

Autenticazione e Autorizzazione

- [API](#)
 - [Endpoint di autenticazione](#)
- [Login Utente](#)
- [Logout utente](#)

API

API

Endpoint di autenticazione

API Base Url:

dev: <https://b2b-auth-service-dev.agyo.io/api>

test: <https://b2b-auth-service-test.agyo.io/api>

prod: <https://b2b-auth-service.agyo.io/api>

Swagger:

<https://b2b-auth-service-test.agyo.io/swagger-ui/index.html>

Login Utente

Il flusso di autenticazione di un utente all'interno di TS Digital si suddivide in 2 parti: **generazione di un nonce** e **generazione del token JWT**.

Generazione di un nonce

Un [nonce](#) è una stringa generata randomicamente utilizzata per assicurare l'univocità di una richiesta di login verso TS Digital. La generazione del nonce è effettuata attraverso una chiamata all'apposita API:

[POST] [/api/v3/nonces](#)

Headers

Sono richiesti gli [header standard di TS Digital](#), con l'eccezione dell'header Authorization.

Body

```
{
  "id": "mail@test.com"
}
```

- **id:** identificativo dell'utente all'interno di TS Digital. Per le utenze personali si tratta dell'indirizzo email utilizzato in fase di registrazione, per le utenze tecniche si tratta invece dell'ID fornito al momento della creazione della stessa.

Risposte

Tutte le risposte sono in formato JSON

HTTP 200

Il nonce è stato generato con successo

```
{
  "nonce": "nonce-string"
}
```

- **nonce:** il nonce generato per l'utente, da utilizzare nella chiamata di generazione del token JWT

HTTP 400

Parametro obbligatorio mancante nella richiesta

```
{
  "code": "string",
  "status": "string",
  "error": "string",
  "message": "string",
  "timestamp": "string"
}
```

HTTP 404

Non esiste alcun utente con l'ID specificato

```
{
  "code": "string",
  "status": "string",
  "error": "string",
  "message": "string",
  "timestamp": "string"
}
```

HTTP 500

Si è verificato un errore interno del server nella generazione del nonce

```
{
  "code": "string",
  "status": "string",
  "error": "string",
  "message": "string",
}
```

```
"timestamp": "string"
}
```

Generazione del token JWT

Il [token JWT](#) è il token di autenticazione utilizzato per tutte le chiamate effettuate verso i servizi di TS Digital. All'interno del token possono essere disponibili alcuni dati sull'utente loggato sul token stesso:

```
{
  "sub": "id-utente",
  "passwordExpirationDate": 32506271999999,
  "iss": "https://agyo.io",
  "tsId": "tsid@tsid.com",
  "given_name": "Name",
  "locale": "it-IT",
  "uid": "uuid-v4-identifier",
  "aud": "https://agyo.io",
  "provider": "agyo",
  "name": "Name Surname",
  "appKey": false,
  "userType": "P",
  "exp": 1600109670,
  "family_name": "Surname",
  "iat": 1600088070,
  "jti": "uuid-v4-identifier",
  "hash": "token hash"
}
```

- **sub***:** soggetto a cui fa riferimento il token. Corrisponde con la mail per le utenze personali e ad un UUIDV4 per le utenze tecniche/applicative
- **passwordExpirationDate:** unix timestamp (in millisecondi) della data di scadenza della password associata all'utente
- **iss***:** issuer del token
- **tsId:** mail dell'account Teamsystem ID associato all'utenza TS Digital, se presente
- **given_name:** nome dell'utente
- **locale:** locale dell'utente
- **uid:** identificativo univoco dell'utente all'interno di TS Digital

- **aud***:** audience bersaglio del token
- **provider:** provider che ha generato il token
- **name:** stringa che combina first_name e family_name
- **appKey:** se true, il token fa riferimento ad una utenza applicativa
- **userType:** enum che indica la tipologia di utente cui fa riferimento il token. I valori possibili sono:
 - **P:** utenza personale
 - **T:** utenza tecnica
 - **A:** utenza applicativa
- **exp:** data di scadenza del token, espressa come unix timestamp (secondi)
- **family_name:** cognome dell'utente
- **iat:** data di creazione del token, espressa come unix timestamp (secondi)
- **jti:** identificativo univoco del token
- **hash:** hash del token. Utilizzato dal servizio di autenticazione e autorizzazione per assicurare che il token non sia contraffatto.

*** **Claim presente in tutti i token.**

Il token JWT può essere generato, una volta recuperato il nonce, utilizzando la seguente API:

[\[POST\] /api/v3/tokens](#)

Headers

Sono richiesti gli [header standard di TS Digital](#), con l'eccezione dell'header Authorization.

Body

```
{
  "id": "string",
  "digest": "string",
  "resources": [
    "string"
  ]
}
```

- **id:** identificativo dell'utente all'interno di TS Digital. Per le utenze personali si tratta dell'indirizzo email utilizzato in fase di registrazione, per le utenze tecniche si tratta invece dell'ID fornito al momento della creazione della stessa.

- **digest:** digest ottenuto applicando la formula `sha256(sha256(userId + password) + nonce)`, dove:
 - *sha256* è una funzione in grado di calcolare il digest [SHA-256](#) di una data stringa
 - *userId* è l'identificativo dell'utente fornito nel parametro *id*
 - *password* è la password dell'utente
 - *nonce* il nonce recuperato tramite [l'apposita API](#)
- **resources:** (deprecato) array di risorse per le quali il token deve avere i permessi

Risposte

Tutte le risposte sono in formato JSON

HTTP 200

Il nonce è stato generato con successo

```
{
  "refreshToken": "string",
  "accessToken": "string",
  "tokenType": "Bearer"
}
```

- **refreshToken:** token utilizzabile per ottenere un nuovo accessToken. Da utilizzare al posto del parametro *digest* in questa stessa chiamata
- **accessToken:** token d'autenticazione. Utilizzabile come valore per l'header Authorization in ogni servizio di TS Digital
- **tokenType:** tipologia di token ritornato. Unico valore possibile: `Bearer`

HTTP 400

Parametro obbligatorio mancante nella richiesta

```
{
  "code": "string",
  "status": "string",
  "error": "string",
  "message": "string",
  "timestamp": "string"
}
```

HTTP 401

Il digest fornito è errato

```
{
  "code": "string",
  "status": "string",
  "error": "string",
  "message": "string",
  "timestamp": "string"
}
```

HTTP 404

Non esiste alcun utente con l'ID specificato

```
{
  "code": "string",
  "status": "string",
  "error": "string",
  "message": "string",
  "timestamp": "string"
}
```

HTTP 500

Si è verificato un errore interno del server nella generazione del token

```
{
  "code": "string",
  "status": "string",
  "error": "string",
  "message": "string",
  "timestamp": "string"
}
```

Logout utente

Tramite l'API di logout è possibile invalidare un token d'autenticazione, rendendolo inutilizzabile.

[\[DELETE\] /api/v3/tokens](#)

Headers

Sono richiesti gli [header standard di TS Digital](#), con l'eccezione dell'header Authorization.

Body

```
{
  "accessToken": "string"
}
```

- **accessToken:** il token da invalidare

Risposte

Tutte le risposte sono in formato JSON

HTTP 200

Il token è stato invalidato con successo

```
{}
```

HTTP 400

Parametro obbligatorio mancante nella richiesta o token invalido

```
{
  "code": "string",
  "status": "string",
}
```

```
"error": "string",  
"message": "string",  
"timestamp": "string"  
}
```

HTTP 500

Si è verificato un errore interno del server nella generazione del nonce

```
{  
  "code": "string",  
  "status": "string",  
  "error": "string",  
  "message": "string",  
  "timestamp": "string"  
}
```