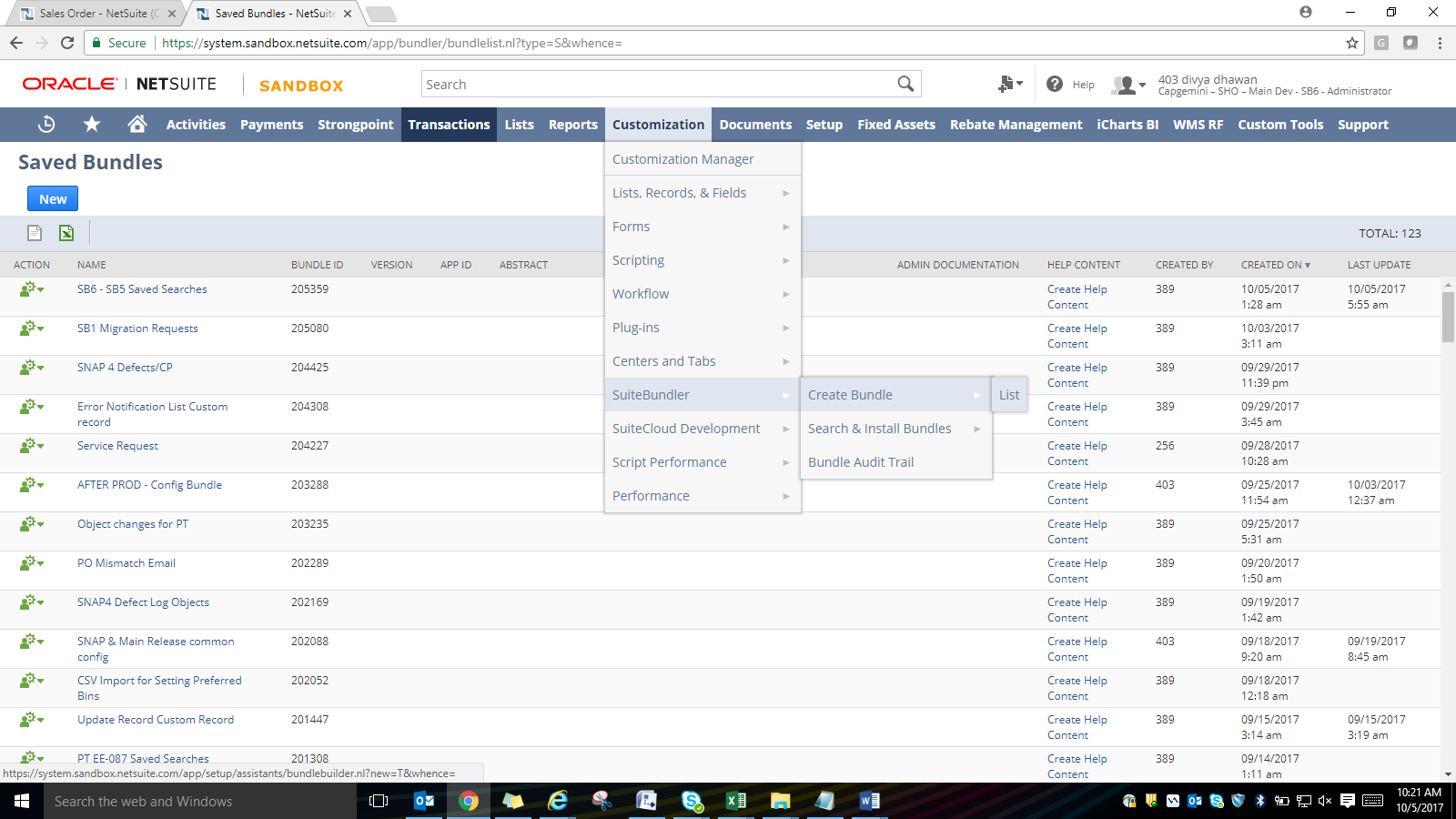
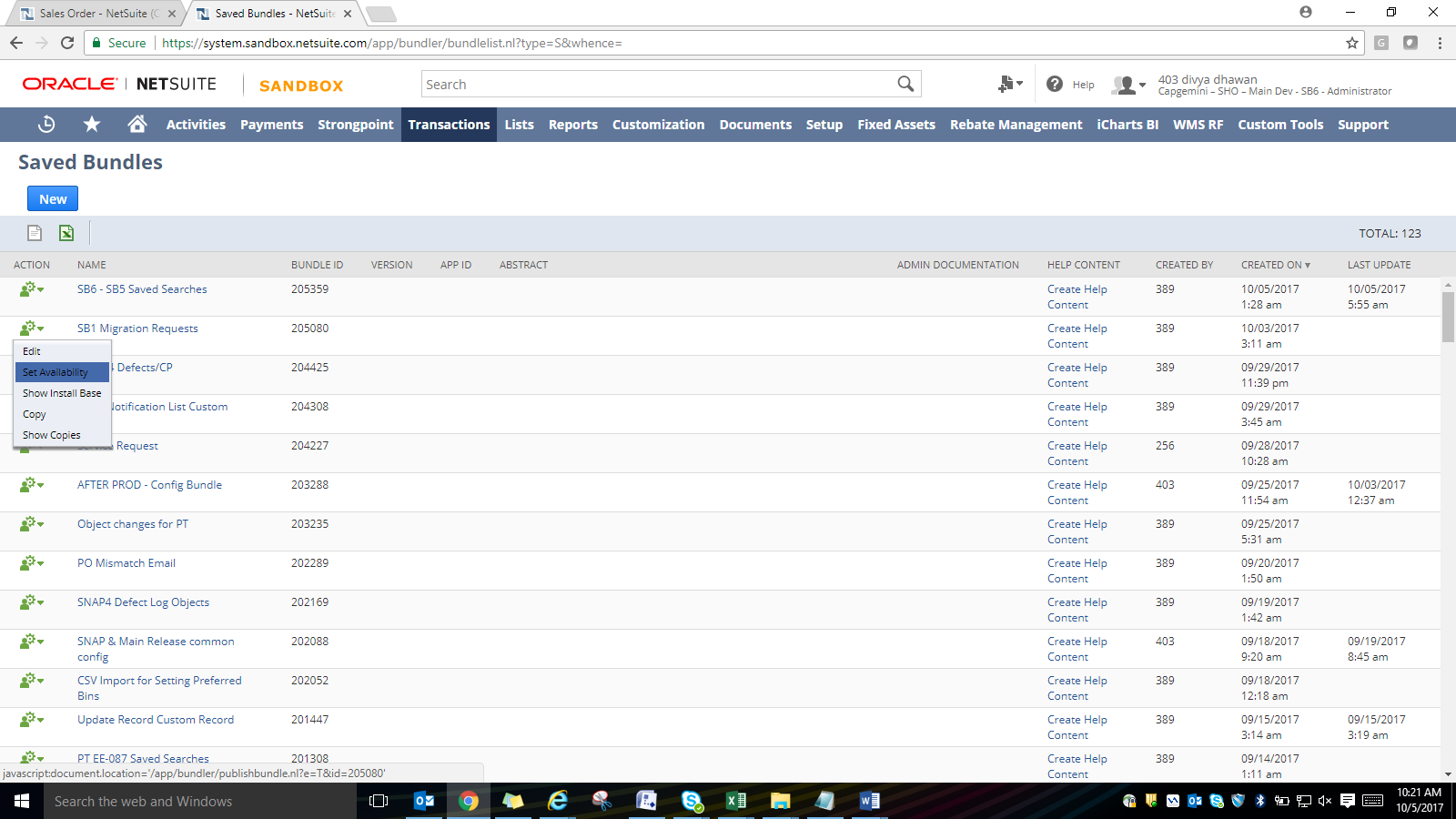
**HANDOVER DOCUMENT FOR ADMINISTRATOR TASKS**

1. Migration between environments using Suite Bundler
2. Token Based Access
3. Account Information for JDBC Users and Web Services from NetSuite
4. Sandbox Refresh
5. Deployment of Files
6. Create Users
7. **Migration between environments:**

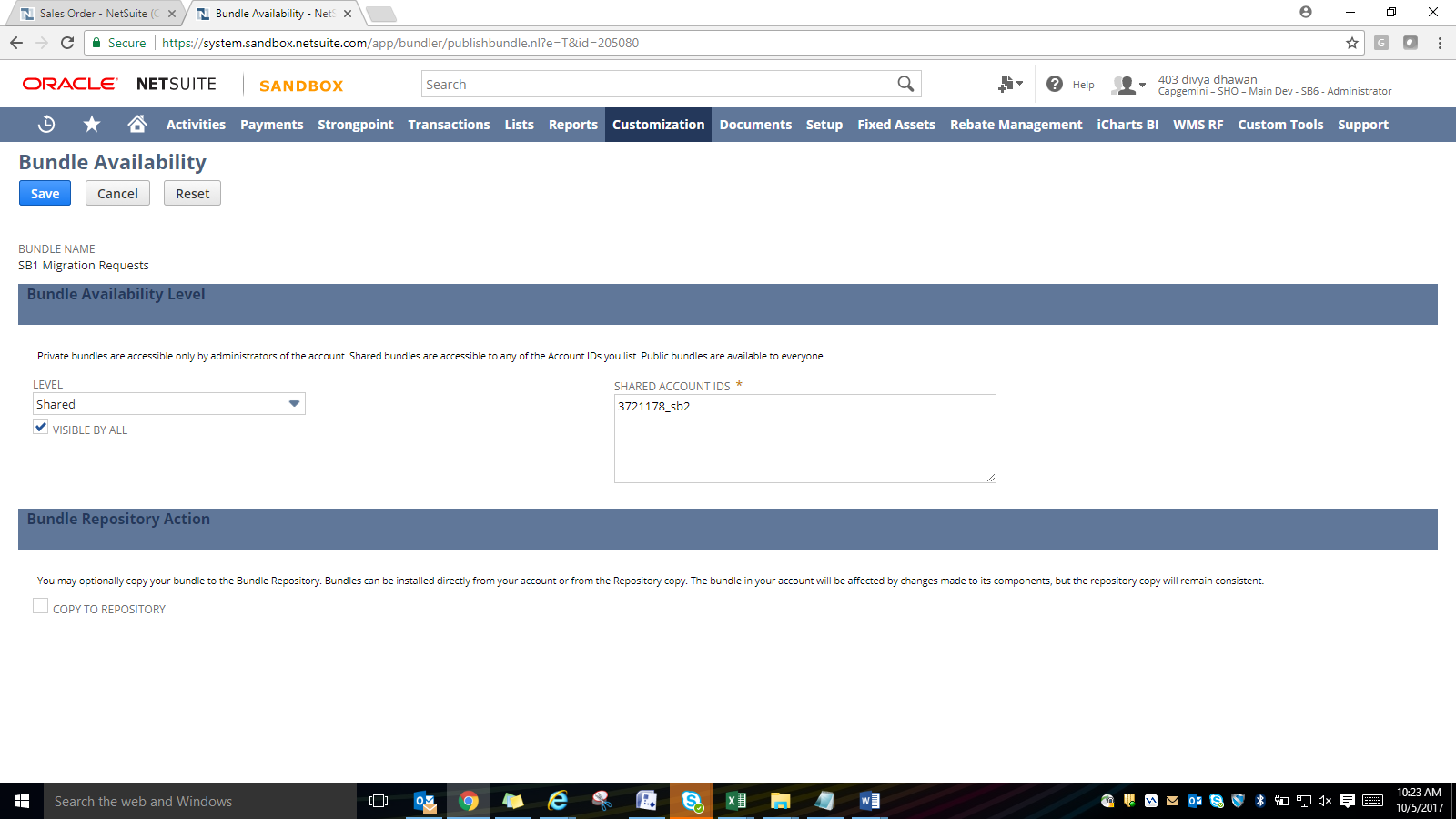
Create bundle in source environment with the objects required to be migrated.



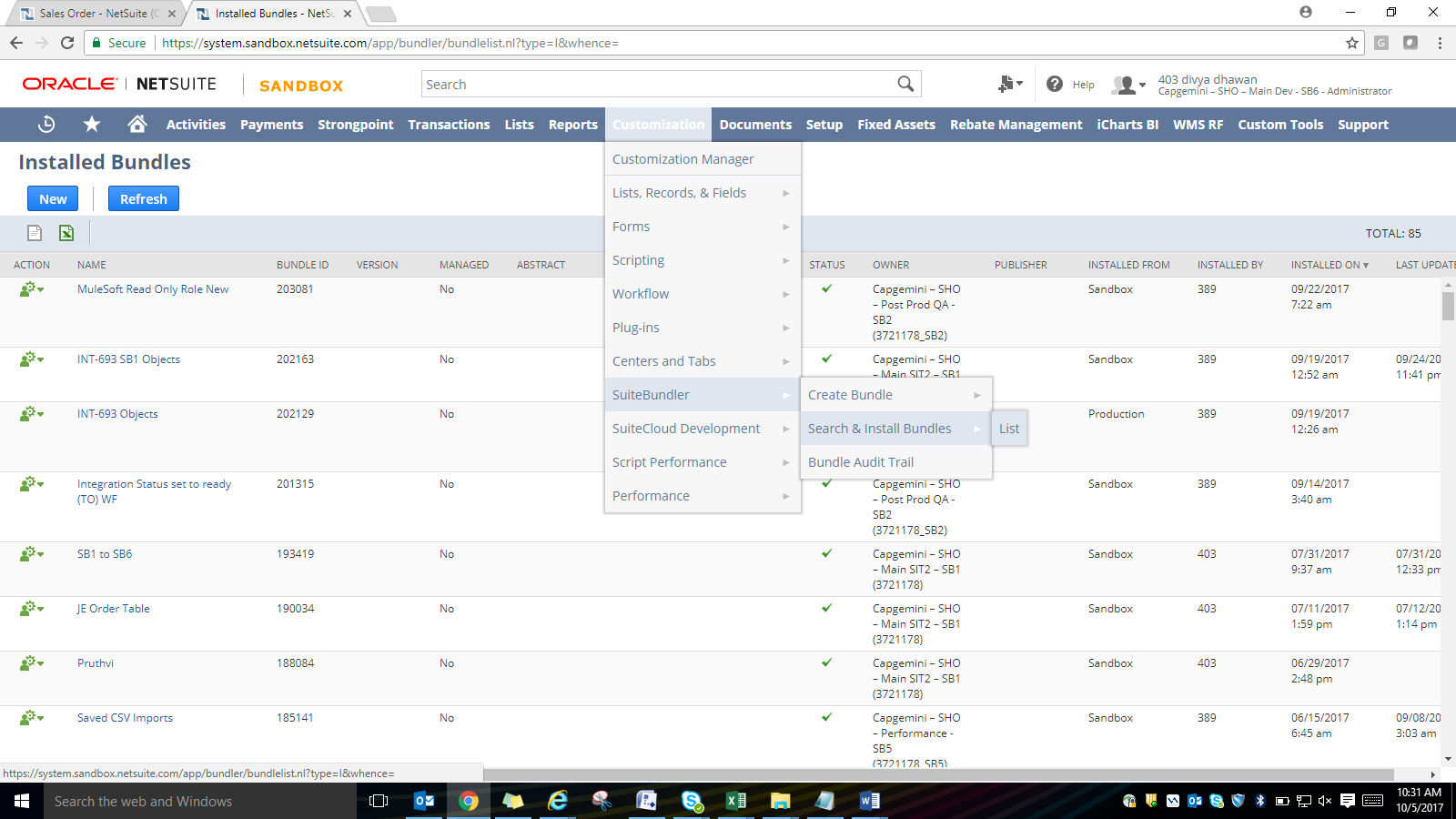
Set Availability by clicking on the small icon besides bundle name:

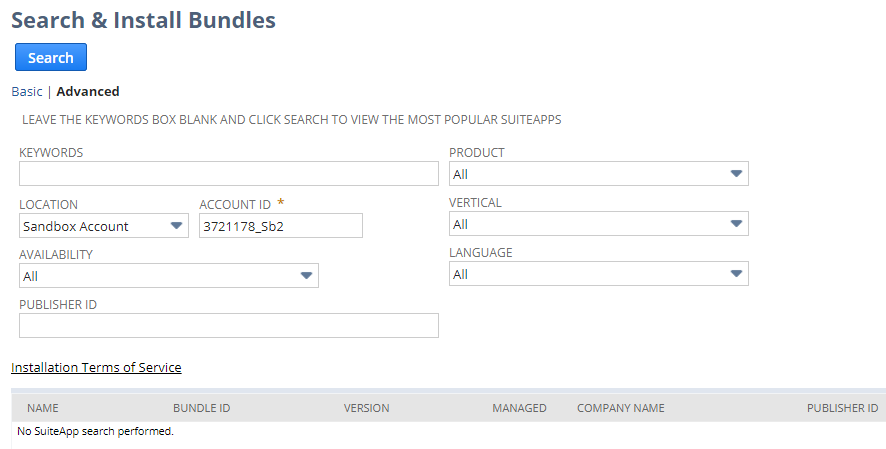


Change the level to Shared and add the target account number.

Install a bundle in target environment:

Customization >> Suite Bundler >> Search & Install Bundles





**List of bundles will appear here**

**Target Account ID**

**Bundle Name**

Select the required preferences and click on Install button.

1. **Handling Web Services Users and JDBC Users**
2. We are currently having 8 Concurrent User Licenses out of which 7 are being used by web services users and 1 by POS users.
3. After every Sandbox refresh we need to setup web services users with email IDs specific to that environment and assign Access Tokens to these users. The step by step description to assign the same is provided in below link:

<https://netsuite.custhelp.com/app/answers/detail/a_id/41898/kw/access%20tokens>

To set up token-based authentication (TBA) in your NetSuite account, do the following:

* Enable the feature. See [Enabling the Token-based Authentication Feature](https://netsuite.custhelp.com/app/answers/detail/a_id/41898/kw/access%20tokens#bridgehead_4253254429).
* Set up roles. See [Setting Up Token-based Authentication Roles](https://netsuite.custhelp.com/app/answers/detail/a_id/41898/kw/access%20tokens#bridgehead_4248124361).
  + See also [Token-based Authentication Permissions](https://netsuite.custhelp.com/app/answers/detail/a_id/41898/kw/access%20tokens#bridgehead_4249074259).
* Assign roles to users. See [Assigning Users to Token-based Authentication Roles](https://netsuite.custhelp.com/app/answers/detail/a_id/41898/kw/access%20tokens#bridgehead_4249025340).
* Set up applications for token-based authentication. See [Creating Applications for Token-based Authentication](https://netsuite.custhelp.com/app/answers/detail/a_id/41898/kw/access%20tokens#bridgehead_4249032125).

## Enabling the Token-based Authentication Feature

#### To enable the token-based authentication feature:

1. Go to Setup > Company > Setup Tasks > Enable Features.
2. Click the **SuiteCloud** subtab.
3. Scroll down to the SuiteScript section, and check the following boxes:
   * **Client SuiteScript**.
   * **Server SuiteScript**. Click **I Agree** on the SuiteCloud Terms of Service page.
4. Scroll down to the **Manage Authentication** section, and check the **Token-based Authentication**box. Click **I Agree** on the SuiteCloud Terms of Service page.
5. Click **Save**.

## Setting Up Token-based Authentication Roles

An account administrator can modify existing roles to add token-based authentication permissions, then assign users to those roles as needed. If you need more information about these tasks, see:

* [NetSuite Users & Roles](https://netsuite.custhelp.com/app/answers/detail/a_id/30530)
* [NetSuite Roles Overview](https://netsuite.custhelp.com/app/answers/detail/a_id/9903)

### Token-based Authentication Permissions

The following token-based authentication permissions can be added to roles as appropriate:

* **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.

* **User 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.

* **Log in using 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.

## Assigning Users to Token-based Authentication Roles

After modifying roles with the appropriate token-based authentication permissions, an account administrator can assign users to those roles. The following is a brief procedure for assigning a role to an existing employee. If you need more information on assigning users to roles, see [NetSuite Users Overview](https://netsuite.custhelp.com/app/answers/detail/a_id/9904).

#### To assign an employee to a token-based authentication role:

1. Go to Lists > Employees > Employees.
2. Click **Edit** next to the name of the employee you want to assign the token-based authentication role.
3. Click the **Access** subtab.
4. In the **Role** field, select the token-based authentication role for this employee.
5. Click **Add**.
6. Click **Save**.

## Creating Applications for Token-based Authentication

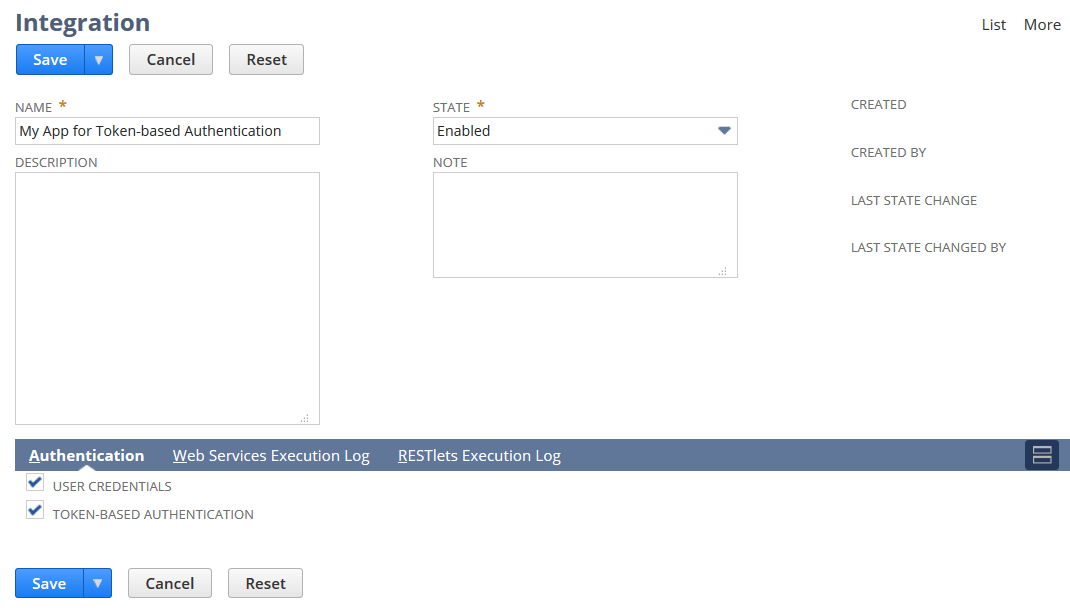
Applications must be created with the Integration record for use with token-based authentication before tokens can be created and assigned to users. Administrators or users assigned the Full level of the Setup Type Integration Application permission can create applications for use with token-based authentication.

* For more information about the Integration record, see [Integration Management](https://netsuite.custhelp.com/app/answers/detail/a_id/44197).
* For more information about using token-based authentication with web services, see [Token-Based Authentication Details](https://netsuite.custhelp.com/app/answers/detail/a_id/44708).

#### To create an application using the Integration record:

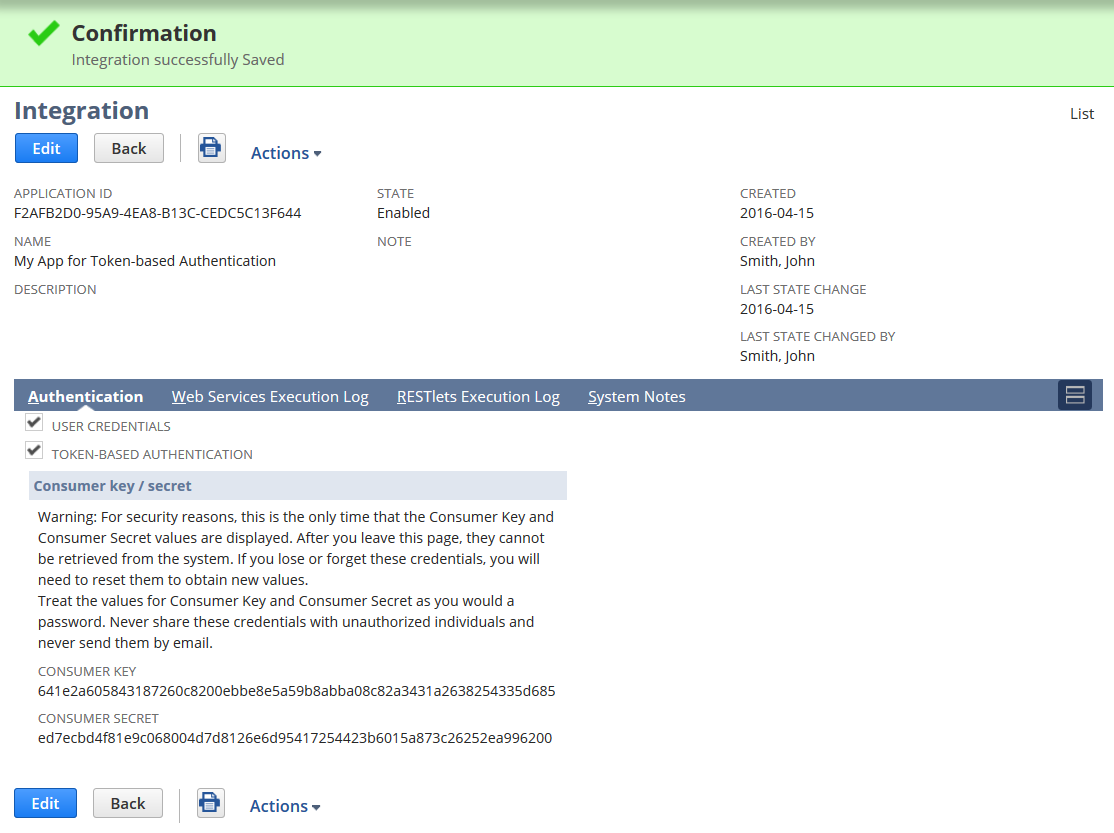
The following procedure briefly describes completing an Integration record. For more detailed information about the fields in this record, see [Creating an Integration Record](https://netsuite.custhelp.com/app/answers/detail/a_id/44135).

1. Go to Setup > Integration > Integration Management > Manage Integrations > New
2. Enter a **Name** for your application.
3. Enter a **Description**, if desired.
4. The application **State** is Enabled by default. (The other option available for selection is Blocked.)
5. Enter a **Note**, if desired.
6. Check the **Token-based Authentication** box on the **Authentication** subtab.

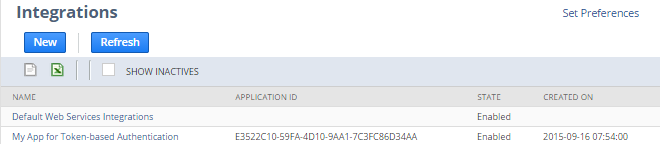


1. Click **Save**.

The confirmation page displays the Consumer Key and Consumer Secret for this application.



1. Click List to view all Integrations in your account.



After these basic setup tasks are complete, you can begin using token-based authentication in your account.

## Access Token Management – Create and Assign a TBA Token

Users assigned a role that has the **Access Token Management** permission can create, assign, and manage a token for any user in the company. For example, they could assign a token to those users who are assigned a role with only the **Log in using Access Tokens** permission.

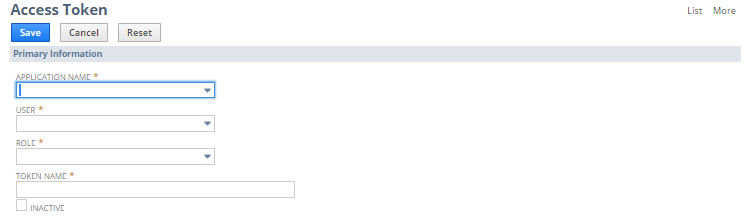
### Important

Tokens created in your production account are not copied to your sandbox during a refresh. To test token-based authentication in your sandbox, you must create tokens in the sandbox account. Each time your sandbox is refreshed, you will need to create new tokens in the sandbox.

#### To create and assign a TBA token:

1. Log in as a user with the **Access Token Management** permission.
2. Go to Setup > Users/Roles > Access Tokens > New.
3. On the Access Tokens page, click **New Access Token**.

The Access token page displays.



1. On the Access Token page:
   1. Select the **Application Name**.
   2. Select the **User**.
   3. Select the **Role**.
   4. The **Token Name** is already populated by default with a concatenation of Application Name, User, and Role. Enter your own name for this token, if desired.
2. Click **Save**.

The confirmation page displays the Token ID and Token Secret.

### Warning

For security reasons, the only time the Token ID and Token Secret values are displayed is on the confirmation page. After you leave this page, these values cannot be retrieved from the system. If you lose or forget these credentials, you will need to create a new token and obtain new values.

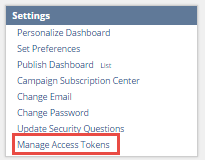
Treat these values as you would a password. Never share these credentials with unauthorized individuals and never send them by email.

## User Access Token – Create a TBA Token

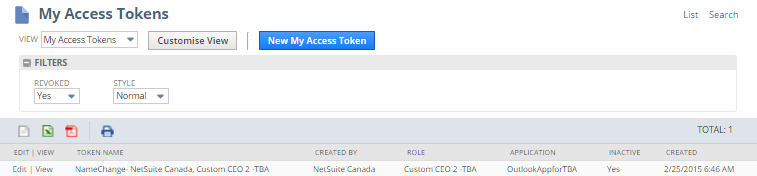
Users assigned a role that has the **User Access Token** permission can create, assign, and manage tokens for the current user and current role.

#### To create a token using the Manage Access Tokens link:

1. Log in using a role with the **User Access Token** permission.
2. In the **Settings** portlet, click **Manage Access Tokens**.

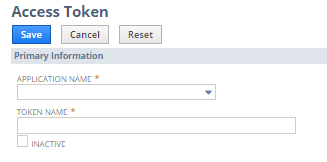


The My Access Tokens page displays, listing all the tokens for the current user in the current role.



1. Click **New My Access Token**.

The Access Token page displays.



1. On the Access Token page:
   1. Select the **Application Name**.
   2. The **Token Name** is already populated by default with a concatenation of Application Name, User, and Role. Enter your own name for this token, if desired.
2. Click **Save**.

The confirmation page displays the Token ID and Token Secret.

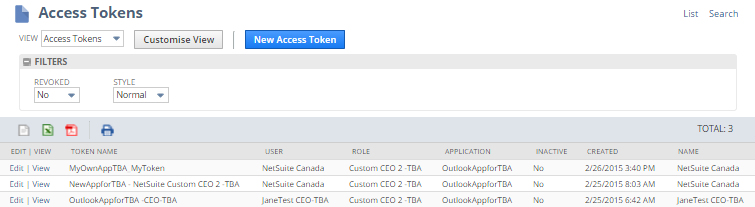
## Viewing, Editing, Creating, and Revoking TBA Tokens

You can see a list view of tokens in your system.

#### To view tokens:

1. Go to Setup > Users/Roles > Access Tokens ( Administrator ) **or** go to Setup > Other Setup > Access Tokens.

The Access Tokens page displays.



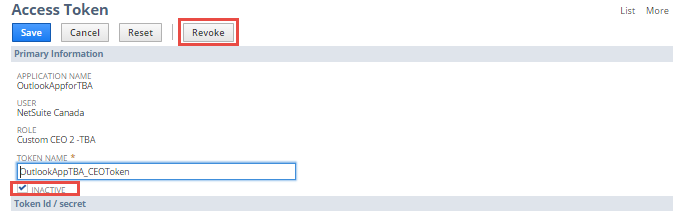
1. Actions you can take from this page include:
   * Click **View** to open the Access Token page and review the details of a specific token.
   * Click **New Access Token** to open the Access Token page and create a new token. For more information, see [Access Token Management – Create and Assign a TBA Token](https://netsuite.custhelp.com/app/answers/detail/a_id/41902#bridgehead_4254081947).
   * Click **Edit** to open the Access Token page and:
     + Edit specific details about the token, or
     + Click **Revoke** to revoke the token. For more information, see [Revoking TBA Tokens](https://netsuite.custhelp.com/app/answers/detail/a_id/41902#bridgehead_4249079467).
   * Open the **Filters** panel to select a value for **Revoked** status (All, Yes, or No).
   * Click **Search** at the top right corner of the Access Tokens page. For more information, see [Searching for TBA Tokens](https://netsuite.custhelp.com/app/answers/detail/a_id/41902#bridgehead_4249079066).

## Revoking TBA Tokens

Revoking a token makes it inactive forever, but does not remove the token from the system. The token is still accessible for auditing purposes.

**Revoke and Inactive Statuses**

* When a token is revoked, it cannot be edited, and will display with an Inactive status in list views.
* When the **Inactive** box is checked for a token, the token will display as Inactive in list views, but the token can still be edited. To make the token active again, click **Edit**, clear the **Inactive** box, and click **Save**.



**Additional Situations Under Which Tokens are Revoked**

* When an application used for token-based authentication is deleted, all tokens associated with that application are revoked.
* When an administrator removes roles from an entity (an employee, a vendor, a partner, a customer, or a contact) the tokens are still active in the system. These active tokens cannot be used by the entity for log in to NetSuite (unless the administrator adds the roles back to the entity).
* When an administrator deletes an entity, (an employee, a vendor, a partner, a customer, or a contact) the associated tokens are revoked.

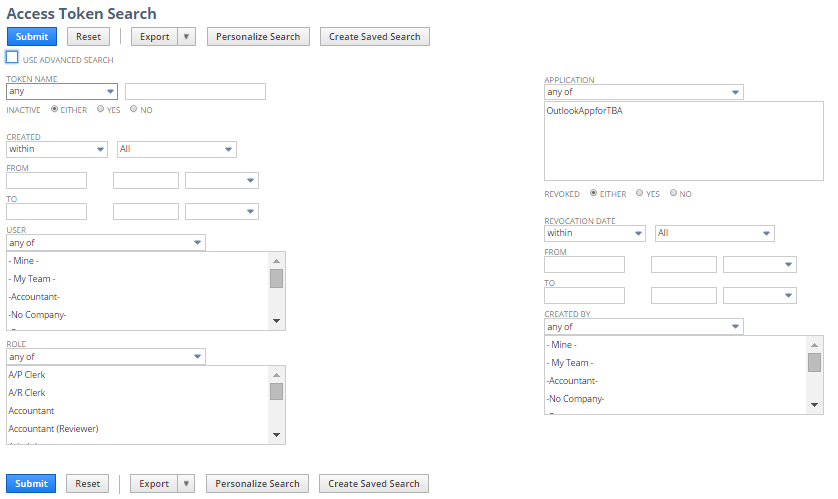
## Searching for TBA Tokens

There are two methods of opening the Access Token Search page. One method is to click the Search link on the top right corner of a page. See the following procedure for the other method of opening the search page.

#### To search for a token:

1. Go to Setup > Users/Roles > Access Tokens > Search.

The Access Token Search page displays.



1. Enter or select from the available criteria, as appropriate.
2. Click **Submit**.

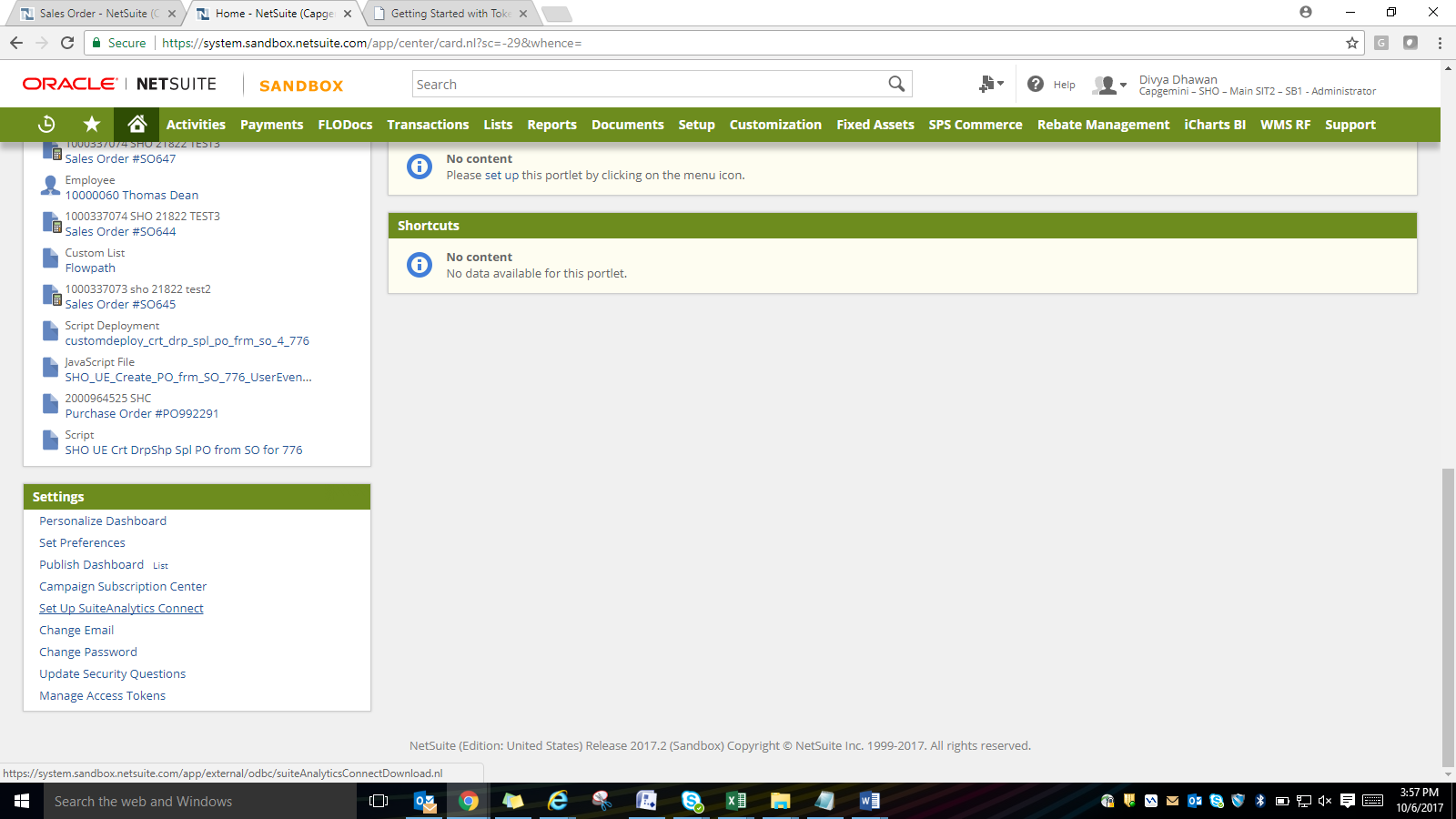
For information on NetSuite’s search capabilities, see:

* [Running Searches](https://netsuite.custhelp.com/app/answers/detail/a_id/8434)
* [Using Saved Searches](https://netsuite.custhelp.com/app/answers/detail/a_id/8493)

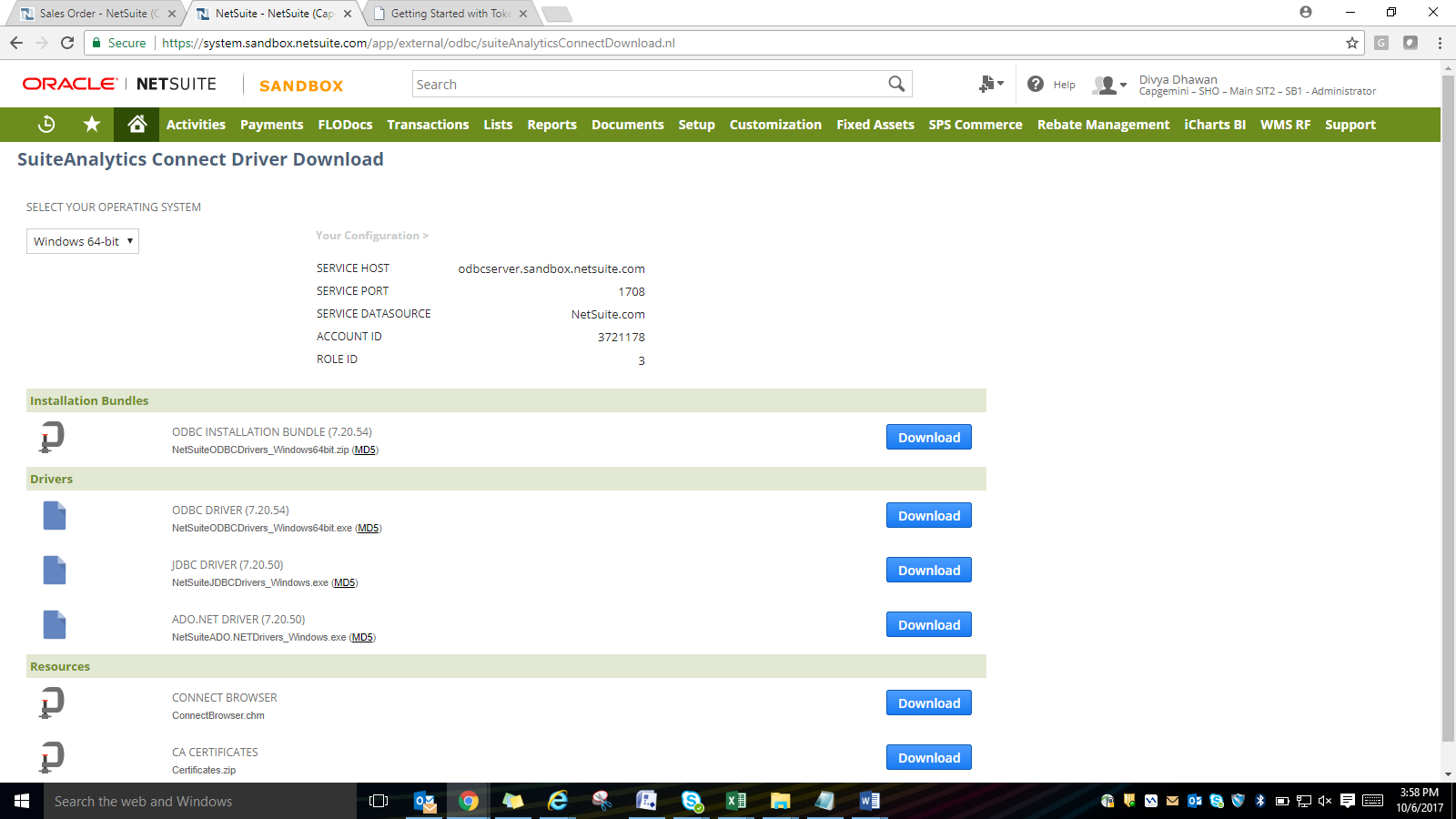
**JDBC users also need to be created in each environment with environment specific email ID.**

**Passwords for these users should not be shared in emails of Skype directly and should be added in a password protected excel before sharing.**

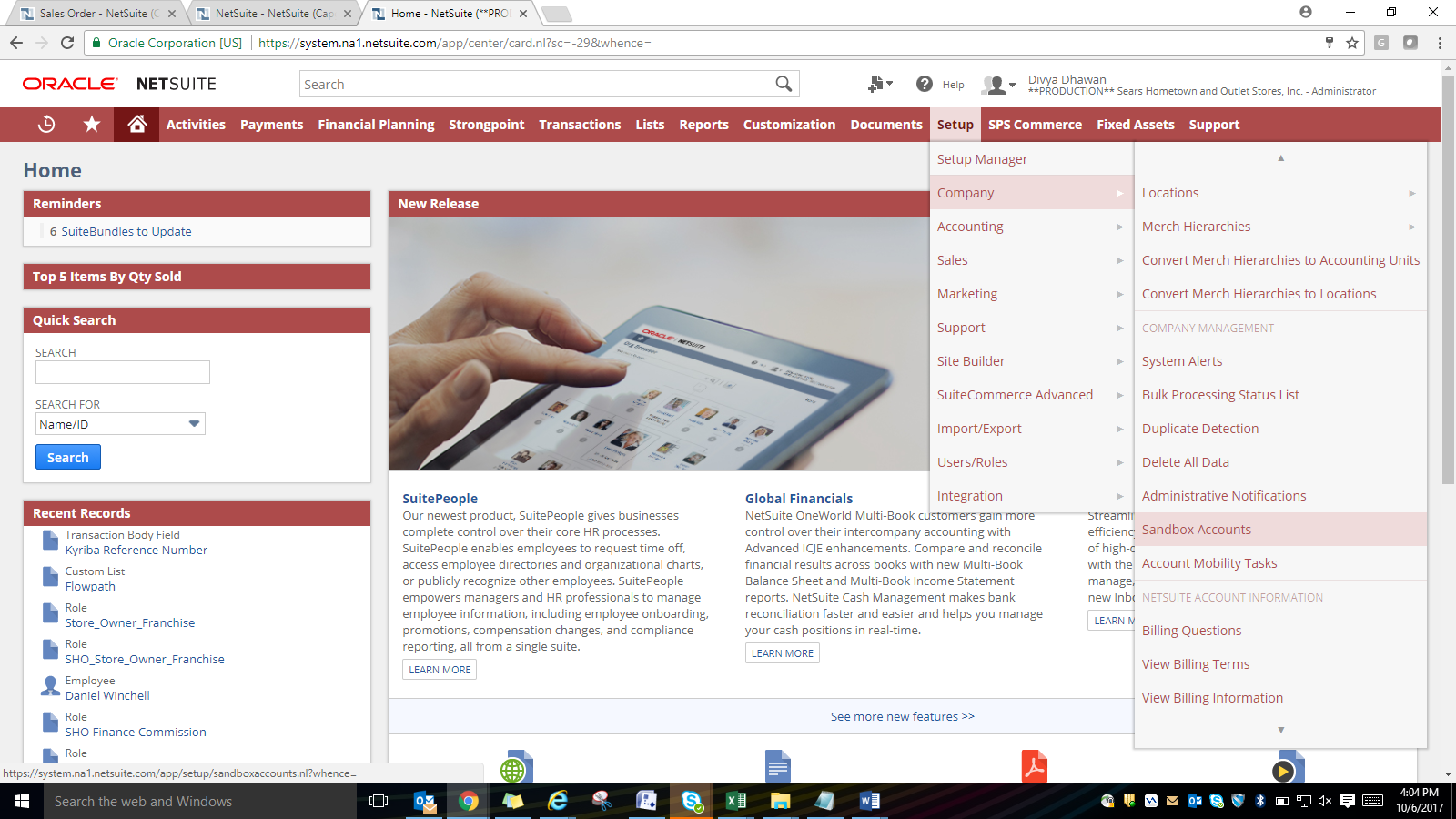
1. **Account Information for JDBC Users and Web Services from NetSuite**
2. Go to Homepage and click on Suite Analytics Connect



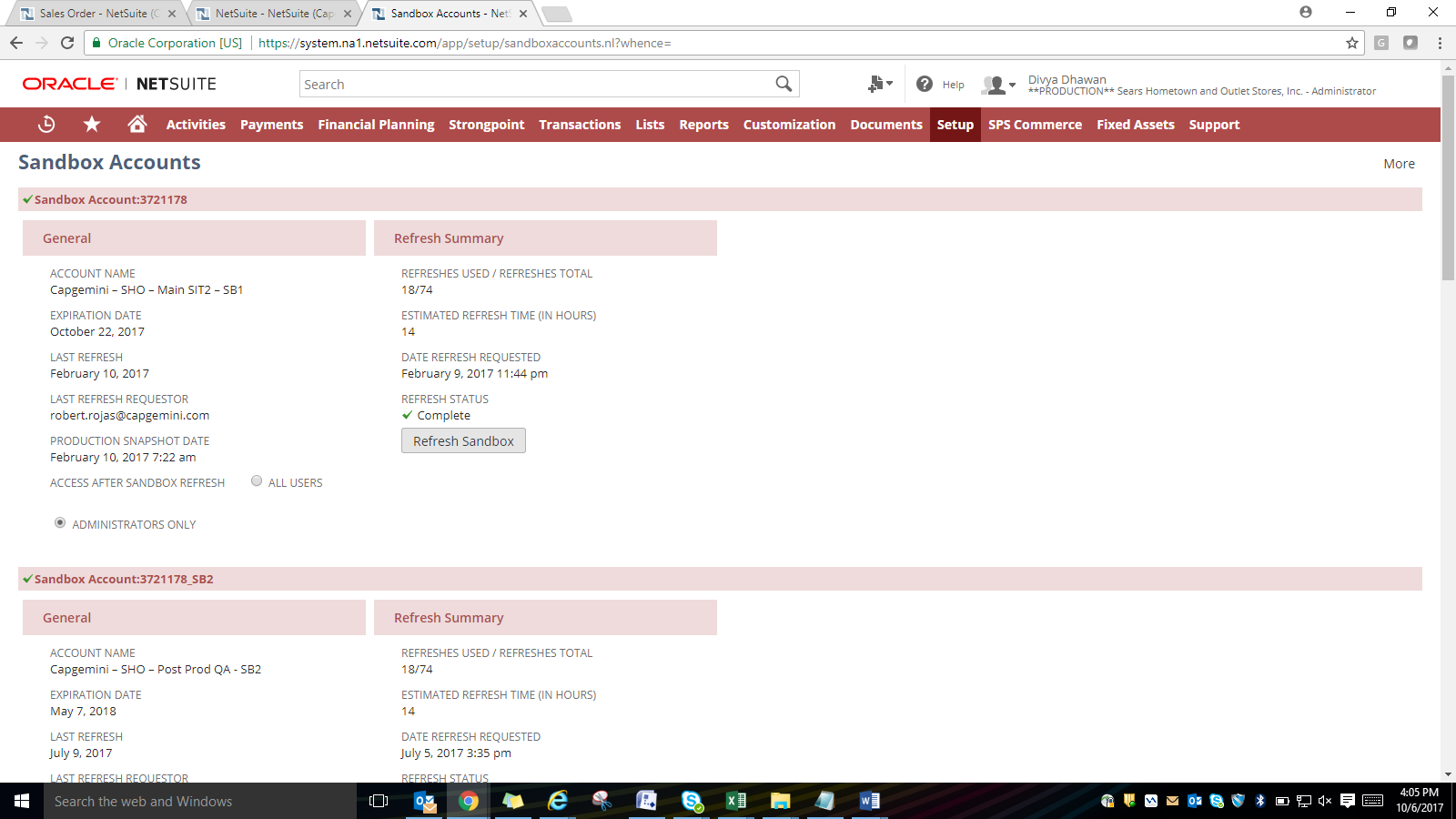
1. Click on Your Configuration:



1. **Sandbox Refresh**



Click on Refresh Sandbox and select “Administrators Only” if you do not want all the users to have access.

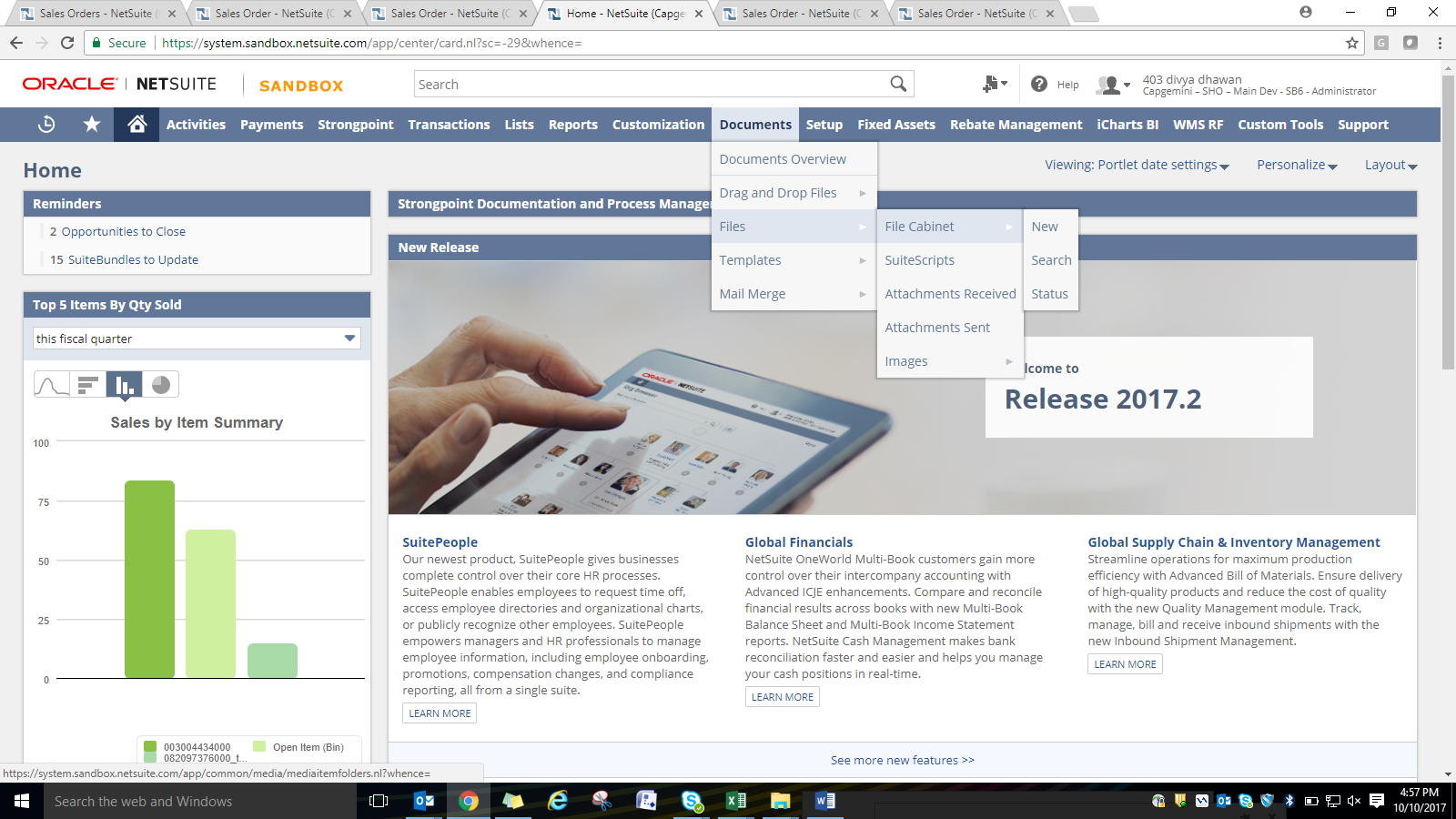


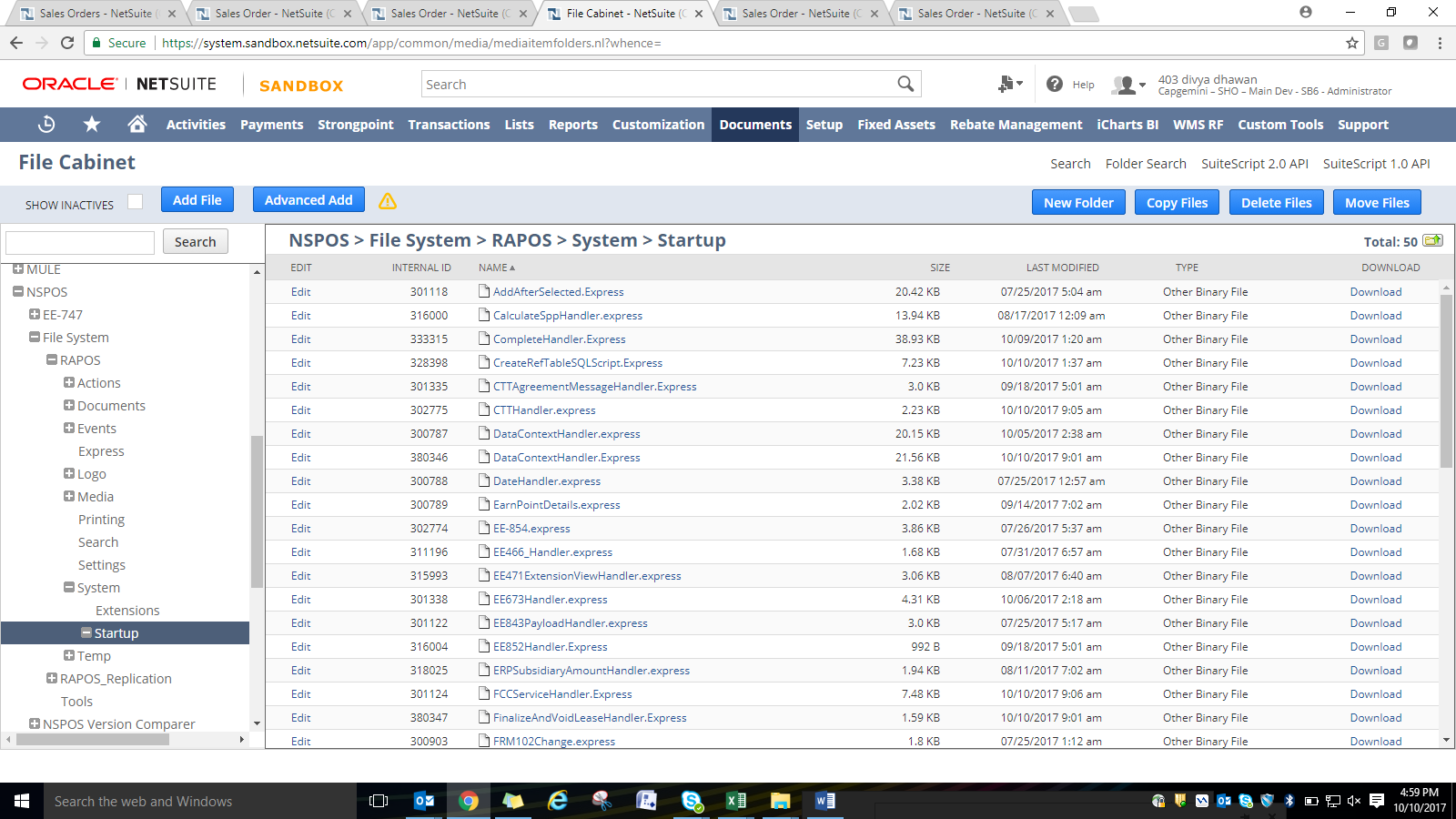
You can check the progress of refresh by coming to same page till status is complete.

1. **Deployment of Files**

In order to deploy the files in NetSuite they need to be available in some SVN location. Download the file from SVN and navigate to the location provided by requestor in File Cabinet. Sample request:

Please upload this file in SB1 File System> NSPOS> File System>  RAPOS > System> StartUp Folder for Receipt Text Issue for Payment on Account.





Click on Add File and upload the file in the SVN path sent by requestor.

1. **Create Users**

Capgemini Administrator will be responsible for creating new users in all sandbox environments where as this task is divided between Cap admin and SHO security for Production. Cap Admin will be responsible for creating new Cap user in NetSuite/Launchpad and SHO Security will be creating the same for SHO users. This process is subjected to change and may be handled by only SHO security team. Detailed description of creating users in Launchpad will be shared by Roland.

All the users need to be uploaded with respective roles after sandbox refresh.

1. **Roles Management**
2. Cap Administrator will be responsible to assign roles only to all users in Sandboxes and cap users in production.
3. No change should be done in sandbox or production without approval from Phil/Randy.
4. Any change in permissions in production should require a SNOW ticket and should be tested in Sandbox first.