

MANUALE PIRACY SHIELD

VERSIONE PER ISP



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	7
4. Raggiungimento piattaforma	9
5. Sicurezza.....	10
Sistema di autenticazione	10
Processo di Autenticazione	10
Primo accesso	10
Access Token	11
Refresh Token.....	11
Limitazioni	12
Rate limit.....	12
Interruzione temporanea del servizio per abuso	14
Whitelist.....	15
Segnalazione e risoluzione problematiche	16
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. Sblocco per segnalazione errore.....	25
11. Manuale operativo – Interfaccia.....	26
Autenticazione	26
Login.....	26
Logout	27
Ticket.....	28
Visualizza tutti i ticket	28

Visualizza un singolo ticket	29
Preleva solo gli FQDN di un singolo ticket	32
Preleva solo gli IPv4 di un singolo ticket	35
Preleva solo gli IPv6 di un singolo ticket	38
Ticket Item	40
Preleva tutti gli FQDN di tutti i ticket	40
Preleva tutti gli IPv4 di tutti i ticket	43
Preleva tutti gli IPv6 di tutti i ticket	46
Impostare lo stato del dato	48
Whitelist	51
Inserire un dato in whitelist	51
Visualizzare tutti i dati presenti nella whitelist della propria utenza	52
Rimuovere dati dalla whitelist	53
12. API	55
Autenticazione	55
Login	55
Refresh	57
Logout	59
Ticket	60
Preleva un singolo ticket	60
Preleva tutti i dati di tutti i ticket	62
Preleva solo gli FQDN di un singolo ticket	63
Preleva solo gli IPv4 di un singolo ticket	66
Preleva solo gli IPv6 di un singolo ticket	70
Ticket Item	73
Preleva tutti gli FQDN di tutti i ticket	73
Preleva tutti gli IPv4 di tutti i ticket	76
Preleva tutti gli IPv6 di tutti i ticket	79
Impostare lo stato del dato	83
Ping	87
Whitelist	88
Inserire un dato in whitelist	88



Visualizzare tutti i dati presenti nella whitelist	91
Rimuovere dati dalla whitelist	92

1.Introduzione



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.

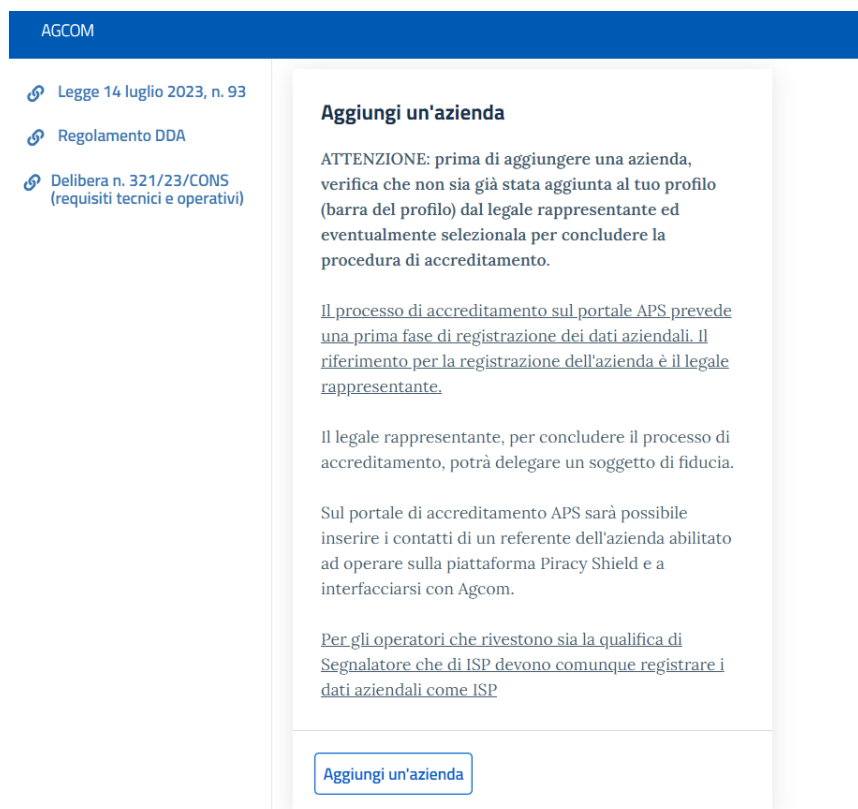
Si prega di notare che questa documentazione è da considerarsi confidenziale e sarà soggetta ad ulteriori aggiornamenti.

2. Processo di accreditamento

L'accesso alla piattaforma Piracy Shield necessita di una procedura di accreditamento da parte degli utenti che utilizzeranno la piattaforma.

Di seguito, le istruzioni per l'accREDITamento:

1. Accedere al [Portale APS](#) e cliccare sul link "Entra con SPID" oppure "Entra con CIE".
2. Inserire le proprie credenziali.
3. Cliccare sul link "Aggiungi un'azienda".



The screenshot shows the AGCOM portal interface. On the left, there is a navigation menu with the following items:

- Legge 14 luglio 2023, n. 93
- Regolamento DDA
- Delibera n. 321/23/CONS (requisiti tecnici e operativi)

The main content area is titled "Aggiungi un'azienda". It contains the following text:

ATTENZIONE: prima di aggiungere una azienda, verifica che non sia già stata aggiunta al tuo profilo (barra del profilo) dal legale rappresentante ed eventualmente selezionata per concludere la procedura di accreditamento.

Il processo di accreditamento sul portale APS prevede una prima fase di registrazione dei dati aziendali. Il riferimento per la registrazione dell'azienda è il legale rappresentante.

Il legale rappresentante, per concludere il processo di accreditamento, potrà delegare un soggetto di fiducia.

Sul portale di accreditamento APS sarà possibile inserire i contatti di un referente dell'azienda abilitato ad operare sulla piattaforma Piracy Shield e a interfacciarsi con Agcom.

Per gli operatori che rivestono sia la qualifica di Segnalatore che di ISP devono comunque registrare i dati aziendali come ISP

At the bottom of the section, there is a button labeled "Aggiungi un'azienda".



4. Compilare il modulo con le informazioni richieste.
5. Inviare il modulo e attendere la conferma dell'accreditamento.
6. L'esito dell'istanza di accreditamento sarà visibile sul portale di accreditamento.
7. L'esito dell'istanza di accreditamento sarà comunicato anche tramite PEC e all'indirizzo di posta elettronica del referente indicato.
8. Nella medesima comunicazione, se la richiesta di accreditamento è stata accolta, saranno indicate le credenziali per accedere alla piattaforma Piracy Shield.

Le credenziali saranno diverse per le distinte fasi di ambiente di test e di ambiente di produzione.

3. Accesso alla VPN

Per raggiungere la piattaforma Piracy Shield, per ogni ISP sarà predisposto un collegamento VPN site-to-site tra l'infrastruttura Microsoft Azure Cloud, che ospita la piattaforma di live blocking, e l'infrastruttura dell'ISP 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 ISP, 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:

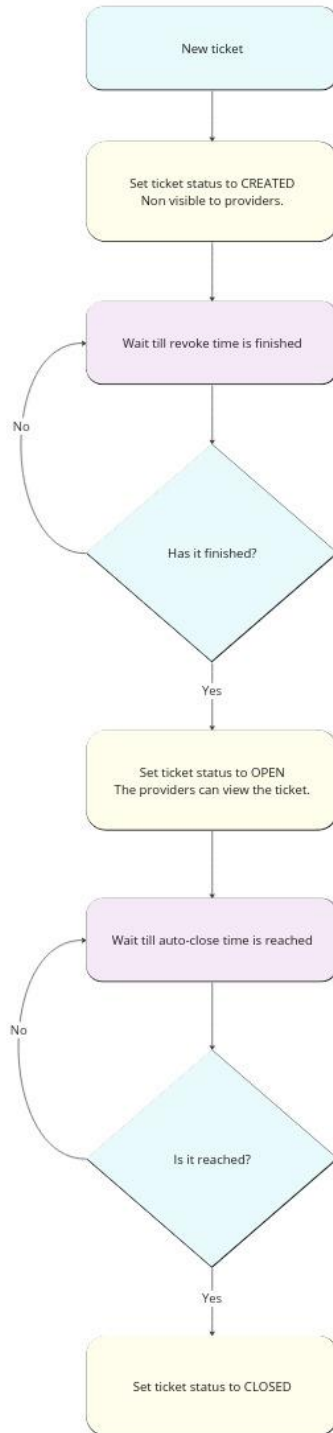
- **FQDN:** un Fully Qualified Domain Name (FQDN) si riferisce a un nome di dominio completo che specifica la sua posizione esatta all'interno del sistema di nomi di dominio gerarchico. Di solito, gli FQDN sono composti da un nome host e un nome di dominio, separati da punti (ad esempio, sottodominio.esempio.com).
- **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, all'indirizzo IPv4 e 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 di un ticket è di 30 minuti.
- Stato "Closed": scaduto il limite di tempo di 30 minuti, il ticket viene chiuso automaticamente. Questo cambio di stato non comporta alcuna limitazione nei confronti dell'operabilità di un ticket da parte dei Provider. Il ticket ed i relativi dati in stato closed saranno comunque visibili sulla piattaforma.



8.Utilizzo

Il provider può operare sugli elementi del ticket in due modalità:

- Interfaccia web: scaricando i ticket item (FQDN/IPv4/IPv6) globali relativi a tutti i ticket o i ticket item di un singolo ticket;

- API: prelevando i ticket item (FQDN/IPv4/IPv6) globali relativi a tutti i ticket o i ticket item di un singolo ticket;

Un flusso operativo di esempio per il Provider potrebbe consistere in:

1. Recuperare i dati: utilizzare le API generali dei ticket item (API FQDN o IPv4 o IPv6) per ottenere le liste complete degli elementi sulla quale operare.
2. Elaborare i ticket item: eseguire le operazioni necessarie al blocco degli elementi.
3. Impostare lo stato dei ticket item: dopo aver completato l'elaborazione di tutti gli elementi, potrà essere impostato lo stato di ciascun elemento per fornire un riscontro sullo stato dell'elaborazione del dato.

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.

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 recuperare il ticket ed i dati di quel ticket ed aggiornare lo stato degli elementi di ogni ticket per un massimo di 48 ore dalla creazione del 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.Sblocco per segnalazione errore

Un primo meccanismo di prevenzione contro errori di inserimento consiste nel permettere ad un segnalatore di eliminare un ticket nei primi 75 secondi di vita, tempo in cui il ticket non sarà visibile ai provider.

Qualora, però, a ticket attivo, si riscontrassero dati inseriti erroneamente, il segnalatore ha a disposizione una segnalazione di errore relativa a quel ticket, che andrà ad eliminare uno o più ticket item dalla lista singola del ticket e, quindi, dalla lista generale dei ticket item.

Ai provider viene richiesto di tenere conto dei cambiamenti, nel tempo, della lista di dati, in modo da bloccare sempre e solo ciò che è correntemente presente e di sbloccare qualsiasi dato risulti eliminato nel tempo.

Questa operazione è concessa, al segnalatore, esclusivamente durante le 24 ore dalla creazione del ticket.

11. Manuale operativo – Interfaccia

Autenticazione

Login

click here.' The right section features a 'Highly Restricted Area' warning box with a red 'x' icon and a close 'x' icon. The text in the box reads: 'Access to this area is strictly prohibited without proper authorization. Unauthorized access is punishable by law and will result in severe consequences.' Below the warning box is the AGCOM logo and text: 'AGCOM AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI'. The version number 'V1.1.0B' is visible in the bottom left corner of the grey section." data-bbox="114 97 875 500"/>

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](#).

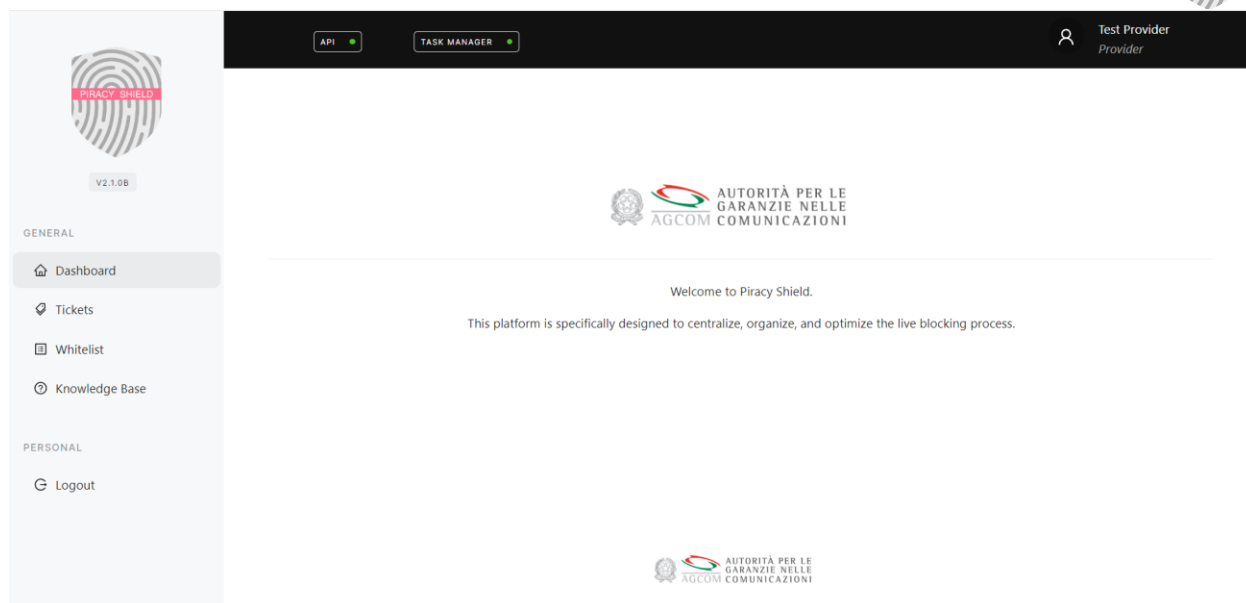
AGCOM **AUTORITÀ PER LE
GARANZIE NELLE
COMUNICAZIONI**

V1.1.0B

Interfaccia iniziale di accesso alla piattaforma.

Procedere con l'accesso attraverso le credenziali fornite.

Logout

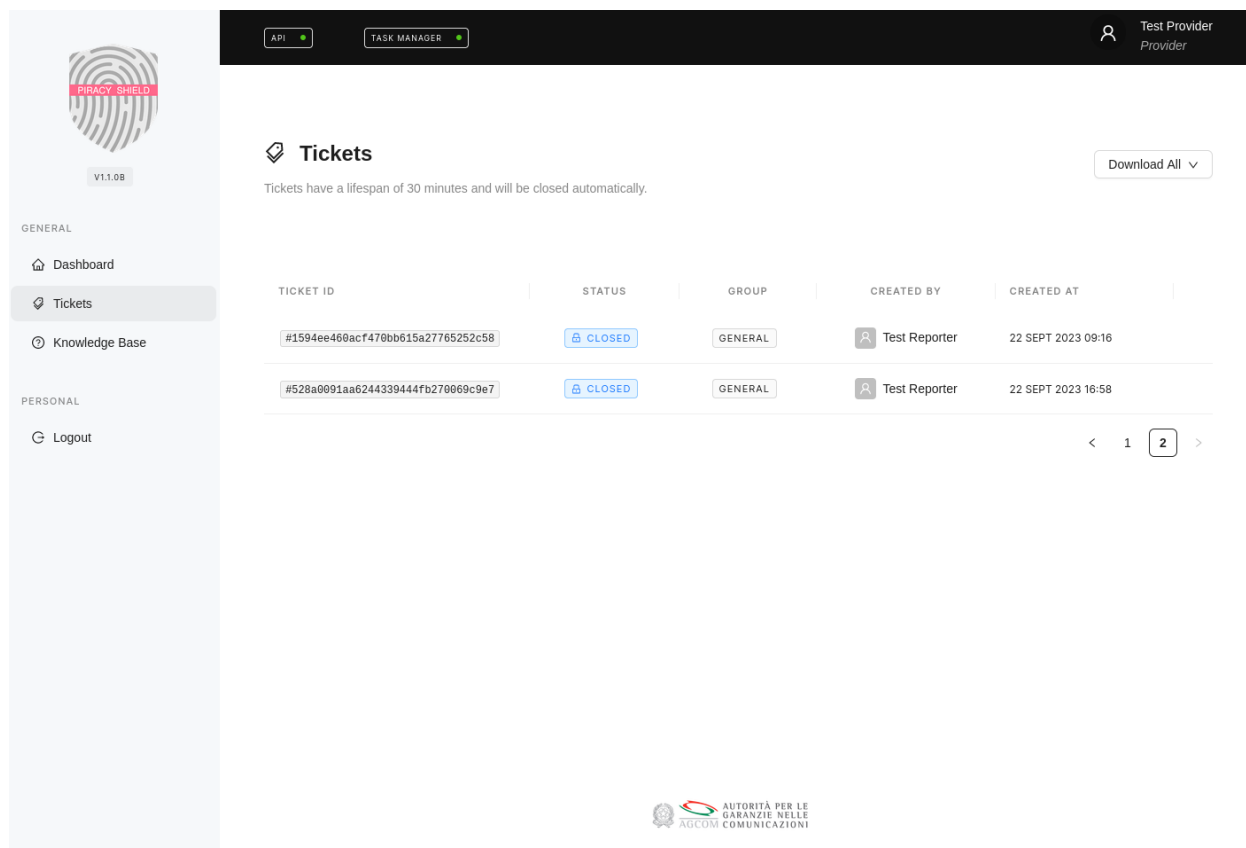


Interfaccia iniziale ad accesso effettuato.

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

Ticket

Visualizza tutti i ticket



Tickets Download All ▾

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

TICKET ID	STATUS	GROUP	CREATED BY	CREATED AT
#1594ee460acf470bb615a27765252c58	CLOSED	GENERAL	Test Reporter	22 SEPT 2023 09:16
#528a0091aa6244339444fb279069c9e7	CLOSED	GENERAL	Test Reporter	22 SEPT 2023 16:58

< 1 **2** >

Interfaccia di gestione dei ticket.

In questa interfaccia è possibile visualizzare la lista di tutti i ticket presenti nella piattaforma.

Visualizza un singolo ticket



API TASK MANAGER Test Provider Provider

Tickets

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

TICKET ID	STATUS	GROUP	CREATED BY	CREATED AT
#1594ee460acf470bb615a27765252c58	CLOSED	GENERAL	Test Reporter	22 SEPT 2023 09:16
#528a0091aa6244339444fb270069c9e7	CLOSED	GENERAL	Test Reporter	22 SEPT 2023 16:58

< 1 2 >

AUTORITÀ PER LE
GARANZIE NELLE
AGCOM COMUNICAZIONI

Interfaccia di gestione dei ticket.

Per visualizzare un singolo ticket, cliccare sul suo ID (nell'immagine cerchiato in rosso) corrispondente.



API TASK MANAGER Test Provider

PIRACY SHIELD V1.1.08

GENERAL

- Dashboard
- Tickets
- Knowledge Base

PERSONAL

- Logout

#528a0091aa6244339444fb270069c9e7

Created at 22 SEPT 2023 16:58 by Test Reporter

CLOSED

Download All

Ticket Items Details

TICKET ITEM	STATUS	UNPROCESSED REASON	ACTION
1.1.1.1	PROCESSED		Set status

< 1 >

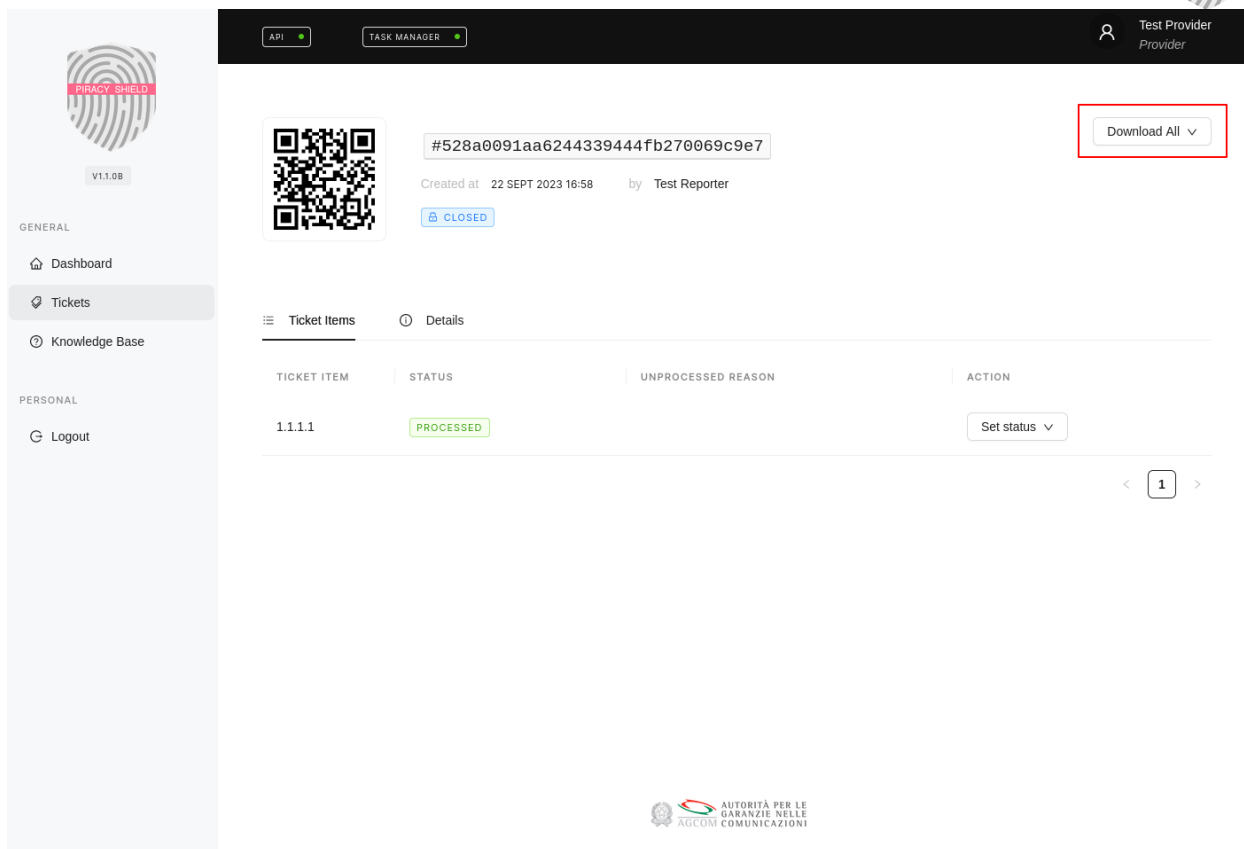
AUTORITÀ PER LE
GARANZIE NELLE
AGCOM COMUNICAZIONI

Interfaccia di gestione di un singolo ticket.

Da questa pagina sarà possibile effettuare tutte le operazioni riguardanti il singolo ticket e visualizzare tutte le sue informazioni.



Preleva solo gli FQDN di un singolo ticket



API TASK MANAGER Test Provider Provider

PIRACY SHIELD V1.1.08

GENERAL

- Dashboard
- Tickets
- Knowledge Base

PERSONAL

- Logout

#528a0091aa6244339444fb270069c9e7

Created at 22 SEPT 2023 16:58 by Test Reporter

CLOSED

Download All

Ticket Items Details

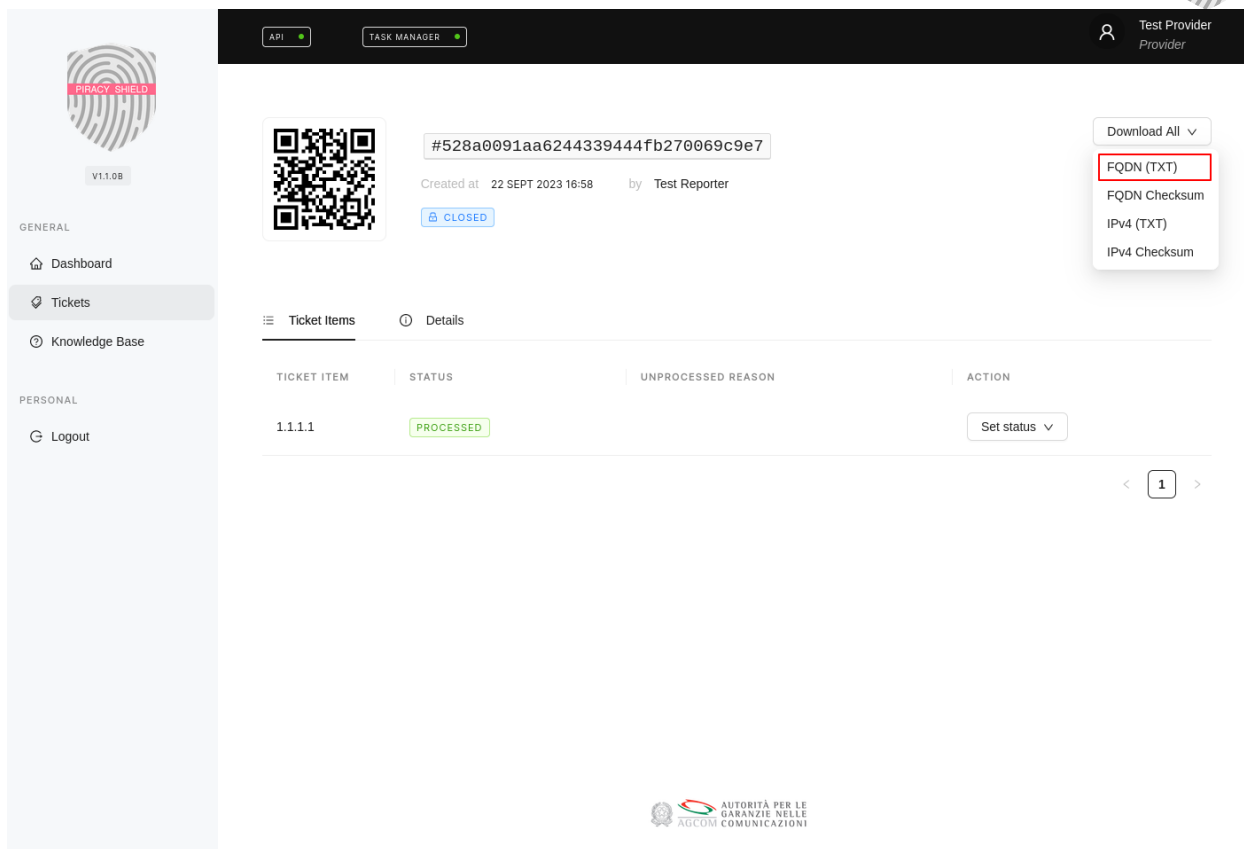
TICKET ITEM	STATUS	UNPROCESSED REASON	ACTION
1.1.1.1	PROCESSED		Set status

< 1 >

AUTORITÀ PER LE
GARANZIE NELLE
AGCOM COMUNICAZIONI

Interfaccia di gestione di un singolo ticket.

Per effettuare il download della lista degli FQDN è necessario cliccare sull'ID del ticket e poi cliccare in alto a destra sulla voce "Download All".



The screenshot displays the PIRACY SHIELD ticket management interface. On the left is a sidebar with navigation options: Dashboard, Tickets, Knowledge Base, and Logout. The main content area shows a ticket with ID #528a0091aa6244339444fb270069c9e7, created on 22 SEPT 2023 16:58 by Test Reporter, with a status of CLOSED. Below this is a table of ticket items with columns for TICKET ITEM, STATUS, UNPROCESSED REASON, and ACTION. A single item with ID 1.1.1.1 is shown with a status of PROCESSED. A 'Download All' dropdown menu is open, showing options: FQDN (TXT), FQDN Checksum, IPv4 (TXT), and IPv4 Checksum. The 'FQDN (TXT)' option is highlighted with a red box.

Interfaccia di gestione di un singolo ticket, voce "Download All".

Da questo menù a tendina sarà possibile selezionare FQDN per scaricare la lista in formato TXT ed, eventualmente, il suo relativo checksum (file di hash che permette di garantire l'inalterabilità del dato fornito).



Preleva solo gli IPv4 di un singolo ticket



API TASK MANAGER Test Provider Provider

PIRACY SHIELD V1.1.08

GENERAL

- Dashboard
- Tickets
- Knowledge Base

PERSONAL

- Logout

#528a0091aa6244339444fb270069c9e7

Created at 22 SEPT 2023 16:58 by Test Reporter

CLOSED

Download All

Ticket Items Details

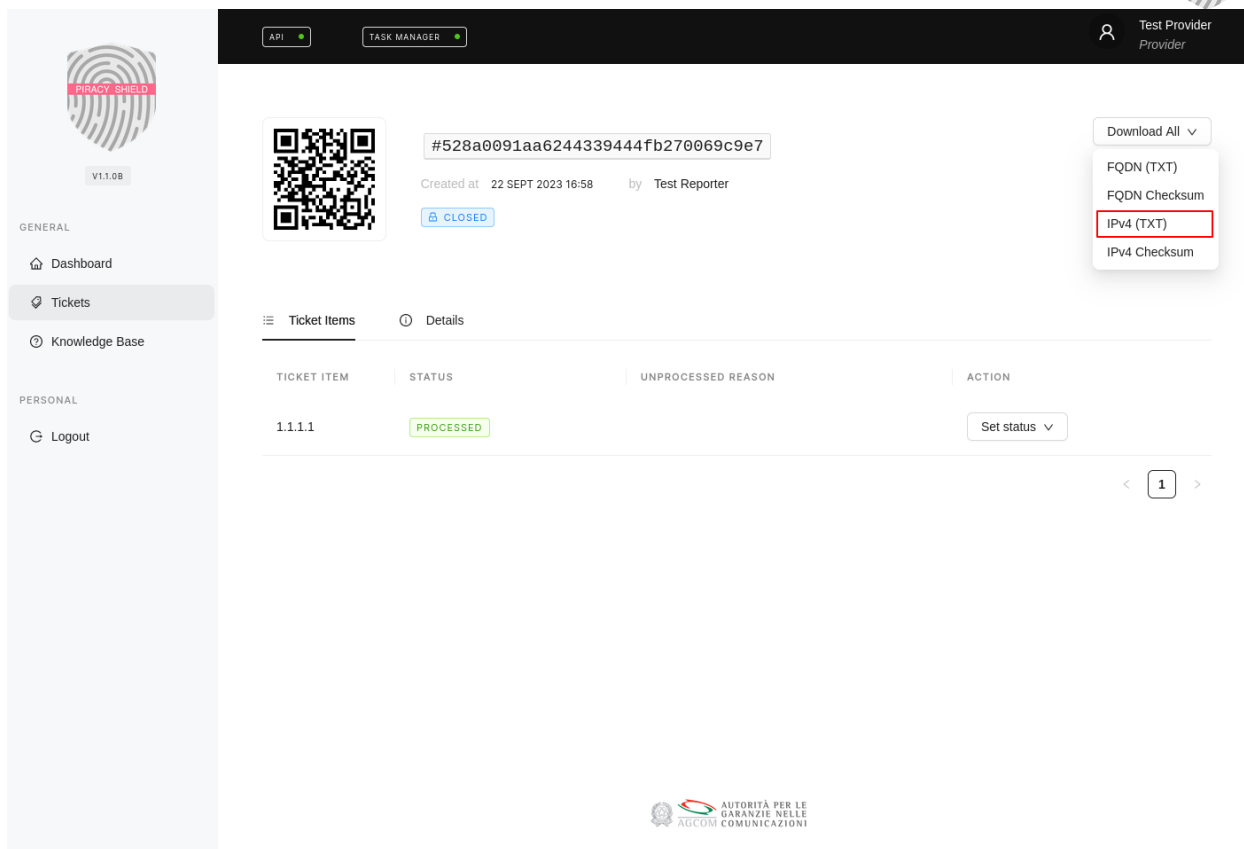
TICKET ITEM	STATUS	UNPROCESSED REASON	ACTION
1.1.1.1	PROCESSED		Set status

< 1 >

AUTORITÀ PER LE
GARANZIE NELLE
AGCOM COMUNICAZIONI

Interfaccia di gestione di un singolo ticket.

Per effettuare il download della lista degli IPv4 FQDN è necessario cliccare sull'ID del ticket e poi cliccare in alto a destra sulla voce "Download All".

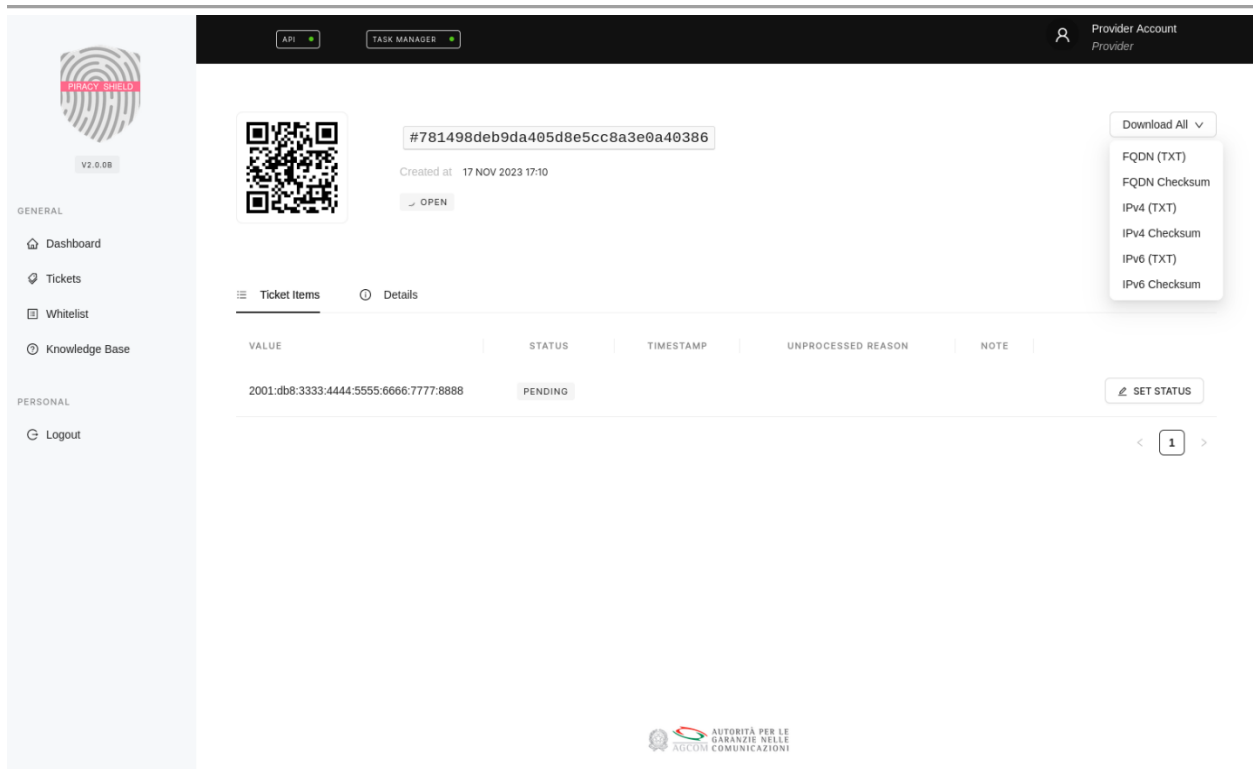


Interfaccia di gestione di un singolo ticket, voce "Download All".


Da questo menù a tendina sarà possibile selezionare IPv4 per scaricare la lista in formato TXT ed, eventualmente, il suo relativo checksum. (file di hash che permette di garantire l'inalterabilità del dato fornito).



Preleva solo gli IPv6 di un singolo ticket



API TASK MANAGER Provider Account Provider

 V2.0.08

GENERAL

- Dashboard
- Tickets
- Whitelist
- Knowledge Base

PERSONAL

- Logout

#781498deb9da405d8e5cc8a3e0a40386

Created at 17 NOV 2023 17:10

OPEN

Download All


- FQDN (TXT)
- FQDN Checksum
- IPv4 (TXT)
- IPv4 Checksum
- IPv6 (TXT)
- IPv6 Checksum

Ticket Items Details

VALUE	STATUS	TIMESTAMP	UNPROCESSED REASON	NOTE
2001:db8:3333:4444:5555:6666:7777:8888	PENDING			

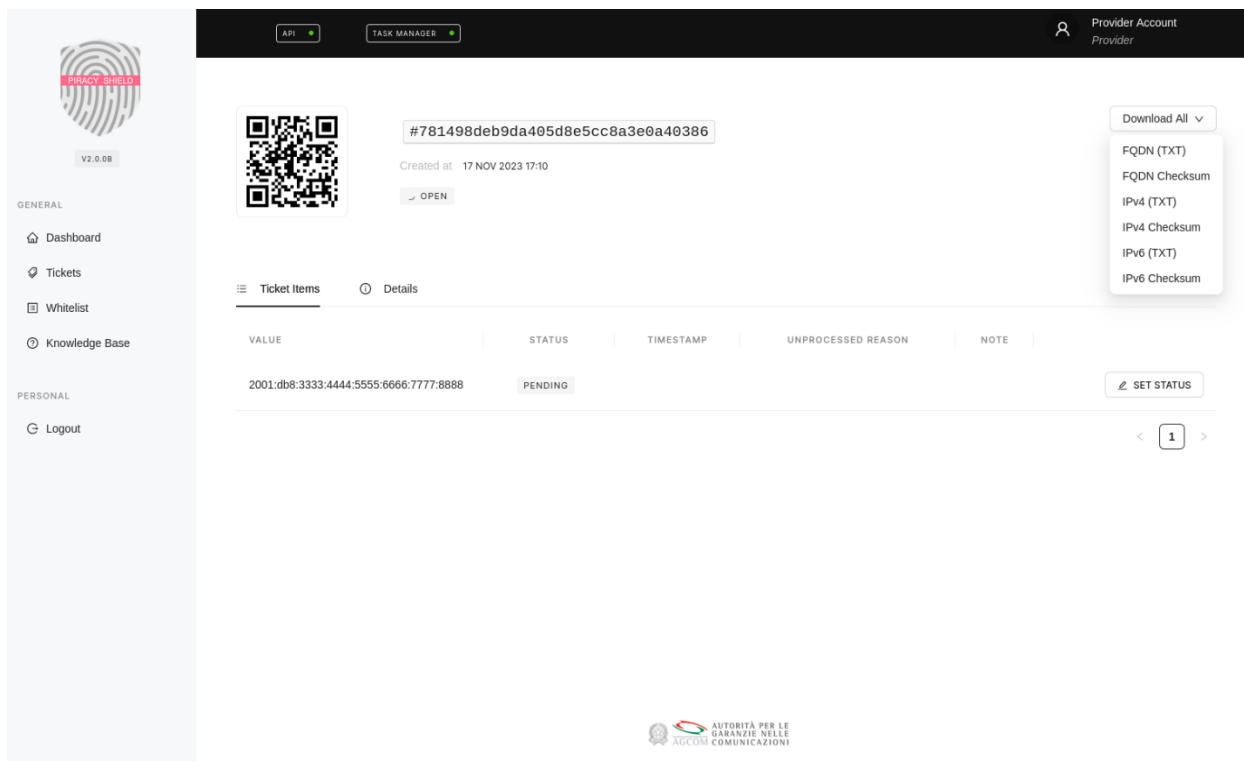
SET STATUS

1

 **AUTORITÀ PER LE
GARANZIE NELLE
AGCOM COMUNICAZIONI**

Interfaccia di gestione di un singolo ticket.

Per effettuare il download della lista degli IPv6 è FQDN è necessario cliccare sull'ID del ticket e poi cliccare in alto a destra sulla voce "Download All".



The screenshot shows the PIRACY SHIELD interface for managing a single ticket. The top navigation bar includes 'API' and 'TASK MANAGER' buttons, and a 'Provider Account' dropdown. The main content area features a QR code, a ticket ID (#781498deb9da405d0e5cc8a3e0a40386), and a 'Created at' timestamp of 17 NOV 2023 17:10. A 'Download All' dropdown menu is open, showing options for FQDN (TXT), FQDN Checksum, IPv4 (TXT), IPv4 Checksum, IPv6 (TXT), and IPv6 Checksum. Below the dropdown, a table displays a single ticket item with a 'PENDING' status and a 'SET STATUS' button. The table has columns for VALUE, STATUS, TIMESTAMP, UNPROCESSED REASON, and NOTE.

Interfaccia di gestione di un singolo ticket, voce "Download All".

Da questo menù a tendina sarà possibile selezionare IPv6 per scaricare la lista in formato TXT ed, eventualmente, il suo relativo checksum. (file di hash che permette di garantire l'inalterabilità del dato fornito).

Ticket Item

Preleva tutti gli FQDN di tutti i ticket



API TASK MANAGER Test Provider Provider

Tickets

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

Download All

TICKET ID	STATUS	GROUP	CREATED BY	CREATED AT
#1594ee460acf470bb615a27765252c58	CLOSED	GENERAL	Test Reporter	22 SEPT 2023 09:16
#528a0091aa6244339444fb270069c9e7	CLOSED	GENERAL	Test Reporter	22 SEPT 2023 16:58

< 1 2 >

Interfaccia di gestione dei ticket.

Per effettuare il download della lista di tutti gli FQDN presenti nella piattaforma è necessario posizionarsi nell'interfaccia di gestione di tutti i ticket presenti nella piattaforma e cliccare in alto a destra sulla voce "Download All".

API TASK MANAGER Test Provider Provider

Tickets

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

Download All ▾
FQDN (TXT)
FQDN Checksum
IPv4 (TXT)
IPv4 Checksum

TICKET ID	STATUS	GROUP	CREATED BY	CREATED AT
#1594ee460acf470bb615a27765252c58	CLOSED	GENERAL	Test Reporter	22 SEPT 2023 09:16
#528a0091aa6244339444fb270069c9e7	CLOSED	GENERAL	Test Reporter	22 SEPT 2023 16:58

< 1 2 >

Interfaccia di gestione dei ticket, voce "Download All".

Da questo menù a tendina sarà possibile selezionare FQDN per scaricare la lista completa in formato TXT ed, eventualmente, il suo relativo checksum. (file di hash che permette di garantire l'inalterabilità del dato fornito).



Preleva tutti gli IPv4 di tutti i ticket



API TASK MANAGER Test Provider Provider

Tickets

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

Download All

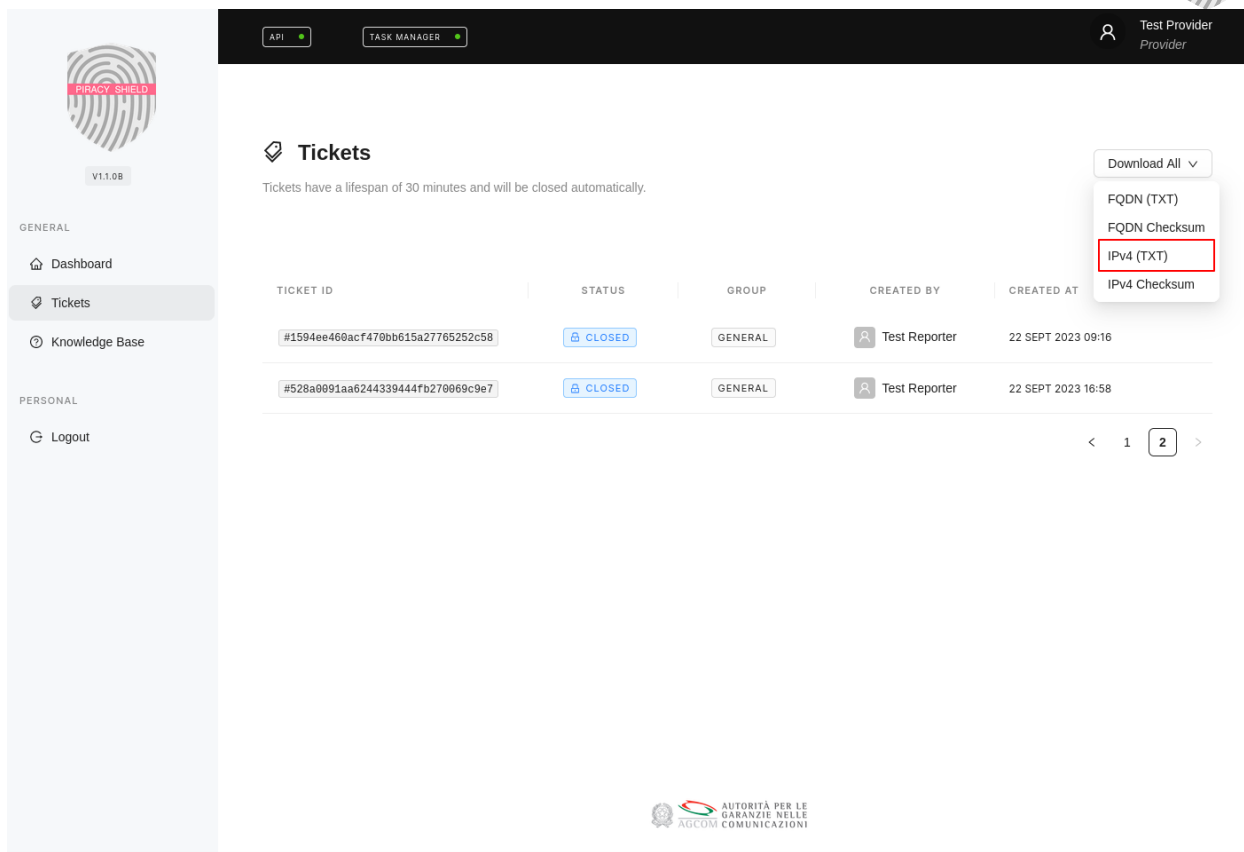
TICKET ID	STATUS	GROUP	CREATED BY	CREATED AT
#1594ee460acf470bb615a27765252c58	CLOSED	GENERAL	Test Reporter	22 SEPT 2023 09:16
#528a0091aa6244339444fb270069c9e7	CLOSED	GENERAL	Test Reporter	22 SEPT 2023 16:58

< 1 2 >

AUTORITÀ PER LE
GARANZIE NELLE
AGCOM COMUNICAZIONI

Interfaccia di gestione dei ticket.

Per effettuare il download della lista di tutti gli IPv4 presenti nella piattaforma è necessario posizionarsi nell'interfaccia di gestione di tutti i ticket presenti nella piattaforma e cliccare in alto a destra sulla voce "Download All".



API TASK MANAGER Test Provider Provider

Tickets


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

Download All

- FQDN (TXT)
- FQDN Checksum
- IPv4 (TXT)**
- IPv4 Checksum

TICKET ID	STATUS	GROUP	CREATED BY	CREATED AT
#1594ee460acf470bb615a27765252c58	CLOSED	GENERAL	Test Reporter	22 SEPT 2023 09:16
#528a0091aa6244339444fb270069c9e7	CLOSED	GENERAL	Test Reporter	22 SEPT 2023 16:58

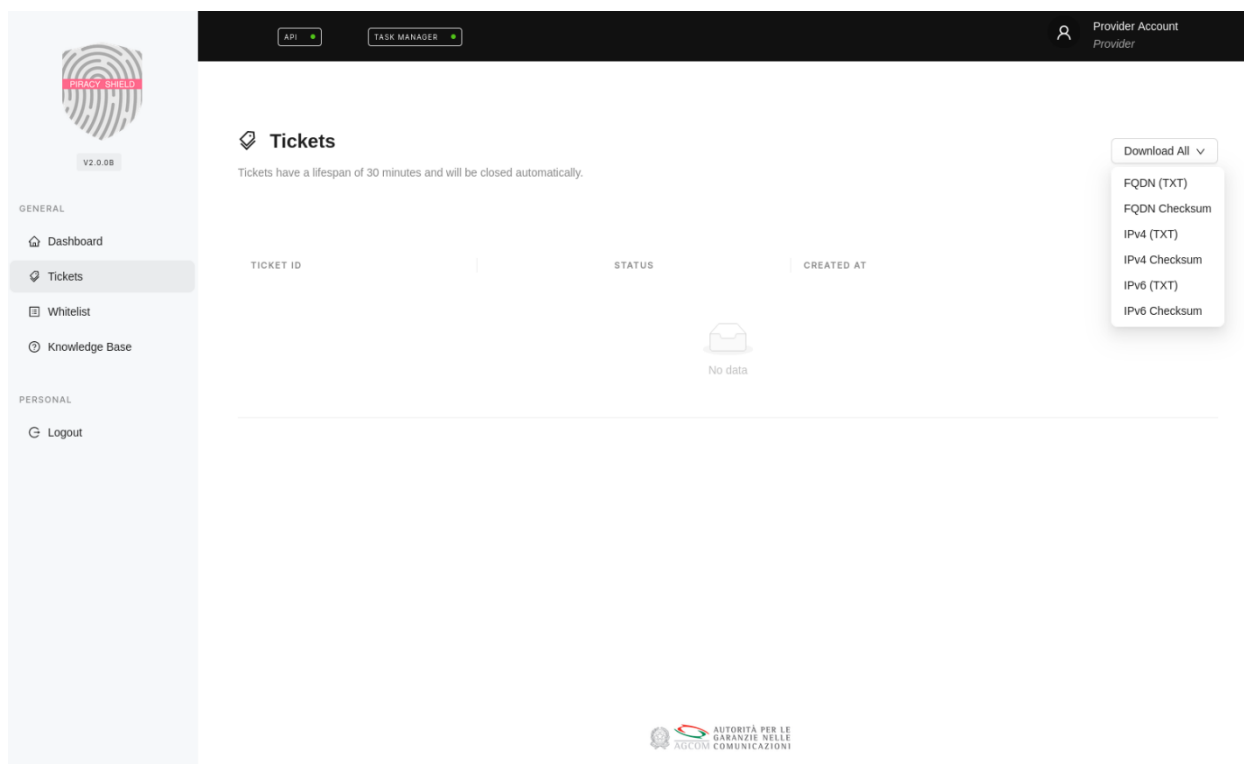
1 2


 AUTORITÀ PER LE
 GARANZIE NELLE
 AGCOM COMUNICAZIONI

Interfaccia di gestione dei ticket, voce "Download All".

Da questo menù a tendina sarà possibile selezionare IPv4 per scaricare la lista completa in formato TXT ed, eventualmente, il suo relativo checksum. (file di hash che permette di garantire l'inalterabilità del dato fornito).

Preleva tutti gli IPv6 di tutti i ticket



Tickets

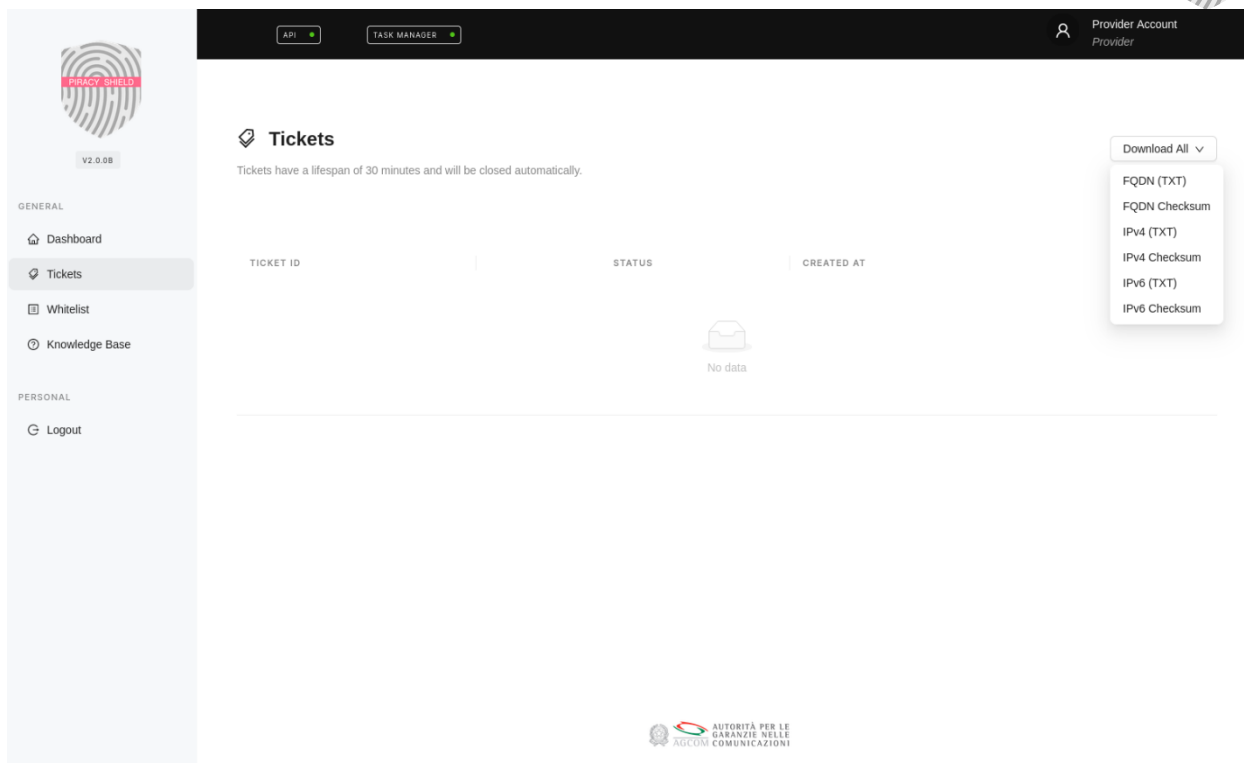
Tickets have a lifespan of 30 minutes and will be closed automatically.

TICKET ID	STATUS	CREATED AT
No data		

- Download All
- FQDN (TXT)
- FQDN Checksum
- IPv4 (TXT)
- IPv4 Checksum
- IPv6 (TXT)
- IPv6 Checksum

Interfaccia di gestione dei ticket.

Per effettuare il download della lista di tutti gli IPv6 presenti nella piattaforma è necessario posizionarsi nell'interfaccia di gestione di tutti i ticket presenti nella piattaforma e cliccare in alto a destra sulla voce "Download All".



Tickets

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

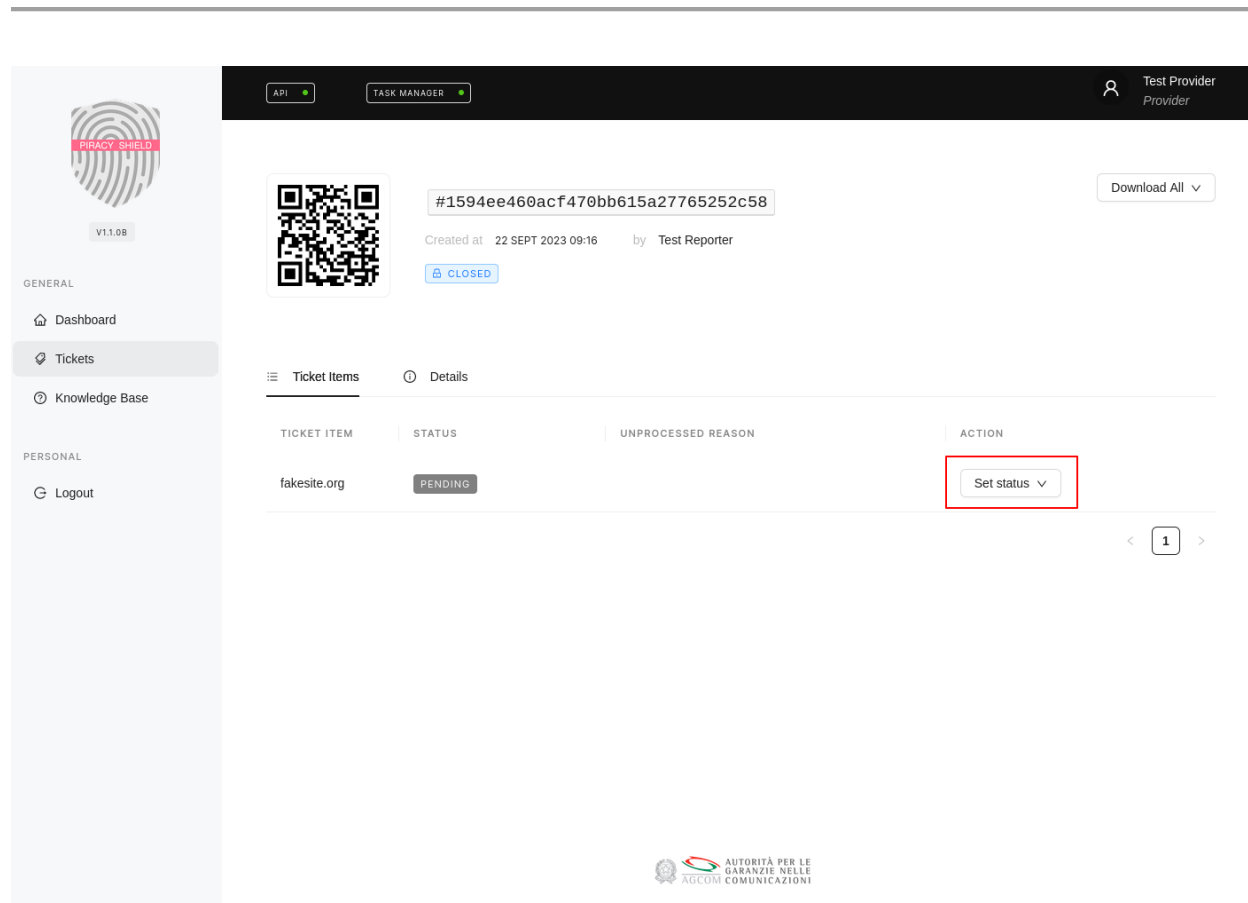
TICKET ID	STATUS	CREATED AT
No data		

- Download All ▾
- FQDN (TXT)
- FQDN Checksum
- IPv4 (TXT)
- IPv4 Checksum
- IPv6 (TXT)
- IPv6 Checksum

Interfaccia di gestione dei ticket, voce "Download All".

Da questo menù a tendina sarà possibile selezionare IPv6 per scaricare la lista completa in formato TXT ed, eventualmente, il suo relativo checksum. (file di hash che permette di garantire l'inalterabilità del dato fornito).

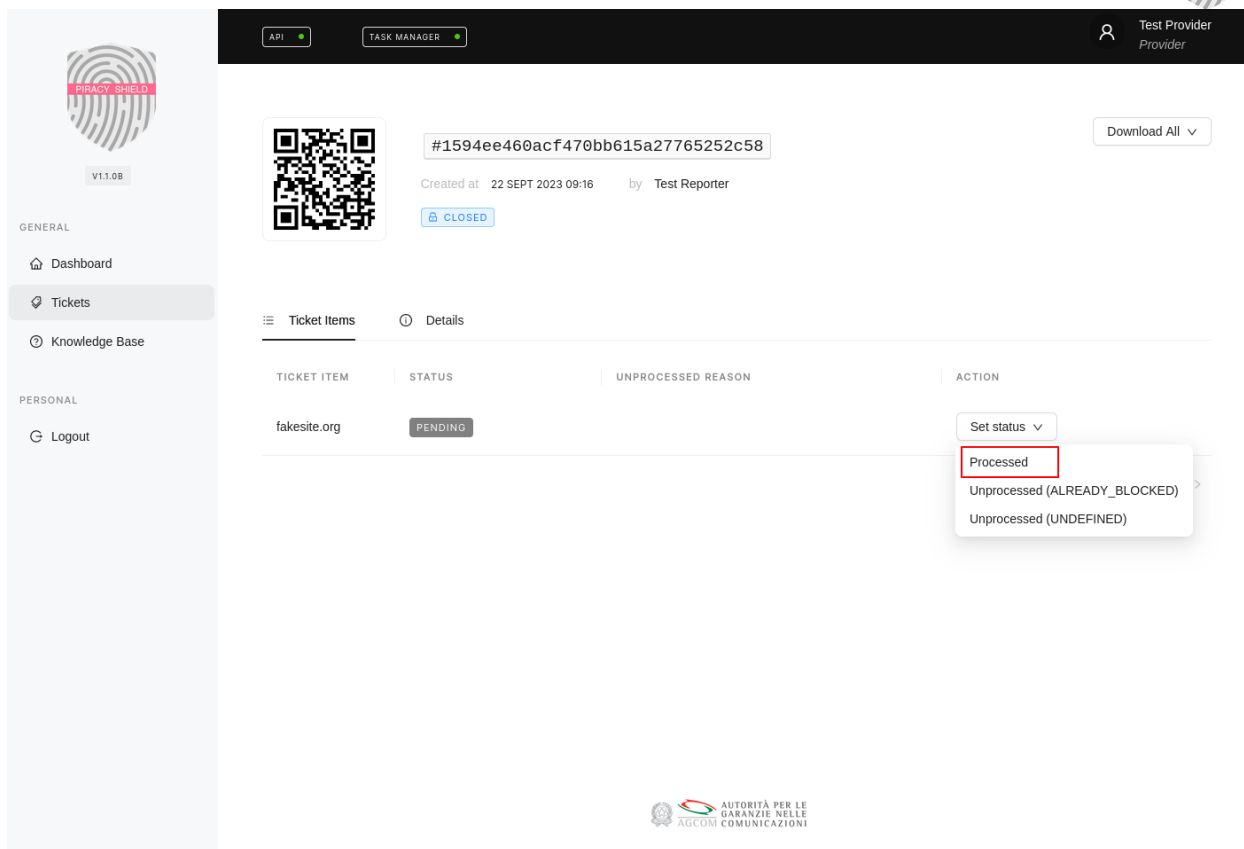
Impostare lo stato del dato



The screenshot displays the PIRACY SHIELD interface. On the left is a sidebar with navigation options: Dashboard, Tickets, Knowledge Base, and Logout. The main content area shows a ticket item with a QR code, a unique ID (#1594ee460acf470bb615a27765252c58), and a 'CLOSED' status. Below this is a table of ticket items. The table has columns for 'TICKET ITEM', 'STATUS', 'UNPROCESSED REASON', and 'ACTION'. A single row is visible with 'fakesite.org' as the ticket item and 'PENDING' as the status. The 'ACTION' column for this row contains a dropdown menu labeled 'Set status', which is highlighted with a red box. The interface also includes a 'Download All' button and a pagination control showing '1'.

Interfaccia di gestione dei ticket.

Per impostare lo stato di un singolo ticket item è possibile cliccare su "Set status".



API TASK MANAGER Test Provider Provider

Download All

#1594ee460acf470bb615a27765252c58

Created at 22 SEPT 2023 09:16 by Test Reporter

CLOSED

Ticket Items Details

TICKET ITEM	STATUS	UNPROCESSED REASON	ACTION
fakeite.org	PENDING		Set status Processed Unprocessed (ALREADY_BLOCKED) Unprocessed (UNDEFINED)

AUTORITÀ PER LE
GARANZIE NELLE
AGCOM COMUNICAZIONI

Interfaccia di gestione dei ticket, voce "Set status".

Da questo menù a tendina sarà possibile selezionare lo stato relativo al ticket item. In questo esempio verrà selezionato lo stato "Processed". Sarà possibile inserire anche lo stato del dato non processato con una motivazione preconfigurata o scrivendola in un campo note messo a disposizione tra le opzioni del menu a tendina.



API TASK MANAGER Test Provider

PIRACY SHIELD V1.1.08

GENERAL

- Dashboard
- Tickets
- Knowledge Base

PERSONAL

- Logout

#1594ee460acf470bb615a27765252c58

Created at 22 SEPT 2023 09:16 by Test Reporter

CLOSED

Download All

Ticket Items Details

TICKET ITEM	STATUS	UNPROCESSED REASON	ACTION
fakesite.org	PROCESSED		Set status

< 1 >

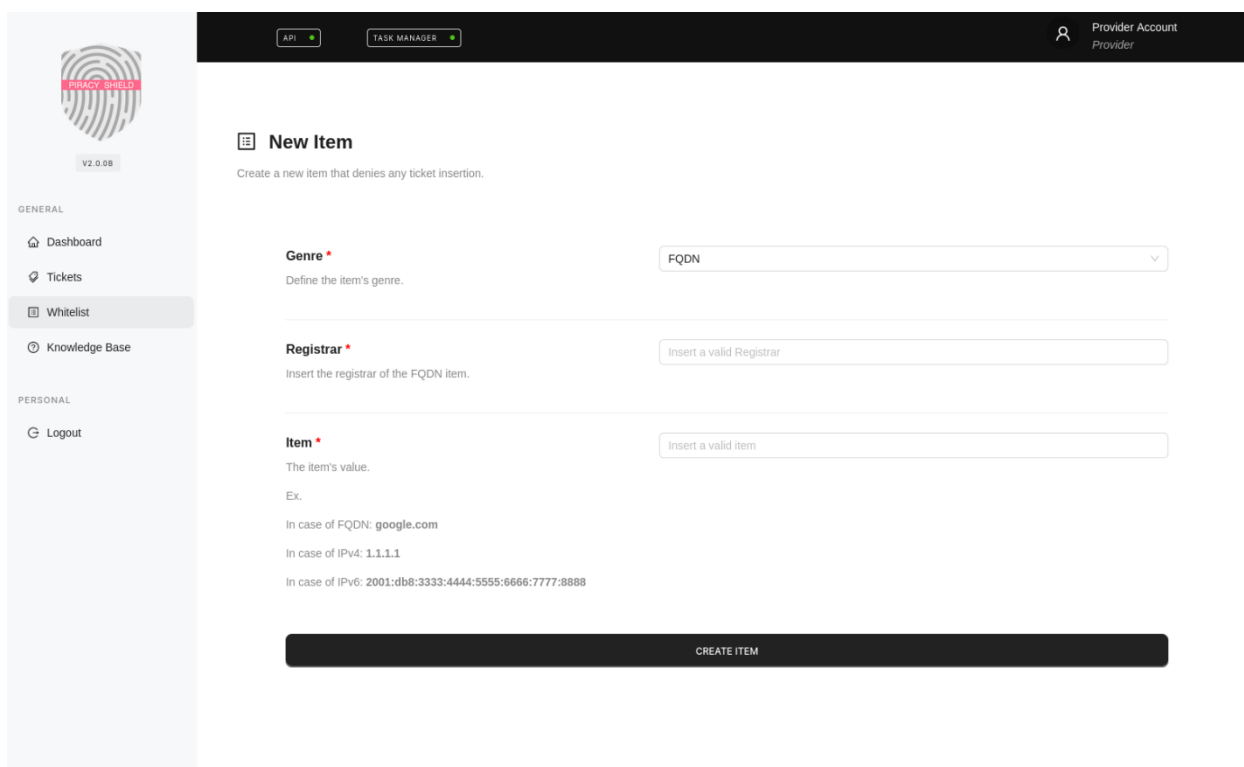
AUTORITÀ PER LE
GARANZIE NELLE
AGCOM COMUNICAZIONI

Interfaccia di gestione dei ticket, cambio di stato del ticket item.

E' possibile notare il cambio di stato evidenziato da "Pending" a "Processed".

Whitelist

Inserire un dato in whitelist

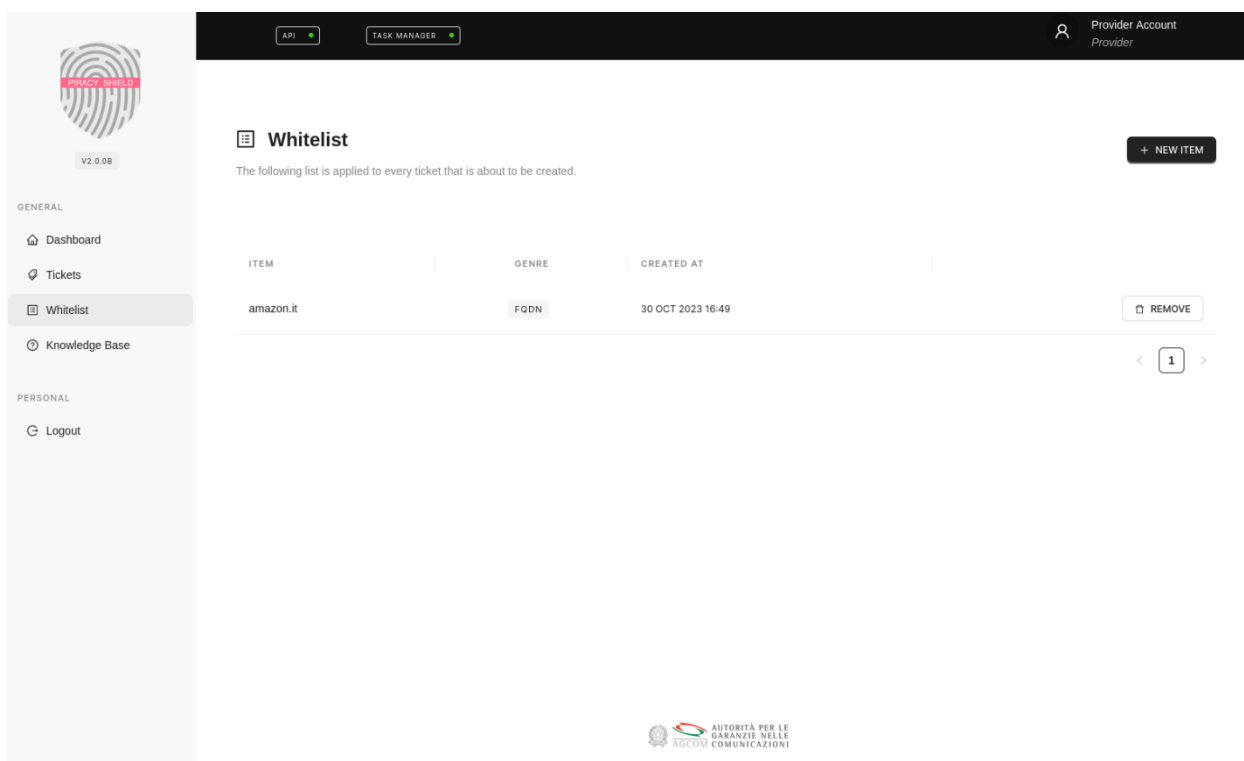


The screenshot shows the 'New Item' form in the PIRACY SHIELD interface. The interface includes a top navigation bar with 'API' and 'TASK MANAGER' buttons, and a user profile section for 'Provider Account' and 'Provider'. A left sidebar contains navigation links for 'Dashboard', 'Tickets', 'Whitelist', and 'Knowledge Base', along with a 'Logout' option. The main content area is titled 'New Item' and contains three input fields: 'Genre' (a dropdown menu with 'FQDN' selected), 'Registrar' (a text input field with the placeholder 'Insert a valid Registrar'), and 'Item' (a text input field with the placeholder 'Insert a valid item'). Below the 'Item' field, there are examples: 'Ex.', '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'. A 'CREATE ITEM' button is located at the bottom of the form.

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 o IPV4 con il relativo ASN di riferimento o IPV6 con il relativo ASN di riferimento.

Visualizzare tutti i dati presenti nella whitelist della propria utenza



The screenshot shows the PIRACY SHIELD interface. On the left is a sidebar with a 'PIRACY SHIELD' logo and version 'V2.0.08'. Below the logo are sections for 'GENERAL' (Dashboard, Tickets, Whitelist, Knowledge Base) and 'PERSONAL' (Logout). The main content area has a top navigation bar with 'API' and 'TASK MANAGER' buttons, and a 'Provider Account' section. The 'Whitelist' section is active, showing a table with the following data:

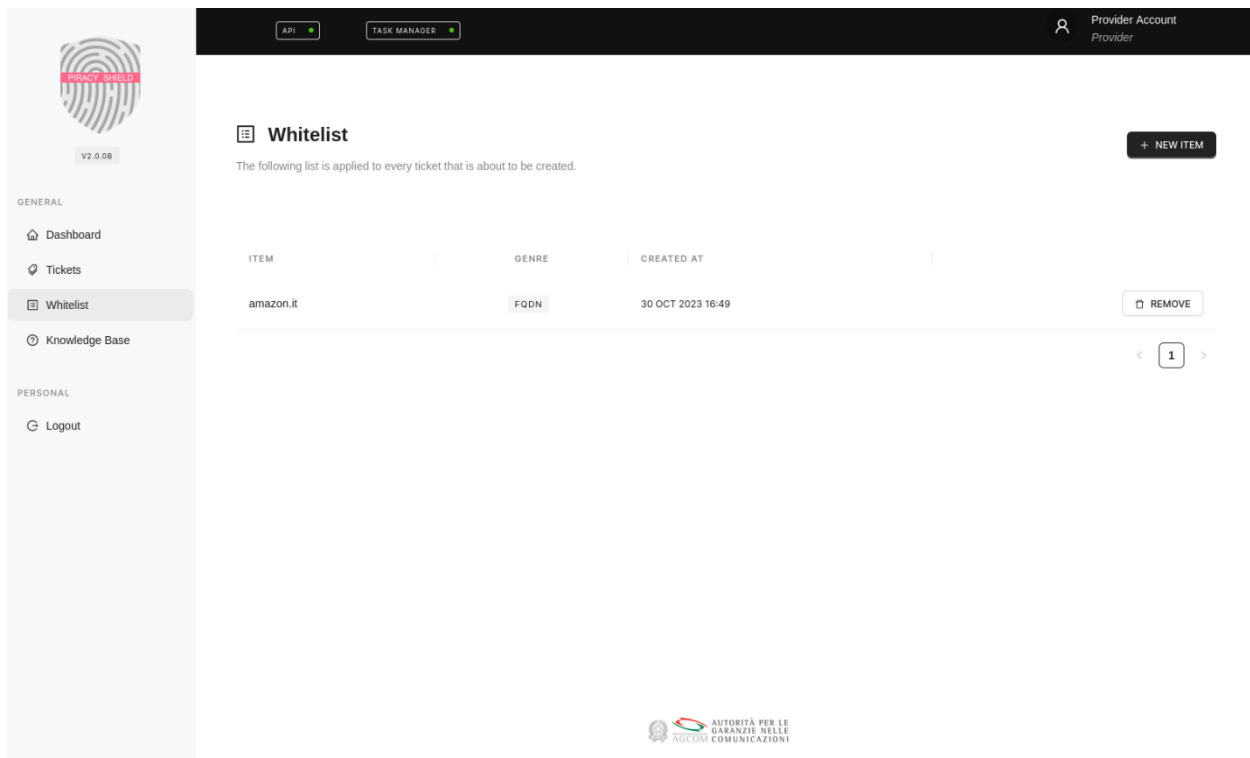
ITEM	GENRE	CREATED AT	
amazon.it	FQDN	30 OCT 2023 16:49	REMOVE

At the bottom of the page is the AGCOM logo and text: 'AUTORITÀ PER LE GARANZIE NELLE AGCOM COMUNICAZIONI'.

Interfaccia di per visualizzare dati in whitelist.

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

Rimuovere dati dalla whitelist



The screenshot displays the PIRACY SHIELD user interface. At the top, there is a navigation bar with 'API' and 'TASK MANAGER' buttons, and a user profile section for 'Provider Account' and 'Provider'. The main content area is titled 'Whitelist' and includes a '+ NEW ITEM' button. Below the title, a table lists the whitelisted items. The table has columns for 'ITEM', 'GENRE', and 'CREATED AT'. One item is listed: 'amazon.it' with genre 'FQDN' and creation date '30 OCT 2023 16:49'. A 'REMOVE' button is located to the right of this item. A pagination indicator shows '1' items. The left sidebar contains navigation options under 'GENERAL' (Dashboard, Tickets, Whitelist, Knowledge Base) and 'PERSONAL' (Logout). The AGCOM logo is visible at the bottom center of the page.

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



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.

12.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 due token JSON Web Token (JWT), che potranno essere utilizzato per autorizzare le richieste successive verso altri endpoint.

Endpoint	Metodo
/api/v1/authentication/login	POST

ESEMPIO

REQUEST BODY

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

RESPONSE 200 OK

```
{  
  "status": "success",  
  "data": {  
    "access_token": "eyJhbGc..."  
    "refresh_token": "abnbDc..."  
  }  
}
```

}

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": "eyJhbBc...",  
}
```

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.
- Si consiglia di eliminare eventuali token di accesso o token di aggiornamento memorizzati sul lato client dopo aver eseguito l'operazione di logout.

Ticket

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...",  
    "fqdn": [  
      "example.com",  
      "subdomain.example.com"  
    ],  
    "ipv4": [  
      "1.2.3.4",  
      "4.3.2.1"  
    ],  
    "ipv6": [  
      "d705:0224:2c73:d1ae:d05c:73c2:4059:33d5",  
      "2399:3764:3d84:071e:909b:ec8b:448e:2913"  
    ],  
    "status": "open",  
    "metadata": {  
      "created_at": "2023-05-01T15:00:00.526108"  
    }  
  }  
}
```

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.

Preleva tutti i dati di tutti i ticket

Questo API endpoint restituisce tutti i dati di tutti i ticket presenti in piattaforma.

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

ESEMPIO

RESPONSE 200 OK

```
{
  "status": "success",
  "data": [
    {
      "ticket_id": "c61f694...",
      "status": "open",
      "fqdn": [
        "example.com",

```

```
    "subdomain.example.com"
  ],
  "ipv4": [
    "1.2.3.4",
    "4.3.2.1"
  ],
  "ipv6": [
    "d705:0224:2c73:d1ae:d05c:73c2:4059:33d5",
    "2399:3764:3d84:071e:909b:ec8b:448e:2913"
  ],
  "metadata": {
    "created_at": "2023-11-17T17:10:07.749601+01:00"
  }
}
]
```

NOTE

- La lista dei ticket restituita rappresenta tutti i ticket disponibili nel sistema.

Preleva solo gli FQDN di un singolo ticket

Questo API endpoint restituisce la lista di tutti gli FQDN associati ad un determinato ticket.

Endpoint	Metodo
/api/v1/ticket/get/fqdn	POST

ESEMPIO

REQUEST BODY
{

```
  "ticket_id": "c61f694..."  
}
```

RESPONSE 200 OK

```
{  
  "status": "success",  
  "data": [  
    "example.com",  
    "subdomain.example.com"  
  ]  
}
```

Preleva solo gli FQDN di un singolo ticket in formato TXT

Questo API endpoint restituisce la lista di tutti gli FQDN associati ad un determinato ticket in formato TXT.

Endpoint	Metodo
<code>/api/v1/ticket/get/fqdn/txt</code>	POST

ESEMPIO

REQUEST BODY

```
{  
  "ticket_id": "c61f694..."  
}
```

RESPONSE 200 OK

```
example.com  
subdomain.example.com
```

Preleva checksum del formato TXT

Questo API endpoint restituisce il checksum della lista di tutti gli FQDN associati ad un determinato ticket in formato TXT. Il suo utilizzo è previsto per verificare la corretta ricezione della precedente lista TXT degli FQDN.

Endpoint	Metodo
/api/v1/ticket/get/fqdn/txt/checksum	POST

ESEMPIO

REQUEST BODY

```
{
```

```
“ticket_id”: “c61f694...”  
}
```

RESPONSE 200 OK
19e7c45... fqdn.txt

Preleva solo gli IPv4 di un singolo ticket

Questo API endpoint restituisce la lista di tutti gli IPv4 associati ad un determinato ticket.

Endpoint	Metodo
/api/v1/ticket/get/ipv4	POST

ESEMPIO

REQUEST BODY

```
{  
  "ticket_id": "c61f694..."  
}
```

RESPONSE 200 OK

```
{  
  "status": "success",  
  "data": [  
    "1.2.3.4",  
    "9.8.7.6"  
  ]  
}
```

Preleva solo gli IPv4 di un singolo ticket in formato TXT

Questo API endpoint restituisce la lista di tutti gli IPv4 associati ad un determinato ticket in formato TXT.

Endpoint	Metodo
<code>/api/v1/ticket/get/ipv4/txt</code>	POST

ESEMPIO

REQUEST BODY

```
{  
  "ticket_id": "c61f694..."  
}
```

RESPONSE 200 OK

```
1.2.3.4  
9.8.7.6
```

Preleva checksum del formato TXT

Questo API endpoint restituisce il checksum della lista di tutti gli IPv4 associati ad un determinato ticket in formato TXT. Il suo utilizzo è previsto per verificare la corretta ricezione della precedente lista TXT degli IPv4.

Endpoint	Metodo
<code>/api/v1/ticket/get/ipv4/txt/checksum</code>	POST

ESEMPIO

REQUEST BODY

```
{  
  "ticket_id": "c61f694..."  
}
```

RESPONSE 200 OK

```
9ea9b6b... ipv4.txt
```

Preleva solo gli IPv6 di un singolo ticket

Questo API endpoint restituisce la lista di tutti gli IPv6 associati ad un determinato ticket.

Endpoint	Metodo
/api/v1/ticket/get/ipv6	POST

ESEMPIO

REQUEST BODY

```
{  
  "ticket_id": "c61f694..."  
}
```

RESPONSE 200 OK

```
{  
  "status": "success",  
  "data": [  
    "1050:0000:0000:0000:0005:0600:300c:326b",  
    "2050:0000:0000:0000:0005:0600:300c:326b"  
  ]  
}
```

Preleva solo gli IPv6 di un singolo ticket in formato TXT

Questo API endpoint restituisce la lista di tutti gli IPv6 associati ad un determinato ticket in formato TXT.

Endpoint	Metodo
<code>/api/v1/ticket/get/ipv6/txt</code>	POST

ESEMPIO

REQUEST BODY

```
{  
  "ticket_id": "c61f694..."  
}
```

RESPONSE 200 OK

```
1050:0000:0000:0000:0005:0600:300c:326b  
2050:0000:0000:0000:0005:0600:300c:326b
```

Preleva checksum del formato TXT

Questo API endpoint restituisce il checksum della lista di tutti gli IPv6 associati ad un determinato ticket in formato TXT. Il suo utilizzo è previsto per verificare la corretta ricezione della precedente lista TXT degli IPv6.

Endpoint	Metodo
<code>/api/v1/ticket/get/ipv6/txt/checksum</code>	POST

ESEMPIO

REQUEST BODY

```
{  
  "ticket_id": "c61f694..."  
}
```

RESPONSE 200 OK

```
9ea9b6b... ipv6.txt
```


Ticket Item

Preleva tutti gli FQDN di tutti i ticket

Questo API endpoint restituisce la lista totale di tutti gli FQDN associati a tutti i ticket presenti in piattaforma.

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

ESEMPIO

RESPONSE 200 OK

```
{
  "status": "success",
  "data": [
    "example.com",
    "subdomain.example.com"
  ]
}
```

Preleva solo tutti gli FQDN di tutti i ticket in formato TXT

Questo API endpoint restituisce la lista totale di tutti gli FQDN associati a tutti i ticket disponibili in formato TXT.

Endpoint	Metodo
<code>/api/v1/fqdn/get/all/txt</code>	GET

ESEMPIO

RESPONSE 200 OK
example.com
subdomain.example.com

Preleva checksum del formato TXT

Questo API endpoint restituisce il checksum del formato TXT della lista totale di tutti gli FQDN associati a tutti i ticket disponibili. Il suo utilizzo è previsto per verificare la corretta ricezione della precedente lista TXT.

Endpoint	Metodo
<code>/api/v1/fqdn/get/all/txt/checksum</code>	GET

ESEMPIO

RESPONSE 200 OK
19e7c45... fqdn.txt

Preleva tutti gli IPv4 di tutti i ticket

Questo API endpoint restituisce la lista totale di tutti gli IPv4 associati a tutti i ticket.

Endpoint	Metodo
/api/v1/ipv4/get/all	GET

ESEMPIO

RESPONSE 200 OK

```
{  
  "status": "success",  
  "data": [  

```

```
"1.2.3.4",  
"9.8.7.6"  
]  
}
```

Preleva tutti gli IPv4 di tutti i ticket in formato TXT

Questo API endpoint restituisce la lista totale di tutti gli IPv4 associati a tutti i ticket disponibili in formato TXT.

Endpoint	Metodo
/api/v1/ipv4/get/all/txt	GET

ESEMPIO

RESPONSE 200 OK

1.2.3.4

9.8.7.6

Preleva checksum del formato TXT

Questo API endpoint restituisce il checksum del formato TXT della lista totale di tutti gli IPv4 associati a tutti i ticket disponibili. Il suo utilizzo è previsto per verificare la corretta ricezione della precedente lista TXT.

Endpoint

Metodo

/api/v1/ipv4/get/all/txt/checksum

GET

ESEMPIO

RESPONSE 200 OK
9ea9b6b... ipv4.txt

Preleva tutti gli IPv6 di tutti i ticket

Questo API endpoint restituisce la lista totale di tutti gli IPv6 associati a tutti i ticket.

Endpoint	Metodo
<code>/api/v1/ipv6/get/all</code>	GET

ESEMPIO

RESPONSE 200 OK

```
{
  "status": "success",
  "data": [
    "1050:0000:0000:0000:0005:0600:300c:326b",
    "2050:0000:0000:0000:0005:0600:300c:326b",
    ...
  ]
}
```


Preleva tutti gli IPv6 di tutti i ticket in formato TXT

Questo API endpoint restituisce la lista totale di tutti gli IPv6 associati a tutti i ticket disponibili in formato TXT.

Endpoint	Metodo
<code>/api/v1/ipv6/get/all/txt</code>	GET

ESEMPIO

RESPONSE 200 OK

1050:0000:0000:0000:0005:0600:300c:326b

2050:0000:0000:0000:0005:0600:300c:326b

...

Preleva checksum del formato TXT

Questo API endpoint restituisce il checksum del formato TXT della lista totale di tutti gli IPv6 associati a tutti i ticket disponibili. Il suo utilizzo è previsto per verificare la corretta ricezione della precedente lista TXT.

Endpoint	Metodo
<code>/api/v1/ipv6/get/all/txt/checksum</code>	GET

ESEMPIO

RESPONSE 200 OK
a7c5e6b51b... ipv6.txt

Impostare lo stato del dato

Processato

Questo API endpoint permette all'utente di marcare un ticket item associato ad un ticket come correttamente processato.

Questa operazione può essere effettuata esclusivamente durante le 48 ore dalla creazione del ticket di blocco.

Endpoint	Metodo
<code>/api/v1/ticket/item/set/processed</code>	POST

ESEMPIO

REQUEST BODY

```
{  
  "value": "1.2.3.4"  
}
```

RESPONSE 200 OK

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

Non processato

Questo API endpoint permette all'utente di marcare un ticket item associato ad un ticket come non correttamente processato. L'invio della richiesta prevede l'utilizzo di un campo "reason" predefinito come motivazione della non avvenuta processazione.

In aggiunta, possono essere utilizzati i campi "note", per associare un testo aggiuntivo che si desidera comunicare in relazione al blocco, ed il campo "timestamp", per indicare l'ora esatta del blocco. Qualora il campo "timestamp" non fosse utilizzato, il sistema applicherà l'orario di invio della richiesta API come valore finale.

Questa operazione può essere effettuata esclusivamente durante le 48 ore dalla creazione del ticket di blocco.

Endpoint	Metodo
/api/v1/ticket/item/set/unprocessed	POST

Lista delle opzioni del campo "reason".

Motivazione	Spiegazione
ALREADY_BLOCKED	Il ticket risulta già processato sulla piattaforma.
UNDEFINED	Procedere comunque, senza indicare una motivazione valida.
UNKNOWN	Motivazione da utilizzare in caso di errori non meglio specificati.

ESEMPIO

REQUEST BODY

```
{  
  "value": "subdomain.example.com",
```

```
  "reason": "ALREADY_BLOCKED"  
}
```

RESPONSE 200 OK

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

ESEMPIO CON DATI AGGIUNTIVI

REQUEST BODY

```
{  
  "value": "subdomain.example.com",  
  "reason": "ALREADY_UNDEFINED",  
  "note": "This item has been manually marked.",  
  "timestamp": "2024-01-28T22:50Z"  
}
```

RESPONSE 200 OK

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

NOTE

- Il parametro opzionale "note" accetta i seguenti caratteri speciali: `.,- & / \$ € @`.
- Il parametro opzionale "timestamp" prevede l'uso del formato ISO 8601.
- La lista delle motivazioni sarà soggetta a futuri cambi e/o espansioni.

Ping

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

Endpoint	Metodo
/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.

Endpoint	Metodo
<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
<code>/api/v1/whitelist/item/get/all</code>	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"  
}
```