



NETSUITE INTEGRATION

# Guide to Setting up Token-Based Authentication in NetSuite



# This walk-thru guide will provide a step-by-step 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 illustrates 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.

Navigation: Activities Payments Transactions Lists Reports Documents **Setup** Customization Fixed Assets Support

**SERVICE**

**Manage Authentication**

- ☒ SUITESIGNON  
USE NETSUITE AS THE TRUSTED SYSTEM TO AUTHENTICATE ACCESS TO INTEGRATED EXTERNAL APPLICATIONS THROUGH SINGLE SIGN-ON. BY ENABLING THIS FEATURE, YOU AGREE TO [SUITECLOUD TERMS OF SERVICE](#)
- ☒ OPENID SINGLE SIGN-ON  
ENABLE GOOGLE OPENID AS AN ADDITIONAL AUTHENTICATION MECHANISM FOR YOUR USERS. BY ENABLING THIS FEATURE, YOU AGREE TO [SUITECLOUD TERMS OF SERVICE](#)
- ☐ SAML SINGLE SIGN-ON  
ENABLE SAML AS AN ADDITIONAL AUTHENTICATION MECHANISM FOR YOUR USERS. BY ENABLING THIS FEATURE, YOU AGREE TO [SUITECLOUD TERMS OF SERVICE](#)
- ☒ **TOKEN-BASED AUTHENTICATION**  
ENABLE TOKEN-BASED AUTHENTICATION AS AN ADDITIONAL AUTHENTICATION MECHANISM FOR YOUR USERS. BY ENABLING THIS FEATURE, YOU AGREE TO [SUITECLOUD TERMS OF SERVICE](#)

**Integration Add-ons**

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.

PERMISSION*	LEVEL
Access Token Management	Full
Log in using Access Tokens	Full
User Access Tokens	Full
View Web Services Logs	Full
Web Services	Full

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

The screenshot shows a software interface with a top navigation bar containing icons and menu items: Activities, Payments, Transactions, Lists, Reports, Documents, Setup, Customization, Fixed Assets, and Support. Below this is a form with various fields. The 'Access' tab is selected, showing a table of roles. The 'Token Authentication Role' is highlighted with a red box.

Classification	CLASS	BILLING CLASS
SUBSIDIARY Japan		
DEPARTMENT	LOCATION	
LAST MODIFIED DATE 11/1/2016	EMPLOYEE CODE A	

Communication Address Human Resources Time Tracking Commission Related Records Marketing **Access** System Information Custom Bank Payment

☒ GIVE ACCESS

Roles • Global Permissions History •
ROLE
Administrator
Token Authentication Role

## 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.*



ActivitiesPaymentsTransactionsListsReportsDocumentsSetupCustomization

EditBack

Actions

APPLICATION ID	STATE
	Enabled
NAME	NOTE
DESCRIPTION	

AuthenticationWeb Services Execution LogRESTlets Execution LogSystem Notes

- ☐ USER CREDENTIALS
- ☒ TOKEN-BASED AUTHENTICATION

#### Consumer key / secret

Warning: For security reasons, this is the only time that the Consumer Key and Consumer Secret values are displayed. After you leave this page, they cannot be retrieved from the system. If you lose or forget these credentials, you will need to reset them to obtain new values. Treat the values for Consumer Key and Consumer Secret as you would a password. Never share these credentials with unauthorized individuals and never send them by email.

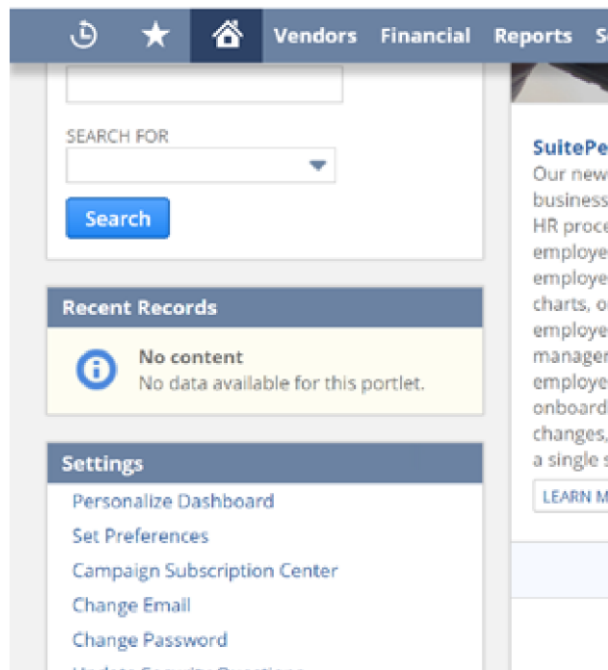
CONSUMER KEY

CONSUMER SECRET

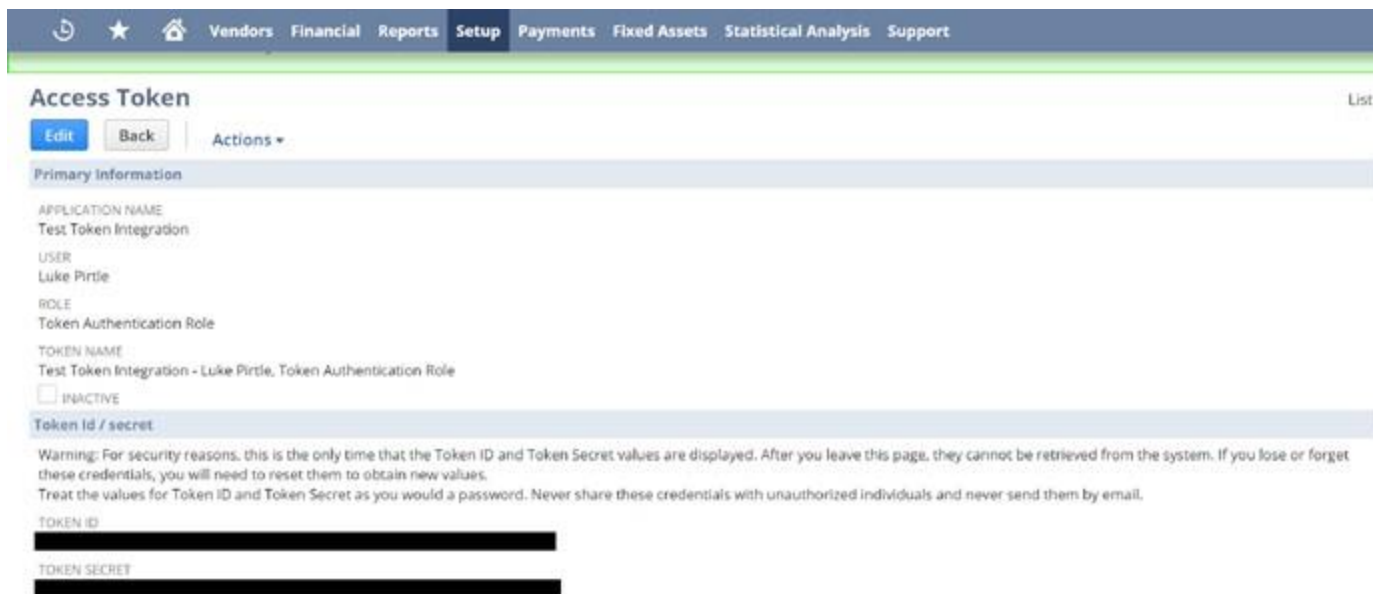
## 1.4 Creating the Token

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*