecnica o gestionale e/o malfunzionamenti della piattaforma sarà possibile utilizzare gli strumenti tecnici messi a disposizione e forniti a seguito della fase di accreditamento.



## 6. Generale

### Cosa è un Ticket?

---

Un ticket rappresenta una raccolta di dati che racchiude varie informazioni relative a un compito o una richiesta specifica. Serve come entità centralizzata per tenere traccia e gestire il progresso degli elementi ad esso associati. Ogni ticket contiene dettagli essenziali, tra cui elenchi di Fully Qualified Domain Names (FQDN) e/o indirizzi IPv4 e/o indirizzi Ipv6, insieme ad ulteriori dati pertinenti.

## Cosa è un Ticket Item?

---

Il ticket item rappresenta una voce individuale all'interno di un ticket, facendo riferimento specificamente a un Fully Qualified Domain Name (FQDN) o a un indirizzo IPv4 e/o indirizzi Ipv6. Serve come nota utilizzata in modo coerente all'interno della documentazione dell'API per identificare e fare riferimento a questi specifici elementi di dati all'interno di un ticket.

I ticket item sono fondamentali per il monitoraggio e la gestione dettagliata dei Fully Qualified Domain Names (FQDN), degli indirizzi IPv4, degli indirizzi Ipv6 associati a un determinato compito o richiesta. Forniscono un modo per affrontare e gestire singolarmente ciascun elemento, consentendo un'elaborazione e una risoluzione mirate.

Attributi di un ticket item:

- **FQDN:** un Fully Qualified Domain Name (FQDN) si riferisce a un nome di dominio completo che specifica la sua posizione esatta all'interno del sistema di nomi di dominio gerarchico. Di solito, gli FQDN sono composti da un nome host e un nome di dominio, separati da punti (ad esempio, sottodominio.esempio.com).
- **IPv4:** un indirizzo IPv4 è una rappresentazione numerica assegnata ai dispositivi connessi a una rete, che consente l'identificazione e la comunicazione. Gli indirizzi IPv4 seguono un formato specifico (ad esempio: 1.1.1.1) e sono fondamentali per la connettività e l'instradamento delle reti.
- **Ipv6:** un indirizzo Ipv6 è una rappresentazione numerica assegnata ai dispositivi connessi a una rete, che consente l'identificazione e la comunicazione. Gli indirizzi Ipv6 seguono un formato specifico e sono fondamentali per la connettività e l'instradamento delle reti.

Questi attributi possono includere anche metadati, stati, timestamp o qualsiasi altra informazione rilevante associata al FQDN o all'indirizzo IPv4 o all'indirizzo Ipv6.



## 7. Ciclo di vita del ticket

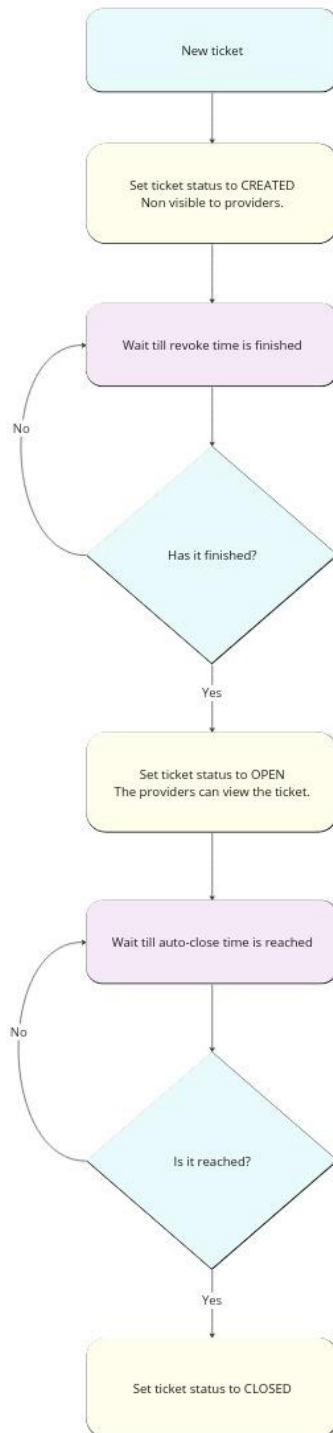
---

Le principali fasi del ciclo di vita del ticket sono:

- Stato "Created": al momento della creazione, un ticket entra in uno stato non visibile ai Provider. Questo periodo ha la durata di 75 secondi e consente al ticket di essere, eventualmente, cancellato in caso di errori o inaccurately. Terminato questo periodo, il ticket passa dallo stato "Created" allo stato "Open" e diventa quindi visibile a tutti i Provider.
- Stato "Open": durante questo stato, i provider possono accedere al ticket. La durata dello stato "Open" di un ticket è di 30 minuti.



- Stato "Closed": scaduto il limite di tempo di 30 minuti, il ticket viene chiuso automaticamente e passa in stato "Closed". Questo cambio di stato non comporta alcuna limitazione nei confronti dell'operabilità di un ticket da parte dei Provider.



## 8. Utilizzo

---

Il segnalatore può creare Ticket in due modalità:

- interfaccia web;
- API.

In fase di creazione del ticket sarà necessario riempire i seguenti campi:

- Identificativo DDA (numero di determina cautelare di riferimento) - si dovrà scegliere da un elenco predefinito la determina di riferimento già presente in piattaforma, per ogni utente saranno visibili esclusivamente le proprie;
- Una descrizione opzionale del ticket;
- Il codice hash della prova;
- L'algoritmo utilizzato per il calcolo del codice hash della prova.
- FQDN (opzionale)
- Indirizzi Ipv4 (opzionale)
- Indirizzi Ipv6 (opzionale)

Almeno uno tra i campi Ipv4/Ipv6/FQDN deve essere compilato con almeno un dato.

Non ci sono limiti di numero Ipv4/Ipv6/FQDN da inserire nel ticket.

Sarà possibile creare un ticket errore per rimuovere un intero ticket o singoli ticket item contenuti in uno specifico ticket entro 24 ore dalla creazione dello specifico ticket.

## 9. SLA

All'invio di un nuovo ticket da parte di un Segnalatore, trascorreranno 75 secondi in cui il ticket non sarà visibile ed operabile da parte dei Provider ed il Segnalatore potrà rimuovere il ticket. Trascorso questo periodo, il ticket passerà ad uno stato aperto e, quindi, visibile a tutti i provider.

Questo stato, chiamato "Open", ha la durata di 30 minuti, durante la quale entrerà in vigore l'obbligo di servizio (SLA). L'obiettivo di questa fase è di completare il blocco entro i 30 minuti dall'apertura del ticket.

Esauriti i 30 minuti (stato "Closed"), sarà comunque sempre possibile da parte dei Provider recuperare e processare il ticket ed i dati di quel ticket ed aggiornare lo stato degli elementi di ogni ticket.

Le performance temporali e di monitoraggio generale vengono costantemente registrate in ogni fase di ogni ticket, per determinare le tempistiche assolute e relative rispetto all'implementazione del blocco.



# 10. Manuale operativo - Interfaccia

## Autenticazione

### Login

click here.' The right panel has a teal-to-orange gradient background and features a white error message box at the top right with a red 'x' icon and a close 'x' icon. The message reads: 'Highly Restricted Area. Access to this area is strictly prohibited without proper authorization. Unauthorized access is punishable by law and will result in severe consequences.' At the bottom of the right panel is the AGCOM logo and the text 'AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI'." data-bbox="113 358 875 762"/>

**Highly Restricted Area**

Access to this area is strictly prohibited without proper authorization. Unauthorized access is punishable by law and will result in severe consequences.

**PIRACY SHIELD**

E-Mail

Password

**LOGIN**

For any access issue, please [click here](#).

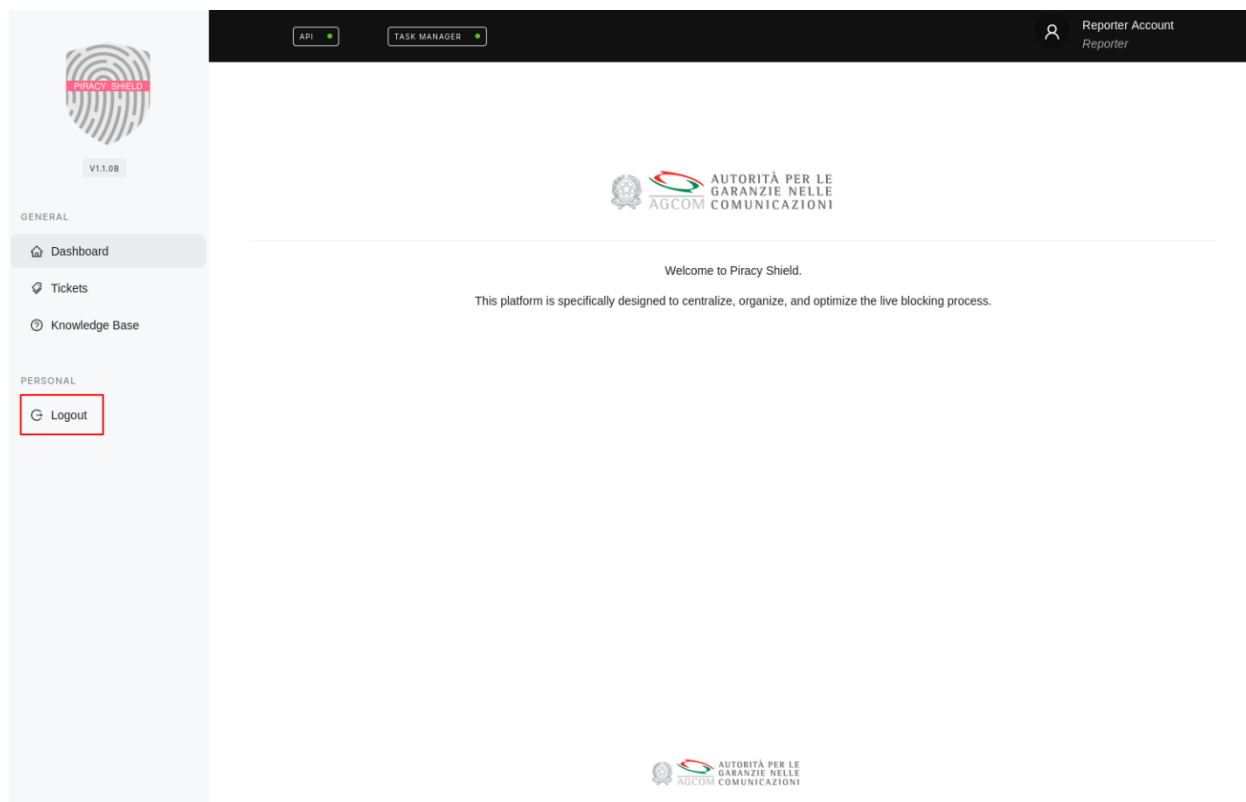
**AGCOM** **AUTORITÀ PER LE  
GARANZIE NELLE  
COMUNICAZIONI**

V1.1.0B

*Interfaccia iniziale di accesso alla piattaforma.*

Procedere con l'accesso attraverso le credenziali fornite.

## Logout



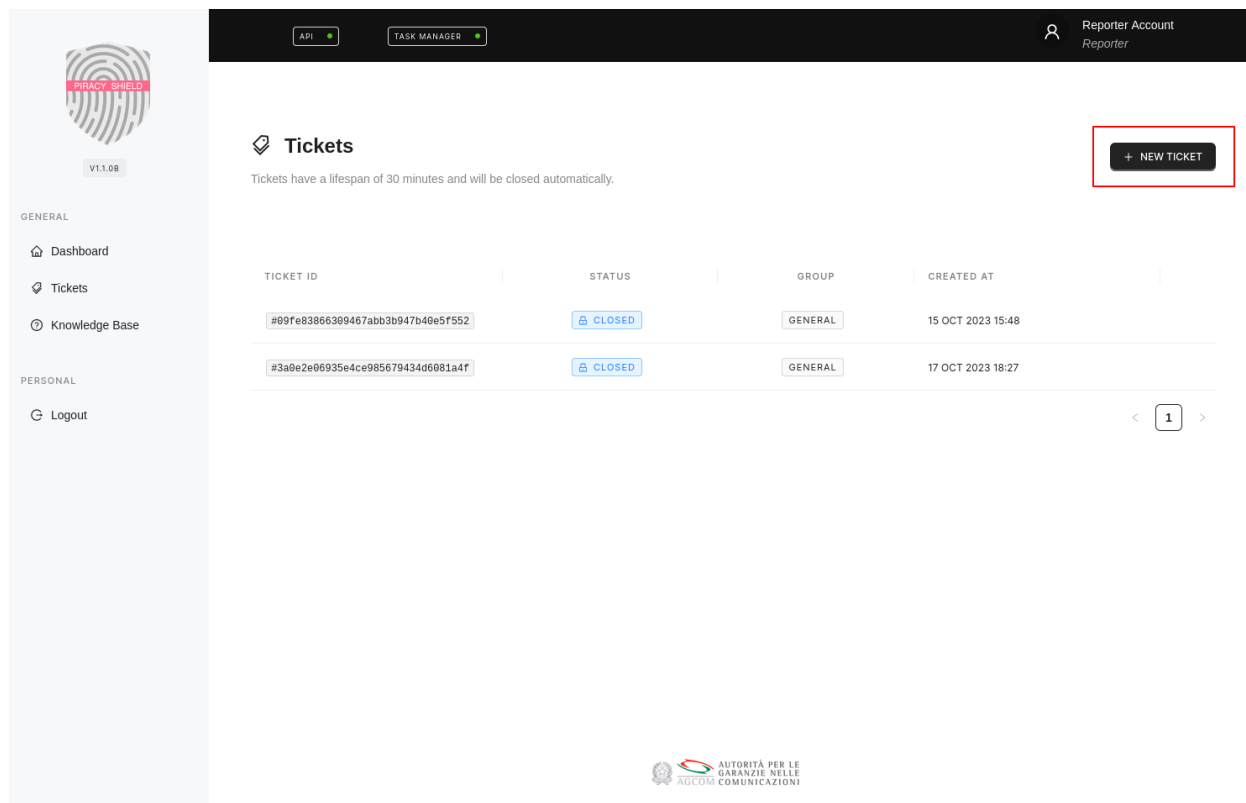
The screenshot displays the Piracy Shield dashboard interface. At the top, there is a navigation bar with 'API' and 'TASK MANAGER' dropdown menus, and a user profile section for 'Reporter Account' with the role 'Reporter'. The main content area features the AGCOM logo and a welcome message: 'Welcome to Piracy Shield. This platform is specifically designed to centralize, organize, and optimize the live blocking process.' On the left side, a sidebar menu is visible, categorized into 'GENERAL' and 'PERSONAL'. The 'PERSONAL' section includes a 'Logout' option, which is highlighted with a red rectangular box.

*Interfaccia iniziale ad accesso effettuato.*

Per effettuare il logout è possibile cliccare sulla voce del menù in basso a sinistra.

# Ticket

## Creazione di un nuovo ticket



API TASK MANAGER Reporter Account Reporter

**Tickets** + NEW TICKET

Tickets have a lifespan of 30 minutes and will be closed automatically.

TICKET ID	STATUS	GROUP	CREATED AT
#09fe83866389467abb3b947b40e5f552	CLOSED	GENERAL	15 OCT 2023 15:48
#3a0e2e06935e4ce985679434d6081a4f	CLOSED	GENERAL	17 OCT 2023 18:27

1

*Interfaccia di gestione dei ticket.*

Per creare un nuovo ticket, cliccare su "New Ticket".



API TASK MANAGER Reporter Account Reporter

PIRACY SHIELD V2.0.08

GENERAL

- Dashboard
- Tickets
- Whitelist
- Knowledge Base

PERSONAL

- Logout

### New Ticket

Create a new ticket to be processed by the registered providers.

**Warning**

Please check your input carefully before submitting. The data you're about to insert is critical and will be transmitted to the relative providers. This operation cannot be undone after the revoke time is expired. After creating the ticket, you will have 75 seconds to remove it if there is any mistake.

**DDA** \*

Associate a DDA to this ticket.

Select a DDA instance

**Description**

A short description, max 255 characters

A very short, non mandatory, description to help identify the ticket goal.

Avoid repetitions and, even if it's not required, refrain to insert descriptions that are already been used.

**Forensic Evidence Hash** \*

The hash of the associated forensic acquisition archive that should have been previously produced.

Select the hash type

Forensic evidence hash string

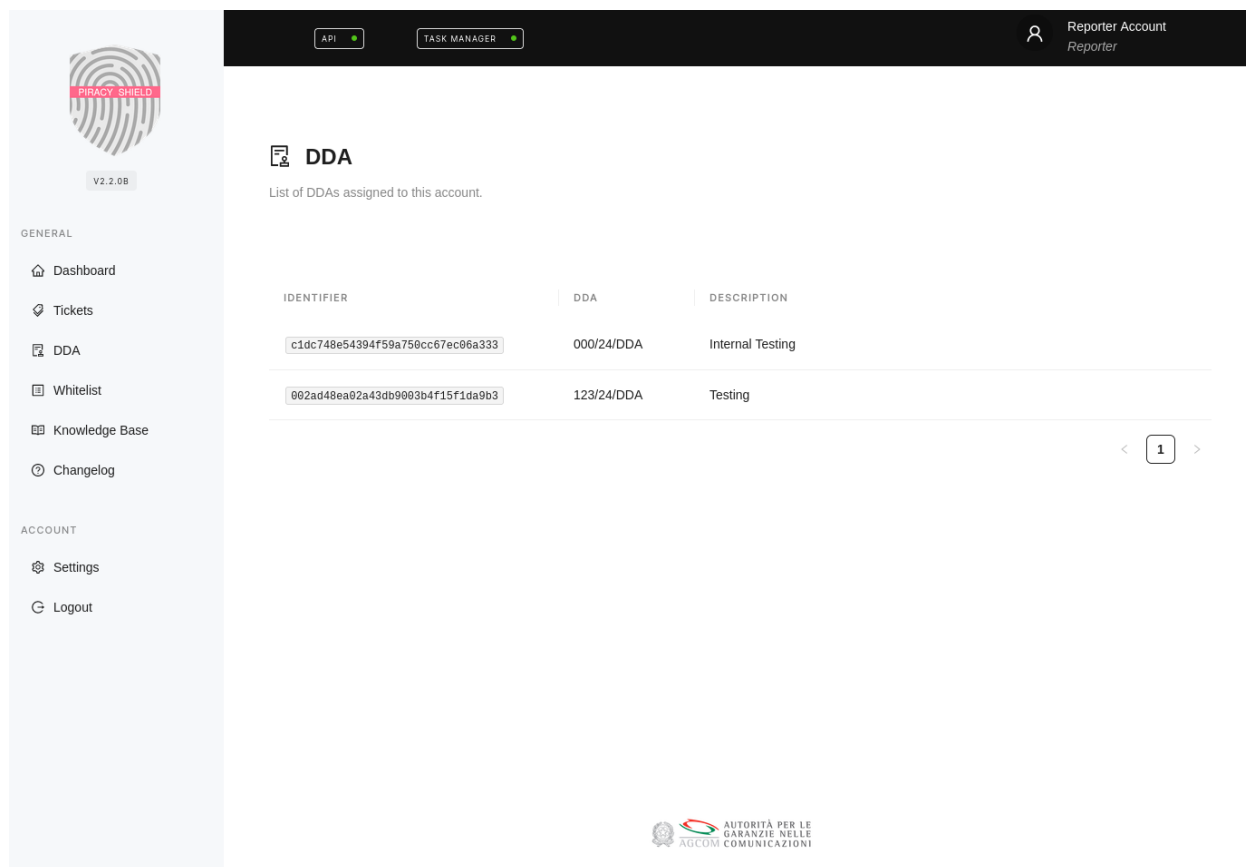
**Fully Qualified Domain Names**

myiptv.com

*Interfaccia di creazione dei ticket.*

In questa interfaccia è possibile compilare ed inviare un nuovo ticket.

## Visualizza la lista dei DDA



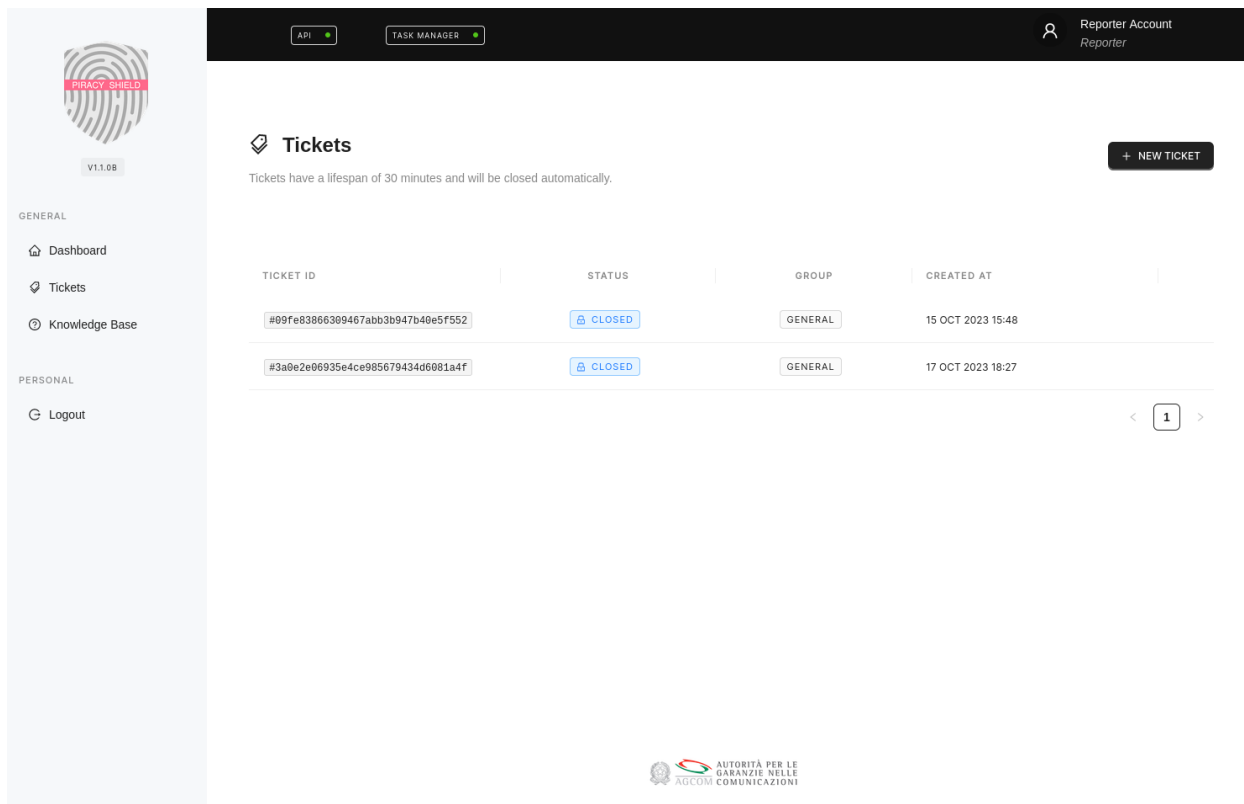
The screenshot shows the PIRACY SHIELD user interface. At the top, there is a navigation bar with 'API' and 'TASK MANAGER' buttons, and a user profile for 'Reporter Account' with the role 'Reporter'. On the left, a sidebar contains a 'PIRACY SHIELD' logo and a version indicator 'v2.2.0B'. Below the logo, the sidebar is divided into 'GENERAL' and 'ACCOUNT' sections. The 'GENERAL' section includes links for Dashboard, Tickets, DDA, Whitelist, Knowledge Base, and Changelog. The 'ACCOUNT' section includes Settings and Logout. The main content area is titled 'DDA' and contains the text 'List of DDAs assigned to this account.' Below this is a table with three columns: IDENTIFIER, DDA, and DESCRIPTION. The table contains two rows of data. At the bottom right of the table, there is a pagination control showing '1' in a box with left and right arrows. The AGCOM logo is visible at the bottom center of the page.

IDENTIFIER	DDA	DESCRIPTION
c1dc748e54394f59a750cc67ec06a333	000/24/DDA	Internal Testing
002ad48ea92a43db9003b4f15f1da9b3	123/24/DDA	Testing

*Interfaccia di creazione dei ticket.*

In questa interfaccia è possibile visualizzare la lista dei DDA della propria utenza.

## Visualizzare tutti i ticket della propria utenza



**Tickets** + NEW TICKET

Tickets have a lifespan of 30 minutes and will be closed automatically.

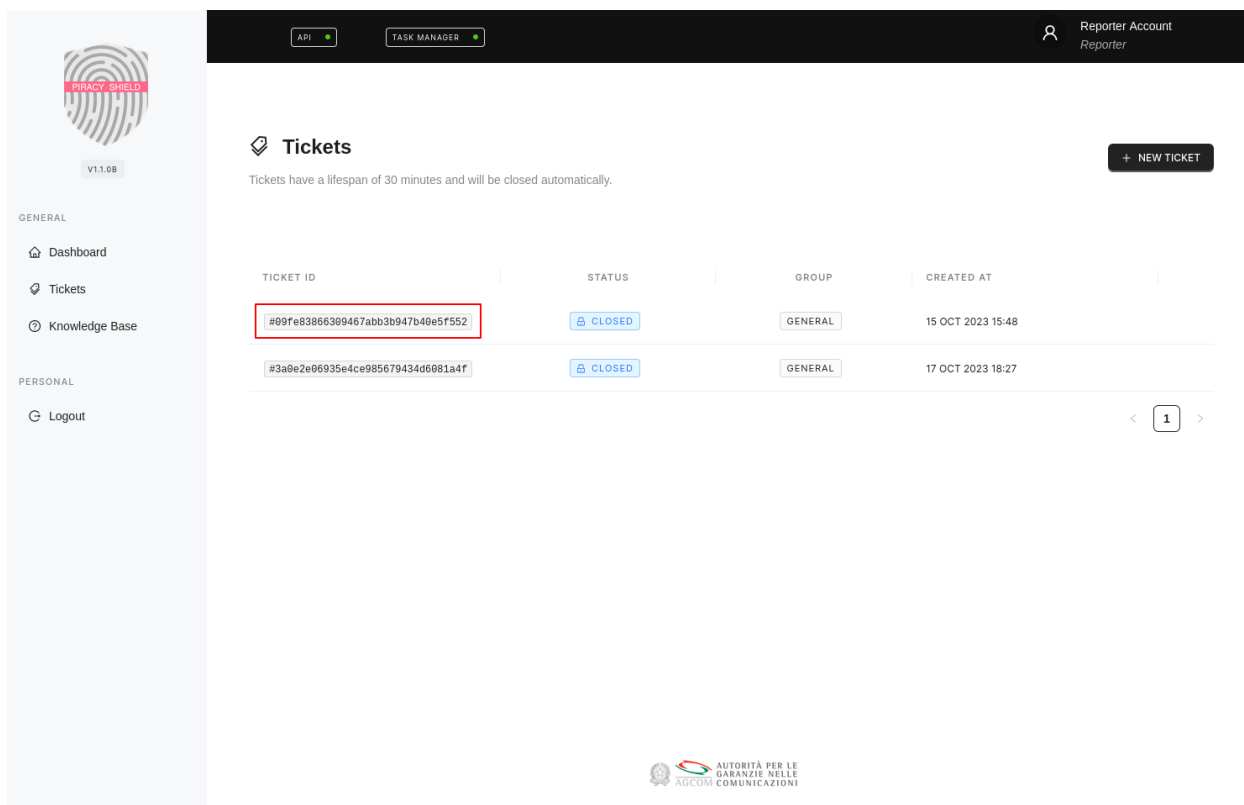
TICKET ID	STATUS	GROUP	CREATED AT
#09fe83866309467abb3b947b40e5f552	CLOSED	GENERAL	15 OCT 2023 15:48
#3a0e2e06935e4ce985679434d6081a4f	CLOSED	GENERAL	17 OCT 2023 18:27

< 1 >

*Interfaccia di gestione dei ticket.*

In questa interfaccia è possibile visualizzare tutti i ticket creati.

## Visualizzare un singolo ticket



**Tickets** + NEW TICKET

Tickets have a lifespan of 30 minutes and will be closed automatically.

TICKET ID	STATUS	GROUP	CREATED AT
#09fe83866309467abb3b947b40e5f552	CLOSED	GENERAL	15 OCT 2023 15:48
#3a0e2e06935e4ce985679434d6081a4f	CLOSED	GENERAL	17 OCT 2023 18:27

*Interfaccia di gestione dei ticket.*

Per visualizzare un singolo ticket, cliccare sul suo ID corrispondente.



The screenshot displays the PIRACY SHIELD interface for viewing a single ticket. The top navigation bar includes 'API' and 'TASK MANAGER' buttons, and a user profile for 'Reporter Account' with the role 'Reporter'. The left sidebar contains navigation options: 'Dashboard', 'Tickets' (selected), 'DDA', 'Whitelist', 'Knowledge Base', 'Changelog', 'Settings', and 'Logout'. The main content area shows a QR code, a ticket ID '#d9b8f6b2d9244facb40150dab5ffc6a3', and a 'Created at' timestamp of '24 JAN 2024 15:32'. The ticket status is 'CLOSED'. Below this, there are tabs for 'Details' and 'Forensic Evidence'. The 'Details' tab is active, showing 'GENERAL INFORMATIONS' and 'METADATA' sections. The 'GENERAL INFORMATIONS' section contains a table with two rows: 'Description' with value 'Test' and 'DDA' with value '000/24/DDA'. The 'METADATA' section contains a table with one row: 'Created at' with value '24 JAN 2024 15:32'. Below these sections is a table with columns 'VALUE', 'IS DUPLICATED', 'IS WHITELISTED', and 'IS ERROR'. The 'VALUE' column contains a folder icon and the text 'No data'.

*Interfaccia di visualizzazione di un singolo ticket.*





## **Rimozione del singolo ticket entro 75 secondi**

---



API TASK MANAGER Reporter Account Reporter

### Tickets

Tickets have a lifespan of 30 minutes and will be closed automatically.

+ NEW TICKET

TICKET ID	STATUS	GROUP	CREATED AT	
#31bfed7a5a4c402c92f37d5c7f420485	CREATED	GENERAL	18 OCT 2023 23:45	REMOVE

< 1 >

AUTORITÀ PER LE  
GARANZIE NELLE  
AGCOM COMUNICAZIONI

*Interfaccia di gestione dei ticket.*

Per rimuovere un ticket creato, cliccare su "Remove".



API TASK MANAGER Reporter Account Reporter

### Tickets

Tickets have a lifespan of 30 minutes and will be closed automatically.

+ NEW TICKET

**Remove the ticket**  
Are you sure to delete this ticket? This operation cannot be undone.

TICKET ID	STATUS	GROUP	
#31bfed7a5a4c402c92f37d5c7f420485	CREATED	GENERAL	18 OCT 2023 23:45 REMOVE

< 1 >


AUTORITÀ PER LE  
GARANZIE NELLE  
AGCOM COMUNICAZIONI

### Interfaccia di gestione dei ticket.

Per confermare la rimozione, cliccare su "Yes".

Questa operazione non è reversibile e potrà essere fatta entro 75 secondi dalla creazione del ticket.

## Creazione di un ticket errore



V2.0.08

GENERAL

- Dashboard
- Tickets
- Whitelist
- Knowledge Base

PERSONAL

- Logout

API TASK MANAGER Reporter Account Reporter

### New Error Ticket

Create a new error ticket to invalidate any ticket item present in the selected ticket.

**Warning**

Please check your input carefully before submitting. The data you are about to insert is critical and will be transmitted to the relative providers.


**Ticket ID \***

Ticket identifier.

---

**FQDN Items**

Select the FQDN items to report as errors.

VALUE	GENRE	REPORT
 No data		

---

**IPv4 Items**

Select the IPv4 items to report as errors.

VALUE	GENRE	REPORT
5.4.3.2	IPv4	<input checked="" type="checkbox"/>



## Interfaccia di gestione dei ticket.

Per creare un ticket errore, cliccare su "New Error Ticket". Selezionare l'identificativo del ticket e selezionare la spunta REPORT per rimuovere i singoli ticket item. Sarà possibile compiere l'operazione entro 24 ore dalla creazione del ticket originale.

## Caricamento della prova

API TASK MANAGER Reporter Account Reporter

### Tickets

Tickets have a lifespan of 30 minutes and will be closed automatically.

+ NEW TICKET

TICKET ID	STATUS	GROUP	CREATED AT
#09fe83866309467abb3b947b40e5f552	CLOSED	GENERAL	15 OCT 2023 15:48
#3a0e2e06935e4ce985679434d6081a4f	CLOSED	GENERAL	17 OCT 2023 18:27

GENERAL: Dashboard, Tickets, Knowledge Base  
PERSONAL: Logout

AUTORITÀ PER LE  
GARANZIE NELLE  
AGCOM COMUNICAZIONI

## Interfaccia di gestione dei ticket.

Per caricare la prova di un ticket, cliccare sul ID corrispondente del ticket.

API TASK MANAGER Reporter Account Reporter

#04cd43d99d8b4f57b420e3268741a9cc  
Created at 20 NOV 2023 15:52  
OPEN 00:29:44

REPORT ERROR

GENERAL  
Dashboard  
Tickets  
Whitelist  
Knowledge Base

PERSONAL  
Logout

Details Forensic Evidence

ARCHIVE

**Expected Data**  
Expected archive with the following specifications:

Hash Type	SHA256
Hash String	4b772a40f081a91023b397696f766e556b072c6d29d8c40e34ce014da521463a

**Current Data**

Archive Name	
Status	PENDING

REQUIREMENTS INFORMATIONS

Supported Archive Formats RAR

SELECT ARCHIVE  
START UPLOAD

## Interfaccia di gestione dei ticket.

Per caricare la prova, cliccare su “Forensic Evidence”, poi cliccare su “Select Archive”, scegliere e selezionare il file da caricare e poi cliccare su “Start Upload”.

Gli archivi supportati saranno i seguenti formati:

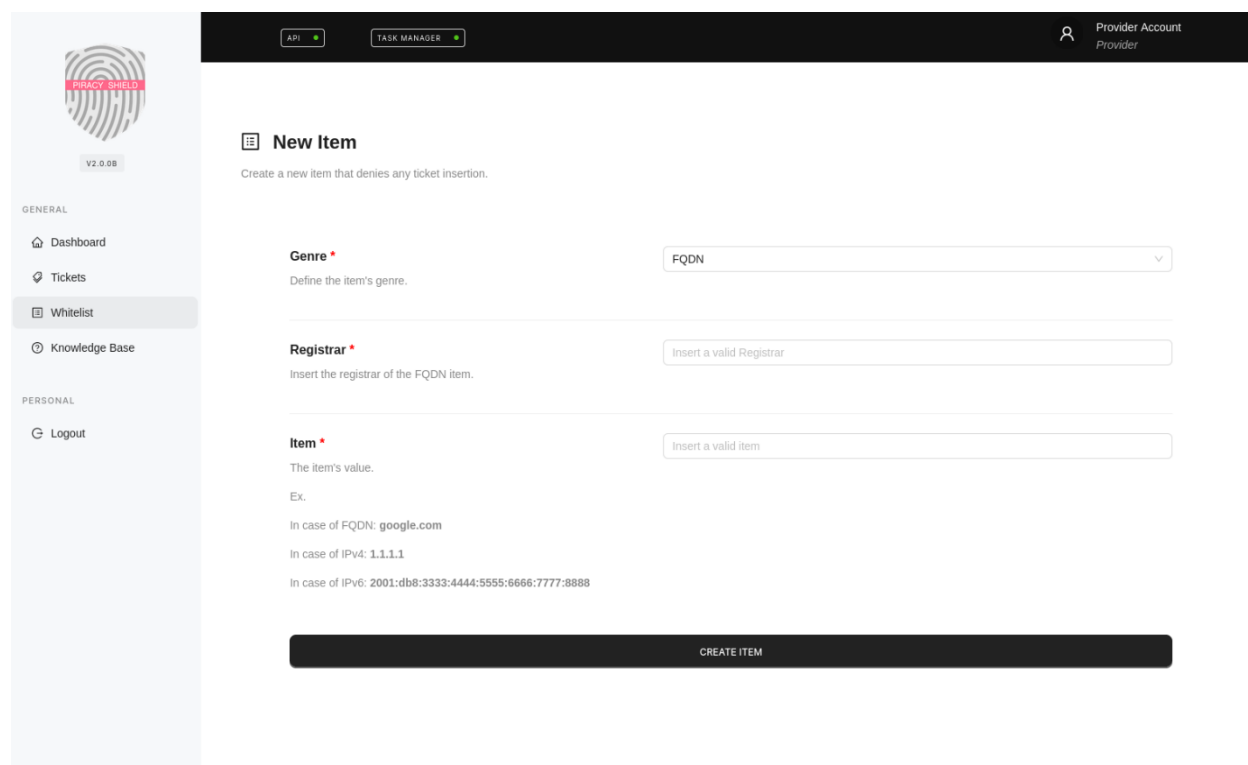
- .rar
- .zip

Gli algoritmi di hash supportati saranno i seguenti:

- SHA256
- SHA384
- SHA512
- BLAKE2B
- BLAKE2S

## Whitelist

### Inserire un dato in whitelist



The screenshot shows the 'New Item' form in the PIRACY SHIELD interface. The form is titled 'New Item' and includes a sub-header 'Create a new item that denies any ticket insertion.' The form contains three main input fields:

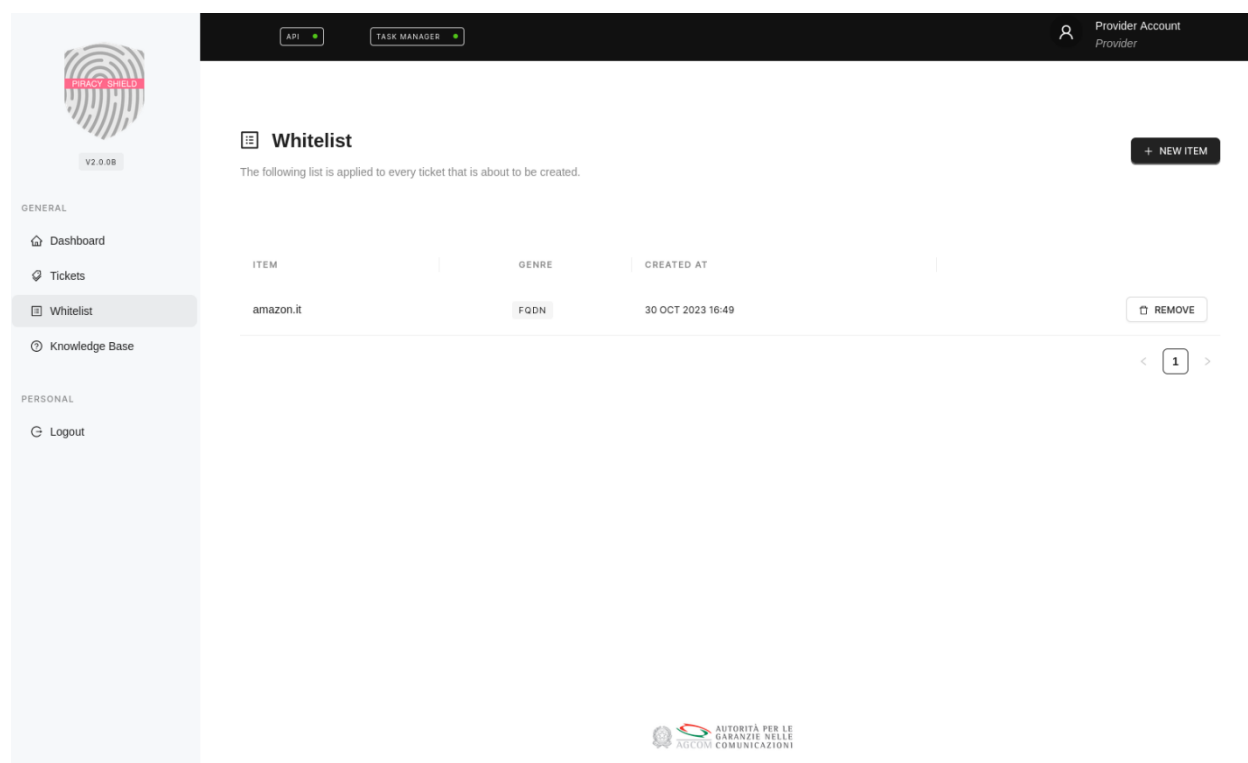
- Genre \***: A dropdown menu with 'FQDN' selected. Below it, the text reads 'Define the item's genre.'
- Registrar \***: A text input field with the placeholder 'Insert a valid Registrar'. Below it, the text reads 'Insert the registrar of the FQDN item.'
- Item \***: A text input field with the placeholder 'Insert a valid item'. Below it, the text reads 'The item's value.' followed by 'Ex.' and three examples: 'In case of FQDN: google.com', 'In case of IPv4: 1.1.1.1', and 'In case of IPv6: 2001:db8:3333:4444:5555:6666:7777:8888'.

At the bottom of the form is a large black button labeled 'CREATE ITEM'. The left sidebar shows navigation options: Dashboard, Tickets, Whitelist (selected), Knowledge Base, and Logout. The top navigation bar includes 'API', 'TASK MANAGER', and 'Provider Account Provider'.

### *Interfaccia di per inserire dati in whitelist.*

Per inserire un dato in whitelist è possibile cliccare sulla voce whitelist e poi cliccare su “NEW ITEM”, inserire le informazioni necessarie e cliccare su “CREATE ITEM”. È possibile inserire FQDN con il relativo registrar di riferimento

## Visualizzare tutti i dati presenti nella whitelist della propria utenza



The screenshot displays the 'Whitelist' management interface. At the top, there are navigation tabs for 'API' and 'TASK MANAGER', and a user profile section for 'Provider Account' and 'Provider'. The main heading is 'Whitelist' with a '+ NEW ITEM' button. Below the heading, a note states: 'The following list is applied to every ticket that is about to be created.' A table lists the whitelisted items:

ITEM	GENRE	CREATED AT	
amazon.it	FQDN	30 OCT 2023 16:49	REMOVE

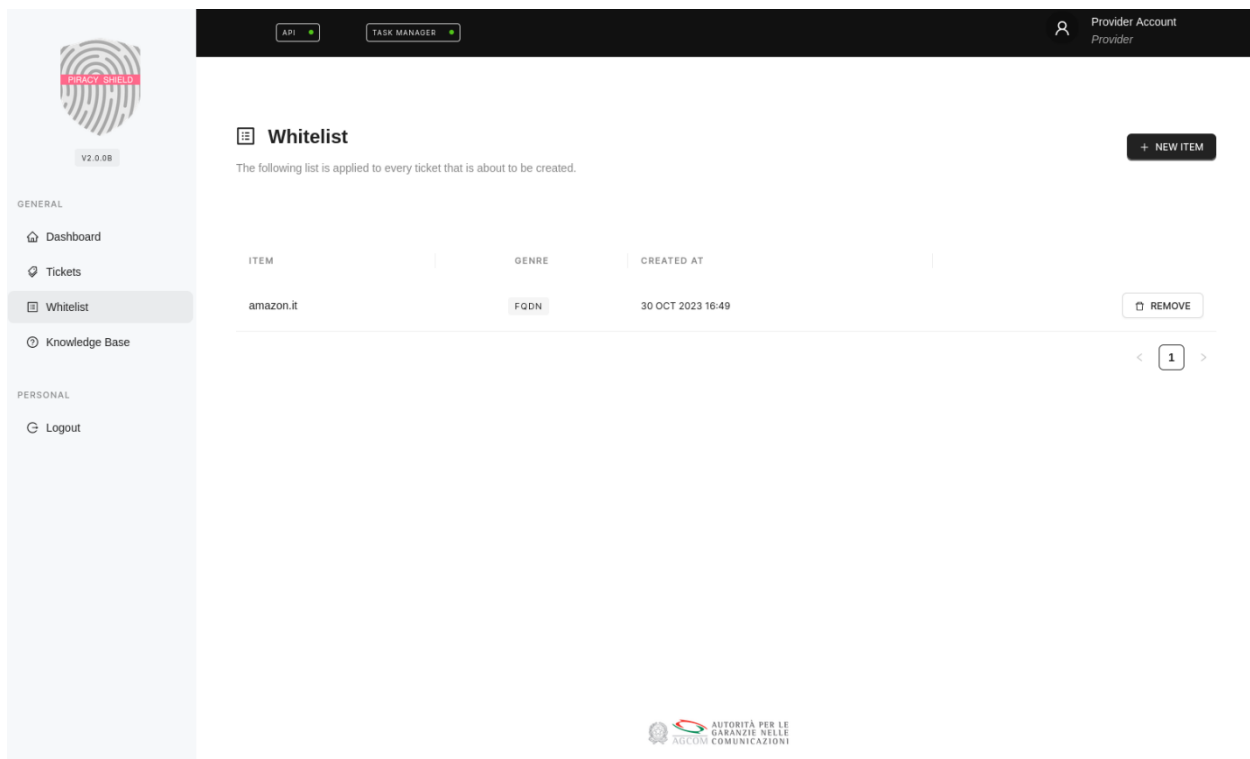
At the bottom of the table, there is a pagination control showing '1' items. The footer of the page contains the AGCOM logo and text: 'AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI'.

### *Interfaccia di per visualizzare dati in whitelist.*

Per visualizzare la propria whitelist è possibile cliccare sulla voce whitelist.



## Rimuovere dati dalla whitelist



**Whitelist** + NEW ITEM

The following list is applied to every ticket that is about to be created.

ITEM	GENRE	CREATED AT	
amazon.it	FQDN	30 OCT 2023 16:49	REMOVE

< 1 >

*Interfaccia di per gestire dati in whitelist.*

Per rimuovere un dato in whitelist è possibile cliccare sulla voce whitelist e poi cliccare su “REMOVE” che si trova di fianco al dato.

## 11. API

### Autenticazione

#### Login

---

L'endpoint di accesso consente agli utenti di autenticarsi e ottenere l'accesso alle risorse protette all'interno del sistema. Questa API accetta un payload JSON contenente l'email dell'utente e la password per l'autenticazione. In caso di autenticazione riuscita, l'endpoint risponde con: - un token di accesso JSON Web Token (JWT), che può essere utilizzato per autorizzare le richieste successive verso altri endpoint; - un token di refresh, per ricevere ulteriori token di accesso terminato il loro periodo di vita.

---

<b>Endpoint</b>	<b>Metodo</b>
<code>/api/v1/authentication/login</code>	POST

## ESEMPIO

### REQUEST BODY

```
{  
  'email': 'user@test.com',  
  'password': 'a_secure_password'  
}
```

### RESPONSE 200 OK

```
{  
  'status': 'success',  
  'data': {  
    'access_token': 'eyJhbGc...',  
    'refresh_token': 'ayJkhmHc...'  
  }  
}
```

## NOTE

- L'email e la password devono essere fornite nel corpo della richiesta come un oggetto JSON.
- Il token di accesso è un JSON Web Token (JWT) che deve essere incluso nell'intestazione Authorization per le successive richieste autenticate.
- Il refresh token viene anche fornito nella risposta e può essere utilizzato per ottenere un nuovo token di accesso quando quello corrente scade.
- Il cookie HTTP-only viene impostato negli header della risposta e dovrebbe essere memorizzato dal client. Fornisce uno spazio sicuro per l'archiviazione del token aggiornato (refresh token) ed è automaticamente inviato dal client nelle successive richieste.

## Refresh

---

L'endpoint di aggiornamento (refresh endpoint) consente agli utenti di ottenere un nuovo token di accesso fornendo un token di aggiornamento valido. Questo endpoint API viene utilizzato per aggiornare il token di accesso quando scade o diventa non valido. L'endpoint accetta il token di aggiornamento come parametro e risponde con un nuovo token di accesso JWT.

Endpoint	Metodo
/api/v1/authentication/refresh	POST

### ESEMPIO

#### REQUEST BODY

```
{  
  'refresh_token': 'eyJhbGc...',  
}
```

#### RESPONSE 200 OK

```
{
  'status': 'success',
  'data': {
    'access_token': 'eyJhbXc...'
  }
}
```

#### NOTE

- Il token di aggiornamento (refresh token) deve essere fornito nel corpo della richiesta come un oggetto JSON.
- Il token di aggiornamento (refresh token) viene ottenuto durante il processo di accesso e dovrebbe essere memorizzato in modo sicuro dal client.
- In caso di successo di una richiesta di aggiornamento, viene restituito un nuovo token di accesso nel corpo della risposta.
- Il nuovo token di accesso dovrebbe sostituire il precedente token di accesso nell'intestazione Authorization del client per le successive richieste autenticate.

## Logout

---

L'endpoint di logout consente agli utenti di invalidare la loro sessione corrente e di effettuare il logout dal sistema. Questo endpoint API viene utilizzato per terminare la sessione dell'utente e revocare l'accesso alle risorse protette. L'operazione di logout non richiede ulteriori parametri e può essere attivata inviando una richiesta GET all'endpoint corrispondente.

Endpoint	Metodo
/api/v1/authentication/logout	GET

#### ESEMPIO

#### RESPONSE 200 OK

```
{
  'status': 'success',
  'data': 'Goodbye!'
}
```

## NOTE

- L'operazione di logout viene eseguita inviando una semplice richiesta GET all'endpoint di logout.
- Dopo un logout riuscito, il token di accesso e il token di aggiornamento diventano invalidi e ulteriori richieste fatte utilizzando questi token saranno respinte.
- Si consiglia di eliminare eventuali token di accesso o token di aggiornamento memorizzati sul lato client dopo aver eseguito l'operazione di logout.

## Ticket

### Creazione di un nuovo ticket

---

L'endpoint di creazione del ticket consente agli utenti di creare un nuovo ticket all'interno del sistema. Questo endpoint API accetta vari parametri come la descrizione, le prove forensi, l'identificativo dell'istanza cautelare, il nome di dominio completo qualificato (FQDN), gli indirizzi IPv4 e gli indirizzi IPv6. Il campo prove forensi sono obbligatori, mentre il campo FQDN o IPv4 (o entrambi) devono essere forniti e non vuoti.

Prima della creazione del ticket, è necessario fornire un hash delle prove forensi. Questo garantisce che sia stato prodotto un pacchetto di prove forensi corrispondente ai dati inseriti. Non sono consentiti duplicati di FQDN e indirizzi IPv4 e indirizzi IPv6.

Dopo la creazione del ticket, viene applicato un periodo di revoca di 75 secondi per evitare eventuali errori. Solo durante questo periodo di tempo è possibile rimuovere con successo il ticket.

Endpoint	Metodo
/api/v1/ticket/create	POST

## ESEMPIO

### REQUEST BODY

```
{
  'dda_id': '...',
  'description': 'My first ticket example',
  'forensic_evidence': {
    'hash': {
      'sha256': 'a40de5d...'
    }
  },
  'fqdn': [
    'example.com',
    'subdomain.example.com'
  ],
  'ipv4': [
    '8.8.8.8',
    '1.1.1.1'
  ],
  'ipv6': [
    '1XX0:00..0:0000:0000:0005:0600:300c:326b',
    '2XX0:0..0:0000:0000:0005:0600:300c:326b'
  ]
}
```

### RESPONSE 200 OK

```
{
  'status': 'success',
  'data': {
    'ticket_id': 'c61f694...'
  },
  'note': 'Ticket created. If this is a mistake, you have 75 seconds to remove it before it gets visible to the providers.'
}
```

## NOTE

- I campi FQDN, IPv4, IPv6 sono opzionali, ma almeno uno di essi deve essere fornito e non vuoto. Questi campi accettano un array di valori.
- In futuro potrebbe essere introdotto un limite fisso per i campi FQDN , IPv4 e IPv6.

- Il `ticket_id` viene generato al momento della creazione del ticket e può essere utilizzato per riferimenti futuri o per recuperare i dettagli del ticket.
- Per la creazione del ticket, è necessario fornire un identificativo DDA (numero di determina cautelare di riferimento). In `'dda_id': '....'` è necessario inserire l'identificativo di riferimento che viene fornito come risultato della chiamata riportata nella voce **Preleva la lista DDA** e **Preleva singolo DDA** del presente manuale.

## Preleva la lista DDA

Endpoint	Metodo
<code>/api/v1/dda/get/all</code>	GET

### ESEMPIO

RESPONSE 200 OK

```
{
  "data" : [
    {
      "dda_id" : "c1dc978e54394f59a750cc67ec66a333",
      "description" : "Test1",
      "instance" : "034/24/DDA",
      "is_active" : true,
      "metadata" : {
        "created_at" : "2024-01-02T10:54:09.163120+01:00"
      }
    },
  ],
}
```



```
"dda_id" : "002ad48e542a4rtb9003b4f15f1da9b3",
"description" : "Test2",
"instance" : "456/23/DDA",
"is_active" : true,
"metadata" : {
  "created_at" : "2023-12-21T07:34:45.444065+01:00"
}
},
"status" : "success"
}
```

## Preleva un singolo DDA

Endpoint	Metodo
----------	--------

/api/v1/dda/get	GET
-----------------	-----

### ESEMPIO

#### REQUEST BODY

```
{
  'dda_id': ' c1dc978e54394f59a750cc67ec66a333'
}
```

#### RESPONSE 200 OK

```
{
  "data" : [
    {
      "dda_id" : "c1dc978e54394f59a750cc67ec66a333",
      "description" : "Test1",
      "instance" : "034/24/DDA",
      "is_active" : true,
      "metadata" : {
        "created_at" : "2024-01-02T10:54:09.163120+01:00"
      }
    }
  ]
}
```

```
    },  
  
  ],  
  "status" : "success"  
}
```

## Preleva un singolo ticket

---

L'endpoint "get ticket" consente agli utenti di recuperare i dettagli di un ticket specifico fornendo il suo ID del ticket.

Endpoint	Metodo
/api/v1/ticket/get	POST

### ESEMPIO

#### REQUEST BODY

```
{  
  'ticket_id': 'c61f694...'  
}
```

#### RESPONSE 200 OK

```
{  
  'status': 'success',  
  'data': {  
    'ticket_id': 'c61f694...',  
    'dda_id': '....',  
    'fqdn': [  
      'example.com',  
      'subdomain.example.com'  
    ],  
    'ipv4': [  
      '8.8.8.8',  
    ]  
  }  
}
```

```
'1.1.1.1'  
],  
'ipv6': [  
  '1XX0:00..0:0000:0000:0005:0600:300c:326b',  
  '2XX0:0..0:0000:0000:0005:0600:300c:326b'  
],  
  
'status': 'open',  
'metadata': {  
  'created_at': '2023-05-01T15:00:00.526108'  
},  
'settings': {  
  'revoke_time': 75,  
  'autoclose_time': 1875,  
  'report_error_time': 86400  
},  
}  
}  
}
```

#### NOTE

- Il ticket\_id dovrebbe essere passato come parametro di query nell'URL per recuperare il ticket specifico.
- Se un ticket con l'ID fornito non viene trovato, verrà restituito un codice di stato 404 Not Found, indicando che il ticket non è stato trovato.
- Verificare che il ticket che si intende recuperare non sia scaduto prima di effettuare la richiesta.

## Preleva tutti i ticket presenti nella propria utenza

---

Questo API endpoint restituisce l'elenco di tutti i ticket.

Endpoint	Metodo
/api/v1/ticket/get/all	GET

### ESEMPIO

RESPONSE 200 OK

```
{
  'status': 'success',
  'data': [
    {
      'ticket_id': 'c61f694...',
      'dda_id': '...',
      'fqdn': [
        'example.com',
        'subdomain.example.com'
      ],
      'ipv4': [
        '8.8.8.8',
        '1.1.1.1'
      ],
      'ipv6': [
        '1XX0:00..0:0000:0000:0005:0600:300c:326b',
        '2XX0:0..0:0000:0000:0005:0600:300c:326b'
      ],
      'status': 'open',
      'metadata': {
        'created_at': '2023-05-01T15:00:00.526108'
      },
      'settings': {
        'revoke_time': 75,
        'autoclose_time': 1875,
        'report_error_time': 86400
      },
    },
    ...
  ]
}
```

## NOTE

- La lista dei ticket restituita rappresenta tutti i ticket della propria utenza in tutti gli stati nel sistema.

## **Rimozione del singolo ticket entro 75 secondi**

---

---

L'endpoint "remove ticket" consente agli utenti di rimuovere un ticket specifico dal sistema entro 75 secondi dalla creazione e prima che esso diventi fruibile da parte dei Provider. Questo endpoint API richiede che il parametro ticket\_id sia fornito per identificare il ticket da rimuovere.

Endpoint	Metodo
/api/v1/ticket/remove	POST

#### ESEMPIO

```
REQUEST BODY
{
  'ticket_id': 'c61f694...'
}
RESPONSE 200 OK
{
  'status': 'success'
}
```

#### NOTE

- Se si tenta di rimuovere un ticket dopo che è trascorso il periodo di tempo consentito, verrà restituita una risposta "400 Bad Request", indicando che il tempo per la rimozione del ticket è scaduto. Se si pensa di aver commesso un errore sarà possibile utilizzare la funzionalità del ticket errore.

## Creazione del ticket errore

---

L'endpoint "error ticket" consente agli utenti di rimuovere un ticket specifico o singoli ticket item riferiti ad un ticket specifico dal sistema. Questo endpoint API richiede che il parametro ticket\_id sia fornito per identificare il ticket da rimuovere o in cui siano presenti i dati da rimuovere.

È importante notare che la funzionalità del ticket errore può essere utilizzata solo entro 24 dalla creazione del ticket originale.

Endpoint	Metodo
/api/v1/ticket/error/create	POST

#### ESEMPIO

##### REQUEST BODY

```
{
  'ticket_id': 'c61f694...'....,
  'fqdn': [
    '...'
  ],
  'ipv4': [
    '...'
  ],
  'ipv6': [
    '...'
  ],
}
```

##### RESPONSE 200 OK

```
{
  'ticket_error_id': '...',
  'ticket_id': '...'
}
```



## Caricare la prova di un ticket

---

L'endpoint di caricamento della prova consente agli utenti di caricare un pacchetto contenente la prova di un ticket specifico dal sistema. Questo endpoint API richiede che il parametro `ticket_id` sia fornito per identificare il ticket di riferimento.

Endpoint	Metodo
<code>/api/v1/forensic/upload/"id_ticket"</code>	POST

Per garantire il corretto invio delle prove forensi, l'archivio originale dovrà essere spezzettato in parti non superiori a 50mb e queste dovranno essere inviate in modalità multipart/form-data utilizzando la modalità descritta di seguito.

Indicare i parametri POST:

- **chunkIndex**: un numero rappresentante la parte corrente che si sta inviando.
- **totalChunks**: il totale delle parti da inviare.
- **originalFileName**: il nome originale dell'archivio.

Indicare i file:

- **archive**: la parte dell'archivio che si sta inviando.

Tale modalità permetterà l'invio frammentato dell'archivio originale, che verrà ricomposto e verificato dalla piattaforma.

I pesi supportati sono:

- Peso minimo: 10kb
- Peso massimo: 10gb

Gli archivi supportati saranno i seguenti formati:

- .rar
- .zip

Gli algoritmi di hash supportati saranno i seguenti:

- SHA256
- SHA384
- SHA512
- BLAKE2B
- BLAKE2S

La prova deve essere caricata entro 24 ore dalla creazione del ticket.

## ESEMPIO

### REQUEST

```
{  
  "chunkIndex": 1,  
  "totalChunks": 20,  
  "originalFileName": "Archivio.zip",  
}  
{  
  "files": {  
    "archive": <FILE_PARTE_ARCHIVIO>  
  }  
}
```

### RESPONSE 200 OK

```
{  
  "status": "success"  
}
```

## Visualizzare dati del pacchetto prova caricato per un ticket

---

Questo endpoint consente agli utenti di visualizzare i dati di un pacchetto contenente la prova di un ticket specifico dal sistema. Questo endpoint API richiede che il parametro `ticket_id` sia fornito per identificare il ticket di riferimento.

Endpoint	Metodo
<code>/api/v1/forensic/get/by_ticket</code>	POST

### ESEMPIO

#### REQUEST BODY

```
{  
'ticket_id': 'c61f694...'...'  
}
```

#### RESPONSE 200 OK

```
{  
  "forensic_id": "...",  
  "ticket_id": "...",  
  "hash_type": "...",  
  "hash_string": "..."  
}
```

## Ping

---

Questo punto di accesso API funge da semplice test di controllo dello stato per verificare che la piattaforma sia online e funzionante correttamente.

<b>Endpoint</b>	<b>Metodo</b>
/api/v1/ping	GET

#### ESEMPIO

```
RESPONSE 200 OK
{
  'status': 'success',
  'data': 'Pong!'
}
```

## Whitelist

### Inserire un dato in whitelist

Questo punto di accesso API permette all'utente di caricare dati nella propria whitelist.

La whitelist generale della piattaforma non prevede l'inserimento di duplicati.

<b>Endpoint</b>	<b>Metodo</b>
<code>/api/v1/whitelist/item/create</code>	POST

#### ESEMPIO FQDN IN WHITELIST

##### REQUEST BODY

```
{  
  "genre": "fqdn",  
  "item": "dominio.it",  
  "registrar": "Test Registrar"  
}
```

##### RESPONSE 200 OK

```
{  
  "status": "success"  
}
```

#### ESEMPIO IPV4 IN WHITELIST

##### REQUEST BODY

```
{  
  "genre": "ipv4",  
  "item": "4.3.2.1",  
  "as_code": "AS123456789"  
}
```

RESPONSE 200 OK

```
{  
  "status": "success"  
}
```

#### ESEMPIO IPV6 IN WHITELIST

REQUEST BODY

```
{  
  "genre": "ipv6",  
  "item": "2001:0db8:85a3:0000:0000:8a2e:0370:7334",  
  "as_code": "AS123456789"  
}
```

RESPONSE 200 OK

```
{  
  "status": "success"  
}
```

#### ESEMPIO CIDR IPV4 IN WHITELIST

REQUEST BODY

```
{  
  "genre": "cidr_ipv4",  
  "item": "192.168.0.0/24",  
}
```

```
  "as_code": "AS123456789"  
}
```

RESPONSE 200 OK

```
{  
  "status": "success"  
}
```

#### ESEMPIO CIDR IPV6 IN WHITELIST

REQUEST BODY

```
{  
  "genre": "cidr_ipv6",  
  "item": "2001:0db8:85a3::/48",  
  "as_code": "AS123456789"  
}
```

RESPONSE 200 OK

```
{  
  "status": "success"  
}
```

#### NOTE

- Il campo registrar è una stringa indicante il nome del registrar stesso.
- Il codice ASN rappresenta una sequenza numerica lunga al massimo 9 numeri, contenente – in via opzionale - il prefisso 'AS'.

## Visualizzare tutti i dati presenti nella whitelist

Questo punto di accesso API permette all'utente di visualizzare tutti i dati presenti nella propria whitelist.



### Endpoint

### Metodo

/api/v1/whitelist/item/get/all

GET

### ESEMPIO

RESPONSE 200 OK

```
{
  [
    {
      "genre": "fqdn",
      "item": "dominio.it",
      "registrar": "Test Registrar"
    },
    {
      "genre": "ipv4",
      "item": "4.3.2.1",
      "as_code": "AS123456789"
    },
    ...
  ]
}
```

## Rimuovere dati dalla whitelist

Questo punto di accesso API permette all'utente di rimuovere dati presenti nella propria whitelist.

Endpoint	Metodo
<code>/api/v1/whitelist/item/remove</code>	POST

### ESEMPIO FQDN IN WHITELIST

#### REQUEST BODY

```
{  
  "item": "dominio.it"  
}
```

#### RESPONSE 200 OK

```
{  
  "status": "success"  
}
```

### ESEMPIO IPV4 IN WHITELIST

#### REQUEST BODY

```
{  
  "item": "4.3.2.1"  
}
```

#### RESPONSE 200 OK

```
{
```

```
  "status": "success"  
}
```

#### ESEMPIO IPV6 IN WHITELIST

##### REQUEST BODY

```
{  
  "item": "2001:0db8:85a3:0000:0000:8a2e:0370:7334"  
}
```

##### RESPONSE 200 OK

```
{  
  "status": "success"  
}
```

#### ESEMPIO CIDR IPV4 IN WHITELIST

##### REQUEST BODY

```
{  
  "item": "192.168.0.0/24"  
}
```

##### RESPONSE 200 OK

```
{  
  "status": "success"  
}
```

#### ESEMPIO CIDR IPV6 IN WHITELIST

##### REQUEST BODY

```
{  
  "item": "2001:0db8:85a3::/48"  
}
```



}

RESPONSE 200 OK

```
{  
  "status": "success"  
}
```