



Token-based Authentication

Token-based authentication is a protocol which allows users to verify their identity, and in return receive a unique access token. During the life of the token, users then access the UFM APIs that the token has been issued for, rather than having to re-enter credentials each time they need to use any UFM API.




Note

Under the Settings section there is a tab titled called “Access Tokens”.

The functionality of the added tab is to give the user the ability to create new tokens & manage the existing ones (list, copy, revoke, delete):

Access Token	Issued At	Actions
TZhcEdLFHpkRdC9DBdwK9A9iajyJ0m	2022-04-28 17:34:41	✕ 🗑️ 📄
tb5s5gfp68LeTx09m7C:FPs6DN9cqV	2022-04-28 17:34:40	✕ 🗑️ 📄
nINcqmrBgdreFhBLBG0AJV7movZgR4	2022-04-28 17:34:39	✕ 🗑️ 📄

Actions:

Name	Icon	Description
Revoke		<p>Revoke a specific token.</p> <p>Note The revoked token will no longer be valid.</p>
Delete		Delete a specific token.
Copy		Copy specific token into the clipboard.

Note

Each user is able to list and manage only the tokens that have been created by themselves. Only the users with `system_admin` role will be able to create tokens.

Copyright 2024. PDF Generated on 06/06/2024