SAML認証設定マニュアル

最終更新日: 2023/04/18

1. はじめに

　このマニュアルでは、Grafferコンソールに対してユーザーがSAML認証でログインできるようになるまでの設定方法を解説します。なお、システムバージョンアップ等の要因により、本マニュアルに最新の状態が反映されていない可能性がありますが、予めご了承ください。

2. SAML認証機能の仕様

　Grafferコンソールにおいて、ユーザーはパスワード認証とSAML認証の2種類の認証方法のうち、予め定められた方法でログインすることができます。
　SAML認証では、SAML2.0の規格に則ったIdP（例: Google Workspace、Azure Active Directory、Okta）との間でSP InitiatedおよびIdP Initiatedのシングルサインオンを行うことができます。SAML認証のユーザーは外部ユーザーIDとしてIdPのNameID（一意キー）が登録されており、IdPにログインしていれば、認証情報を再度入力することなくGrafferコンソールを利用することができます。

3. 設定の流れ

3-1. SAML認証利用の登録

　Graffer導入担当者にご連絡いただき、SAML認証を利用する旨をお伝えください。Graffer側でGrafferコンソールの設定を変更し、貴社のテナントでSAML認証を有効化します。

3-2. IdPの設定（アプリケーションの作成）

　貴社のIdPにおいて、GrafferコンソールとのSAML連携用のアプリケーションを作成してください。その際、ACS URLとEntity IDにGrafferコンソールが指定する値を次の通り入力してください。

- ACS URL
  - https://console.graffer.jp/api/saml/callback
  - ※IdPによっては「Single sign-on URL」という表記の場合があります。
- Entity ID
  - https://console.graffer.jp/${slug}
  - ※IdPによっては「Audience URI」という表記の場合があります。
  - ※${slug}の箇所には貴社テナントのスラグ（組織コード）が入ります。

設定例1: OktaをIdPとして利用している場合

Admin権限のあるユーザーでOktaにログインします。Admin Consoleのサイドメニューにおいて「Applications」グループにある 「Applications」のメニューを選択し、「Create App Integration」ボタンを押下して新規アプリケーションの作成を開始します。

「Create a new app integration」のモーダルにおいて、「SAML 2.0」のSign-in methodを選択してください。

Step1の「General Settings」ではアプリケーションの基本情報を任意の値で入力してください。

Step2の「Configure SAML」では以下のように情報を記入してください。

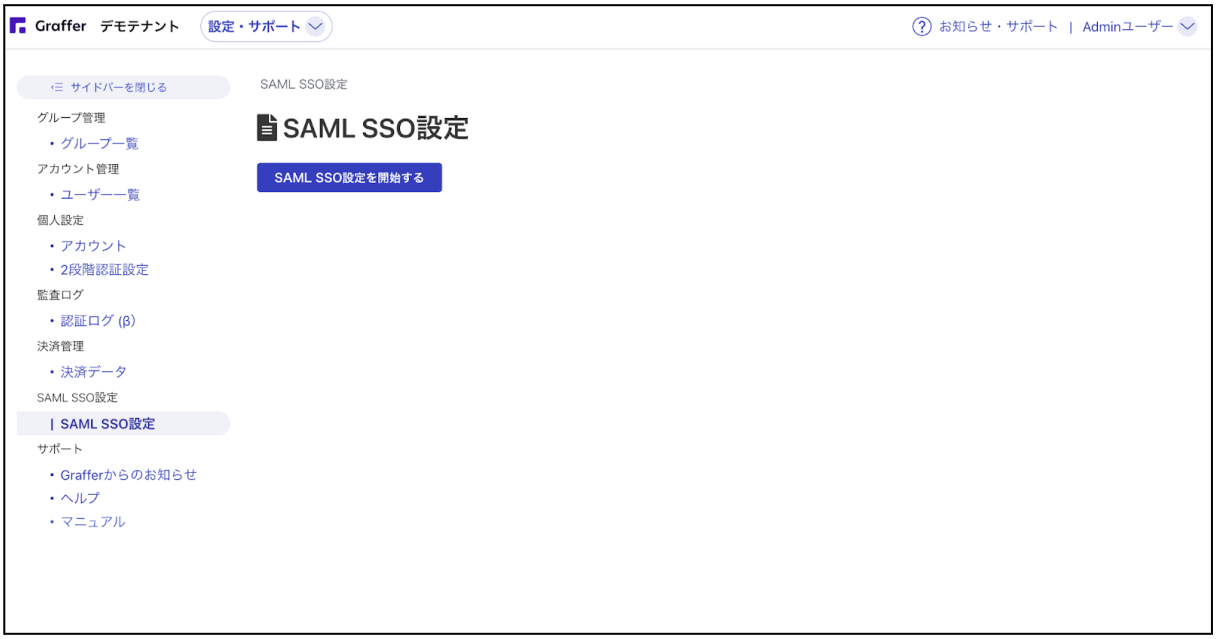
- Single sign-on URL
  - `https://console.graffer.jp/api/saml/callback`
- Audience URI (SP Entity ID)
  - `https://console.graffer.jp/sample-tenant`
  - ※スラグ（組織コード）が `sample-tenant` のテナントに対する設定例です。
- Default RelayState
  - 空欄
  - ※IdP Initiated SSOを行う場合、3-4のステップで入力が必要です。
- Name ID format
  - Grafferコンソールでユーザーを作成する際に外部ユーザーIDとして利用するフォーマットを選択してください

Step3の「Feedback」では任意の情報を入力してください。

3-3. SPの設定（SAML設定の作成）

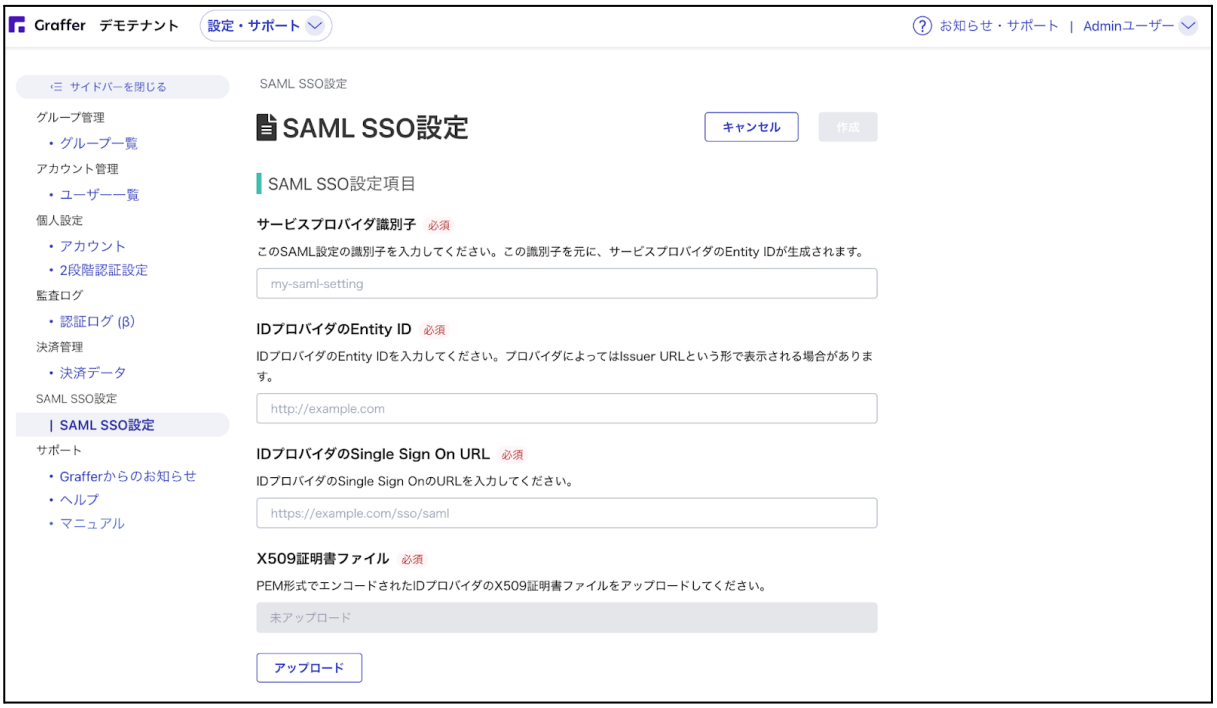
GrafferコンソールにAdmin権限のユーザー（※）でログインします。「設定・サポート」メニューから「SAML SSO設定」を選択し、「SAML SSO設定を開始する」ボタンを押下してSAML SSO設定を開始します。

※この設定の際に利用するユーザーは、SAML認証ではなくパスワード認証でGrafferの導入担当者から予め払い出しを受けてください。



以下の項目に、次の通り値を入力して、設定を保存してください。

- サービスプロバイダ識別子
  - 任意の値（半角英数字または半角ハイフンのみ）
- IDプロバイダのEntity ID
  - 3-2で作成したアプリケーションのEntity ID
  - ※IdPによっては「Issuer URL」という表記の場合があります。
- IDプロバイダのSingle Sign On URL
  - 3-2で作成したアプリケーションのSingle Sign ON URL
- X509証明書ファイル
  - 3-2で作成したアプリケーションから証明書ファイルをpem形式でダウンロードし、こちらにアップロードします。



設定例1: OktaをIdPとして利用する場合

3-2で作成したアプリケーションの詳細画面を開き、「Sign On」タブを開きます。「Settings」 > 「Metadata details」の領域内にある以下の値をコピーして、GrafferコンソールのSAML設定画面に入力します。

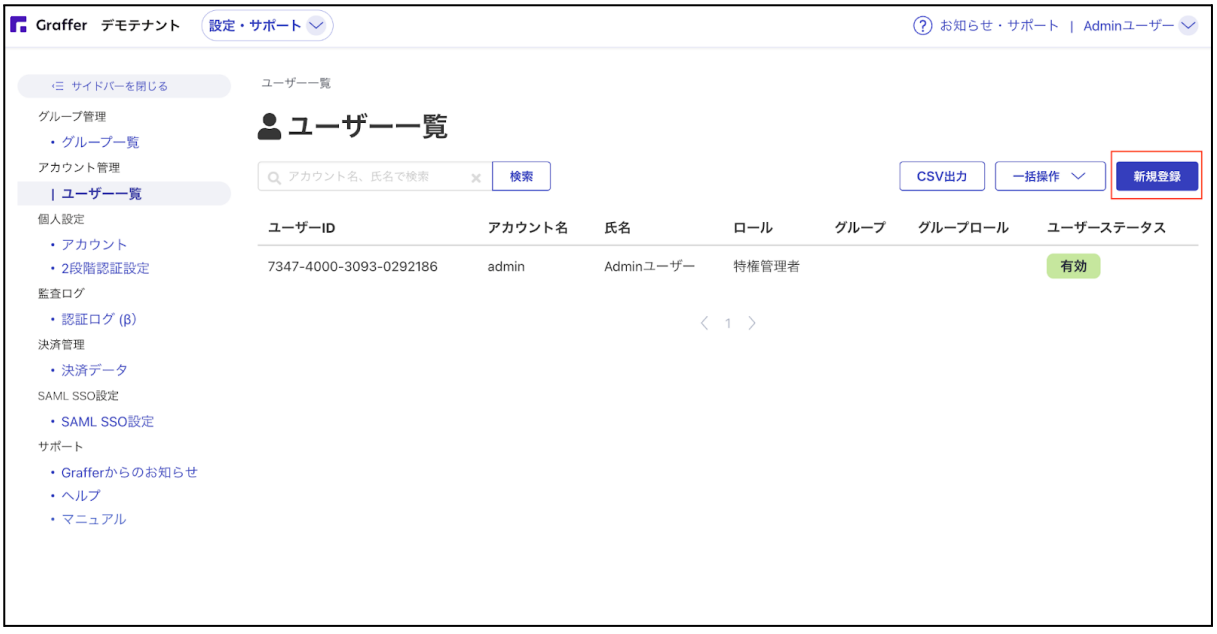
- Sign on URL
  - -> IDプロバイダのSingle Sign On URL
- Issuer
  - -> IDプロバイダのEntity ID
- Signing Certificate
  - -> ダウンロードしてX509証明書ファイルにアップロード

3-4. RelayStateの登録（任意）

IdP InitiatedのSSOを行う場合、IdPのアプリケーションにRelayState（リレー状態）の設定が必要です。SAML SSOの設定完了後、SAML SSO設定画面にRelay Stateが表示されますので、その値をIdP側に登録してください。

3-5. SAML認証ユーザーの作成

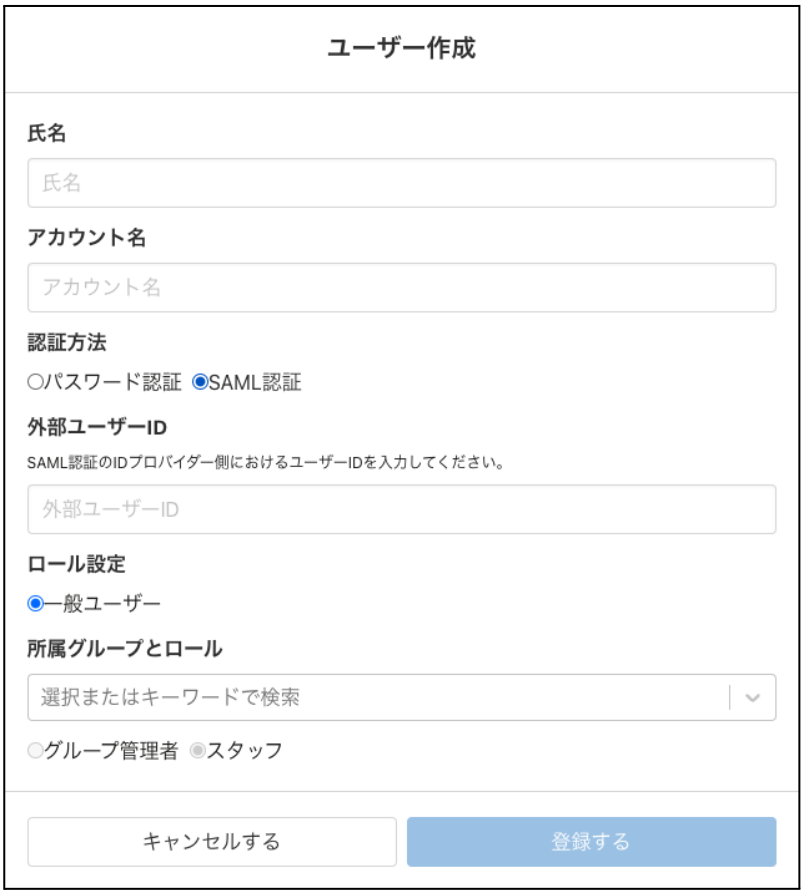
GrafferコンソールにAdmin権限のユーザーでログインします。「設定・サポート」メニューから「ユーザー一覧」を選択し、「新規登録」ボタンを押下してユーザー作成を開始します。



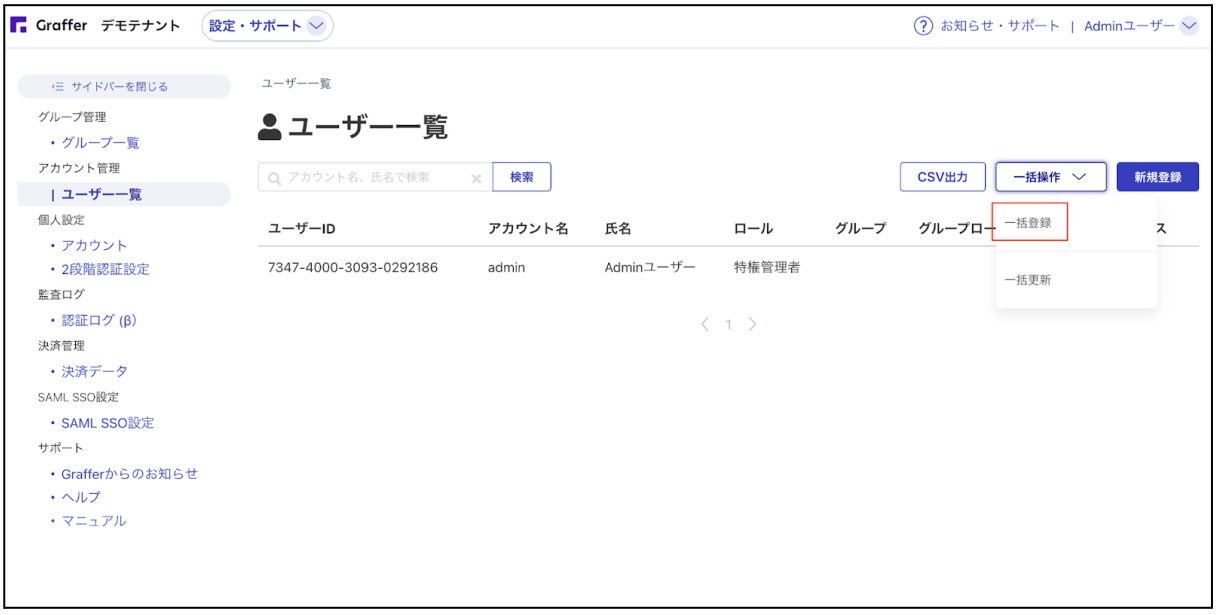
ユーザー作成画面が開くので、以下の情報を入力し、ユーザーを作成してください。

- 氏名
  - ユーザーの表示名
- アカウント名
  - 任意の文字列（半角英数字のみ）
  - ※この値がGrafferコンソール内の一意キーとなります。

- 認証方法
    - 「SAML認証」を選択
- 外部ユーザーID
    - IdP側のユーザーの一意キー
    - ※IdPのアプリケーション作成時に選択したNameIDを利用してください。多くの場合、メールアドレスが一意キーとして利用されます。
- ロール設定
    - 「一般ユーザー」を選択
- 所属グループとロール
    - ユーザーの所属グループとロールを選択
    - ※グループが未作成の場合、「グループ一覧」からグループを作成してください。

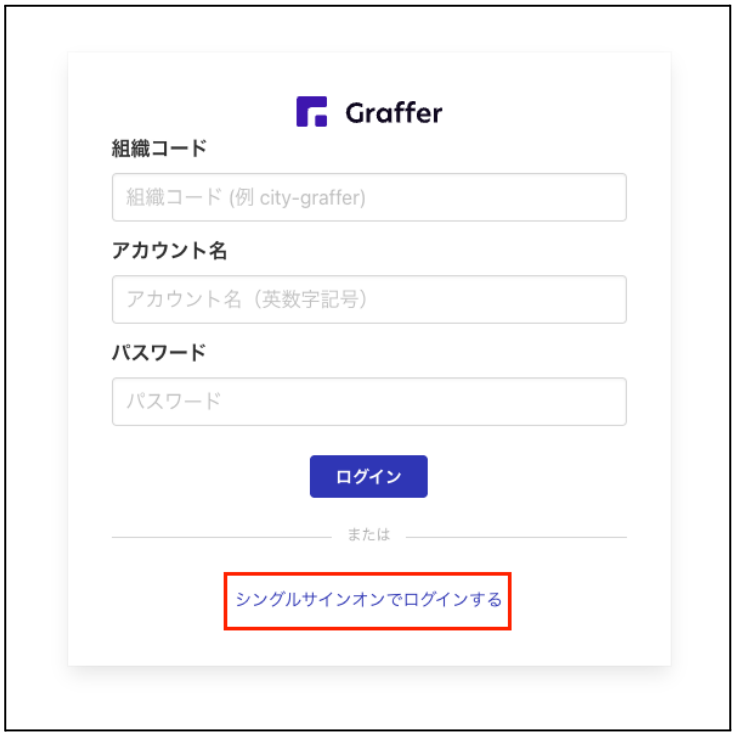


CSV取り込みによりユーザーを一括登録することもできます。ユーザー一覧画面の「一括操作」 > 「一括登録」を選択し、テンプレートCSVをダウンロードしてください。CSVに登録するユーザー情報を入力してアップロードすると、ユーザーが一括登録されます。



3-6. SAML認証でログイン

Grafferコンソールからログアウトした状態でログイン画面（`https://console.graffer.jp/login`）を開き、「シングルサインオンでログインする」を押下します。



組織コード入力画面で組織コード（※）を入力し、「シングルサインオンでログインする」を押下すると、IdPの認証情報が参照され、IdPでログインされていればGrafferコンソールにSAML認証でログインできます。

※ログインURLに `?slug=xxx` というクエリパラメータがついている場合、xxxの値が組織コードとして補完されます。これにより、ユーザーは組織コードを知らなくともクリックだけでログインできます。