zendesk developers

API Basics > Authentication

Understanding the differences between API tokens and OAuth access tokens

Both API tokens and OAuth access tokens let you authenticate Zendesk API requests without providing your Zendesk password. However, the token types support different creation methods and permission setups.

For server-to-server communications where a broad permission set is appropriate, API tokens might be sufficient and easier to manage. For applications needing to act on behalf of specific users, OAuth tokens provide a more secure and targeted approach.

The following table describes some key differences between API tokens and OAuth access tokens.

Difference	API tokens	OAuth access tokens
Creation and management	Created and managed using Admin Center. See Generating a new API token in Zendesk help.	Created and managed using Zendesk API requests. However, you can create OAuth clients using Admin Center. See Registering your application with Zendesk in Zendesk help.
User association	Not associated with a specific Zendesk user. However, you must provide an email address for an admin, agent, or other valid user when authenticating requests.	Associated with a specific Zendesk user.
Permissions	Permissions are limited by the user role associated with the provided email address. This means the scope of what the token can access or change is limited by what the	Permissions are limited using scopes and the associated user's role.

Difference	API tokens	OAuth access tokens
	associated user is permitted to do within Zendesk.	
Cross-origin resource sharing (CORS) requests	Doesn't support client-side CORS requests.	Supports client-side CORS requests. See Making cross-origin, browser-side API requests.

For more information, see Security and authentication.