NetSuite Authentication with Alchemer

Overview

The Alchemer NetSuite integration uses OAuth 2.0 Machine-to-Machine (M2M) authentication with the client credentials flow. This method authenticates the integration itself using a certificate and key pair rather than a signed-in user.

NetSuite API Credentials

What You Need

- Your NetSuite Account ID
- A Client ID and Client Secret from an OAuth 2.0 integration record in NetSuite
- A Certificate ID from the certificate mapped to your integration in NetSuite
- The Private Key that corresponds to the uploaded certificate

---

How to Get Your NetSuite API Credentials

1. Enable the required features

- In NetSuite, go to **Setup → Company → Enable Features**.
- Under the **SuiteCloud** tab, enable **OAuth 2.0**, **Client Credentials (Machine to Machine) Grant**, and **REST Web Services**.

2. Generate a certificate and private key

- Create an X.509 certificate and matching private key pair (for example, using OpenSSL). NetSuite requires the certificate for the M2M client credentials flow. Learn more.
- Keep the **Private Key** secure, you will provide it to Alchemer during authentication.

3. Create an OAuth 2.0 integration record

- Go to **Setup → Integration → Manage Integrations → New**.
- Enable **OAuth 2.0** and select the **Client Credentials (Machine to Machine) Grant** flow. Disable TBA and any unused authentication flows.
- Set the scope to **REST Web Services**.
- Save the integration. NetSuite will display the **Client ID** and **Client Secret** once. Copy and store them securely.

4. Create an integration role with the required permissions

- Go to **Setup → Users/Roles → Manage Roles → New** and create a dedicated role for the integration.
- Under the **Permissions** subtab, add the following:
  - **Setup**: **Log in using OAuth 2.0 Access Tokens** (required for the M2M flow), **REST Web**

Services, and **User Access Tokens**.
    - **Transactions** and **Lists**: add the permissions for each record type the integration will read or write (for example, the appropriate Customer, Employee, or transaction permissions), each set to the access level your actions need (View for read-only, Create/Edit/Full for write).
- Assign the level of access carefully. The role should have only the permissions required for the records your integration uses, following least-privilege practice.
- Save the role, then assign it to the entity (user) that will authenticate the integration.
- Note that the integrations wont work if your role doesn't have access to the different permissions for each 'record type' etc.

5. Map the certificate to an entity and role

- Go to **Setup → Integration → OAuth 2.0 Client Credentials (M2M) Setup → Create New** .
- Select the entity (user), the role you created in the previous step, and the integration record you created, then upload your certificate.
- Save. NetSuite will display the **Certificate ID**. Copy and store it.

Need more help? Click here for NetSuite's API help documents.

Authenticate NetSuite in Alchemer

After obtaining your NetSuite API credentials, add them to the Alchemer NetSuite integration. Credentials are securely stored in Alchemer and can be reused.

How to Authenticate

1. Start a New Authentication

- Inside any NetSuite integration action, select **New Authentication**.

2. Enter Your NetSuite Credentials

Provide the following:

- **Account ID**, your NetSuite account identifier
- **Client ID**, from your OAuth 2.0 integration record
- **Client Secret**, from your OAuth 2.0 integration record
- **Certificate ID**, from the certificate mapped in the M2M setup
- **Private Key**, the private key that corresponds to your uploaded certificate

3. Save Your Authentication

- Select **Create**.
- Once created:
    - The authentication is saved and reused for all NetSuite actions
    - You only need to update it if your API credentials change

Related Articles