Security and authentication

ON THIS PAGE

You must be a verified user to make API requests. You can authorize against the API using your email address and an API token, or with an OAuth access token.

Note: If you're an existing Zendesk customer and are currently using basic authentication, you can continue to use basic authentication for now. However, Zendesk recommends switching your authentication method to API tokens or OAuth tokens for improved security.

Client-side CORS requests are supported if the request is authenticated with an OAuth access token. The requests are not supported if the request uses a Zendesk API token. For more information and a tutorial, see Making cross-origin, browser-side API requests.

Topics covered in this section:

- API token
- OAuth access token
- SSL requirements

For more information, see Differences between API tokens and OAuth access tokens.

API token

API tokens are different from OAuth tokens, which are detailed in the next section. API tokens are auto-generated passwords in the Zendesk Admin Center.

Warning: As passwords, API tokens can be used to impersonate anyone in the account, including admins. Make sure to keep them secure. Delete any unused tokens. Delete a token at once if you suspect it's been compromised and create another one if necessary. Another option is to use OAuth tokens, which are described in the next section.

API tokens are managed in the Admin Center interface at **Apps and integrations** > **APIs** > **Zendesk API**. The page lets you view, add, or delete tokens. More than one token can be active at the same time. Deleting a token deactivates it permanently.

You can have up to 256 tokens. If you're at the limit, you must delete an existing token to add a new one. Accounts that currently have more than 256 tokens have a limit of 2048 tokens.

Basic authentication is used for API tokens. The credentials must be sent with the request in an Authorization header.

Use the following format for the credentials:

```
{email_address}/token:{api_token}
```

Example:

```
jdoe@example.com/token:6wiIBWbGkBMo1mRDMuVwkw1EPsNkeUj95PIz2akv
```

After base64-encoding the resulting string, add it to the Authorization header as follows:

```
Authorization: Basic

amRvZUBleGFtcGxlLmNvbS90b2tlbjo2d2lJQldiR2tCTW8xbVJETXVWd2t3MUVQc05rZVVqOTVQSXoyYWt
```

If you use curl to test different endpoints, you can use the following format:

```
curl https://obscura.zendesk.com/api/v2/users.json \
  -u jdoe@example.com/token:6wiIBWbGkBMo1mRDMuVwkw1EPsNkeUj95PIz2akv
```

If authenticating over HTTP, url-encode the slash character in `{email_address}/token` as `%2F`.

OAuth access token

The Zendesk API supports OAuth authorization flows. Learn more.

OAuth access tokens also permit client-side API requests. See Making cross-origin, browser-side API requests in the Zendesk API guide.

In your requests, specify the access token in an Authorization header as follows:

```
Authorization: Bearer {access_token}
```

Example:

```
Authorization: Bearer gErypPlm4dOVgGRvA1ZzMH5MQ3nLo8bo
```

If you use curl to test different endpoints, you can use the following format:

```
curl https://obscura.zendesk.com/api/v2/users.json \
  -H "Authorization: Bearer gErypPlm4dOVgGRvA1ZzMH5MQ3nLo8bo"
```

SSL requirements

The Zendesk v2 API an SSL-only API, regardless of how your account is configured.

All connections to the Zendesk API must support the TLS 1.2 protocol. Support for TLS 1.0 and 1.1 was removed in June 2018.

Connections to the API must also support the SNI extension to TLS.

If you connect to Zendesk through a client library, make sure it supports both TLS 1.2 and SNI.
