

OBTAINING AND USING A SERVICE TOKEN FOR THE API

Overview

In January 2022 we released support for **service tokens** as a method of system-to-system API access on the Whitespace Platform. This document discusses the use of service tokens, the security principles around their use and the protocol for requesting and revoking them.

Use of Service Tokens

On request, Whitespace Support supplies JSON files named for each dedicated service account or platform user allocated a service token. The three entries in the JSON file are:

- token – the value to be passed in the Authorization: Bearer header
- kid – an identifier to be used for revoking the token
- expiry – the date of expiry for the token

```
{
  "token": "eyJ0eX...7CG27g",
  "kid": "BLACKPOOL_sally.trow.blackpool@wspt.co.uk_1648767599",
  "expiry": "2022-03-31"
}
```

To use the service token from an approved IP Address, take the token value from the JSON file and pass it in the Authorization header, prefixed with "Bearer " (include the space at the end). The following bash script extracts the token value out of a JSON file named sally.trow.blackpool in the same directory and passes it to an API call requesting user details.

```
TOKEN=$(jq -r .token sally.trow.blackpool)
curl https://sandbox.whitespace.co.uk/api/user/myDetails -H "Authorization: Bearer $TOKEN"
```

Calls using a service token may be rejected for various reasons:

- The platform user, if any, associated with the token is not set to 'Live' or 'ReadOnly' in the admin portal. ReadOnly users cannot POST calls to the API, and service accounts are not associated with platform users.
- The token has expired/been revoked
- The IP Address is not one of the allowed values

In such cases, the HTTP return code will be "401 Unauthorized" and the JSON response will be:

```
{
  "error": true,
  "reason": "Invalid WSAUTH"
}
```

Security Principles

The email address for each token needs to either be associated with a dedicated service account, or with an actual user of the platform who has been properly configured by your Whitespace Administrator via the admin portal's 'USERS' screen. Dedicated service accounts are recommended.



Note that for platform users' tokens, the user does not need to have logged in to the system for the service token to function. The user's status should be 'Live' or 'ReadOnly' – if it is 'Draft' or 'Suspended' then API calls will be rejected.

We do not issue platform user service tokens that can be used by multiple users, or tokens that can be used by a single user under multiple organisations, as doing so would break the traceability of system actions which is required by our contractual terms. Service accounts are less restricted, and have specific requirements regarding the format of the email that they are associated with. For a detailed breakdown of this format, see *Requesting a Service Token* below.

We allow an expiry date for Service Tokens as a convenience for customers. For security reasons, the maximum duration of a service token is one year to expiry. We monitor expiry dates for tokens on the PRODUCTION environment and will inform clients of pending expiry, although we advise users to also monitor expiry deadlines themselves. However, please note that we do not monitor token expiry on the SANDBOX environment, so users will need to track that information.

For service tokens for the live platform, we require specification of the IP address for the machine/s from which the API call will originate. This is to fulfil our contractual obligation to have a second authentication factor. Without it, should the token fall into the wrong hands it could be used maliciously. We can support multiple IP addresses or ranges, but we will not allow a universal range of 0.0.0.0-255.255.255.255.

If specifying an IP address or range is impossible, service tokens can still be issued for the Sandbox test environment, and limited-time user-refreshable tokens can be provided for the live platform.

Administrators and users must strictly ensure that tokens are kept confidential. Access to these files may allow another party to operate the platform fraudulently using your credentials.

Requesting a Service Token

Every token is attached to a specific email address. As mentioned above, service accounts have a specific naming format: `wssvc_COMPANYID_contact.email@youremail.domain`

- 'wssvc' is an informative string confirming that this is a Whitespace Service account.
- 'COMPANYID' is the Whitespace Platform internal System ID for your organisation, for example, 'WANTAGELTD'.
- 'contact.email' is the email address of the person at your organisation that Whitespace should contact in case of issues or changes. This must be a monitored email. For example, for sally.adams@wantage.co.uk, 'sally.adams'.

Therefore, a correctly formatted service account name would be:
`wssvc_WANTAGELTD_sally.adams@wantage.co.uk`

We do not support SUMO (Single User, Multiple Organisation) service tokens. If your organisation has multiple corporate identities on the Whitespace platform, separate tokens will be required for each one. Ensuring that service token names contain the COMPANYID field helps keep token use purposes clear.

When requesting a service token, you should email details to support@whitespace.co.uk as follows:

- The name of your organisation or, if you know it, the COMPANYID.
- The contact email at your organisation for the person monitoring the service account. If requesting user service tokens, then list the email/s required separately and in full, with no wildcards, specifying that the request is for one or more individual users. Dedicated service accounts are recommended over tokens for individual platform users.
- The Whitespace environment that the token is required for – SANDBOX for the test system or, when ready, PRODUCTION for the live platform.
- Your preferred token expiry date, up to one year away.
- The IP address/es of the machines that you will call the API from. Multiple single IPs or a reasonable range of IPs (ie. 103.89.10.34 – 103.89.21.34) are acceptable. Please note that no token will be issued for 0.0.0.0 – 255.255.255.255 or similar. IPs are not mandatory for SANDBOX tokens, but are strongly recommended.

Support will provide the token/s requested within 3 working days (GMT) in the form of a password-protected zip file containing one JSON file named for each account for whom a token was requested. The password will be sent separately as a secure email.



It is important to avoid changing the service account's details on the Platform via the admin portal without discussing the change with Support first. Doing so will prevent the service token from working. You will also need to make sure that the contact email address you select is monitored on your system, as we will need to send critical information to that account.

Service accounts do not require a platform log-in, but for individual users requiring a service token, please ensure that the user has been set up on Sandbox and set to 'Live' or 'ReadOnly'. Your internal platform administrators can do this for you via the admin portal.

Revoking a Service Token

If a token needs to be urgently revoked, please take the following steps:

1. Set the user's account, if any, to 'Suspended' in the admin portal.
2. Email support@whitespace.co.uk quoting either the "kid" value of the token to be revoked, or to revoke all of that user's tokens, the associated email address.
3. If the user, if any, still needs access to the Whitespace Platform, then set their account back to 'Live' once support confirms that the token has been revoked.

In less urgent cases, just step (2) is sufficient.

Jonathan Clarke
08 July 2024