Migrate to 0Auth2 from authenticateUser API

Last modified on: 02/19/2025 8:18 am MST

Overview

Keap is enhancing its security for processing sensitive user authentication data. This initiative involves updating your authentication configuration to use our 0Auth2 server to authenticate a user. This update will align with our current API authentication practices managed through 0Auth2, to ensure a higher level of protection for sensitive information.

Please upgrade to a new authentication practice by August 15th, 2025. Keap is removing the DataService.authenticateUser API endpoint, so failure to complete the upgrade will lead to an interruption in your ability to authenticate user credentials.

What to check

User profile information can be found at the following endpoint:

https://api.infusionsoft.com/crm/rest/v1/oauth/connect/userinfo

If you have a third party vendor who is currently validating user credentials against the XMLRPC Data service they will need to migrate their workflow to go through 0Auth2.

Developers

If you are currently validating user credentials against this XMLRPC endpoint, you will need to migrate your workflow to go through 0Auth2.

Customers/Integrators will need to make changes to migrate their workflow for this endpoint through 0Auth2. Because they are 3rd party vendors, this authentication process should already be set up, they will just need to establish how they want to modify their process for user credentials.

Although this will require some adjustment for the integrators to manage/track token access/refresh, this will provide a better end user experience by not forcing them to login in repetitively.

You can use any framework in the language of your choice that can integrate with the 0Auth2 workflow or we have provided an example below if you wish to continue using Keap to authenticate.

How to Upgrade

Developers

If you wish to continue using Keap to authenticate into your third party application without the users needing to remember a different set of credentials, this is one way it could be done using the

Keap OAuth2 flow.

1. Set up a login page in your application to redirect the end user to the Keap OAuth Developer Authorization Page.

2. Once the user has authorized your application, you will receive an authorization code.

3. This authorization code can be used to exchange for an Access Token and Refresh Token.

4. The Access Token can be used to get a user profile by hitting the Keap UserInfo Endpoint. You will receive JSON similar to the following:

    ```json
    {
      "sub": "123",
      "email": "john.doe@acme.com",
      "given_name": "John",
      "family_name": "Doe",
      "middle_name": null,
      "global_user_id": 12345,
      "infusionsoft_id": "john.doe@acme.com",
      "preferred_name": null,
      "is_admin": true
    }
    ```

    5. Refresh Tokens last 45 days, and must be refreshed within that window to maintain authorization. Each time the Refresh Token is consumed a new Access Token valid for 24 hours will be generated that can be used to make requests as a Bearer token.

    6. Refresh Tokens must be saved somewhere on your back end for safe keeping. Once a refresh token is used it is considered stale, the refresh token that is returned must be saved for a subsequent refresh.

Questions?

Reach out here to ask experts.