Sites: API Keys Management

1. Sites: Overview

The Sites section in Wifox Business Content Solution is dedicated to managing API keys. These keys act as secure tokens that allow access to specific API endpoints, which are not public. API keys are essential for interacting with protected APIs and ensuring only authorized access to the system's data and functionalities. Wifox Business Content Solution has its own API, and to access its non-public endpoints, users must first create a site key within this module.

Key Features of API Key Management

1. Secure Access

API keys are used to authenticate requests to protected API endpoints, ensuring only authorized users or systems can access them.

2. Domain Binding

API keys are tied to a specific domain, restricting their use to the designated site for enhanced security.

3. Role Assignment

Each API key is associated with a specific role. The role defines the permissions granted to the key, such as viewing pages, editing content, or deleting entries.

4. Customizable Permissions

By assigning a role to an API key, you control exactly what the key can access, aligning it with your system's security and functionality needs.

Example Use Case

A developer wants to use the API to fetch pages from a website. They create an API key with the following details:

- Domain: example.com
- Full Site URL: https://www.example.com
- Role: A role with permissions to view Pages.

The Sites section in Wifox Business Content Solution is dedicated to managing API keys, which serve as secure tokens granting access to restricted API endpoints. These keys are essential for interacting with protected APIs, ensuring that only authorized users can access system data and functionalities. Wifox Business Content Solution has its own API, and to access its non-public

endpoints, users must first create a site key within this module.

> **When making API requests using site keys, it is necessary to include the following headers:**

> "x-access-type" = "site"

> "x-access-token" = (token from site key)

The developer then uses this API key in their application to securely access the page data. By binding the key to a domain and assigning a role with precise permissions, the system ensures secure and authorized access to the required functionality.

The Sites section simplifies the creation and management of API keys while providing robust security through domain binding and role-based access, ensuring that API interactions are both flexible and secure.

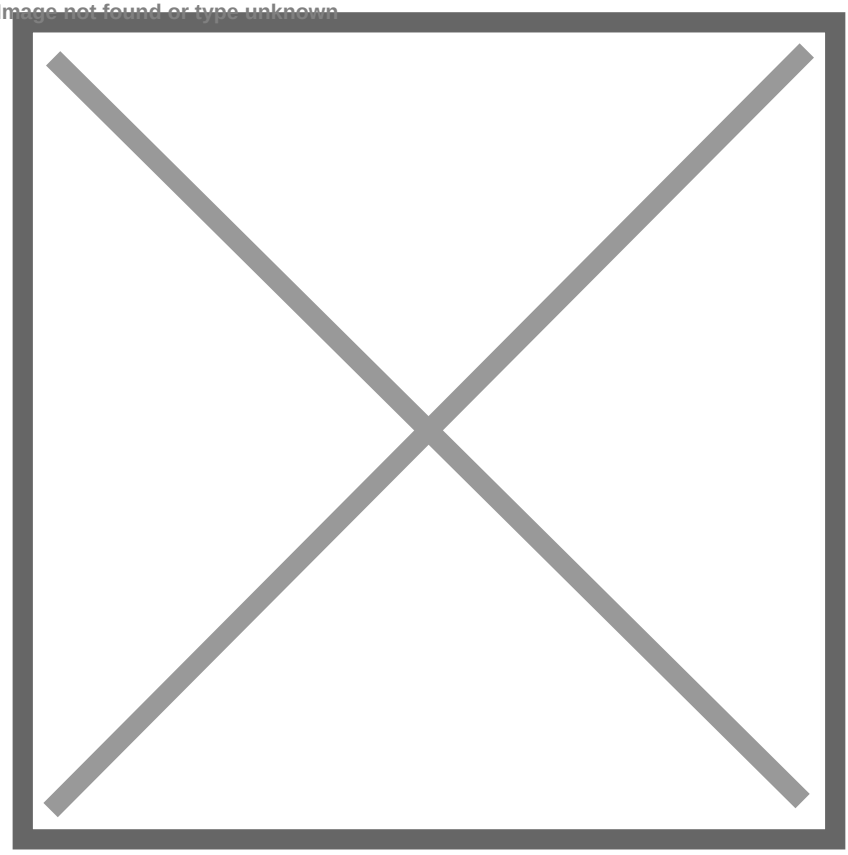
2. How to Add a New API Key

1. Click Add

In the **Sites** section, click the **Add** button to create a new API key.

2. Fill in the Details

Image not found or type unknown



Domain: Enter the domain where the API key will be used (e.g., example.com).

Full Site URL: Provide the full URL of the site (e.g., https://www.example.com).

Role: Select a role from the dropdown menu. This role determines the permissions tied to the API key, such as access to specific modules like Pages or others.

3. Save the API Key

Click **Submit** to generate the API key. Once created, this key can be used to authenticate API requests for the specified domain and role.

3. How to Edit an API Key

1. Select the API Key

Locate the API key in the Sites list and click the pencil icon to open the editing menu.

2. Update the Details

Modify the domain, full site URL, or assigned role as needed.

3. Save Changes

Click Submit to save the updates.

4. How to Delete an API Key

1. Locate the API Key

Find the API key in the **Sites** list.

2. Delete the Key

Click the **trash icon** next to the key and confirm the deletion. The API key will be permanently removed.