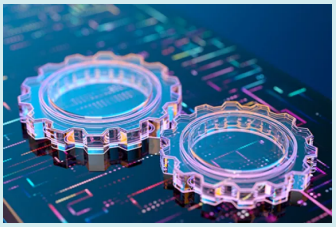
TRACELINK UNIVERSITY

XTT Link Actions Developer Kit Admin Setup for NetSuite



This guide provides step by step instructions for how to generate access credentials and system configuration details for NetSuite, and should only be used:

- By an administrator of your NetSuite instance.
- In conjunction with the **XTT Link Actions Developer Kit setup guide** as part of the secrets.json setup step (this is not a standalone guide).

Overview of the secrets.json file fields

The secrets.json file required to configure the XTT Link Actions Developer Kit, detailed in the setup guide, contains the following components:

```
{
   "API_KEYS": {
       "CONSUMER_KEY": "YOUR_CONSUMER_KEY",
       "CLIENT_SECRET": "YOUR_CLIENT_SECRET",
       "TOKEN_URL": "URL_FOR_YOUR_SERVICE",
       "CERTIFICATE_PRIVATE_KEY": "YOUR_GENERATED_PRIVATE_KEY",
       "CERTIFICATE_ID": "CERTIFICATE_ID_FROM_UPLOADED_PRIVATE_KEY",
       "ALGORITHM": "PS256",
       "SCOPE": "rest_webservices"
   }
}
```

To configure the XTT Link Action Developer Kit you must supply the following items:

- **TOKEN_URL** - URL to the service that generates the authentication token (e.g. https://ab1234567.suitetalk.api.netsuite.com/services/rest/auth/oauth2/v1/token, where ab1234567 is your company identifier)
- **CONSUMER_KEY** - Value that identifies a specific user
- **CLIENT_SECRET** - Value used to authenticate the CONSUMER_KEY
- **CERTIFICATE_PRIVATE_KEY** - A cryptographic key that pairs with the uploaded public key. We create credentials in the next section.
- **CERTIFICATE_ID** - The identifier for the certificate being used

If you are an administrator following this guide for another individual setting up the XTT Link Actions Developer Kit, create a new secrets.json file with the above JSON template.

If you are both the administrator and individual setting up the XTT Link Actions Developer Kit, continue with the existing secrets.json file being used as part of the setup guide.

Obtaining configuration data for the secrets.json file

To create that information in NetSuite, follow the below steps.

Create an integration to obtain a CONSUMER_KEY and CLIENT_SECRET.

1. Log in to NetSuite as a user with Administrator access
2. Navigate to Setup → Company → Enable Features

3. Navigate to the **SuiteCloud** Tab

    1. Enable Rest Web Services

    2. Enable OAUTH 2.0

4. Navigate to **Setup → Integration → Manage Integrations**

    1. Click **New**

    2. Add a **Name**
    3. Enable **Rest Web Services** and **Client Credentials (Machine to Machine) Grant**

    4. Disable all other settings until your settings look like the below

    5. Click **Save**. A summary page appears with important information. The Application ID will be available through the Integrations menu, the credentials are only displayed once upon creation. Copy the following to a secure location:
        1. Application ID
        2. Copy the CONSUMER KEY / CLIENT ID value to secrets.json.

        3. Copy the CONSUMER SECRET / CLIENT SECRET values to secrets.json.

6. Note down the **Application ID** that appears next to the Name of the app chosen in step 4a.

5. Obtain and note your NetSuite account ID. This can be found in the URL. For example, ab1234567 is the account ID of https://ab1234567.app.netsuite.com/app/center/. Copy this value to the secrets.json file.

Creating a certificate for the secrets.json file

Open a terminal (command line) session

Enter the following command

```
openssl req -new -x509 -newkey rsa:4096 -keyout my_private_key.pem -
sigopt rsa_padding_mode:pss -sha256 -sigopt rsa_pss_saltlen:64 -out
my_public_key.pem -nodes
```

Take care to specify different names for the private and public keys.

The certificate must meet the following requirements:

- The public key must be in x.509 format with a file extension of .cer, .pem, or .crt.
- The length of the RSA key must be 3072 bits, or 4096 bits. The length of the EC key must be 256 bits, 384 bits, or 521 bits.
- The maximum certificate validity is two years. If the certificate is valid for a longer time period, the system automatically shortens the validity to two years.
- One certificate can only be used for one combination of integration record, role, and entity. If you want to use the same integration record for multiple

entities or roles, you must use a different certificate for each unique combination.

With both public and private key files on your machine, register your public key in your system of record.

In NetSuite, you would use the **Setup -> Integration -> OAuth 2.0 Client Credentials (M2M) Setup menu**.

Click **Create New** to register a new certificate.

Select the Entity, Role, and Application for which you are registering the certificate.

Click choose a file and select the my_public_key.pem file you generated in the previous step.

After clicking **Save**, the system generates a Certificate ID for you.

Add the contents of your private key file to the secrets.json file.

Next Steps

Once all required values are populated for the secrets.json file, continue with the XTT Link Actions Developer Kit setup guide secrets.json setup step, or supply the created secrets.json file to the individual conducting the setup of the XTT Link Actions Developer Kit.

Related Content

XTT Link Actions Developer Kit

Configure your development environment.
View More

Custom XTT Link Actions Development Guide

Walkthrough of developing new XTT Link Actions.
View More

Use Case: XTT Link Actions

Integrate with external systems using Link Actions.
View More

TraceLink Digital Network Platform for NetSuite

Learn more about XTT Link Actions for NetSuite
View More