NETSUITE INTEGRATION

Guide to Setting up **Token-Based Authentication** in NetSuite

This walk-thru guide will provide a step-bystep guide to getting started with token-based authentication in NetSuite.

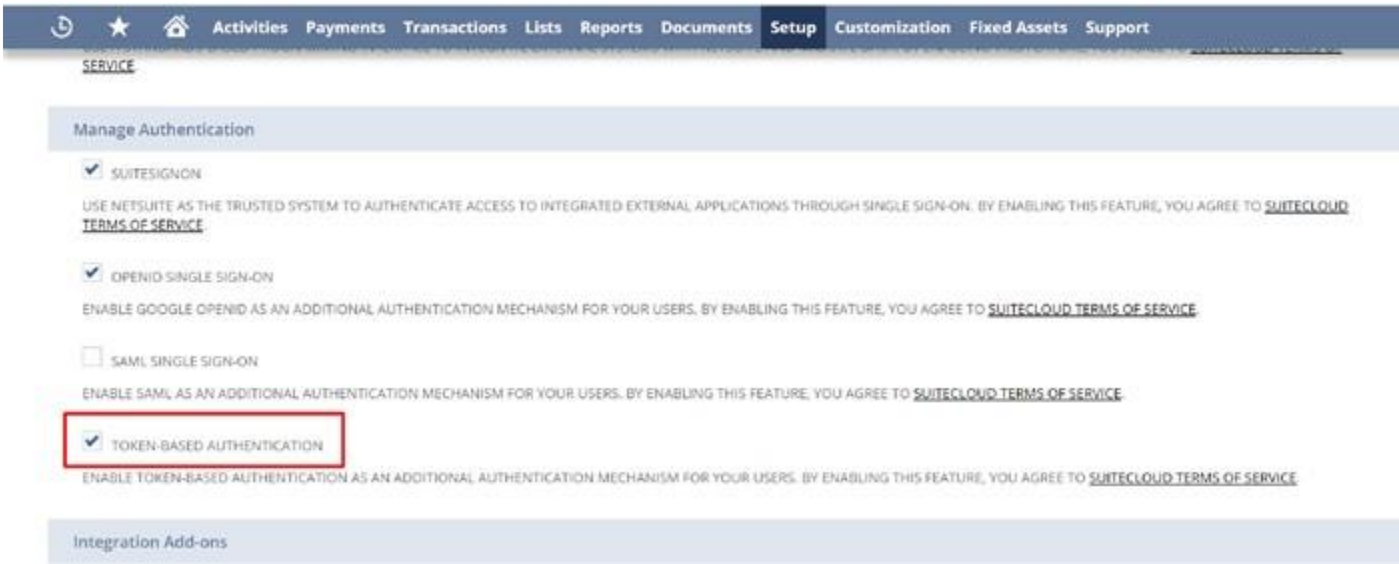
In addition, we provide a SuiteScript 2.0 example of using Token Based Authentication to make SuiteTalk calls to get/set Budget values which are not accessible via the SuiteScript API. We have also provided a python script which illlustrates how to externally connect to a RESTlet using TBA.

1.1 Enable Features

Token Based Authentication must first be enabled in the account. Under **Setup > Company > Setup Tasks > Enable Features** navigate to the SuiteCloud subtab. Enable the required features:

- Client SuiteScript (prerequisite for Server side SuiteScript)
- Server SuiteScript (prerequisite for RESTlets)

Navigate to the manage authentication section and enable the Token-based Authentication if it is not already enabled.



The configuration page must be **saved** for the changes to take effect.

1.2 Role

Token based authentication is a per user authentication and requires certain permissions in NetSuite. An existing role can be used (recommended) or a new role can be created.

The relevant role permissions are under the ‘Setup’ subtab the following details were gleaned from SuiteAnswer(41898).

Access Token Management

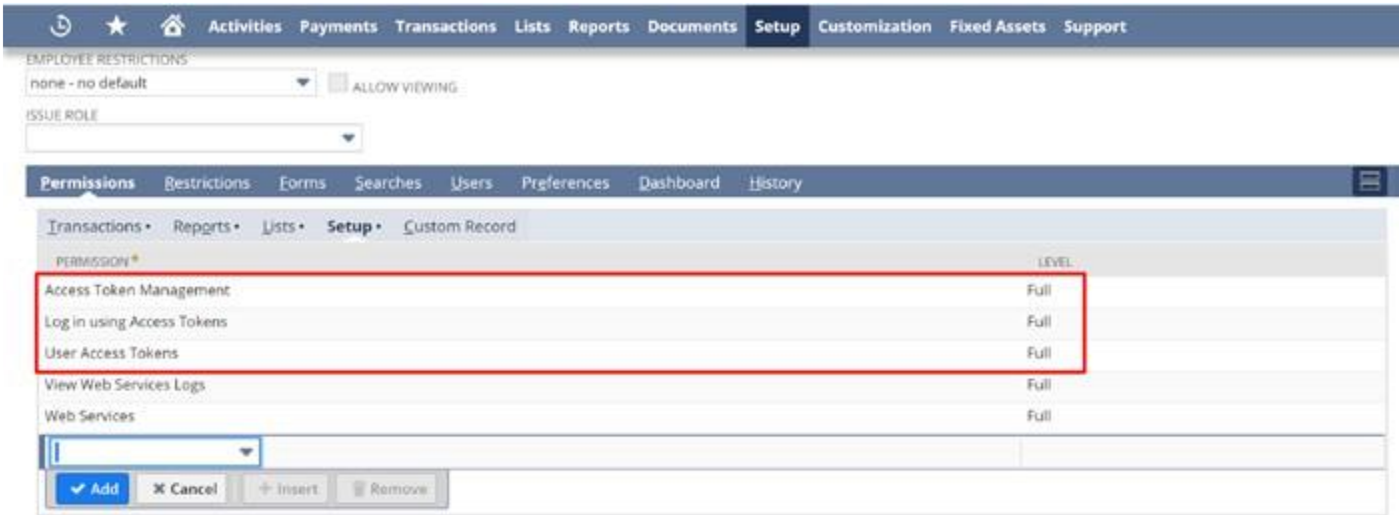
- Users with this permission can create, assign, and manage tokens for any user in the company.
- Users with this permission cannot use token–based authentication to log in to the NetSuite UI.

Log in using Access Tokens

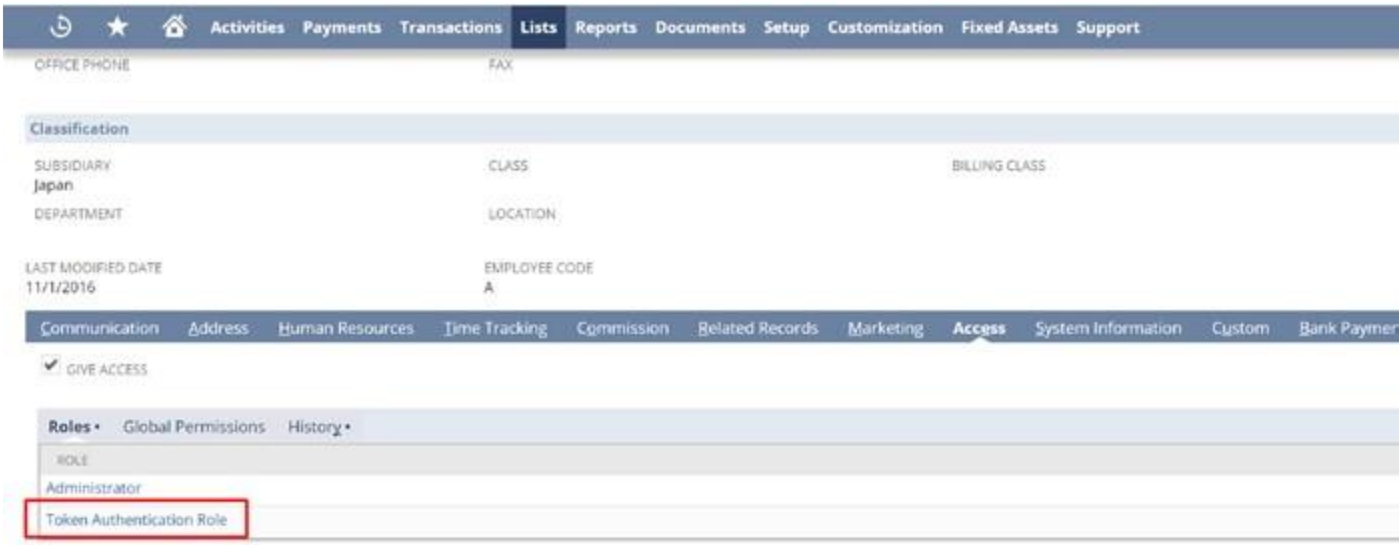
• Users with this permission can manage their own tokens using the Manage Access Tokens link in the Settings portlet, and they can log in using a token.

User Access Tokens

• Users with only this permission can log in using a token, that is, they can to use tokens to call a RESTlet.
• Users with only this permission cannot manage tokens or access pages where tokens are managed.



The Token Authentication Role will need to be assigned to all employees associated with the integration under 'Access' subtab on their employee record

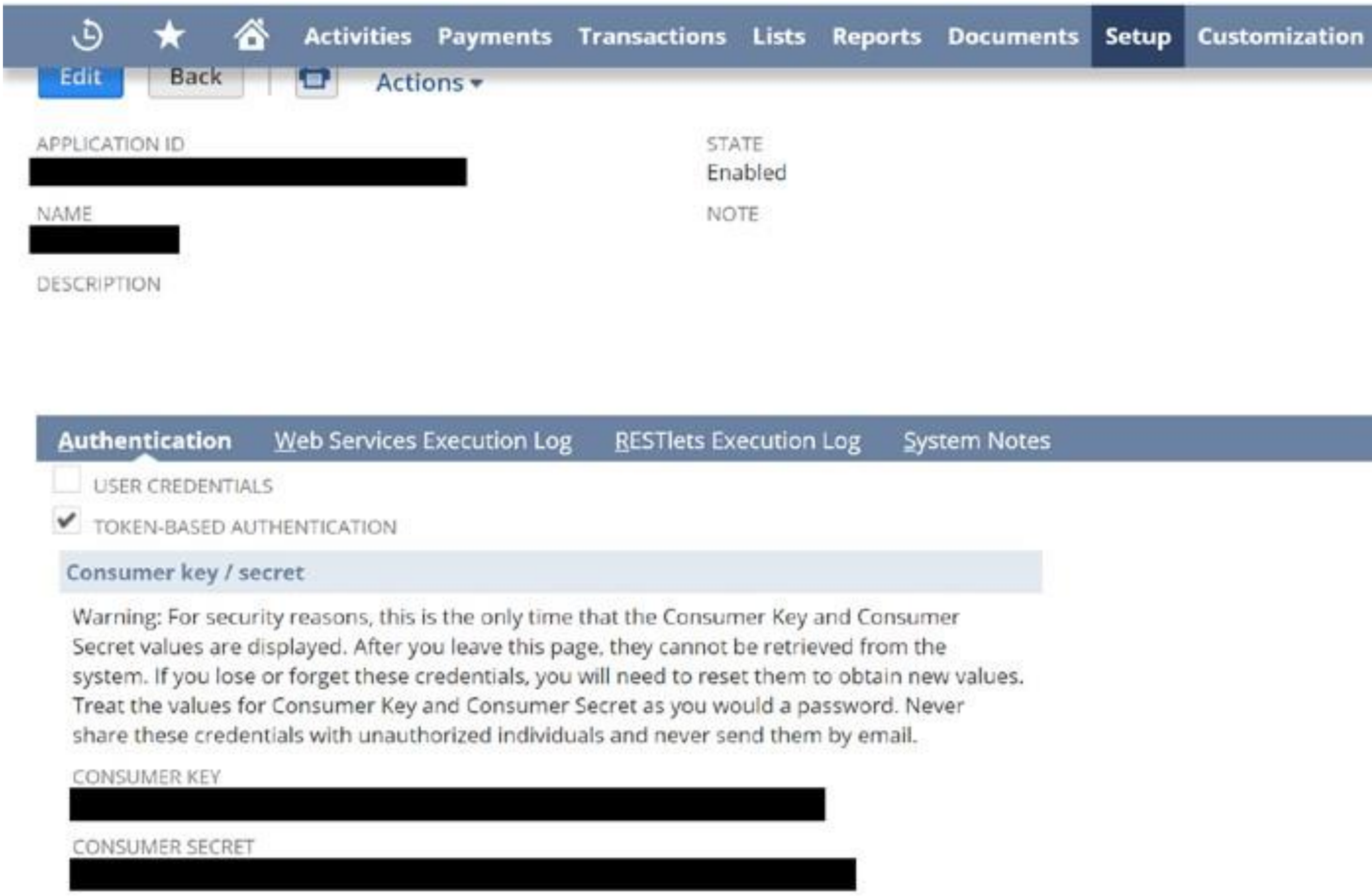


1.3 Integration Record

Before connecting with a token, an integration record is required for authentication. A new integration record should be used and can be created by navigating to **Setup > Manage Integrations > New**.

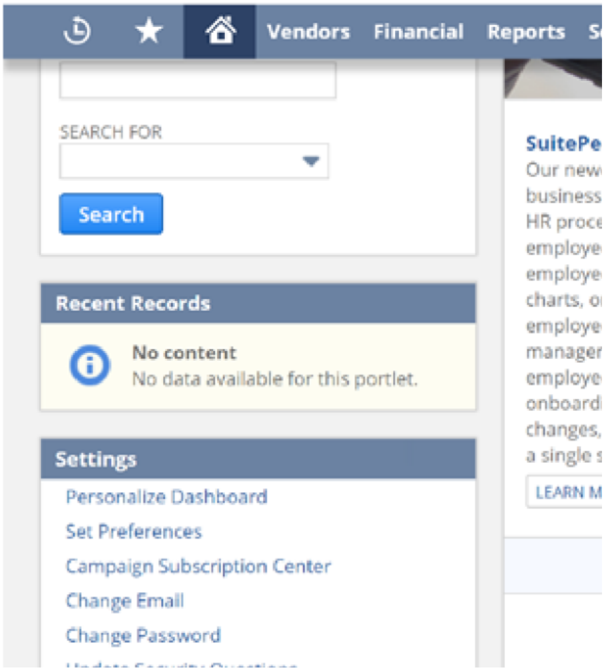
The name field should be filled in along with ensuring that the 'TOKEN-BASED AUTHENTICATION' checkbox is checked. Upon saving you will be given a Consumer key / Consumer secret.

NOTE: These values will not show up again after navigating away from the page for security concerns. Store the values somewhere securely treating them as you would a password. The values will be utilized in authentication later.

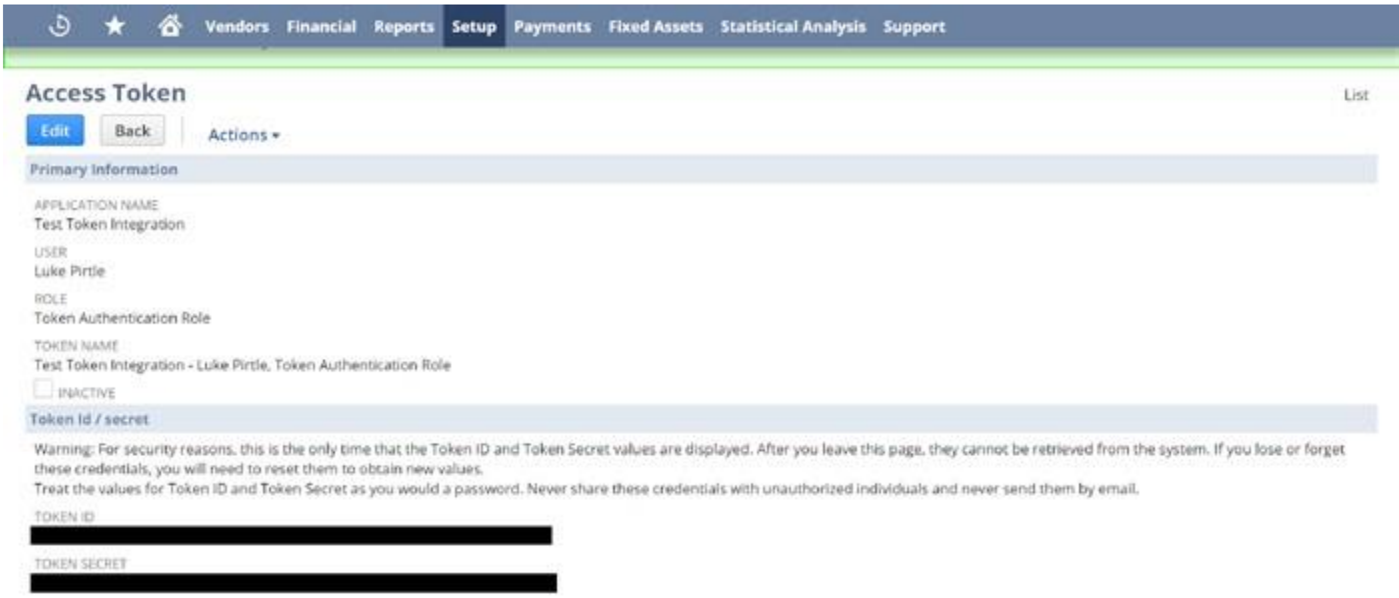


1.4 Creating the Token

With the integration record created and proper role assigned, a token can be created for authentication. To create a token, have the user with the token authentication role login.
Click the ‘Manage Access Tokens’ link available on the home dashboard under settings



Create a new token and select the Application Name that corresponding to the associated integration record created earlier. Again, an ID and secret will be provided.



NOTE: These values will not show up again after navigating away from the page for security concerns. Store the values somewhere securely treating them as you would a password. The values will be utilized in authentication later