**SSO Federation Implementation Guide**

This document outlines the process for customers who want to implement SSO Federation for FutureFeed.

**Data Transmission Requirements**

To ensure security, all sensitive data must be transmitted using encrypted methods to **Chase Berman: CBerman@futurefeed.co**

* The data should be sent via **two separate encrypted emails**:
  + If the customer cannot send two encrypted emails, they must use **two encrypted ZIP files**.
  + The ZIP file containing the client secret must be **encrypted again**.
  + The password for the encrypted ZIP file must be transmitted via a **different channel**.
  + **Emails should be treated as public information** and should not contain sensitive data without encryption.
* **Important:** The client secret must always be sent separately from other connection data.
  + Any information that includes the secret must be deleted from FutureFeed, including emails, ZIP files, and notes.

**Required Information for SSO Federation**

Customers must provide the following details for integration:

|  |  |
| --- | --- |
| **Description** | **Details** |
| **Endpoint 1** | OAuth 2.0 authorization endpoint (v2) |
| **Endpoint 2** | OAuth 2.0 token endpoint (v2) |
| **Endpoint 3** | OpenID Connect metadata document |
| **Microsoft Azure AD Domain** | Domain name (e.g., mycompany.com) |
| **Client ID** | Application ID in Azure AD |
| **Client Secret** | Sent separately in a different encrypted email |

**Following these guidelines ensures a secure and successful implementation of SSO Federation with FutureFeed.**