

AQUILA - Salesforce Integration (Username-Password Flow)

In Salesforce, the **Username-Password Flow** is an OAuth 2.0 authentication flow where an application obtains an access token by directly sending a Salesforce username, password, and (usually) security token to Salesforce.\

Important note

The Username-Password Flow is increasingly discouraged for new Salesforce integrations because it requires handling user credentials directly. For most modern integrations, the **JWT Bearer Flow** or **Client Credentials Flow** is usually preferred due to better security and easier compliance with MFA requirements.

How it works

The client application sends a request to Salesforce's OAuth token endpoint with:

- `grant_type=password`
- Salesforce username
- Salesforce password
- Security token (often appended to the password)
- Connected App client ID
- Connected App client secret

Salesforce validates the credentials and returns an access token if authentication succeeds.

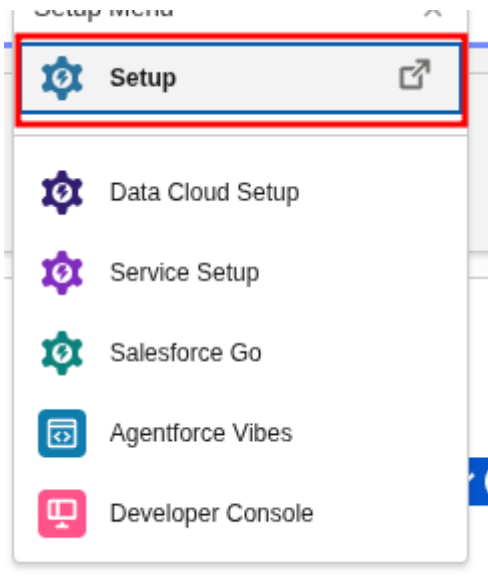
Log in to your Salesforce Organization.

Note: If the salesforce dashboard interface is in classic mode change it to lighting mode.

- In the Upper Right Corner click the gear icon.

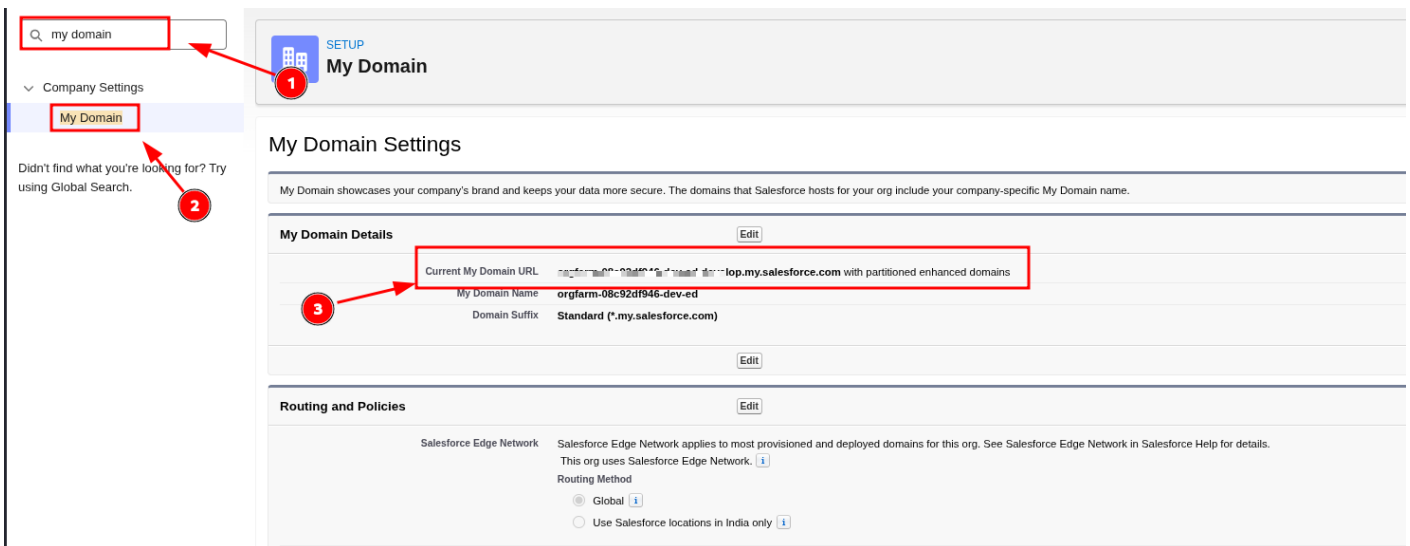


- Select setup.



To find the base URL and instance URL follow the guide below.

- In quick find box, enter my domain then select my domain under Company Settings.
- Under My Domain Details copy Current My Domain URL that's your base URL and Instance URL. (Give it to Cytech Support)



Creating User

- In Setup, enter Users in the Quick Find box, then select **Users**.
- Click **New User**.

The screenshot shows the Salesforce 'Users' page. A search bar at the top left contains the text 'users' (annotated with a red circle 1). Below it, the 'Users' link in the left sidebar is highlighted (annotated with a red circle 2). The main content area is titled 'All Users' and contains a table of users. The 'New User' button at the top right of the table is highlighted (annotated with a red circle 3).

Search: users

Users

Analytics Groups

Permission Set Groups

Permission Sets

Profiles

Public Groups

Queues

Roles

User Management Settings

Users

Feature Settings

Data.com

Prospector Users

Didn't find what you're looking for? Try using Global Search.

SETUP Users

All Users

On this page you can create, view, and manage users.

To get more licenses, use the Your Account app. [Let's Go](#)

View: All Users Edit Create New View

New User Reset Password(s) Add Multiple Users

Action	Full Name	Alias	Username
☐ Edit	User, Integration	integ	
☐ Edit	User, Security	sec	
☐ Edit	Chatter Expert	Chatter	
☐ Edit	EPIC_OrgFarm	OEPIK	
☐ Edit		ben	
☐ Edit	dady, Mac	mdady	
☐ Edit	testing	benj	

New User Reset Password(s) Add Multiple Users

- Fill out the form, and assign the System Administrator.
- Role > None Specified
- User License > Salesforce
- Profile > System Administrator

The screenshot shows the 'User Edit' form in Salesforce. The form is divided into 'General Information' and 'Permissions' sections. Annotations 1 through 8 point to specific fields: 1 points to the 'Last Name' field, 2 points to the 'Alias' field, 3 points to the 'Email' field, 4 points to the 'Username' field, 5 points to the 'Nickname' field, 6 points to the 'Role' dropdown, 7 points to the 'User License' dropdown, and 8 points to the 'Profile' dropdown.

SETUP Users

User Edit

Cancel Save Save & New

General Information

First Name

Last Name testing

Alias benj

Email

Username test001@mail.com

Nickname User1780996643416422664

Title

Company testing Company

Department

Division

Role <None Specified>

User License Salesforce

Profile System Administrator

Active ☒

Marketing User ☐

Offline User ☐

Knowledge User ☐

Flow User ☐

Service Cloud User ☐

Site.com Contributor User ☐

Site.com Publisher User ☐

WDC User ☐

Data.com User Type --None--

Data.com Monthly Addition Limit 300

Accessibility Mode (Classic Only) ☐

High-Contrast Palette on Charts ☐

Load Lightning Pages While Scrolling ☒

Debug Mode ☐

Send Apex Warning Emails ☐

Make Setup My Default Landing Page ☐

Quick Access Menu ☒

Development Mode ☐

Show View State in Development Mode ☐

Cache Diagnostics ☐

Salesforce CRM Content User ☒

Receive Salesforce CRM Content Email Alerts ☒

Receive Salesforce CRM Content Alerts as Daily Digest ☒

Allow Forecasting ☐

- Click **Save**.

Enable Allow Access to External Client App Consumer Secret via REST API

External Client App Setting > Allow Access to External Client App Consumer Secret via REST API

The screenshot shows the Salesforce Setup page for External Client App Settings. The left sidebar has a search bar with 'external' entered. The 'Settings' link under 'External Client App Management' is highlighted. The main content area shows the 'External Client App Settings' page. The 'Allow access to External Client App consumer secrets via REST API' toggle is turned on. Red circles and arrows indicate the steps: 1. Search for 'external', 2. Click on 'Settings', and 3. Turn on the REST API toggle.

External Client App Settings

External Client Apps
Integrate third-party apps with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect using External Client Apps. These settings apply to all External Client Apps configured in your org.

Allow access to External Client App consumer secrets via Metadata API
Allow the View External Client App Consumer Secrets in Metadata user permission to be assigned to users. Users with this permission can view External Client App consumer secrets in Metadata API responses. If this setting is disabled and you want to edit it, contact Salesforce Customer Support.

Allow access to External Client App consumer secrets via REST API
Allow users to access External Client App consumer secrets through the OAuth credentials resources for Connect REST API.

Connected Apps
Use connected apps to integrate third-party apps with Salesforce through APIs and standard protocols, such as SAML, OAuth, and OpenID.

[Learn more about Connected Apps and External Client Apps.](#)

[New Connected App](#)

Enable Event log files

Event Monitoring Settings > Generate event log files

The screenshot shows the Salesforce Setup page for Event Monitoring Settings. The left sidebar has a search bar with 'event monitoring Settings' entered. The 'Event Monitoring Settings' link is highlighted. The main content area shows the 'Event Monitoring Settings' page. The 'Generate event log files' toggle is turned on. Red circles and arrows indicate the steps: 1. Search for 'event monitoring Settings', 2. Click on 'Event Monitoring Settings', and 3. Turn on the 'Generate event log files' toggle.

Event Monitoring Settings

Event Monitoring
Event Monitoring helps you track, troubleshoot, and audit your organization's user activity.

Generate event log files
Generate an event log file when events occur in your org.

Delete event monitoring data
Let users delete event log files and LoginEvent data. Users require the Delete Event Monitoring Records user permission, which is available when this setting is enabled.

Enable Lightning Logger Events
Enable collection of Lightning Logger Events in custom components.

Enable Test Threat Detection Events (Beta)
Opt in to test threat detection events, input test information, and view past test results. Test Threat Detection Events (Beta) is a pilot or beta service that is subject to the Beta Services Terms at [Agreements - Salesforce.com](#) or a written Unified Pilot Agreement if executed by Customer, and applicable terms in the Product Terms Directory. Use of this pilot or beta service is at the Customer's sole discretion.

Transaction Security Policies
Create and manage policies to intercept Real-Time Events and apply actions to monitor and control user activity.

Event Manager
Manage streaming and storage settings for Real-Time Event Monitoring events.

Create A Connected Apps

For security reasons, Salesforce blocks the OAuth 2.0 Username-Password flow by default in recent releases. Prefer the JWT bearer flow. If you must use the Username-Password flow, in **OAuth and OpenID Connect Settings**, select **Allow OAuth Username-Password Flows**. For more information, see the Salesforce release note: [Username-Password OAuth flow blocked by default](#).

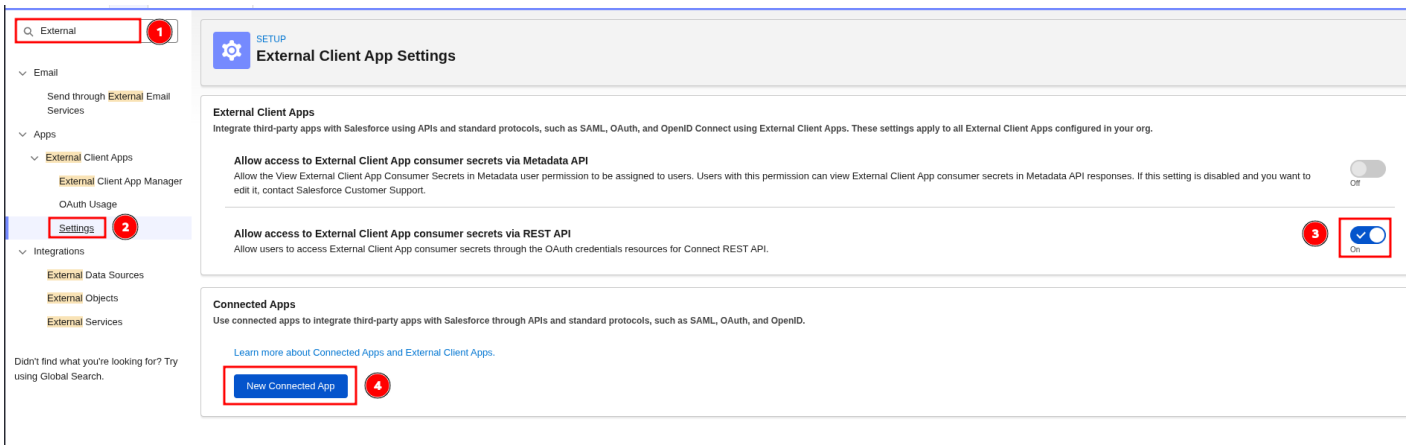
The screenshot shows the Salesforce Setup page for OAuth and OpenID Connect Settings. The left sidebar has a search bar with 'oauth and openid' entered. The 'OAuth and OpenID Connect Settings' link is highlighted. The main content area shows the 'OAuth and OpenID Connect Settings' page. The 'Allow OAuth Username-Password Flows' toggle is turned on. Red circles and arrows indicate the steps: 1. Search for 'oauth and openid', 2. Click on 'OAuth and OpenID Connect Settings', and 3. Turn on the 'Allow OAuth Username-Password Flows' toggle.

OAuth and OpenID Connect Settings

OAuth and OpenID Connect Flows
Control which OAuth 2.0 and OpenID Connect flows your connected apps can use. These settings affect your entire org. Username-password flows are blocked by default in orgs created in Summer '23 or later. Blocking a flow can break managed packages, mobile apps, and other integrations that use the flow. We recommend testing changes in a sandbox before implementing in production.

Allow OAuth Username-Password Flows
Allow your org to use the legacy OAuth 2.0 username-password flow to authorize an app that already has the user's credentials.

- Log in to Salesforce (Lightning UI).
- From **Setup**, in **Quick Find** enter **External Client Apps** and select **Settings**. Turn on **Allow creation of connected apps**. To create a connected app, select **New Connected App**.



- Fill **Basic Information**: **Connected App Name**, **API Name**, **Contact Email**.

New Connected App

Basic Information

Connected App Name	Cytech_Connected_App
API Name	Cytech_Connected_App
Contact Email	t.raj@cytechint.com
Contact Phone	
Logo Image URL	Upload logo image or Choose one of our sample logos
Icon URL	Choose one of our sample logos
Info URL	
Description	

- In **API (Enable OAuth Settings)**, check **Enable OAuth Settings**.
- **Callback URL**:
 - Web apps: your app callback (for example, `https://yourapp.example.com/callback`).
 - Not used by the JWT or Username-Password flows, but Salesforce requires a value; you can enter your instance URL.
- **Select OAuth scopes**:
 - **Manage user data via APIs (api)**
 - **Perform requests at any time (refresh_token, offline_access)**
 - **Full access (full)**
 - **Enable Client Credentials Flow**
 - **Enable Refresh Token Rotation**

▼ API (Enable OAuth Settings)

Enable OAuth Settings ☒

Enable for Device Flow ☐

Callback URL

Use digital signatures ☐

Selected OAuth Scopes

Available OAuth Scopes

- Access Agent-to-Agent API (a2a_api)
- Access Analytics REST API Charts Geodata resources (eclair_api)
- Access Analytics REST API resources (wave_api)
- Access Connect REST API resources (chatter_api)
- Access Einstein GPT services (einstein_gpt_api)
- Access Headless Forgot Password API (forgot_password)
- Access Headless Passwordless Login API (pwdless_login_api)
- Access Headless Registration API (user_registration_api)
- Access Interaction API resources (interaction_api)
- Access Lightning applications (lightning)

Add

Remove

Selected OAuth Scopes

- Full access (full)
- Manage user data via APIs (api)
- Perform requests at any time (refresh_token, offline_access)

Require Proof Key for Code Exchange (PKCE) Extension for Supported Authorization Flows ☒

Require Secret for Web Server Flow ☒

Require Secret for Refresh Token Flow ☒

Enable Client Credentials Flow ☒

Enable Authorization Code and Credentials Flow ☐

Enable Token Exchange Flow ☐

Enable Refresh Token Rotation ☐

Issue JSON Web Token (JWT)-based access tokens for named users ☐

Limit Idle Refresh Token Time-to-Live (TTL) to 30 Days ☐

- Click **Save**. It can take up to 10 minutes for the Connected App to propagate.
- After saving, open **Manage Consumer Details** to obtain **Consumer Key** and **Consumer Secret**.

Manage Consumer Details Appears only once so better to copy consumer key and consumer secret in a safe place.

SETUP

Manage Connected Apps

Review and lock security controls. [Review Controls](#)

Connected App Name
Cytech_Connected_App

« Back to List: Custom Apps

2

Edit Delete **Manage** Migrate to External Client App

Version 1.0

API Name Cytech_Connected_App

Created Date 6/9/2026, 5:54 AM

By: [benjie Janlay](#)

Contact Email [benjie.janlay@cytech.com](#)

Contact Phone

Last Modified Date 6/9/2026, 7:02 AM

By: [benjie Janlay](#)

Description

Info URL

▼ API (Enable OAuth Settings)

Consumer Key and Secret **1** **Manage Consumer Details**

Selected OAuth Scopes

- Manage user data via APIs (api)
- Full access (full)
- Perform requests at any time (refresh_token, offline_access)

Callback URL

Enable for Device Flow ☐

Require Proof Key for Code Exchange (PKCE) Extension for Supported Authorization Flows ☒

Require Secret for Web Server Flow ☒

Require Secret for Refresh Token Flow ☒

Enable Client Credentials Flow ☒

Enable Authorization Code and Credentials Flow ☐

Enable Token Exchange Flow ☐

Enable Refresh Token Rotation ☐

- Then Click Manage to OAuth Policies
 - Permitted Users > All users may self-authorize
 - IP Relaxation > Relax IP Restrictions
 - Refresh Token Policy > Expire refresh token after "365" days

SETUP

Basic Information

Start URL ⓘ
 Mobile Start URL ⓘ

OAuth Policies

Permitted Users **All users may self-authorize** ⓘ 1

Enable Single Logout ☐ ⓘ

IP Relaxation **Relax IP restrictions** ⓘ 2

Refresh Token Policy:

☐ Refresh token is valid until revoked
 ☐ Immediately expire refresh token
 ☐ Expire refresh token if not used for Day(s)
 ☒ Expire refresh token after **365** Day(s) ⓘ 3

Session Policies

Timeout Value **--None--** ⓘ
 ☐ High assurance session required

Custom Connected App Handler

Apex Plugin Class ⓘ

 Run As ⓘ

User Provisioning Settings

☐ Enable User Provisioning ⓘ

Client Credentials Flow

Run As ⓘ

Save Cancel

Verify if LoginEvent is enable in Quick find > Event Manager > enable all

Event manager

Events

21 events • Sorted by Name

Name	Subscription Channel	Type	Description	Streaming Data	Storing Data	
API Anomaly Event	/event/ApiAnomalyEvent	Event Monitoring	Track anomalies in how users make API calls	✓	✓	⌵
API Event	/event/ApiEventStream	Event Monitoring	Track user API queries in your org	✓	✓	⌵
Bulk API Result Event	/event/BulkApiResponseEvent	Event Monitoring	Track when a user downloads the results of a Bulk API request	✓	✓	⌵
Concurrent Long Running Apex Error Event	/event/ConcurLongRunApexErrEvent	Event Monitoring	Track when a Concurrent Long Running Apex error has occurred	✓	Not applicable	⌵
Credential Stuffing Event	/event/CredentialStuffingEvent	Event Monitoring	Track when a user successfully logs in to Salesforce during an identified credential stuffing attack	✓	✓	⌵
File Event	/event/FileEvent	Event Monitoring	Track file activity. For example, track when a user downloads or previews a file	✓	✓	⌵
Guest User Anomaly Event	/event/GuestUserAnomalyEvent	Event Monitoring	Tracks data access anomalies that are caused by guest user misconfiguration	✓	✓	⌵
Identity Provider Event	Not applicable	Event Monitoring	Track identity provider activities	Not applicable	✓	⌵
Identity Verification Event	Not applicable	Event Monitoring	Track when users verify their identity	Not applicable	✓	⌵
Lightning URI Event	/event/LightningUriEventStream	Event Monitoring	Track when a user creates, accesses, updates, or deletes a record in Salesforce Lightning	✓	✓	⌵
List View Event	/event/ListViewEventStream	Event Monitoring	Track when a user accesses data with list views	✓	✓	⌵
Login Anomaly Event	/event/LoginAnomalyEvent	Event Monitoring	This entity detects data access anomalies that are caused by potentially malicious login actions	✓	✓	⌵
Login Event	/event/LoginEventStream	Event Monitoring	Track when a user logs in to your org	✓	✓	⌵
LoginAs Event	/event/LoginAsEventStream	Event Monitoring	Track when an admin logs in to your org as another user	✓	✓	⌵
Logout Event	/event/LogoutEventStream	Event Monitoring	Track when a user clicks Log Out in the Salesforce UI	✓	✓	⌵
Permission Set Event	/event/PermissionSetEvent	Event Monitoring	Track when users are assigned the Modify All Data or View All Data permission through a perm...	✓	✓	⌵
Report Anomaly Event	/event/ReportAnomalyEvent	Event Monitoring	Track anomalies in how users run or export reports	✓	✓	⌵
Report Event	/event/ReportEventStream	Event Monitoring	Track when a user accesses or exports data with reports	✓	✓	⌵
Session Hijacking Event	/event/SessionHijackingEvent	Event Monitoring	Track when an unauthorized user gains ownership of a Salesforce user's session with a stolen ...	✓	✓	⌵
URI Event	/event/UriEventStream	Event Monitoring	Track when a user creates, accesses, updates, or deletes a record in Salesforce Classic	✓	✓	⌵
Universal Anomaly Event	/event/UniversalAnomalyEvent	Event Monitoring	This entity enables detecting data access anomalies with flexible subtype support for universal ...	✓	✓	⌵

Provide this to Cytech Support:

- Username
- Password

- **Consumer Key**
- **Consumer Secret**
- **Instance URL**

If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.

Revision #1

Created 17 June 2026 09:31:41 by Benjie Janlay Jr.

Updated 17 June 2026 09:55:01 by Benjie Janlay Jr.