SAML/SCIM 連携設定手順

2021-04-28 作成
2021-08-31 更新

WANTEDLY ©2021 Wantedly, Inc.

はじめに

- この資料はβリリース用の設定手順書です
- この資料に書かれている内容は正式リリース時に変更される場合があります
- 2021年4月28日時点の情報のため内容が古くなっている場合があります
- 開発中の機能のため各 IdP のギャラリーへの登録は未対応です

©2021 Wantedly, Inc.

想定している利用ケース

- SAML のみ
  - 従業員が Wantedly のサービスを利用するために使用
  - システム管理者による個別のメンバー追加なくして業務を効率化

- SAML + SCIM
  - SAML と同じ + 従業員の入退社に合わせてメンバーの追加や削除する
  - SCIM で招待 → SAML で有効化

©2021 Wantedly, Inc.

必要な権限の確認

1. ID Provider (IdP) の管理権限

各IdP でアプリケーションを登録する権限が必要です

2. Wantedly 企業アカウントの管理権限

全体の管理 の オーナー または 管理者 の権限が必要です
https://help.wantedly.com/hc/ja/articles/204195319

WANTEDLY ©2021 Wantedly, Inc.

各 IdP ごとの対応機能

	SAML	SCIM	補足
Google Workspace (GSuite)	○	✕	SAML のみ利用可
Azure AD	○	○※	SCIM 連携時にエラー表示になるバグがあります (機能的には問題ありません)
OneLogin	○	○※	
Okta	○	△※	SCIM はメンバー追加のみ対応 メンバー削除 (deprovisioning) には非対応

※ SCIM によるプロビジョニングは User API のみの対応しています。Group API は利用できません。

WANTEDLY ©2021 Wantedly, Inc.

設定手順

- 共通の手順
- Google Workspace (GSuite)
- Azure AD
- OneLogin
- Okta

WANTEDLY ©2021 Wantedly, Inc.

FAQ

- SAML によるログイン必須化について
  - 現在は SAML ログイン必須化の機能はありません
  - 企業の情報へのアクセス時にSAML 認証を必須化する機能の開発を検討中です

- 連携時の権限について
  - メンバー追加時のデフォルト権限は管理画面から変更可能です
  - グループ単位で細かく権限設定を行う機能は開発を検討中です

©2021 Wantedly, Inc.

IdP ごとに共通の設定手順

©2021 Wantedly, Inc.

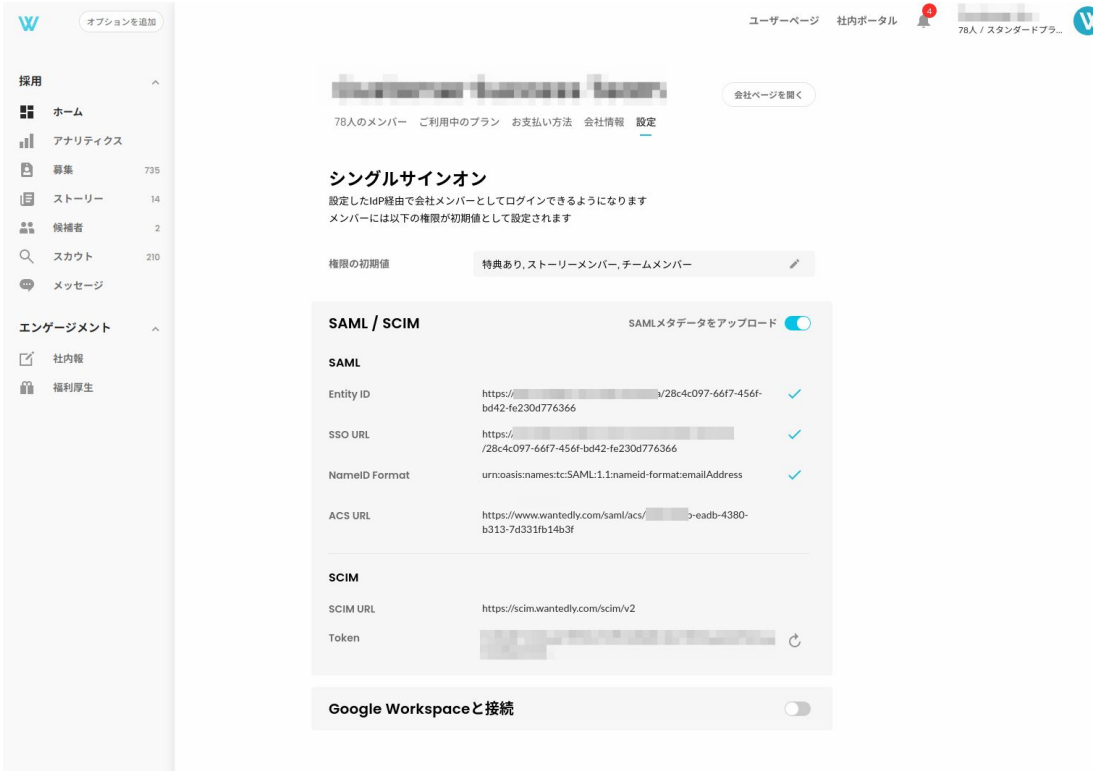
おおまかな手順

1. **SAML (必須)**
    1.1. 各 IdP でアプリケーションを作成
    1.2. アプリケーションの SAML metadata を Wantedly 上の管理画面に登録
    1.3. IdP に Assertion Consumer Service (ACS) URL を登録
    1.4. NameID を Email Address に変更
2. **SCIM (任意)**
    2.1. SCIM URL と Token を IdP に登録
    2.2. userName attribute を Email Address に変更

WANTEDLY ©2021 Wantedly, Inc.

Wantedly 上の管理画面

https://admin.wantedly.com/company-account/settings



WANTEDLY ©2021 Wantedly, Inc.

権限の初期値の変更

https://admin.wantedly.com/company-account/settings

メンバー追加時の権限は「権限の初期値」よりご変更頂けます。

設定できる権限の詳細については ヘルプ をご確認下さい。



WANTEDLY ©2021 Wantedly, Inc.

SAML metadata のアップロード方法

SAMLメタデータをアップロード をクリックして

IdP からダウンロードしたメタデータのファイルを選択します



WANTEDLY ©2021 Wantedly, Inc.

SCIM の動作確認方法

正しく設定できている場合はメンバー管理画面に **招待中** のメンバーが追加されます。（追加されない場合はメールにてご連絡ください。）



WANTEDLY ©2021 Wantedly, Inc.

Google Workspace (GSuite) の設定手順

WANTEDLY ©2021 Wantedly, Inc.

Google Workspace (GSuite) の設定手順

Google Admin の **アプリ → SAML アプリ** から **カスタム SAML アプリ** を追加します



WANTEDLY ©2021 Wantedly, Inc.

Google Workspace (GSuite) の設定手順

Google Admin の **アプリ → SAML アプリ** から **カスタム SAML アプリ** を追加します



WANTEDLY ©2021 Wantedly, Inc.

Google Workspace (GSuite) の設定手順

メタデータをダウンロード して [Wantedly 上の管理画面](#)でアップロードします



WANTEDLY ©2021 Wantedly, Inc.

Google Workspace (GSuite) の設定手順

メタデータをダウンロード して [Wantedly 上の管理画面](#)にアップロードします



WANTEDLY ©2021 Wantedly, Inc.

Google Workspace (GSuite) の設定手順

サービスプロバイダの詳細を入力します
エンティティ ID には [Wantedly の管理画面上](#)の **Entity ID** を入力します



WANTEDLY ©2021 Wantedly, Inc.

Google Workspace (GSuite) の設定手順

サービスプロバイダの詳細を入力します
名前 ID の形式を **EMAIL** に変更します



WANTEDLY ©2021 Wantedly, Inc.

Google Workspace (GSuite) の設定手順

属性のマッピングは何も入力せず**完了** をクリックして設定は完了です



WANTEDLY ©2021 Wantedly, Inc.

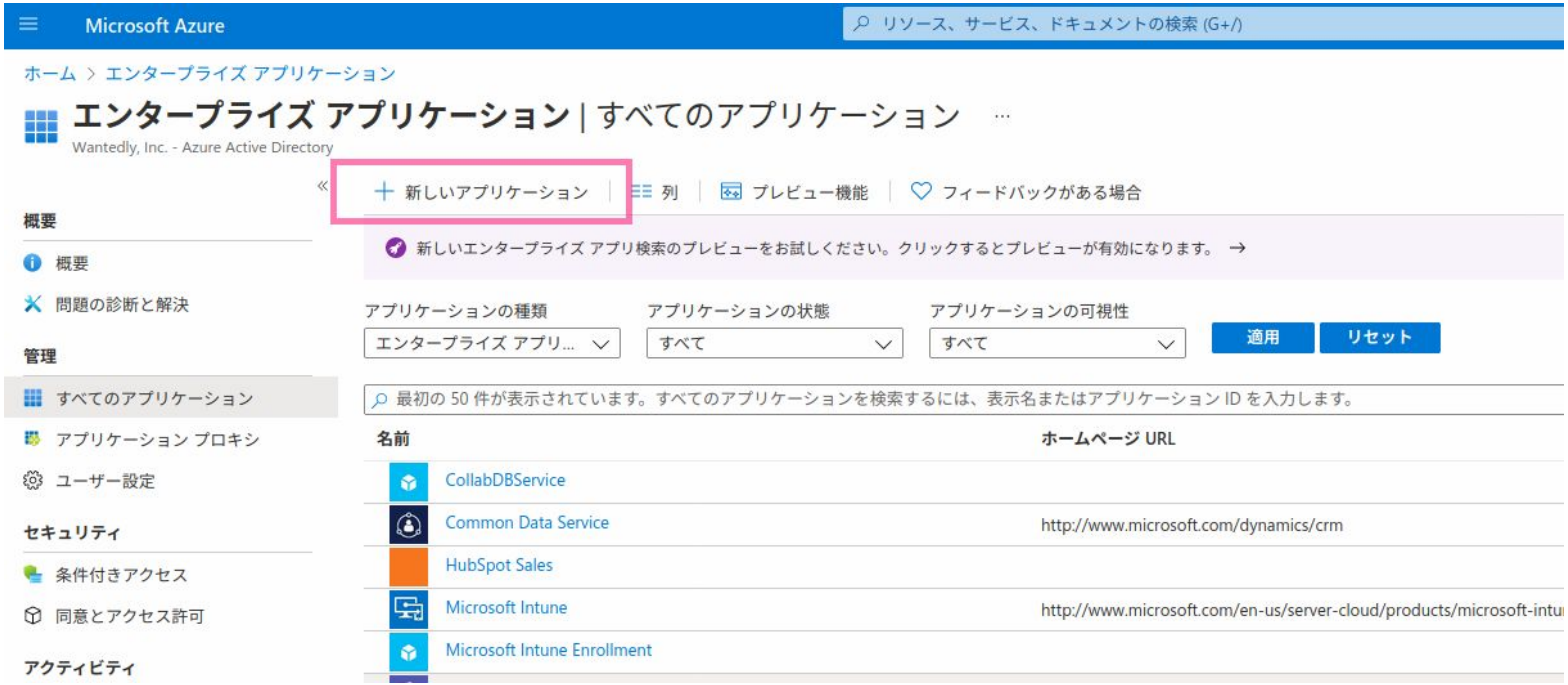
Azure AD の設定手順

©2021 Wantedly, Inc.

Azure AD の設定手順 - SAML

Azure Portal の **Azure AD → エンタープライズアプリケーション** から

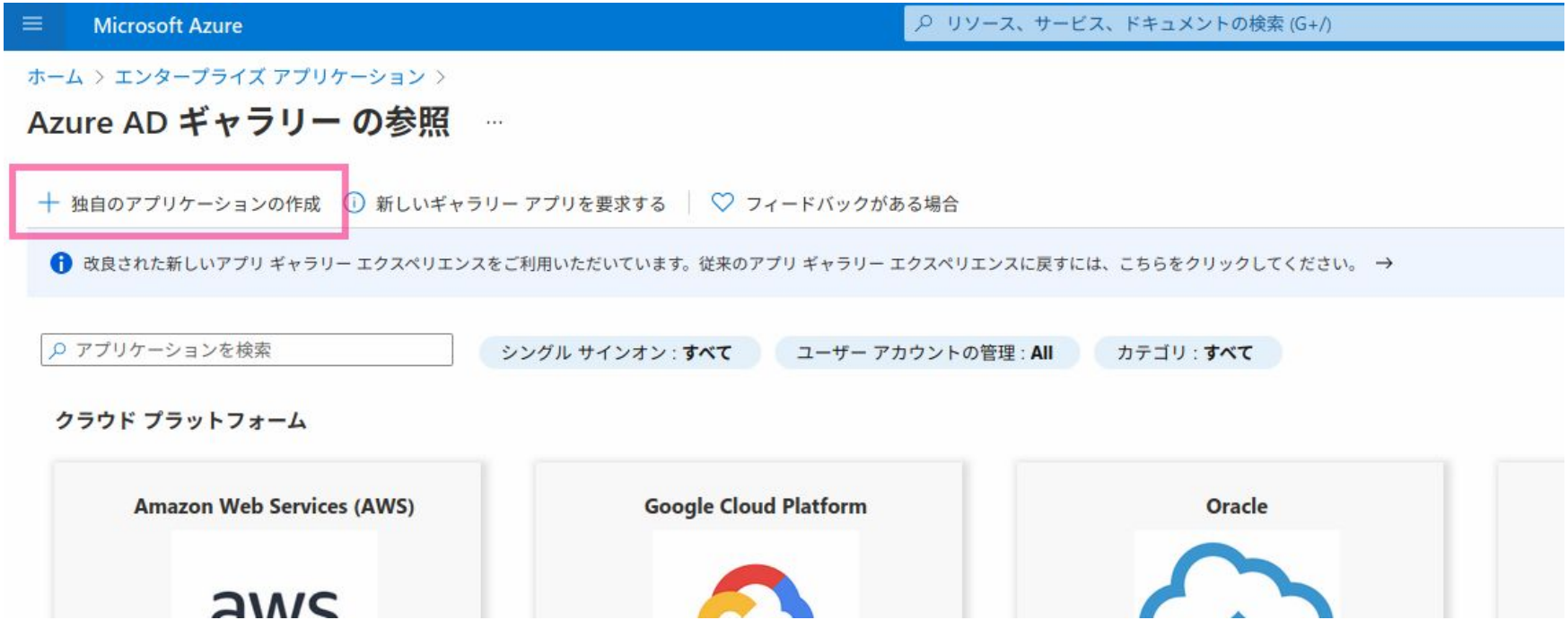
新しいアプリケーションを追加 します



WANTEDLY ©2021 Wantedly, Inc.

Azure AD の設定手順 - SAML

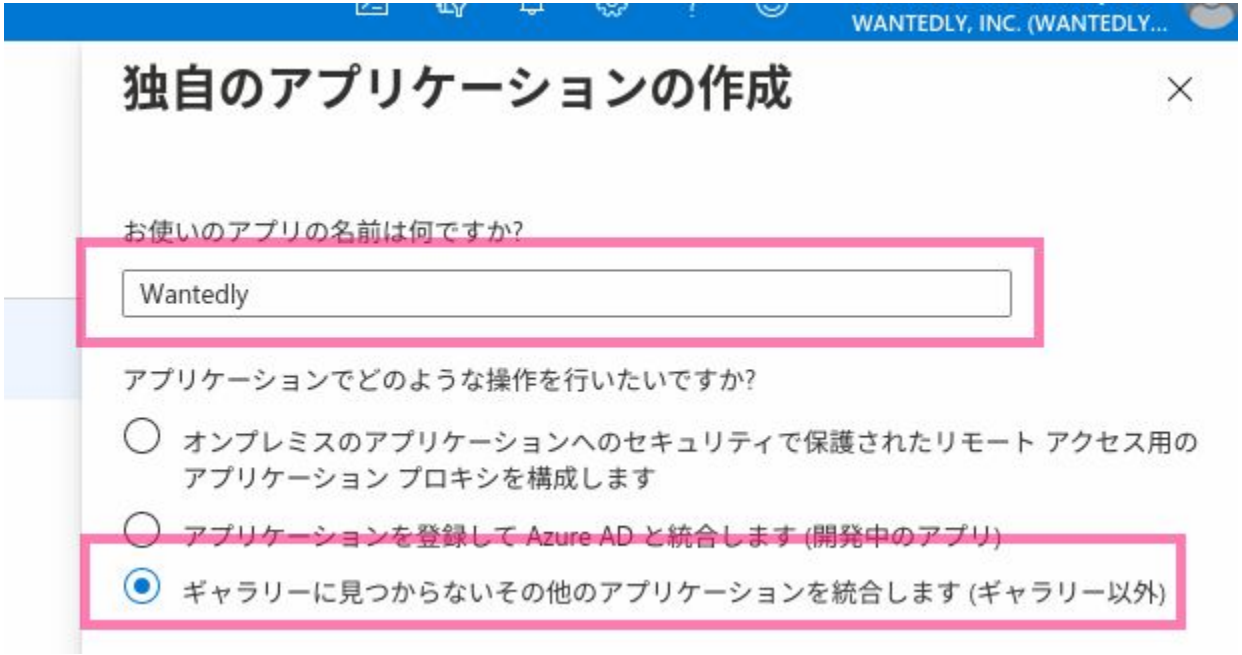
独自のアプリケーションの作成 から **ギャラリー以外** でアプリケーションを作成します



WANTEDLY ©2021 Wantedly, Inc.

Azure AD の設定手順 - SAML

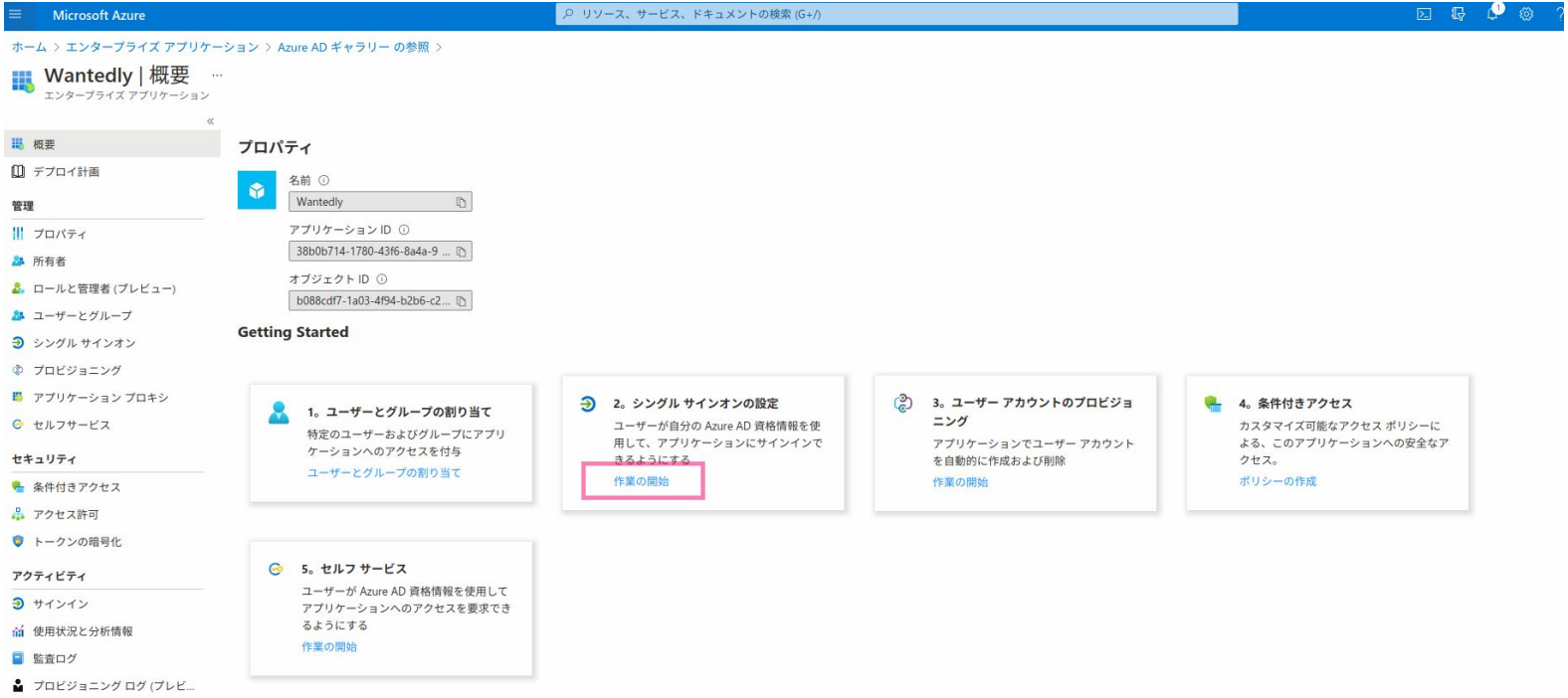
独自のアプリケーションの作成 から **ギャラリー以外** でアプリケーションを作成します



©2021 Wantedly, Inc.

Azure AD の設定手順 - SAML

シングルサインオンの設定 から **SAML** を選択します



WANTEDLY ©2021 Wantedly, Inc.

Azure AD の設定手順 - SAML

シングルサインオンの設定 から **SAML** を選択します

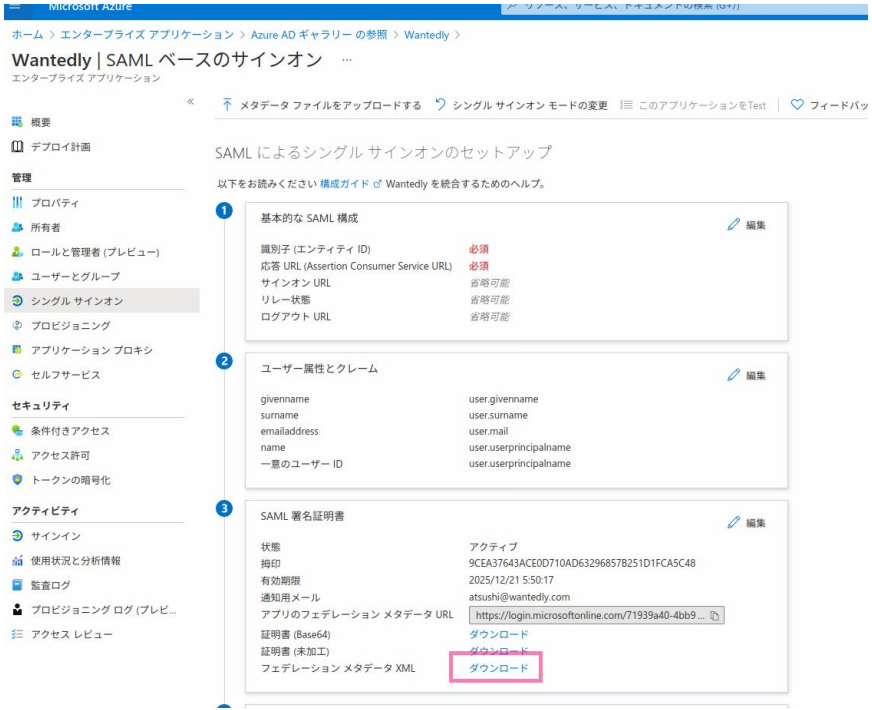


WANTEDLY ©2021 Wantedly, Inc.

Azure AD の設定手順 - SAML

フェデレーション メタデータ XML を ダウンロード して

Wantedly 上の管理画面にアップロードします

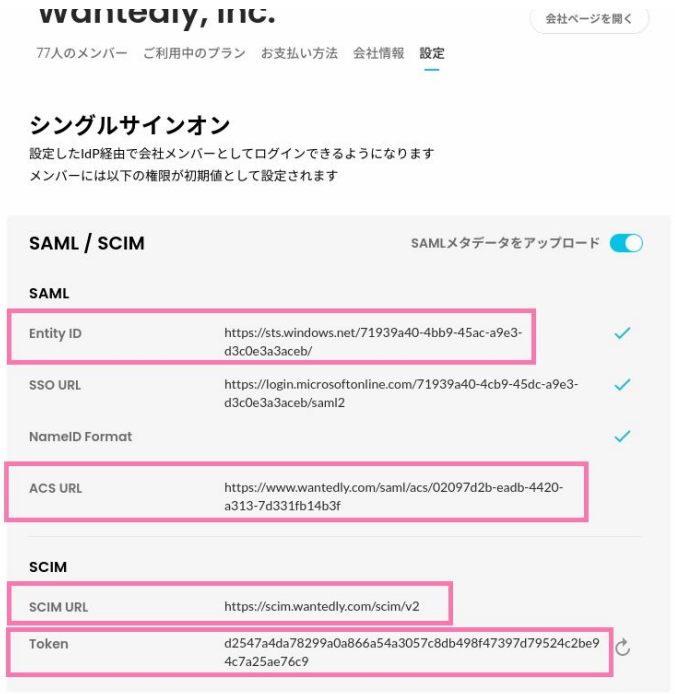


WANTEDLY ©2021 Wantedly, Inc.

Azure AD の設定手順 - SAML

フェデレーション メタデータ XML を ダウンロード して

Wantedly 上の管理画面にアップロードします



WANTEDLY ©2021 Wantedly, Inc.

Azure AD の設定手順 - SAML

基本的な SAML 構成 から **識別子** と **応答 URL** を入力します

識別子 = Entity ID,　応答 URL = ACS URL

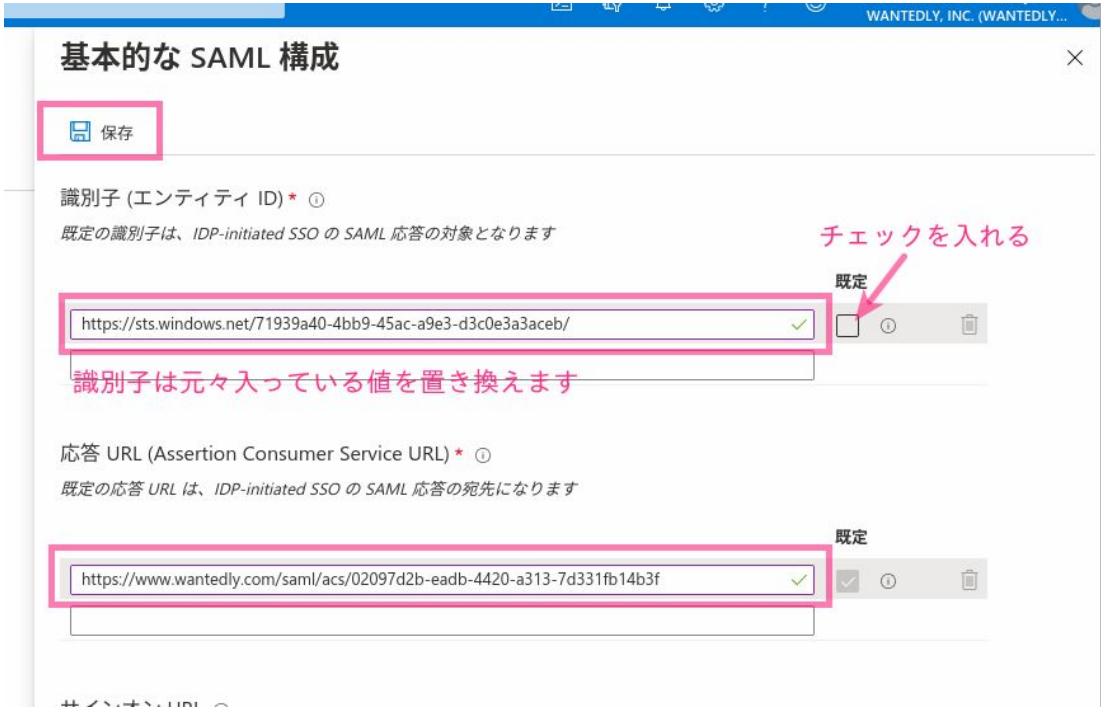


WANTEDLY ©2021 Wantedly, Inc.

Azure AD の設定手順 - SAML

基本的な SAML 構成 から **識別子** と **応答 URL** を入力して **保存** します

(識別子 = Entity ID, 応答 URL = ACS URL)

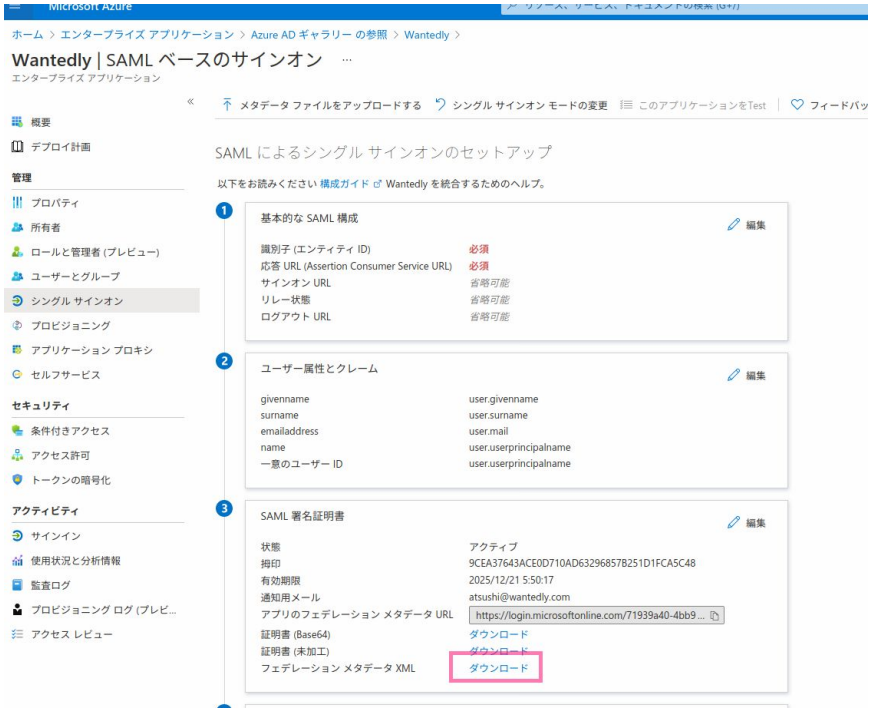


WANTEDLY ©2021 Wantedly, Inc.

Azure AD の設定手順 - SAML

再度**フェデレーション メタデータ XML** を **ダウンロード** して

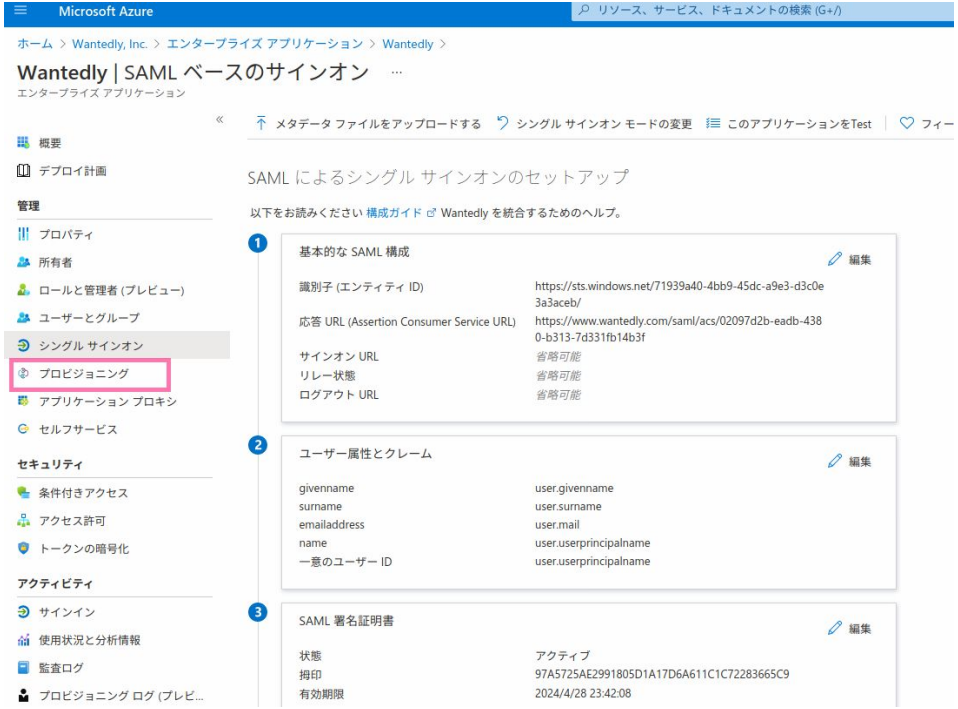
Wantedly 上の管理画面にアップロードします。これでSAMLの設定は完了です。



WANTEDLY ©2021 Wantedly, Inc.

Azure AD の設定手順 - SCIM

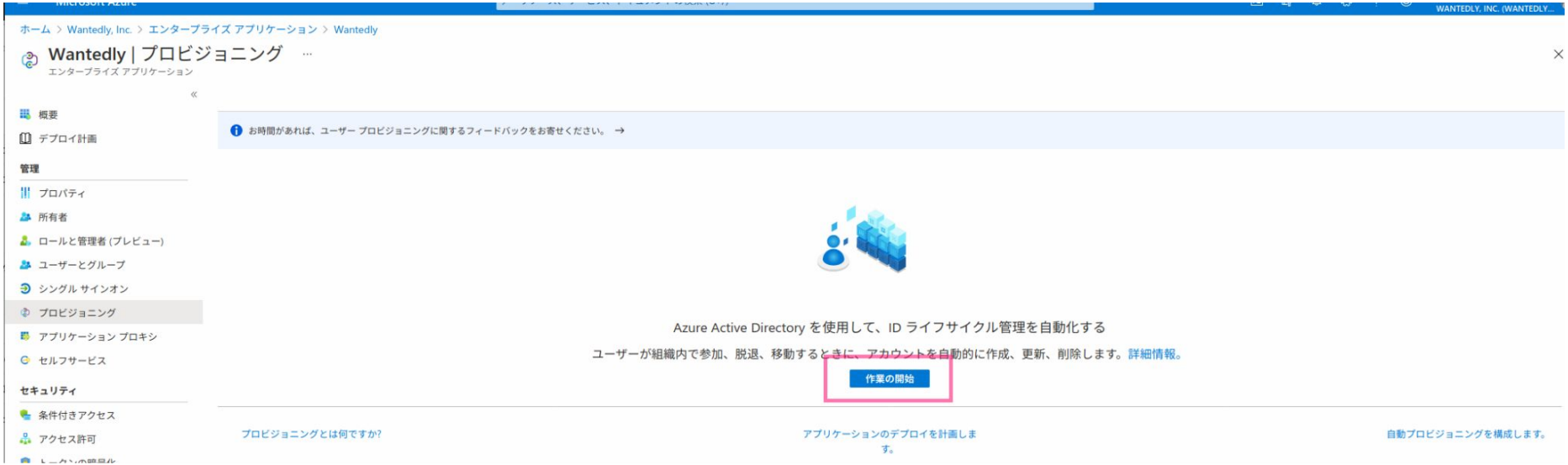
管理 → プロビジョニング から SCIM の設定を行います



WANTEDLY ©2021 Wantedly, Inc.

Azure AD の設定手順 - SCIM

管理 → プロビジョニング から SCIM の設定を行います

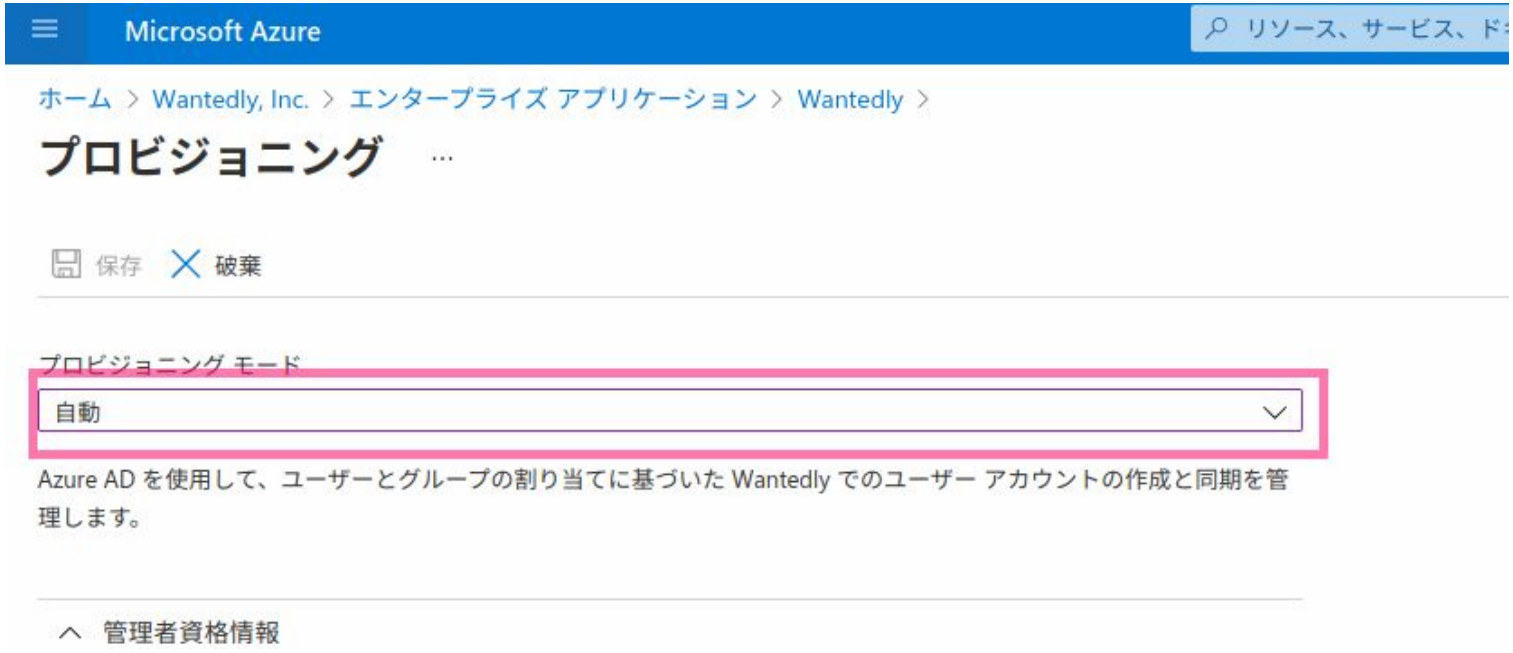


WANTEDLY ©2021 Wantedly, Inc.

Azure AD の設定手順 - SCIM

管理 → **プロビジョニング** から SCIM の設定を行います

プロビジョニングモード は **自動** を選択します



WANTEDLY ©2021 Wantedly, Inc.

Azure AD の設定手順 - SCIM

管理 → プロビジョニング から SCIM の設定を行います

テナントの URL と **シークレット トークン** を入力します



WANTEDLY ©2021 Wantedly, Inc.

Azure AD の設定手順 - SCIM

テスト接続 で設定を確認し、問題なければ**保存** して SCIM の設定は完了です



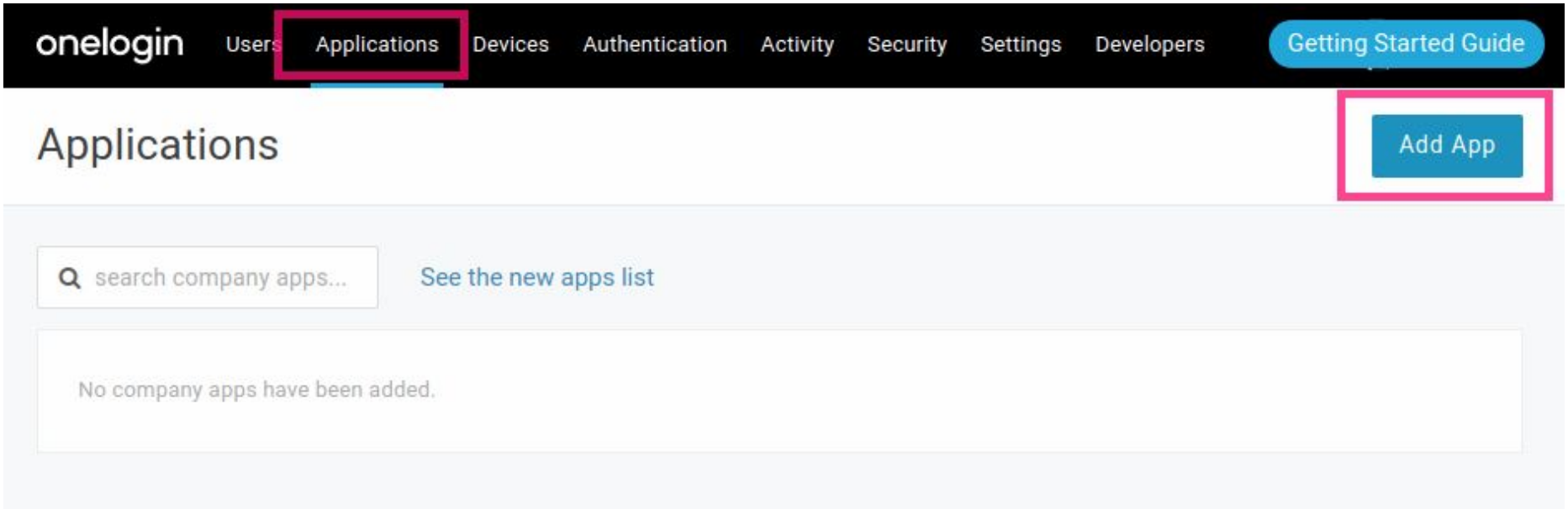
WANTEDLY ©2021 Wantedly, Inc.

OneLogin の設定手順

©2021 Wantedly, Inc.

OneLogin の設定手順 - SAML

Applications → Add App からアプリケーションを追加します

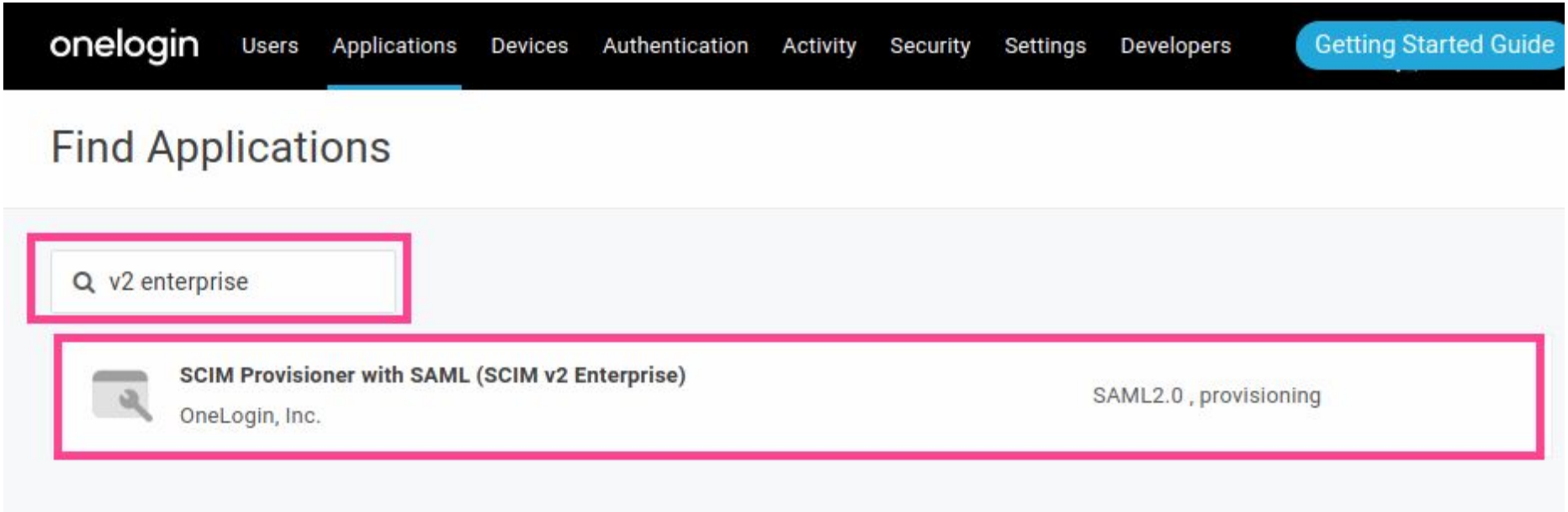


WANTEDLY ©2021 Wantedly, Inc.

OneLogin の設定手順 - SAML

Applications → Add App からアプリケーションを追加します

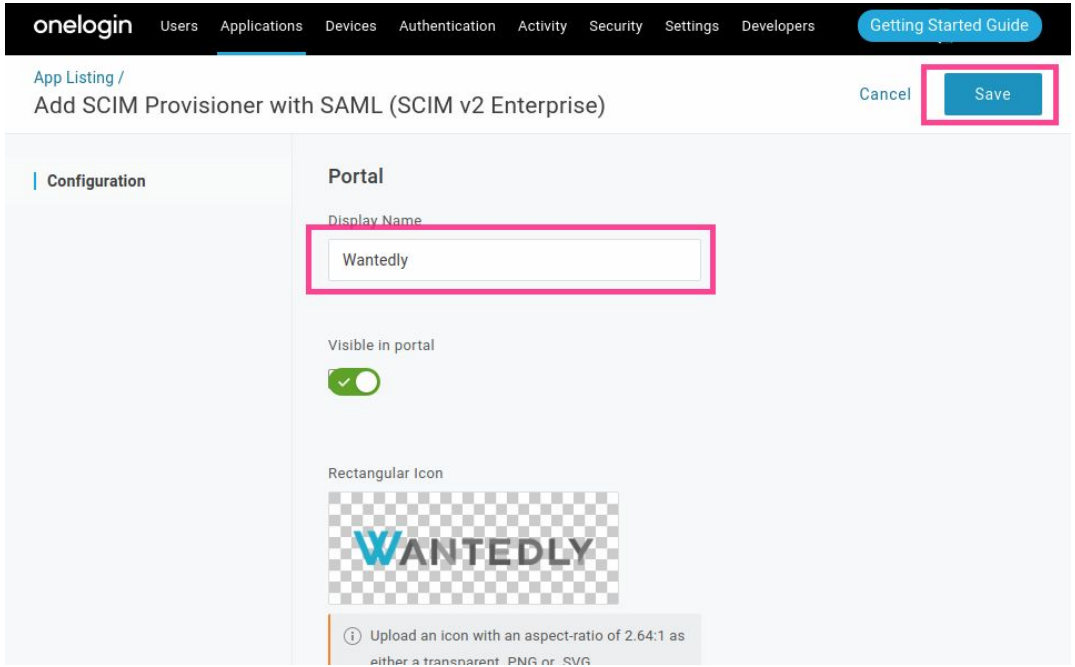
search.. に **v2 enterprise** と入力してヒットしたアプリケーションを選択します



WANTEDLY ©2021 Wantedly, Inc.

OneLogin の設定手順 - SAML

Display Name を設定して **Save** します

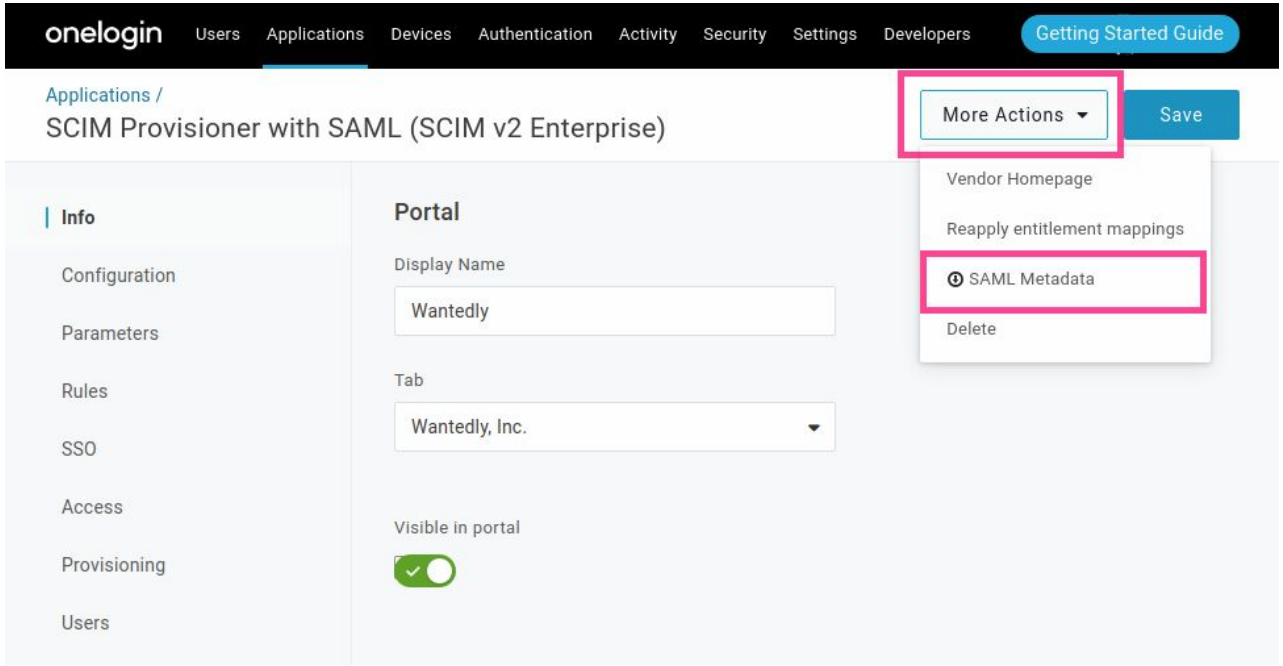


WANTEDLY ©2021 Wantedly, Inc.

OneLogin の設定手順 - SAML

More Actions → SAML Metadata からメタデータをダウンロードして

Wantedly 上の管理画面にアップロードします

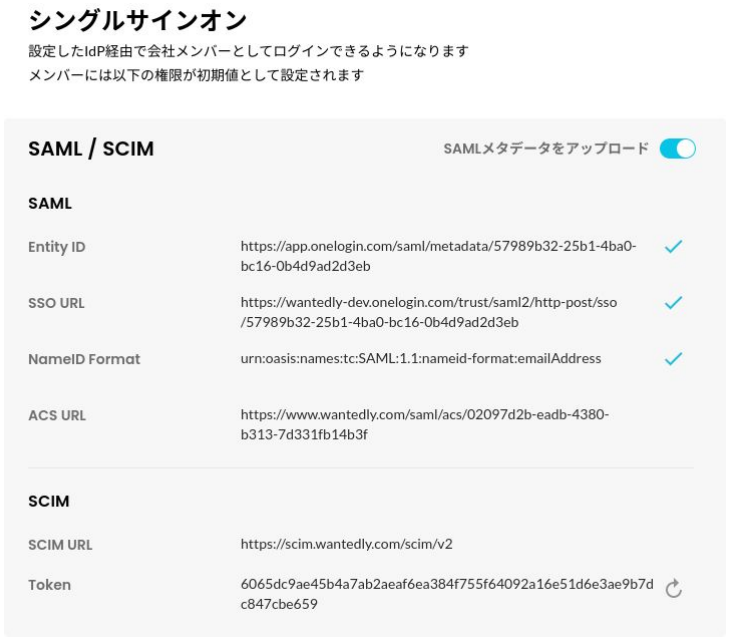


WANTEDLY ©2021 Wantedly, Inc.

OneLogin の設定手順 - SAML

More Actions → SAML Metadata からメタデータをダウンロードして

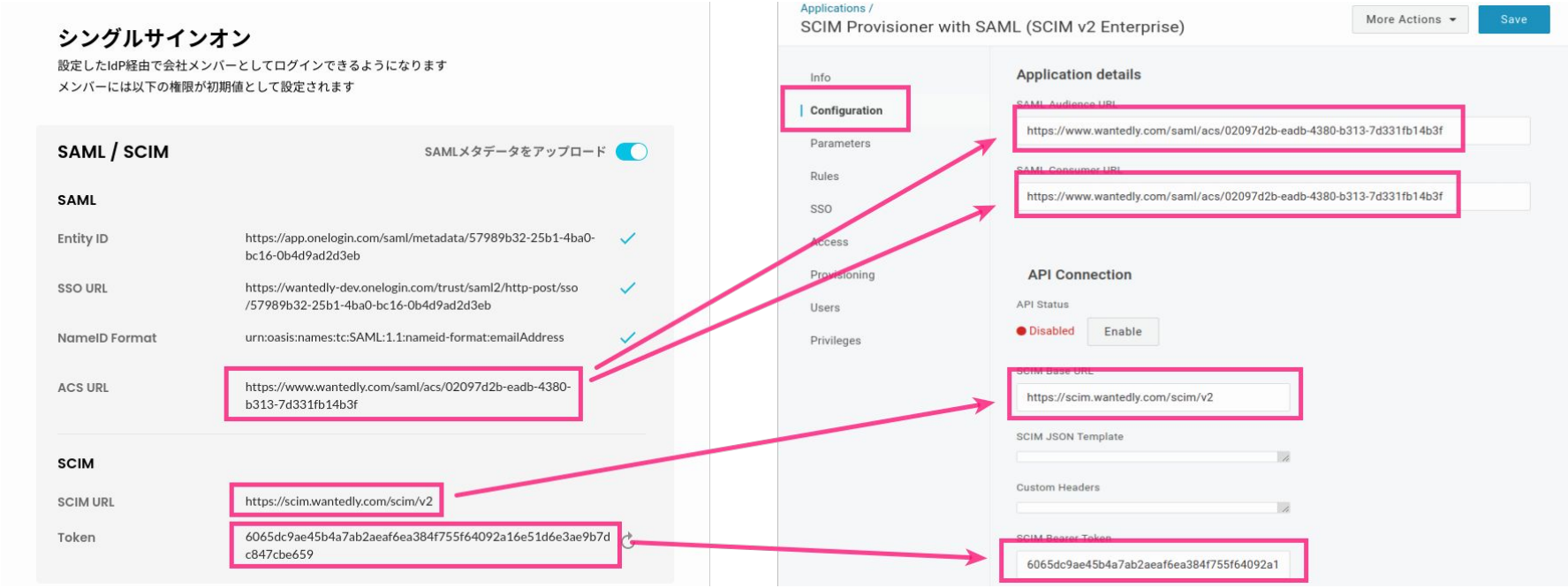
Wantedly 上の管理画面にアップロードします



WANTEDLY ©2021 Wantedly, Inc.

OneLogin の設定手順 - SAML

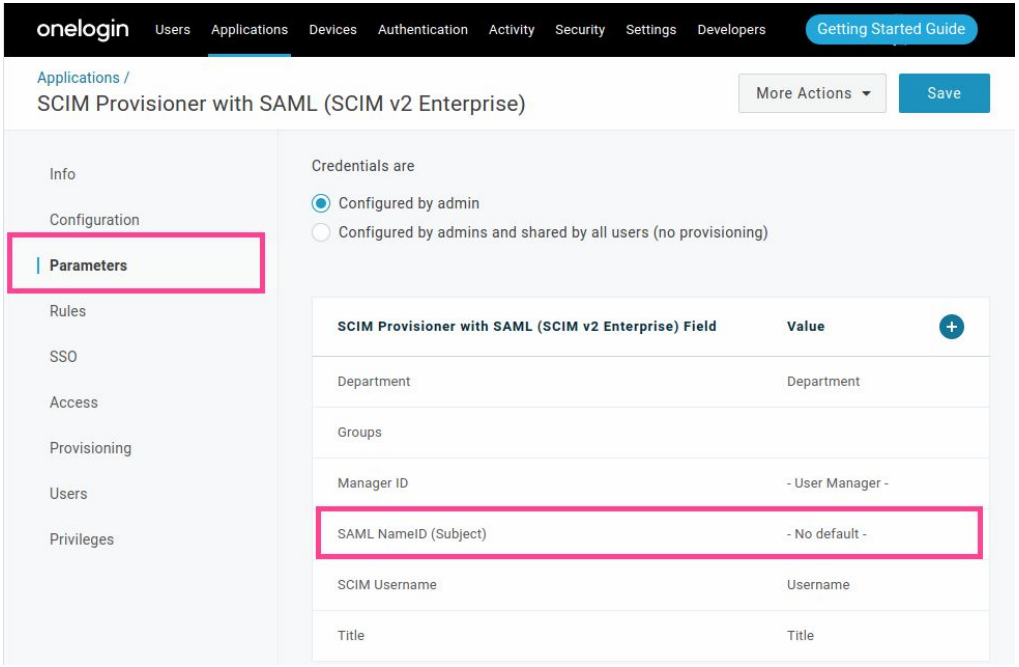
Configuration に **ACS URL**, **SCIM URL**, **Token** を入力します



WANTEDLY ©2021 Wantedly, Inc.

OneLogin の設定手順 - SAML

Parameters の SAML NameID (Subject) を選択します

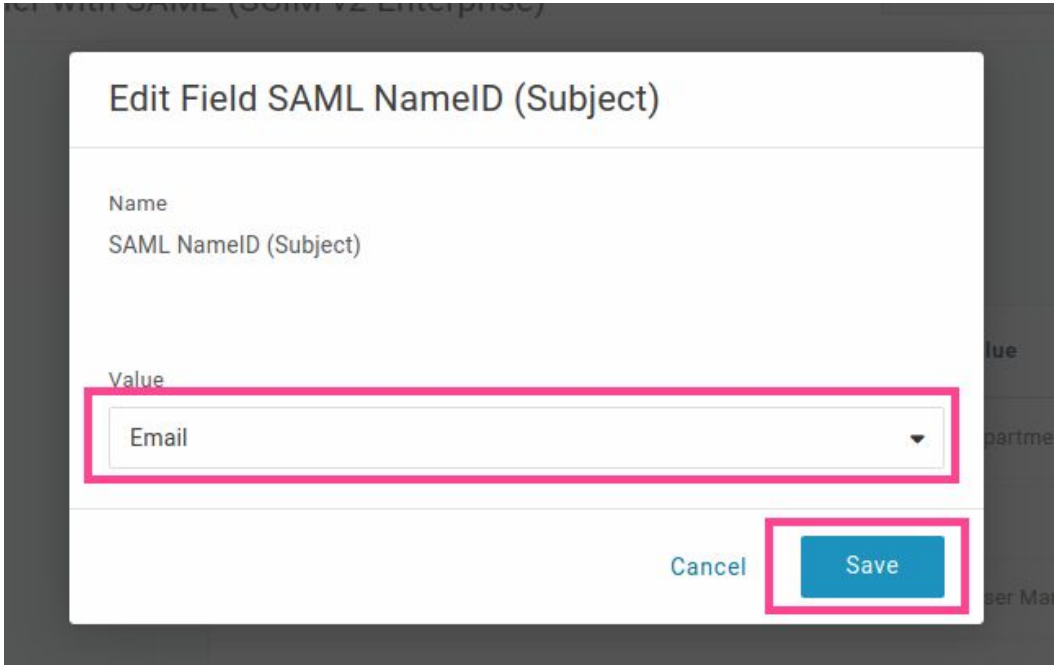


WANTEDLY ©2021 Wantedly, Inc.

OneLogin の設定手順 - SAML

Parameters の **SAML NameID (Subject)** を選択します

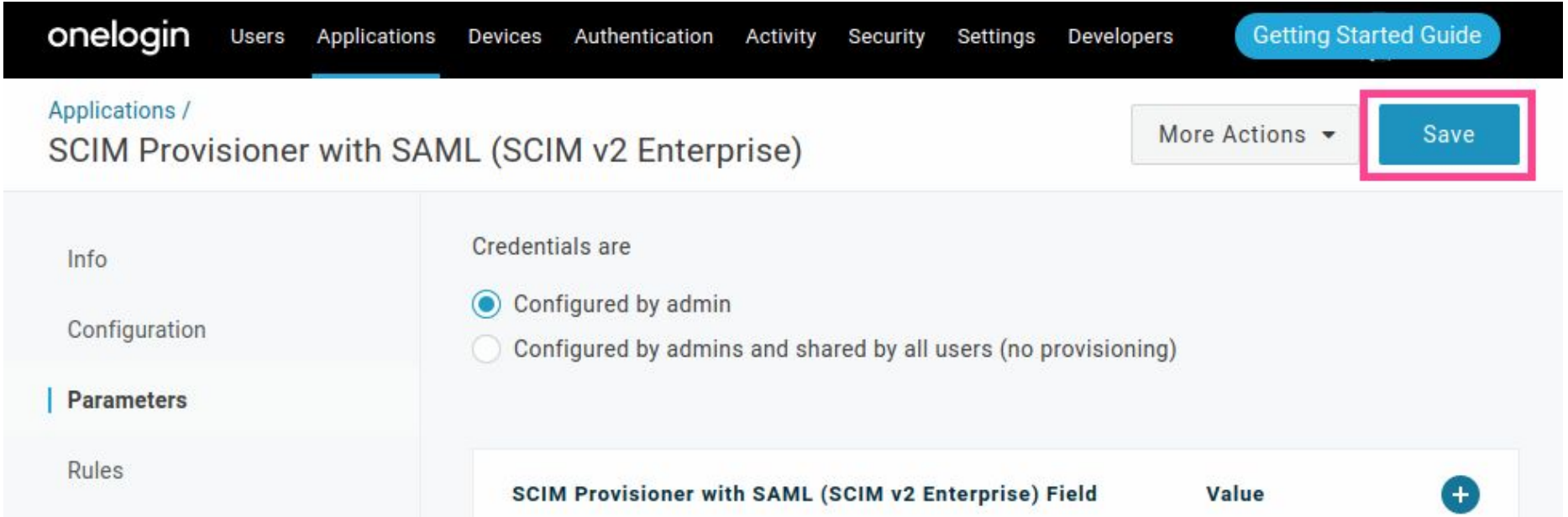
Value を **Email** に変更して **Save** します



WANTEDLY ©2021 Wantedly, Inc.

OneLogin の設定手順 - SAML

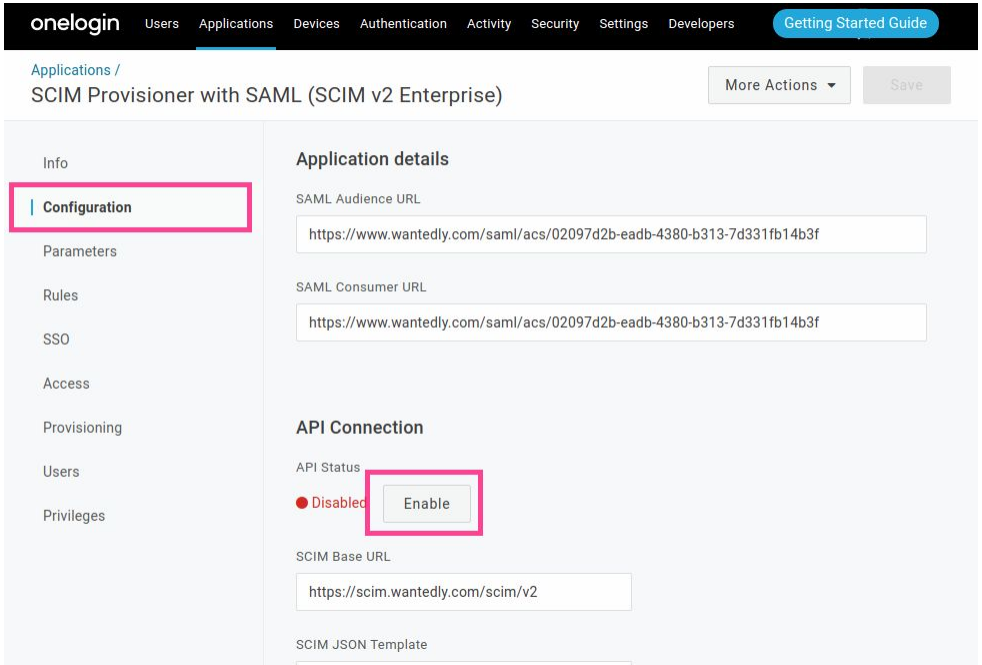
右上の **Save** をクリックして SAML の設定は完了です



WANTEDLY ©2021 Wantedly, Inc.

OneLogin の設定手順 - SCIM

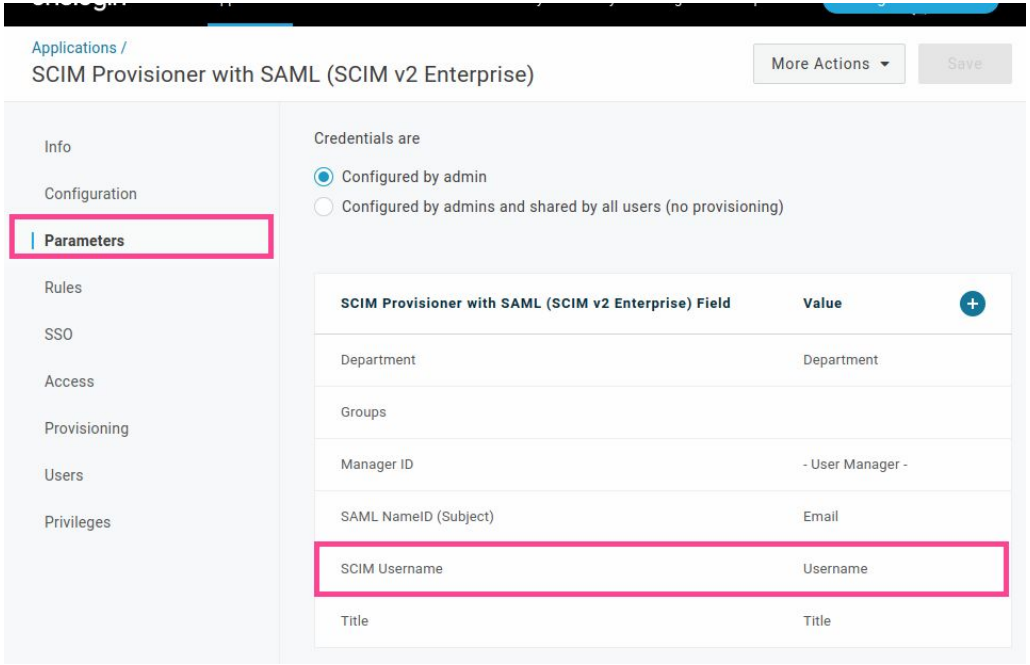
Configurations → API Connection → Enable をクリックします



WANTEDLY ©2021 Wantedly, Inc.

OneLogin の設定手順 - SCIM

Parameters から **SCIM Username** を選択します

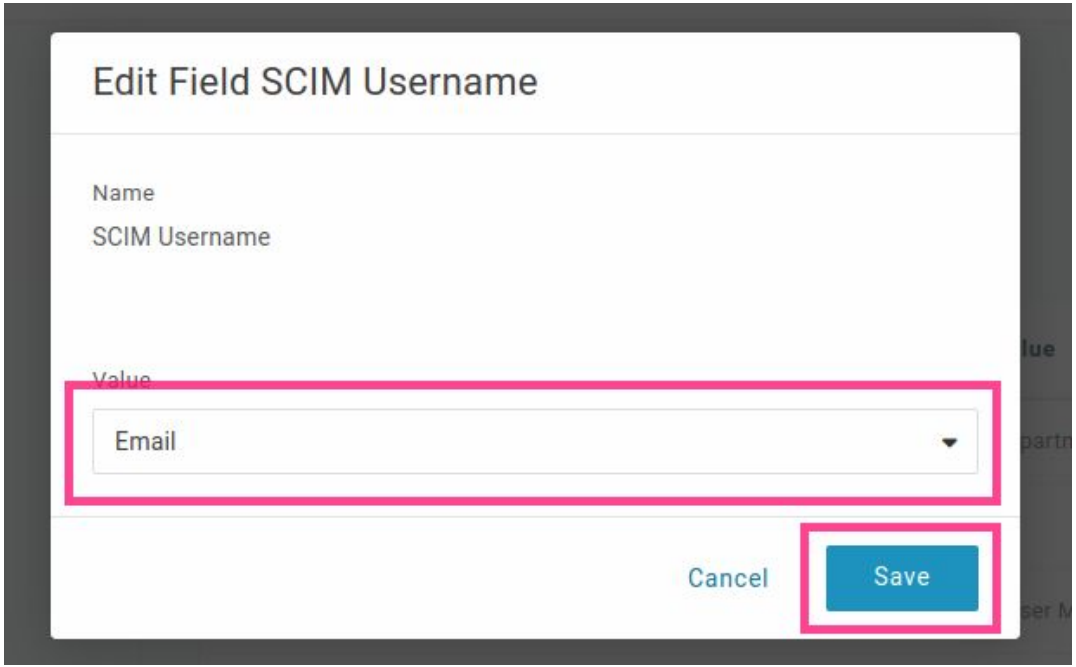


WANTEDLY ©2021 Wantedly, Inc.

OneLogin の設定手順 - SCIM

Parameters から **SCIM Username** を選択します

Value を **Email** に変更して **Save** します

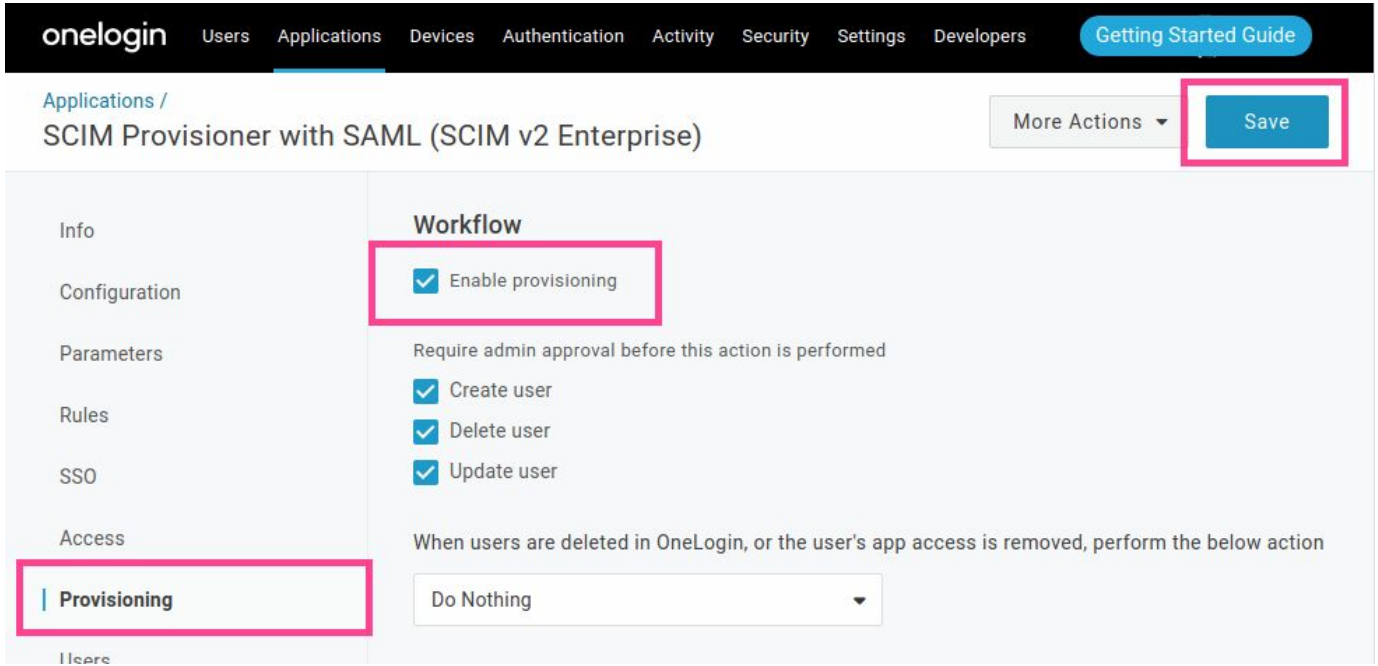


WANTEDLY ©2021 Wantedly, Inc.

OneLogin の設定手順 - SCIM

Provisioning から **Enable provisioning** をチェックします

右上の **Save** をクリックして SCIM の設定は完了です



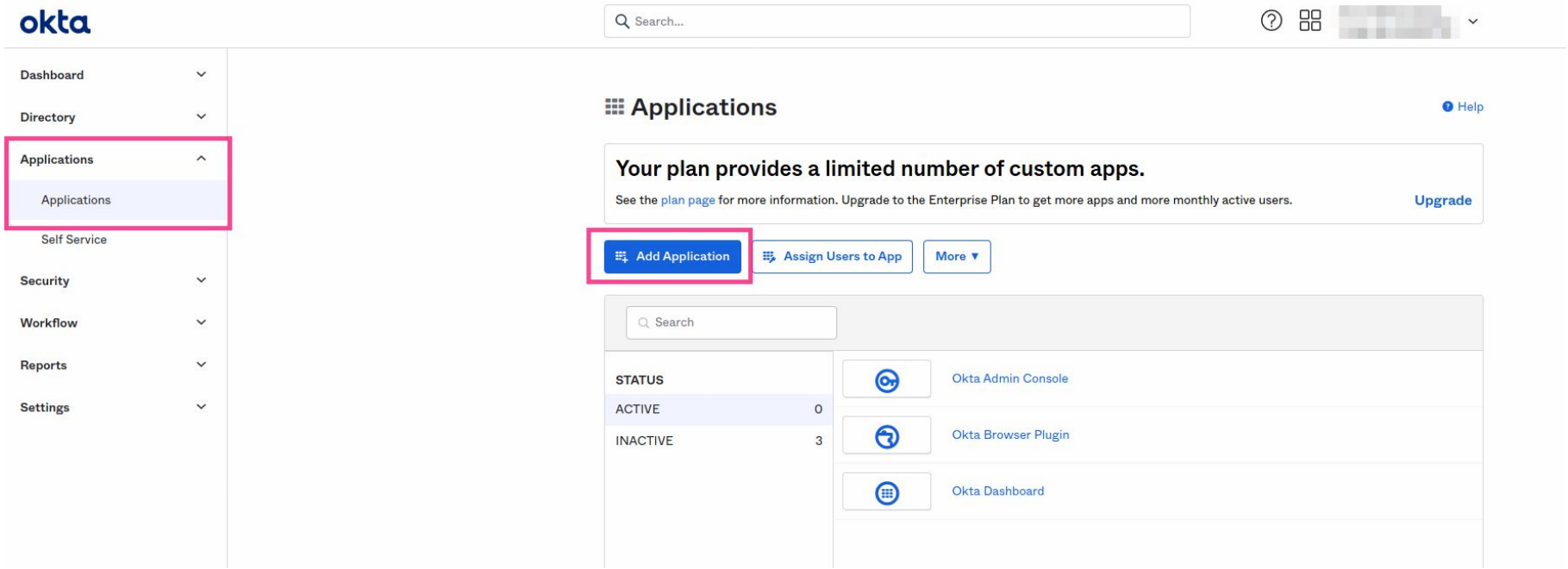
WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順

©2021 Wantedly, Inc.

Okta の設定手順 - SAML

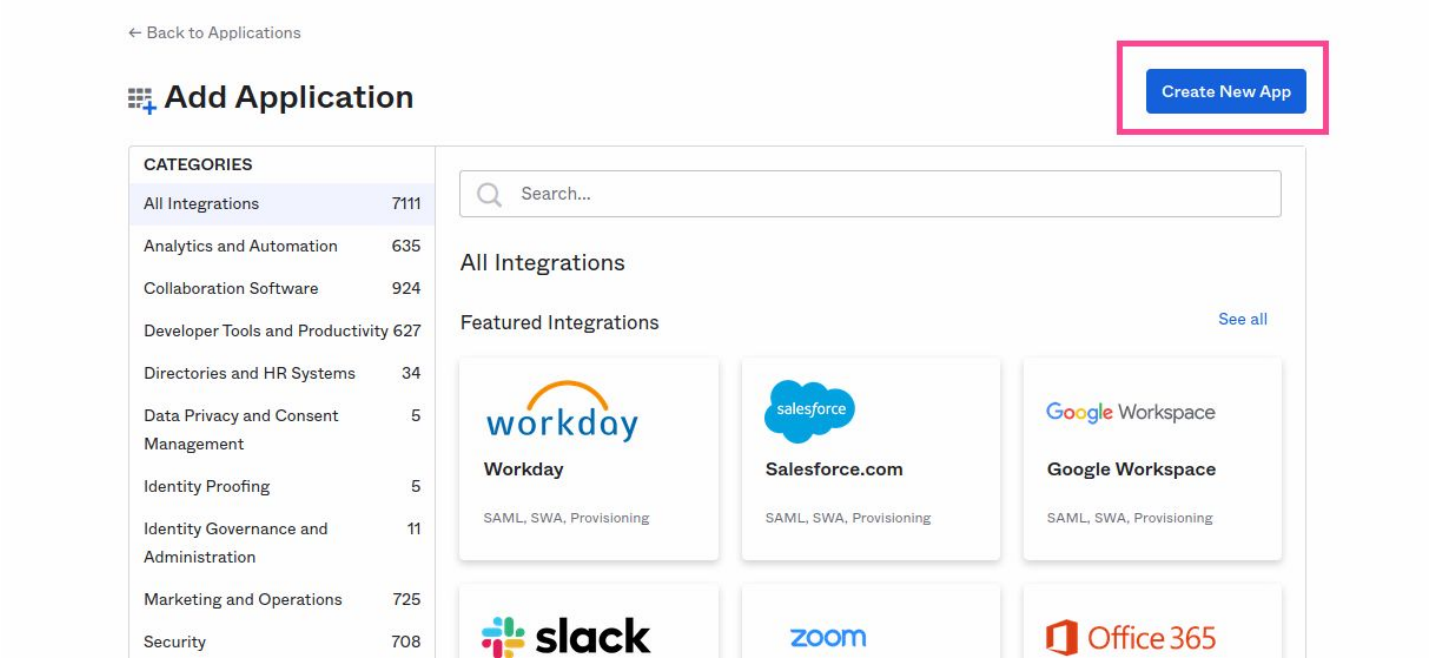
Applications から **Add Application** ボタンをクリックします



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SAML

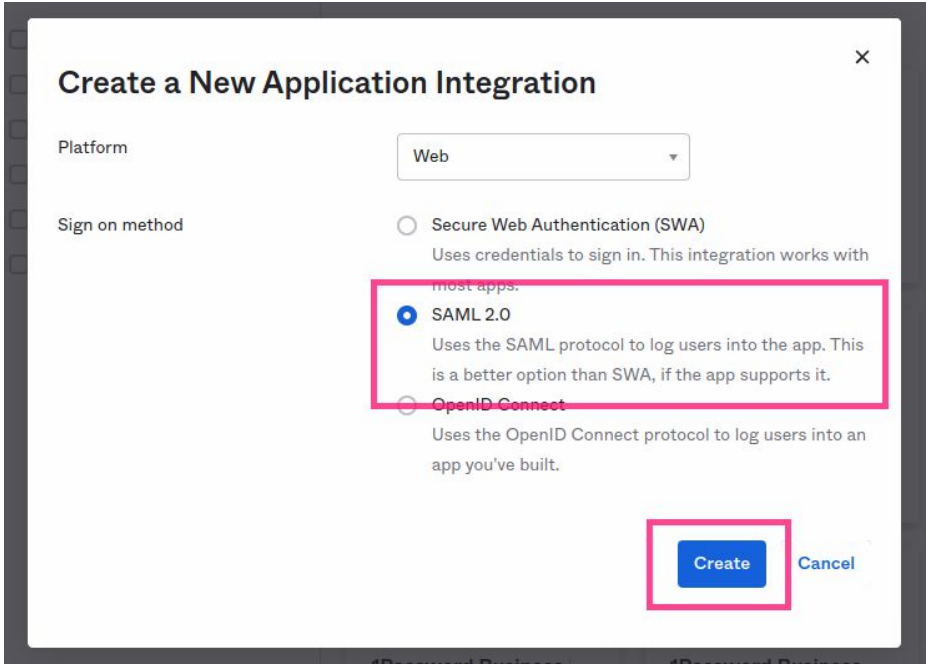
Create New App ボタンをクリックします



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SAML

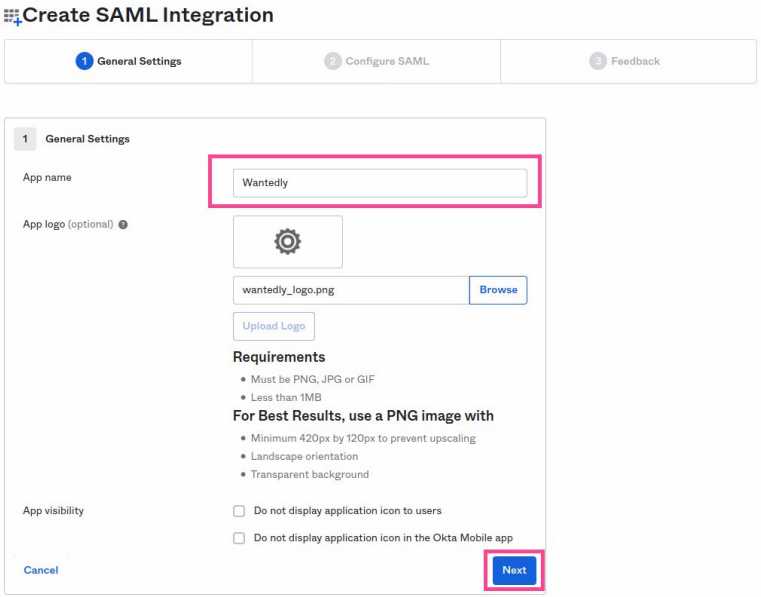
Sign on method を SAML 2.0 に変更して Create します



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SAML

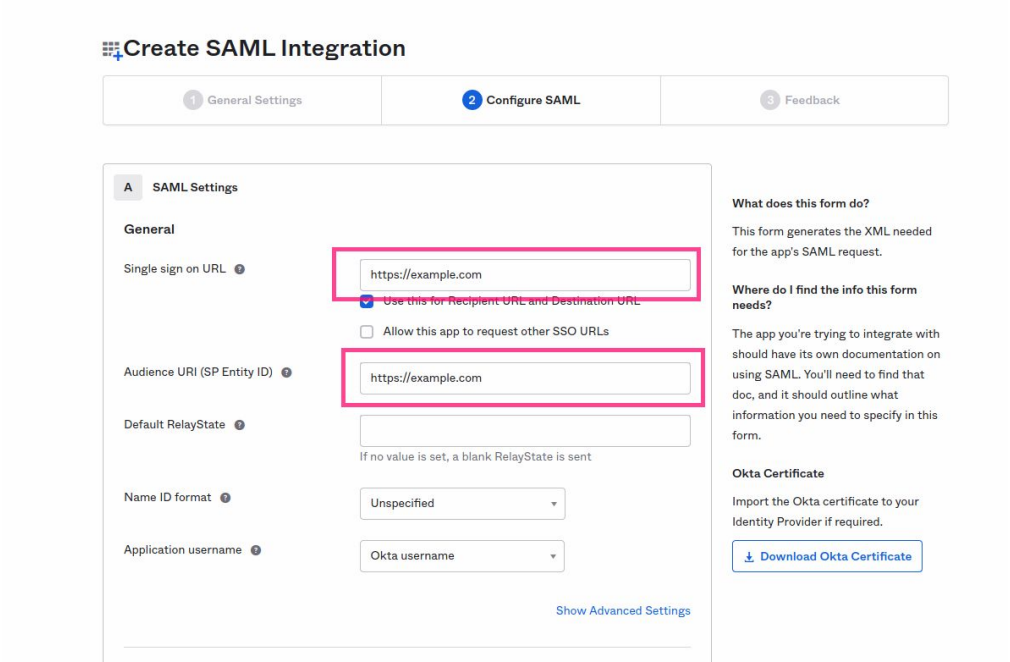
App Name を入力して **Next** をクリックします



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SAML

Single sign on URL と Audience URI (SP Entity ID) に仮の URL を入力します

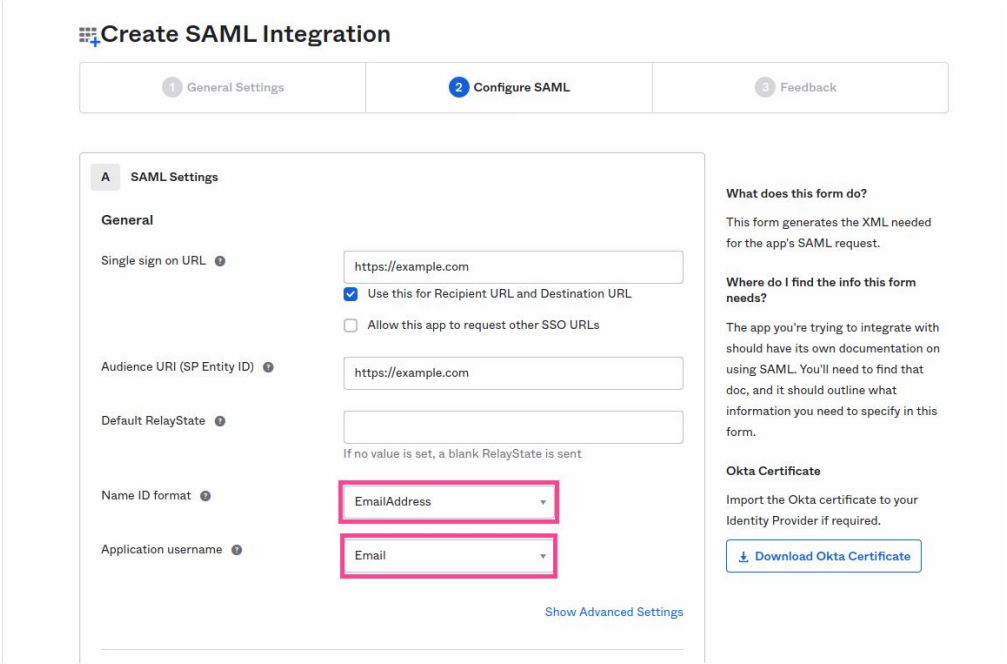


WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SAML

Name ID Format を EmailAddress、Application username を Email に

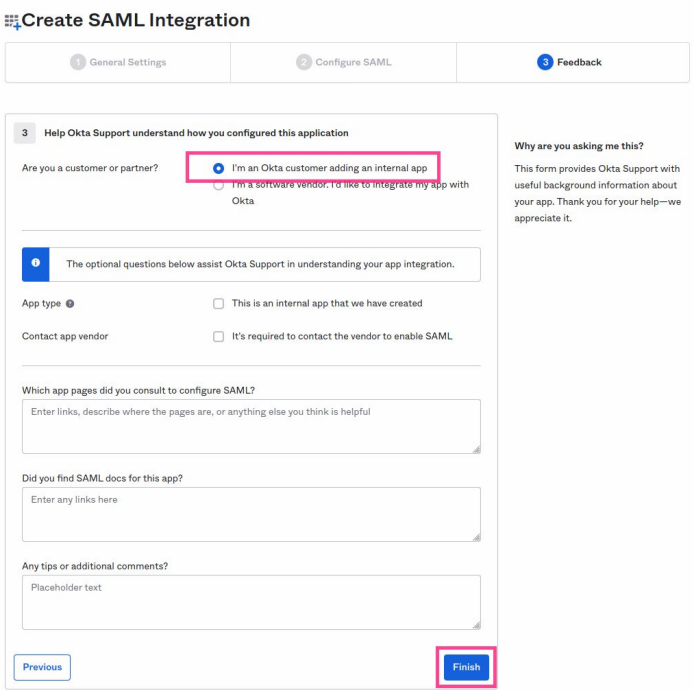
それぞれ変更してページ下部の**Next** ボタンをクリックします



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SAML

フィードバックに回答して**Finish** ボタンをクリックします

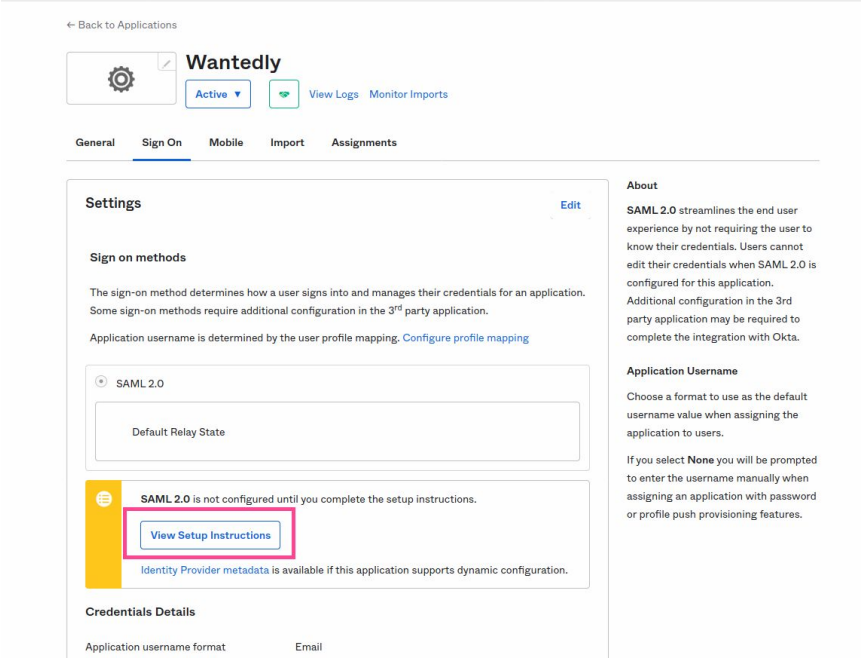


WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SAML

View Setup Instructions ボタンをクリックして

Optional → IDP metadata の内容をファイルとして保存します

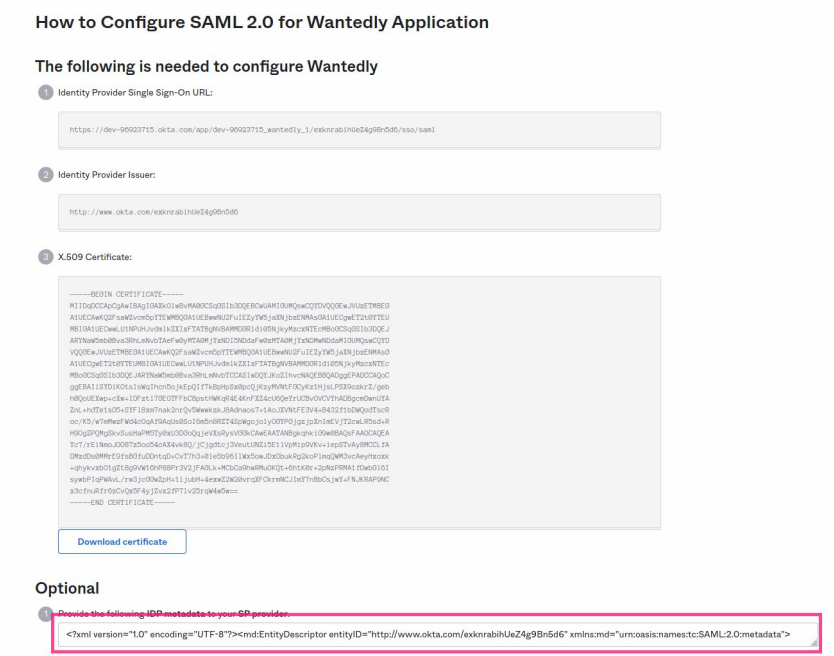


WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SAML

View Setup Instructions ボタンをクリックして

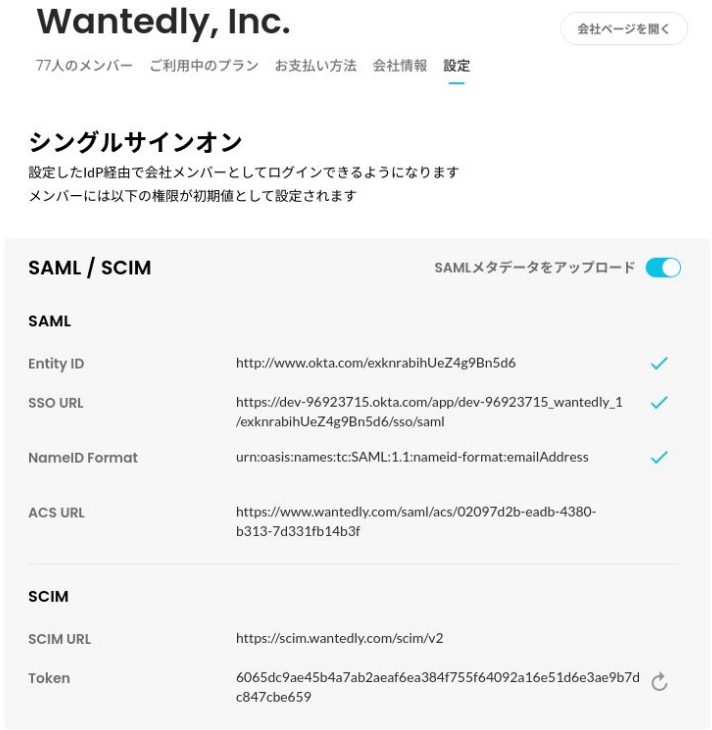
Optional → IDP metadata の内容をファイルとして保存します



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SAML

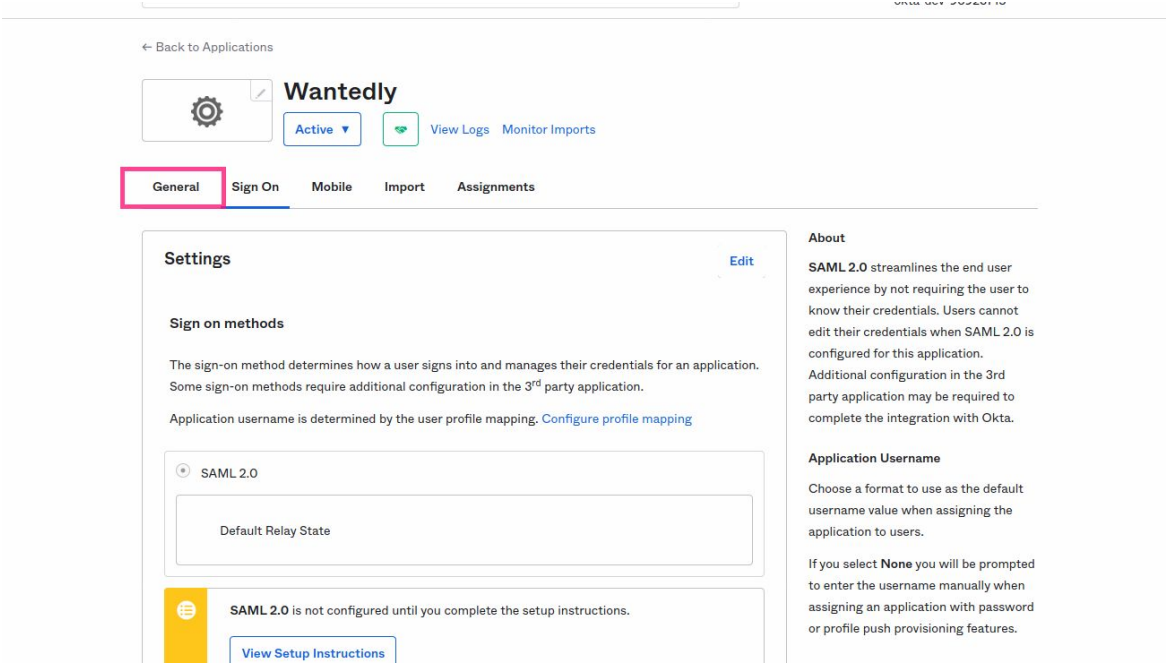
ダウンロードしたメタデータをWantedly 上の管理画面にアップロードします



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SAML

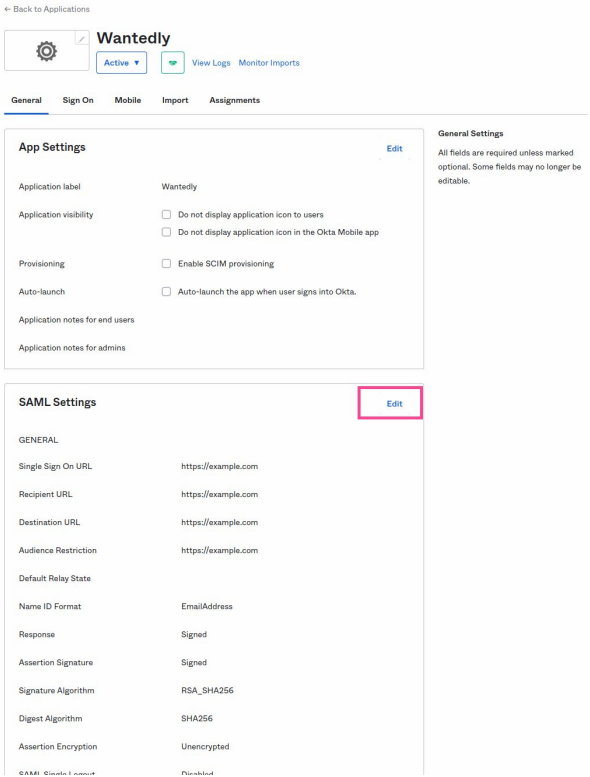
General タブに移動して **SAML Settings** → **Edit** をクリックします



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SAML

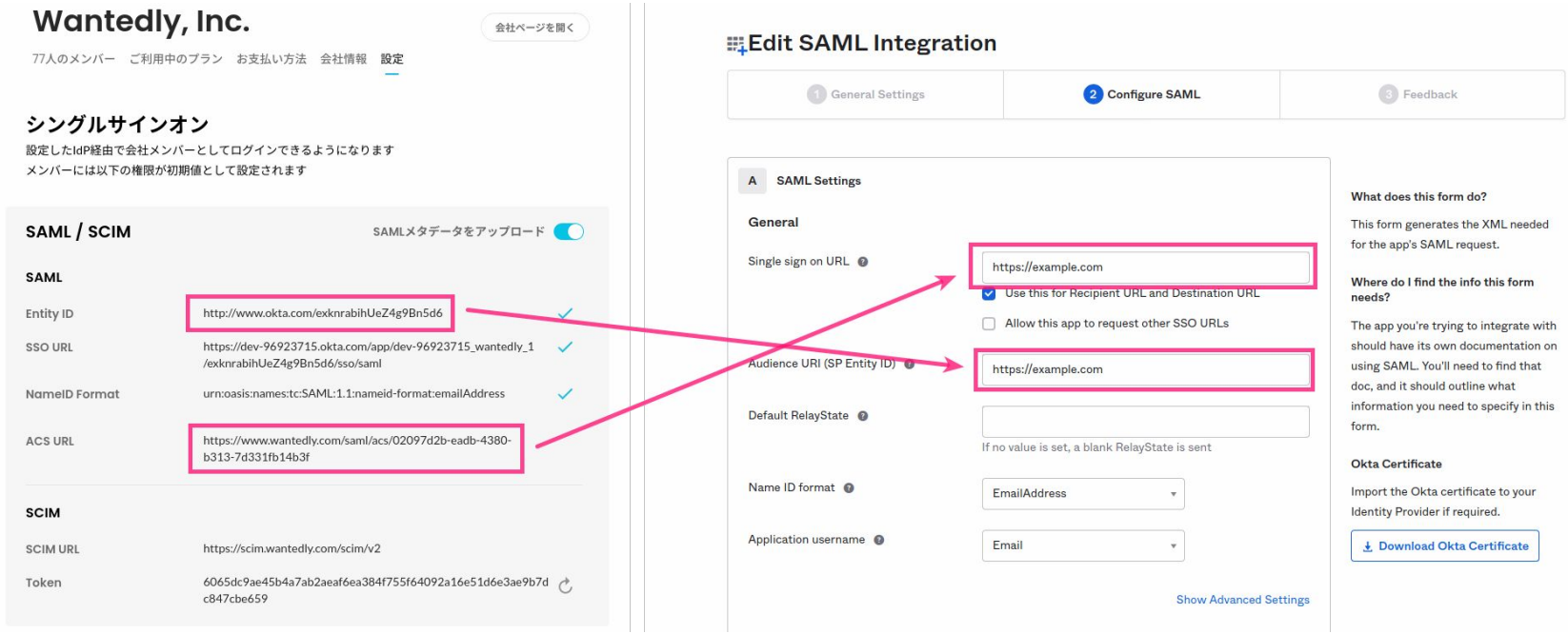
General タブに移動して **SAML Settings** → **Edit** をクリックします



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SAML

Next ボタンをクリックして②**Configure SAML** で仮の URL を置き換えます

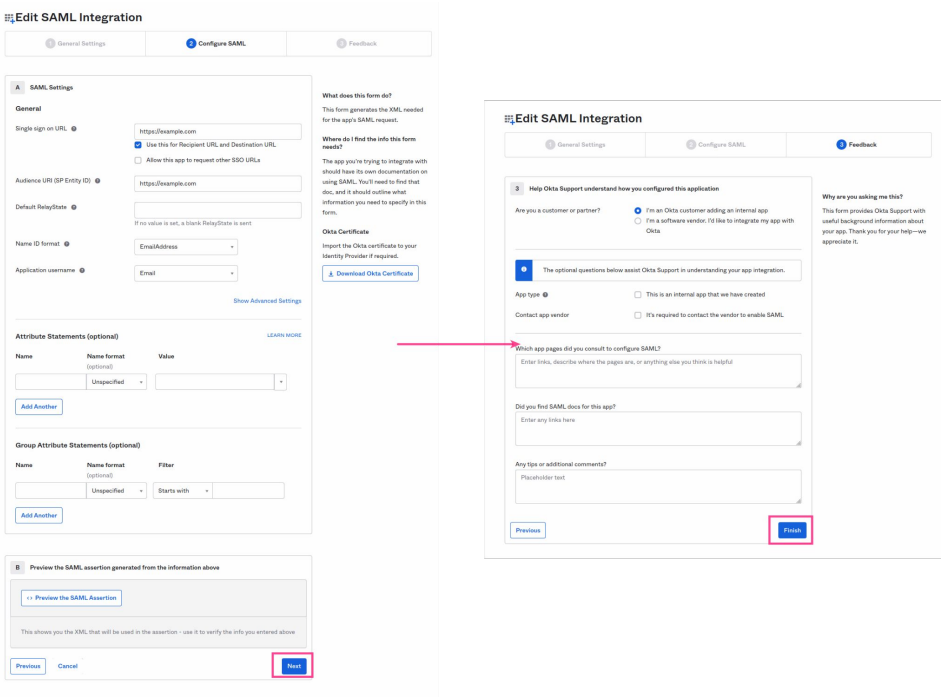


WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SAML

Next ボタンをクリック、

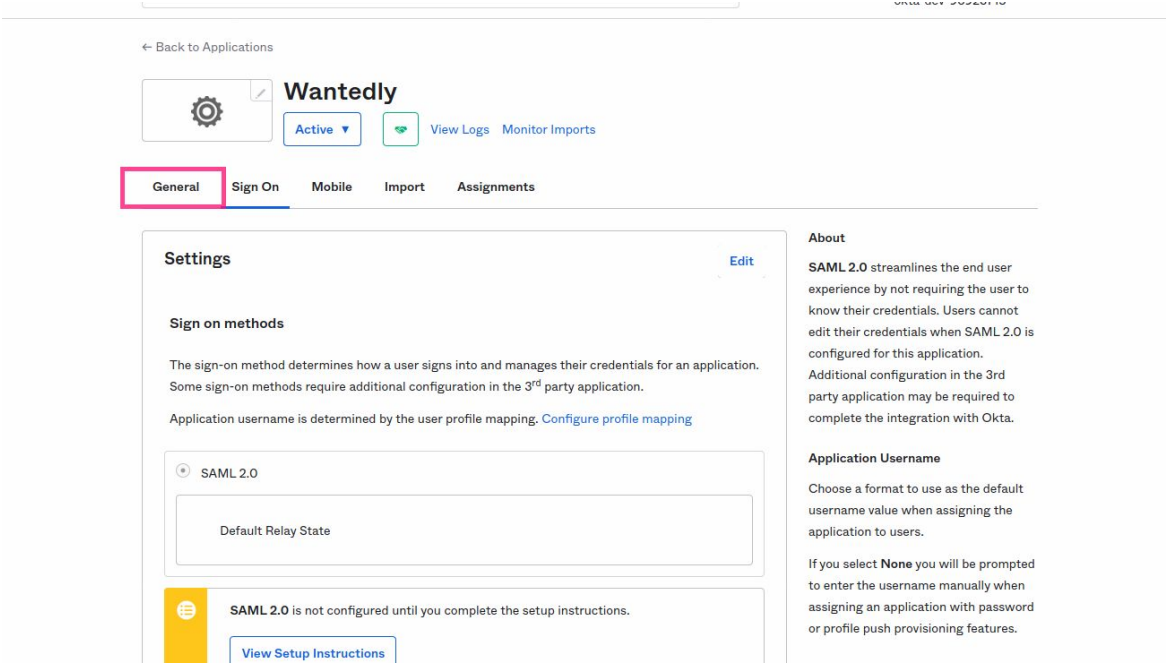
次のページで **Finish** ボタンをクリックしてSAML の設定は完了です



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SCIM

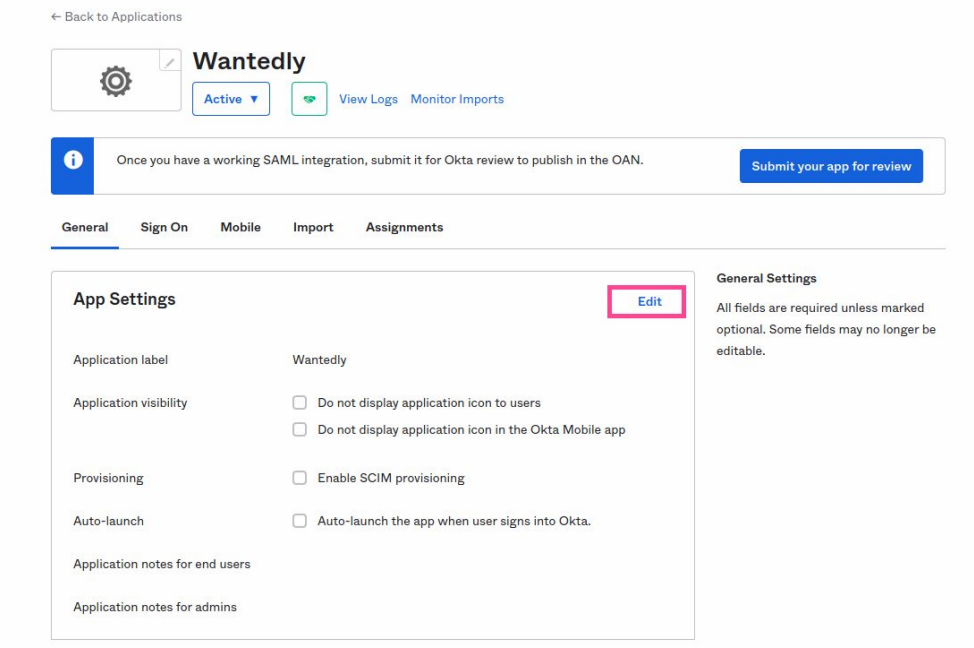
General タブに移動して **App Settings** → **Edit** をクリックします



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SCIM

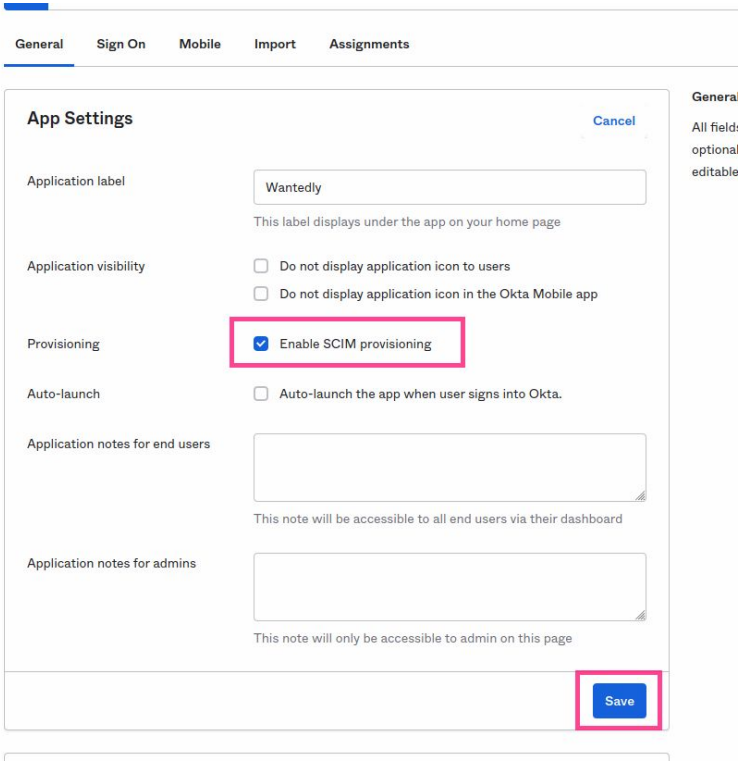
General タブに移動して **App Settings** → **Edit** をクリックします



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SCIM

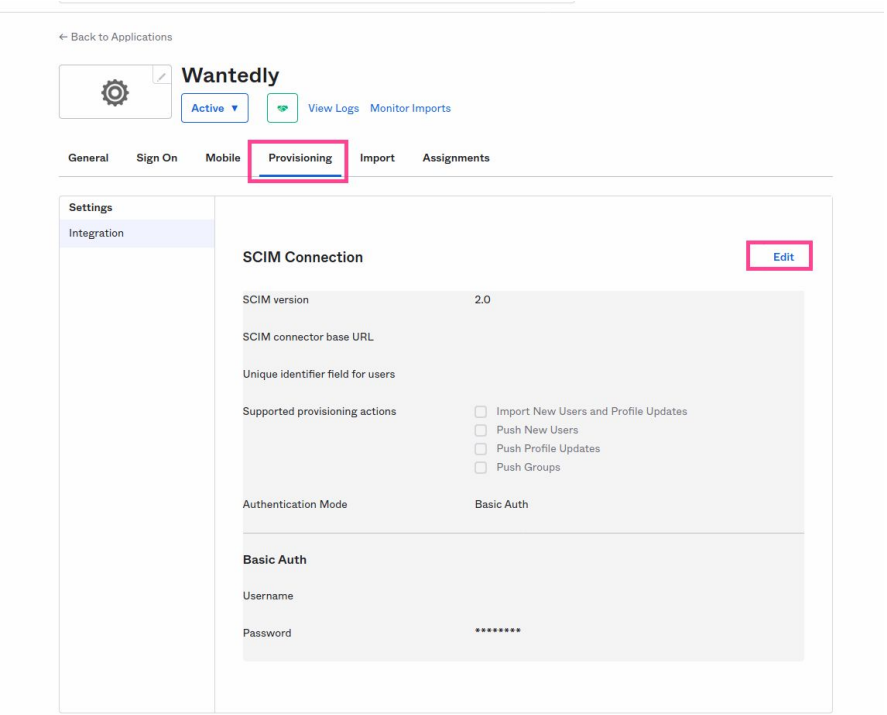
Provisioning → Enable SCIM provisioning にチェックを入れて **Save**します



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SCIM

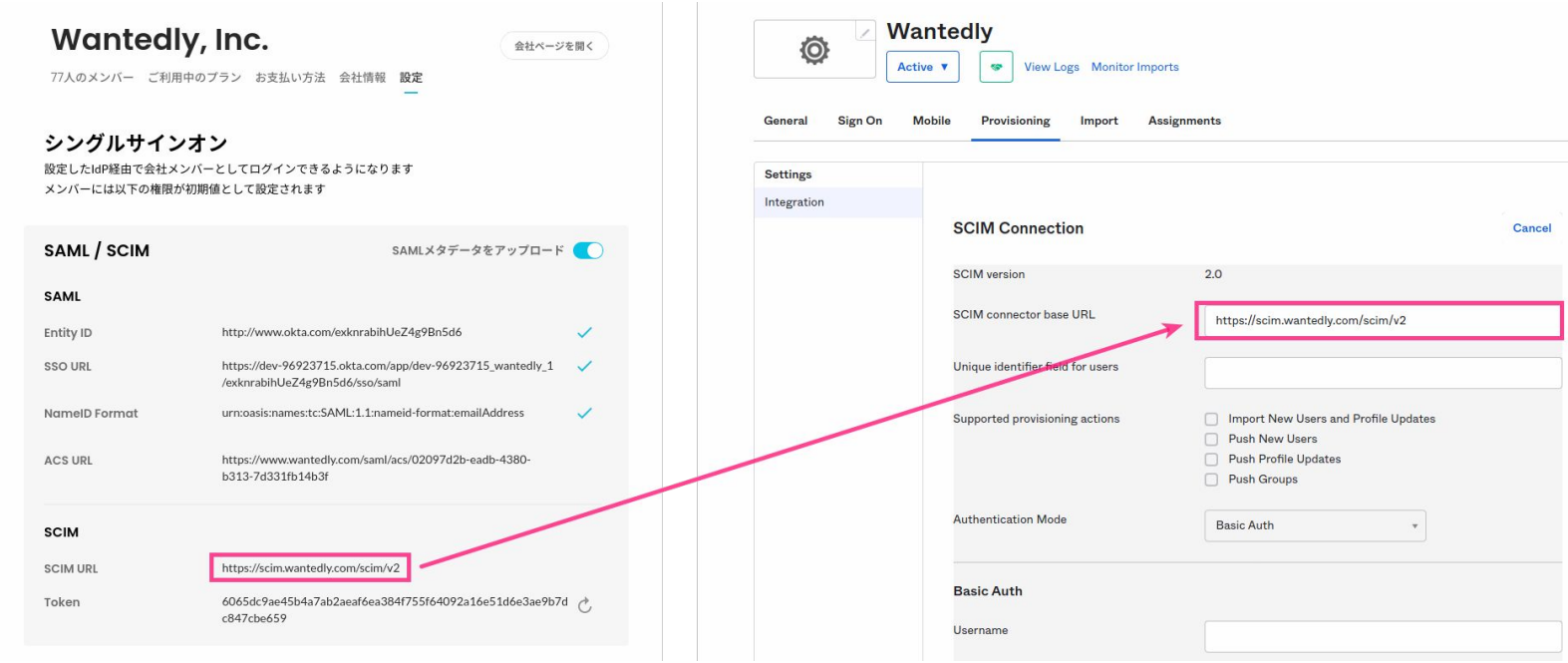
Provisioning タブの **Edit** をクリックします



WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SCIM

SCIM connector base URL に[Wantedly 上の管理画面](#)の **SCIM URL** を入力します

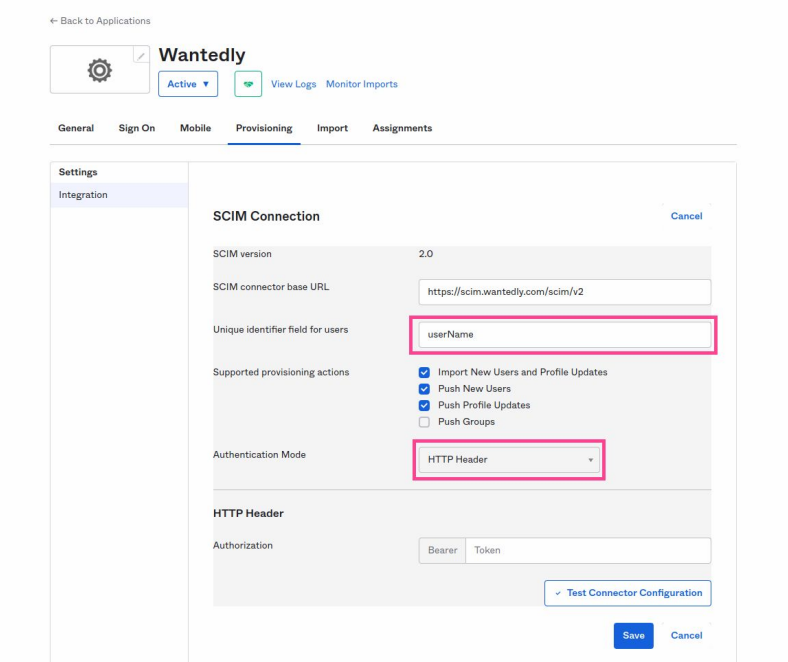


WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SCIM

Unique identifier field for users に **userName** を入力します

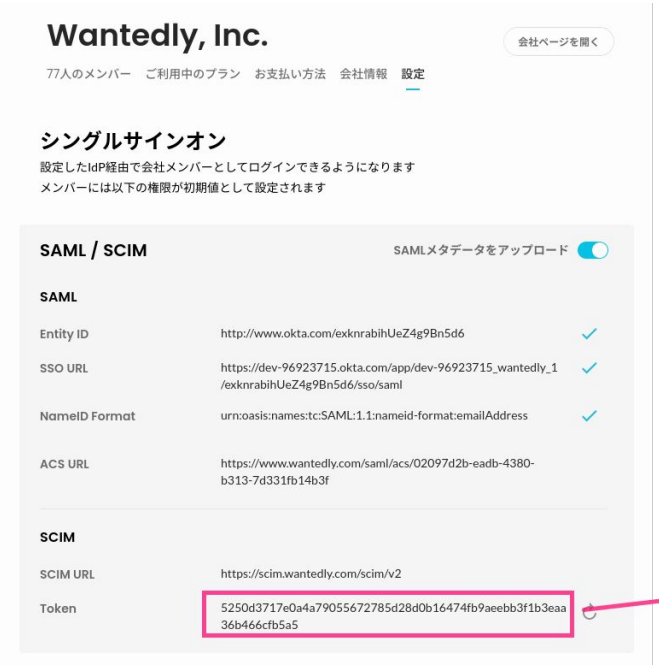
Authentication Mode を **HTTP Header** に変更します

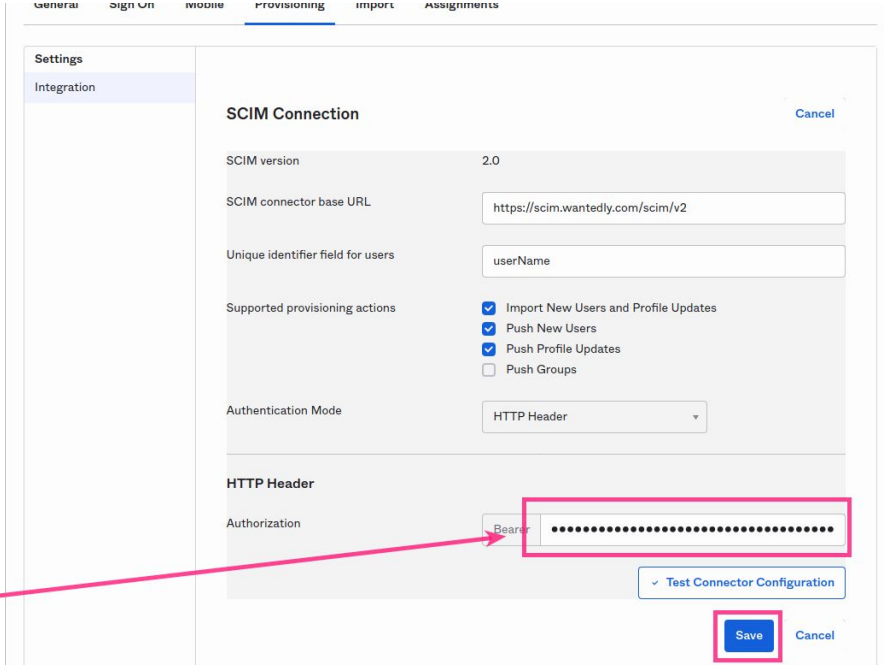


WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SCIM

Authorization に[Wantedly 上の管理画面](#)の **SCIM** → **Token** を入力して **Save** します



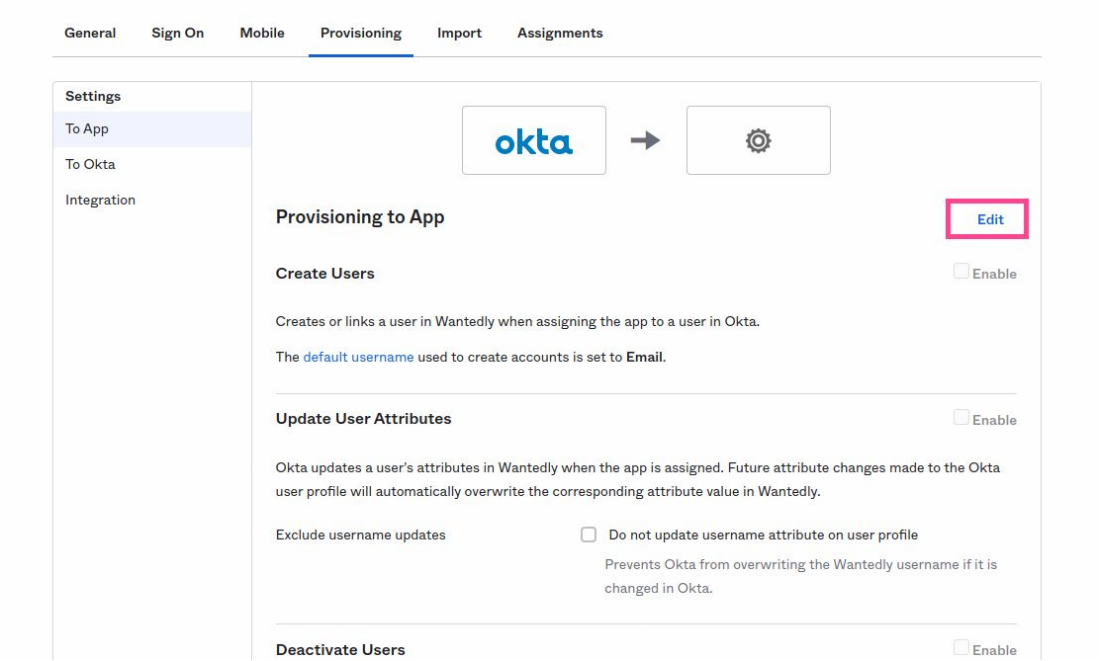


WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SCIM

Provisioning App の **Edit** から **Create Users** → **Enable** にチェックします

Save して SCIM の設定は完了です

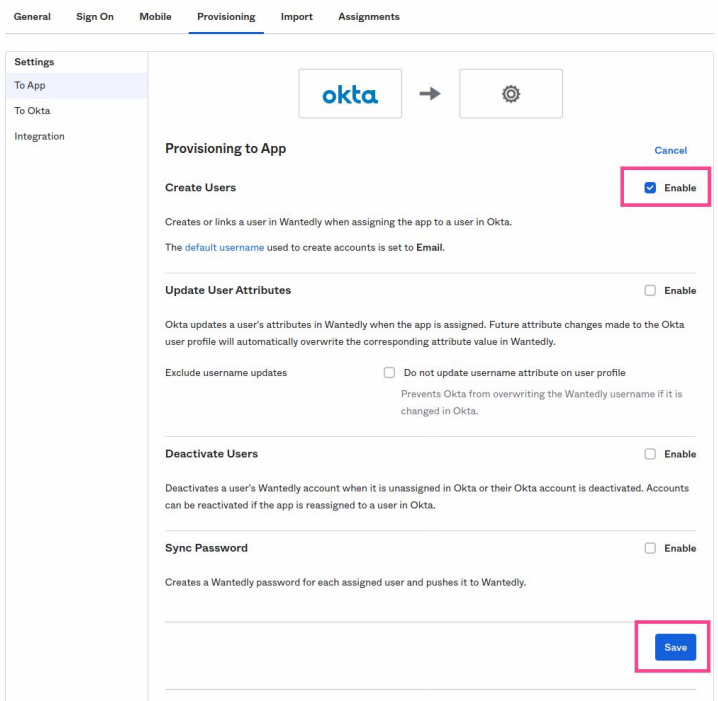


WANTEDLY ©2021 Wantedly, Inc.

Okta の設定手順 - SCIM

Provisioning App の **Edit** から **Create Users** → **Enable** にチェックします

Save して SCIM の設定は完了です



WANTEDLY ©2021 Wantedly, Inc.