



ULIZAプロダクトアカウント

ユーザーガイドv1.2.0

はじめに

本書はULIZAプロダクトアカウントの概要および各種設定方法について記述しています。なお、本書に掲載されている図は、実際のものとは異なる場合がありますのでご了承ください。

用語

ここでは本書で使用される主な用語の定義について記述します。

ULIZAプロダクトアカウント

複数のULIZAプロダクトに対して共通で使用可能なアカウントを指します。これには弊社から提供されるマスターアカウントとお客様が登録可能なサブアカウントが含まれます。

ULIZAプロダクト

ULIZAプロダクトアカウントを使用可能な弊社のプロダクトを指します。これにはULIZA VMS (Cloud)、ULIZA En-Cluster (Cloud)、ULIZA Player (Cloud)、ULIZA Video Analytics (Basic)などが含まれます。

マスターアカウント

弊社から提供されるULIZAプロダクトアカウントを指します。サブアカウントの管理権限を持ちます。

サブアカウント

マスターアカウントにより登録されるULIZAプロダクトアカウントを指します。

チームメンバー

ひとつのULIZAプロダクトアカウントを共同で使用する複数の使用者を指します。チームメンバーはそれぞれ自分だけの認証情報（パスワードなど）を使用して管理画面にログインします。

概要

本章では、ULIZAプロダクトアカウントの概要について記述しています。

ULIZAプロダクトアカウント

ULIZAプロダクトアカウントにはマスターアカウントとサブアカウントがあります。マスターアカウントは、それ自体でULIZAプロダクトを使用可能なことに加えて、登録したすべてのサブアカウントのデータを取得したり更新したりすることができます（サブアカウントに切り替えるを参照）。一方で、サブアカウントが別のサブアカウントやマスターアカウントのデータを取得したり更新したりすることはできません。ただし、サブアカウントが別のサブアカウントのデータを取得したり更新したりすることを許可することもできます。

ULIZAプロダクトアカウントはそれぞれ以下に示す属性を持ちます。

属性名	変更可能	説明
ログインID	×	各ULIZAプロダクトの管理画面にログインする際に使用します。
パスワード	○	各ULIZAプロダクトの管理画面にログインする際に使用します。
名前	△（※1）	アカウントの名前です。
説明	△（※1）	アカウントの説明（省略可能）です。
状態	△（※1）	アカウントの状態です。状態には以下の種類があります。 提供中 ：各ULIZAプロダクトを使用可能な状態です。 停止中 ：各ULIZAプロダクトを使用できない（管理画面へのログインができない）状態です。
API認証キー	○	アカウントがULIZAプロダクトのWeb APIを使用する際に必要なキーです。登録可能なAPI認証キーの個数はアカウントにより異なります。使用方法については、各ULIZAプロダクトのAPI仕様書を参照してください。
操作権限	△（※1）	使用可能なULIZAプロダクトの種類や、各ULIZAプロダクトにおいてアカウントが実行可能な操作権限に関する設定です。マスターアカウントが持たない操作権限をサブアカウントが持つことは許可されません。
サービス利用制限	△（※2）	各ULIZAプロダクトにおいてアカウントが管理できる要素に対する制限です。現在の制限は基本情報画面で確認できます。

※1： 変更対象がサブアカウントである場合は、当該アカウントを登録したマスターアカウントから変更することができます。変更対象がマスターアカウントである場合は、弊社にお問い合わせください。

※2： 変更する必要がある場合は、弊社にお問い合わせください。

チーム機能

ひとつのULIZAプロダクトアカウントを複数の使用者が共同で使用している場合は、チーム機能を使用することで、使用者（チームメンバー）間でパスワードなどの認証情報を共有する必要がなくなるほか、使用者ごとに操作権限を細かく制御でき、運用上のセキュリティを向上させることができます。

チーム機能を使用するには使用者ごとにチームメンバーを作成します。チームメンバーはULIZAプロダクトアカウントごとに最大100個まで作成可能です。チームメンバーは以下に示す属性を持ち、これらはいずれもチームメンバーごとに異なる値を設定することができます。

属性名	変更可能	説明
メンバー名	×	各ULIZAプロダクトの管理画面にログインする際に使用します。
パスワード	○	各ULIZAプロダクトの管理画面にログインする際に使用します。
説明	○	チームメンバーの説明（省略可能）です。
API認証キー	○	チームメンバーがULIZAプロダクトのWeb APIを使用する際に必要なキーです。使用方法については、各ULIZAプロダクトのAPI仕様書を参照してください。
操作権限	○	使用可能なULIZAプロダクトの種類や、各ULIZAプロダクトにおいてチームメンバーが実行可能な操作権限に関する設定です。

ワンタイムパスワードによる2段階認証

ULIZAプロダクトアカウントはTOTP（Time-based One-Time Password）標準規格に準拠した2段階認証をサポートしています。2段階認証を有効化すると、ログイン時に「ログインID」と「パスワード」（チームメンバーとしてログインする場合は「メンバー名」も含む）に加えて、時間経過とともに変化する6桁の認証コードが必要になります。チーム機能を使用している場合は、チームメンバーごとに2段階認証の有効/無効を設定でき、ログイン時に必要な認証コードもチームメンバーごとに異なる値になります。

認証コードはTOTP標準規格をサポートするスマートフォンアプリなどを使用して生成できます。実際の設定方法については2段階認証を有効化/無効化するを参照してください。なお、動作確認済みのアプリは以下の通りです。

- Google Authenticator (Android/iOS)
- Microsoft Authenticator (Android/iOS)
- IIJ SmartKey (Android/iOS)

IPアドレス制限

必要に応じて管理画面へのログインにIPアドレス制限を設定できます。IPアドレス制限を設定すると、あらかじめ許可されたIPアドレス以外からは管理画面にログインできなくなります。チーム機能を使用している場合は、チームメンバーごとに異なるIPアドレスを設定できます。なお、この制限はAPI認証キーを使用したWeb APIリクエストには適用されません。実際の設定方法についてはIPアドレス制限を設定するを参照してください。

アカウント設定画面の使い方

本章では、ULIZAプロダクトアカウントの設定画面の操作方法について説明します。なお、設定画面はPCのGoogle Chromeでの操作を推奨します。画面解像度は1280x720ピクセル以上を推奨します。

ログインする

弊社より案内する情報に従い認証情報を入力し、「ログイン」ボタンをクリックしてください。

アカウント設定画面を表示する

ログインに成功すると各ULIZAプロダクトの管理画面に遷移します。アカウント設定画面に遷移するには、画面右上のログインIDをクリックすると表示されるメニューから「アカウント設定」をクリックします。



現在の設定内容を表示する

アカウント設定画面に遷移すると最初に「基本情報画面」が表示されます。ここでは、アカウントの基本情報やサービス利用制限の確認、パスワードの変更などを行うことができます。

パスワードを変更する

基本情報画面で「パスワードの変更」ボタンをクリックすると、「パスワードの変更」ダイアログが表示されます。現在ログインしているULIZAプロダクトアカウントのパスワードと、新しく設定するパスワードを入力し、「保存」ボタンをクリックするとパスワードが変更されます。なお、新しいパスワードは次回ログイン時から有効になります。

2段階認証を有効化/無効化する

基本情報画面で「2段階認証の有効化」ボタンをクリックすると、「2段階認証の有効化」ダイアログが表示されます。表示されたQRコードをTOTP（Time-based One-Time Password）標準規格に対応したスマートフォンアプリなどで読み取り、生成された6桁の認証コードを入力し、「有効化」ボタンをクリックすると2段階認証が有効化されます。既に2段階認証が有効な場合は、「2段階認証の無効化」ボタンをクリックすることで、2段階認証が無効化されます。

IPアドレス制限を設定する

基本情報画面で「IPアドレス制限設定」ボタンをクリックすると、「IPアドレス制限設定」ダイアログが表示されます。IPアドレス制限を使用するには、「IPアドレス制限を使用する」にチェックを入れ、ログイン許可IPアドレスを入力し、「保存」ボタンをクリックします。

API認証キーを管理する

サイドバーから「API認証キーの管理」（API認証キーの取得権限がある場合のみ表示されます）をクリックすると、API認証キー管理画面に遷移します。API認証キー管理画面の構成は以下の通りです。



① API認証キーリスト

登録済みAPI認証キーが一覧表示されます。

② API認証キーの検索

ここにキーワードを入力すると、そのキーワードを名前に含むAPI認証キーのみがAPI認証キーリストに表示されます。

③ API認証キーの登録

このボタンをクリックすると、「API認証キーの登録」ダイアログが表示されます。名前を30文字以内で入力して「登録」ボタンをクリックすると、API認証キーが登録されます。なお、名前は半角英数字、ハイフンおよびアンダースコアのみ使用可能で、既に登録されている名前は使用できません。

④ クリップボードにコピー

このアイコンをクリックすると、選択したAPI認証キーがクリップボードにコピーされます。

⑤ API認証キーの削除

このアイコンをクリックすると、「API認証キーの削除」ダイアログが表示されます。「削除」ボタンをクリックすると、選択したAPI認証キーが削除されます。なお、API認証キーの削除がシステムに反映されるまで数分かかる場合があります。

チームメンバーを管理する

サイドバーから「チームメンバーの管理」（チームメンバーの取得権限がある場合のみ表示されます）をクリックすると、チームメンバー管理画面に遷移します。チームメンバー管理画面の構成は以下の通りです。



① チームメンバーリスト

登録済みチームメンバーが一覧表示されます。各列は以下を表します。

列名	説明
メンバー名	チームメンバーのメンバー名を表します。
説明	チームメンバーの説明を表します。
最終ログイン	チームメンバーが各ULIZAプロダクトの管理画面に最後にログインを行った日時を表します。
最終更新日時	チームメンバーの設定が最後に更新された日時を表します。
登録日時	チームメンバーが登録された日時を表します。

② チームメンバーの検索

ここにキーワードを入力すると、そのキーワードをメンバー名または説明に含むチームメンバーのみがチームメンバーリストに表示されます。

③ チームメンバーの登録

このボタンをクリックするとチームメンバー設定画面に遷移し、チームメンバーの登録を行うことができます。

④ チームメンバーの編集

このアイコンをクリックするとチームメンバー設定画面に遷移し、選択したチームメンバーの更新を行うことができます。

⑤ チームメンバーの削除

このアイコンをクリックすると「チームメンバーの削除」ダイアログが表示されます。「削除」ボタンをクリックすると、選択したチームメンバーが削除され、以後そのチームメンバーはログインできなくなります。

チームメンバーを登録/更新する

サイドバーから「チームメンバーの登録」をクリックするか、チームメンバー管理画面の「チームメンバーの登録」ボタンまたは任意のチームメンバーの「編集」アイコンをクリックすると、チームメンバー設定画面に遷移します。チームメンバー設定画面は以下のセクションから構成されます。

- 「基本情報」セクション
- 「権限設定」セクション

「基本情報」セクション

チームメンバーに関する基本的な設定を行います。以下の設定項目があります。

設定項目	説明
メンバー名	ログインに使用するメンバー名を100文字以内で指定します。半角英数字、ピリオド、ハイフンおよびアンダースコアのみ使用可能です。また、既に登録されているメンバー名は使用できません。
パスワード	ログインに使用するパスワードを8文字以上30文字以内で指定します。ただし、全角文字や半角スペースを使用することはできません。英大文字、英小文字、数字をそれぞれ1文字ずつ含む必要があります。
説明	チームメンバーの説明を150文字以内で指定します（省略可能）。この説明は使用者の基本情報画面には表示されません。

「権限設定」セクション

各ULIZAプロダクトにおいてチームメンバーが実行可能な操作を選択します。ただし、自分が持たない操作権限をチームメンバーに付与することはできません。各権限の詳細についてはこちらを参照してください。

サブアカウントを管理する

マスターアカウントは、複数のサブアカウントを管理および登録することができます。マスターアカウントでログインした状態で、サイドバーから「サブアカウントの管理」をクリックすると、サブアカウント管理画面に遷移します。サブアカウント管理画面の構成は以下の通りです。

アカウント設定 > サブアカウントの管理

②

③

①

検索

+

サブアカウントの登録

状態	ログイン ID ↑	名前	説明	最終ログイン	最終更新日時	登録日時	④
<div>🟢 提供中</div>	dev@uliza	開発部	管理者：田中	2020/01/17 18:46	2020/06/04 21:33	2019/09/17 12:30	<div>✎</div>
<div>🟢 提供中</div>	planning@uliza	企画部	管理者：山田	—	2020/06/04 21:34	2020/06/04 21:30	
<div>🟢 提供中</div>	sales@uliza	営業部	管理者：鈴木	—	2020/06/04 21:34	2020/06/04 21:31	

① サブアカウントリスト

登録済みサブアカウントが一覧表示されます。各列は以下を表します。

列名	説明
状態	アカウントの状態を表します。
ログイン ID	アカウントのログインIDを表します。
名前	アカウントの名前を表します。
説明	アカウントの説明を表します。

列名	説明
最終ログイン	アカウントが各ULIZAプロダクトの管理画面に最後にログインを行った日時を表します。アカウントのチームメンバーがログインすることでも更新されます。なお、「サブアカウントに切り替え」機能によるログインでは、最終ログイン日時は更新されません。
最終更新日時	アカウントの設定が最後に更新された日時を表します。
登録日時	アカウントが登録された日時を表します。

② サブアカウントの検索

ここにキーワードを入力すると、そのキーワードをログインID、名前または説明に含むサブアカウントのみがサブアカウントリストに表示されます。

③ サブアカウントの登録

このボタンをクリックするとサブアカウント設定画面に遷移し、サブアカウントの登録を行うことができます。

④ サブアカウントの編集

このアイコンをクリックするとサブアカウント設定画面に遷移し、選択したサブアカウントの更新を行うことができます。

サブアカウントを登録/更新する

マスターアカウントとしてログインした状態で、サイドバーから「サブアカウントの登録」をクリックするか、サブアカウント管理画面の「サブアカウントの登録」ボタンまたは任意のサブアカウントの「編集」アイコンをクリックすると、サブアカウント設定画面に遷移します。サブアカウント設定画面は以下のセクションから構成されます。

- 「基本情報」セクション
- 「権限設定」セクション

「基本情報」セクション

サブアカウントに関する基本的な設定を行います。以下の設定項目があります。

設定項目	説明
ログインID	ログインに使用するIDを30文字以内で指定します。ただし、「@」に続く文字列を自由に指定することはできません。半角英数字、ハイフンおよびアンダースコアのみ使用可能です。また、既に登録されているログインIDは使用できません。

設定項目	説明
パスワード	ログインに使用するパスワードを8文字以上30文字以内で指定します。ただし、全角文字や半角スペースを使用することはできません。英大文字、英小文字、数字をそれぞれ1文字ずつ含む必要があります。
名前	サブアカウントの名前を30文字以内で指定します。この名前は使用者の基本情報画面に表示されます。
説明	サブアカウントの説明を150文字以内で指定します（省略可能）。この説明は使用者の基本情報画面には表示されません。

「権限設定」セクション

各ULIZAプロダクトにおいてアカウントが実行可能な操作を選択します。ただし、マスターアカウントが持たない操作権限をサブアカウントに付与することはできません。すべての権限のうち、大分類「ULIZAプロダクト共通」に含まれる権限について、以下に詳細を示します（その他の大分類に含まれる権限については、対応するULIZAプロダクトのUser Guideを参照してください）。

小分類	権限	説明
取得系	チームメンバーの取得	登録済みチームメンバーの一覧を取得する操作を許可します。
	サブアカウントの取得（※1）	登録済みサブアカウントの一覧を取得する操作を許可します。また、登録済みサブアカウントに対して「サブアカウントに切り替え」機能を使用することを許可します。
	API認証キーの取得（※2）	登録済みAPI認証キーの一覧を取得する操作を許可します。
登録系	チームメンバーの登録	チームメンバーを登録する操作を許可します。
	サブアカウントの登録（※1）	サブアカウントを登録する操作を許可します。
	API認証キーの登録（※2）	API認証キーを登録する操作を許可します。
更新系	チームメンバーの更新	チームメンバーを更新する操作を許可します。
	サブアカウントの更新（※1）	サブアカウントを更新する操作を許可します。
削除系	チームメンバーの削除	チームメンバーを削除する操作を許可します。
	サブアカウントの削除（※1）	サブアカウントを削除する操作を許可します。
	API認証キーの削除（※2）	API認証キーを削除する操作を許可します。

※1：意図せず別のアカウントからデータが取得されたり更新されたりすることを防ぐため、通常は別のサブアカウントの管理権限をもつサブアカウントは登録できないよう制限されています。これらの権限を有効化したい場合は、弊社にお問い合わせください。

※2：Web APIオプションの契約がない場合は、これらの権限は選択できなくなっています。これらの権限を有効化したい場合は、弊社にお問い合わせください。

サブアカウントを登録/更新する

設定を終えたら、画面右下の「保存」ボタンをクリックすると、サブアカウントが登録または更新されます。

サブアカウントを無効化/有効化する

サブアカウントを無効化すると、当該アカウントを使用した各ULIZAプロダクトの管理画面へのログインができなくなり、すべてのULIZAプロダクトが使用ができない状態になります。サブアカウントを無効化するには、対象のサブアカウント設定画面に遷移した後、画面左下の「アカウントの無効化」ボタンをクリックします。確認ダイアログが表示されるので、「無効化」ボタンをクリックするとサブアカウントが無効化されます。なお、サブアカウントの無効化がシステムに反映されるまで数分かかる場合があります。

無効化されたサブアカウントを有効化する（サービス利用可能な状態に戻す）には、対象のサブアカウント設定画面に遷移した後、画面左下の「アカウントの有効化」ボタンをクリックします。確認ダイアログが表示されるので、「有効化」ボタンをクリックするとサブアカウントが有効化されます。なお、サブアカウントの有効化がシステムに反映されるまで数分かかる場合があります。

サブアカウントを削除する

サブアカウントを削除するには、あらかじめ対象のサブアカウントを無効化しておく必要があります。その後、対象のサブアカウント設定画面に遷移し、画面左下の「アカウントの削除」ボタンをクリックします。確認ダイアログが表示されるので、対象のサブアカウントのログインIDを入力して「削除」ボタンをクリックするとサブアカウントが削除されます。なお、サブアカウントの削除がシステムに反映されるまで数分かかる場合があります。

ログアウトする

画面右上のログインIDをクリックすると表示されるメニューから「ログアウト」をクリックすると、アカウント設定画面からログアウトし、ログイン画面に遷移します。



サブアカウントに切り替える

マスターアカウントは、管理画面からログアウトすることなくサブアカウントとしてログインした状態に切り替えることができます。画面右上のログインIDをクリックすると表示されるメニューから「サブアカウントに切り替え」をクリックすると、「サブアカウントに切り替え」ダイアログが表示されます。切り替え先のサブアカウントを選択して「決定」ボタンをクリックすると、選択したサブアカウントとしてログインした状態に切り替わります。

切り替え元のアカウントに戻る場合は、画面右上のログインIDをクリックすると表示されるメニューから「マスターアカウントに戻る」をクリックすると、切り替え元のアカウントでログインした状態に戻ります。

ユーザー

Player (Cloud)
マルチデバイスメディアプレイヤー

Video Analytics (Basic)
視聴動向分析ソリューション

sales@uliza ▼

プレイリストの管理

検索

↔ sales@uliza に切り替え中

🔑 マスターアカウントに戻る

詳細

登録日時

表示するデータがありません。

SAML認証

本章では、ULIZAプロダクトアカウントのSAML認証について説明します。

概要

SAML（Security Assertion Markup Language）とは、異なるドメイン間で認証情報を共有するための標準仕様です。SAML 2.0に対応したIdentity Provider（以下、IdPといいます）に対し、ULIZAをService Provider（以下、SPといいます）として登録することで、IdPの認証情報を使用したULIZA管理画面へのシングルサインオンが可能になります。

IdPにより認証された使用者は、特定のULIZAプロダクトアカウントにおける一時的なチームメンバーとして振る舞います。ULIZAプロダクトアカウントに事前にチームメンバーを登録しておく必要はありません。

補足

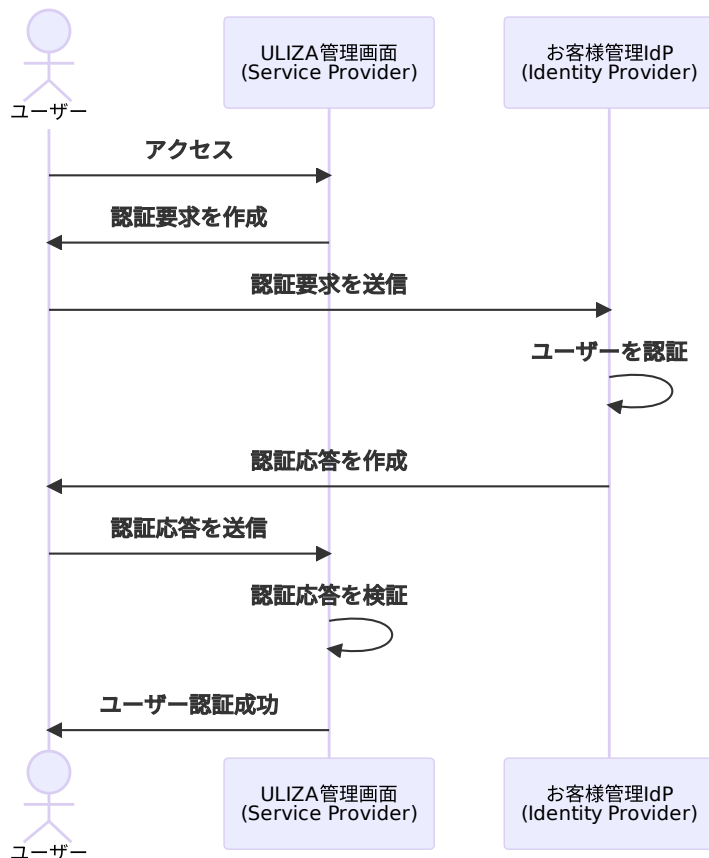
ひとつのULIZAプロダクトアカウントに複数のIdPを関連付けることができます。逆に、ひとつのIdPに複数のULIZAプロダクトアカウントを関連付けることもできます。この場合、ULIZAプロダクトアカウントごとにSP Entity IDが異なるため、IdPに複数のアプリケーションとして登録する（ポータル画面に複数のULIZAアイコンが表示される）形になります。

SAML認証の流れ

ULIZAはSP-initiated SSOとIdP-initiated SSOをサポートします。

SP-initiated SSO

使用者が最初にULIZA管理画面にアクセスすることから始まる認証方式です。以下に基本的なシーケンスを示します。



SP-initiated SSOを行うには、ULIZAログイン画面で「SSOでログイン」をクリックします。



ULIZA

ULIZA プロダクトアカウントでログインしてください。

ログイン ID

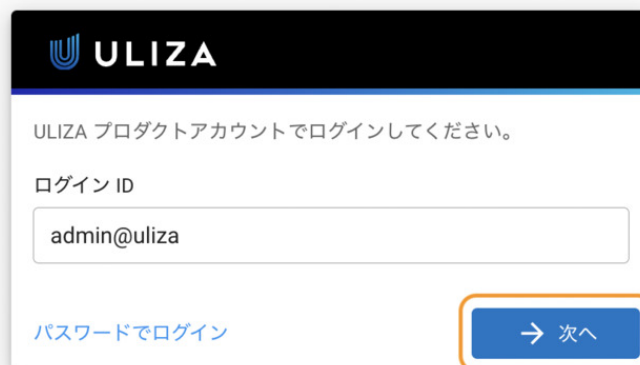
パスワード

☐ チームメンバーとしてログイン ①

[パスワードを忘れた場合](#) [SSO でログイン](#) [ログイン](#)

Powered by **PLAY**

ログインIDを入力して「次へ」ボタンをクリックすると、ULIZA管理画面にログインできます。



ULIZA

ULIZA プロダクトアカウントでログインしてください。

ログイン ID

[パスワードでログイン](#) [→ 次へ](#)

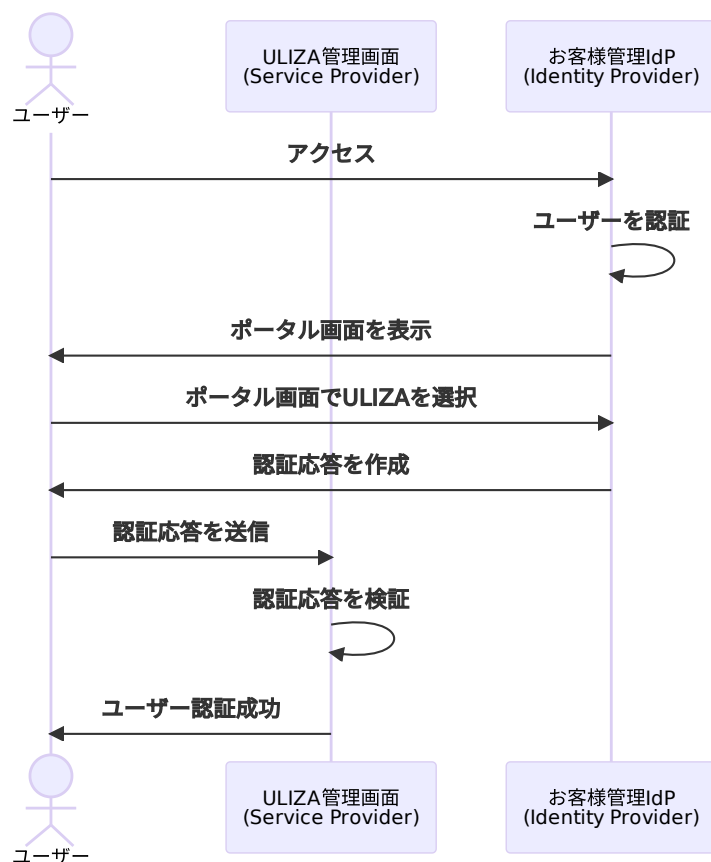
Powered by **PLAY**

補足

指定されたアカウントに複数のIdPが関連付けられている場合は、認証に使用するIdPを選択する画面が表示されます。

IdP-initiated SSO

使用者がIdPが提供するポータル画面を経由してULIZAにログインする認証方式です。以下に基本的なシーケンスを示します。



使用者はIdPが提供するポータル画面でULIZAのアイコンをクリックすることで、ULIZA管理画面にシングルサインオンできます（下図はIdPとしてOktaを利用している場合のダッシュボード画面例）。



SAML認証仕様

認証フロー

ULIZAは以下の認証フローをサポートします。

- SP-initiated SSO
- IdP-initiated SSO

SAMLバインディング

ULIZAは以下のSAMLバインディングをサポートします。

- HTTP POST Binding

Name IDの形式

ULIZAは以下のName IDの形式を要求します。

- urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

SAMLリクエストの署名

ULIZAはSAMLリクエストの署名をサポートしません。

SAMLレスポンスの署名

SAMLアサーションには署名が必須です。SAMLレスポンスの署名は任意です。

ダイジェストアルゴリズム

- http://www.w3.org/2000/09/xmlsig#sha1
- http://www.w3.org/2001/04/xmlenc#sha256
- http://www.w3.org/2001/04/xmlenc#sha512

署名検証アルゴリズム

- http://www.w3.org/2000/09/xmlsig#rsa-sha1
- http://www.w3.org/2001/04/xmlsig-more#rsa-sha256
- http://www.w3.org/2001/04/xmlsig-more#rsa-sha512
- http://www.w3.org/2000/09/xmlsig#hmac-sha1

正規化アルゴリズム

- http://www.w3.org/2001/10/xml-exc-c14n#
- http://www.w3.org/2001/10/xml-exc-c14n#WithComments
- http://www.w3.org/2000/09/xmlsig#enveloped-signature

設定方法

SAML認証を設定するには、以下の手順に従います。

1. **SPメタデータを取得する**： ULIZA管理画面からULIZAのSPメタデータを取得します。
2. **IdPにULIZAを登録する**： 取得したメタデータを使用してIdPにULIZAをSPとして登録します。
3. **ULIZAにIdPを登録する**： IdPから取得したメタデータを使用してULIZAにIdPを登録します。

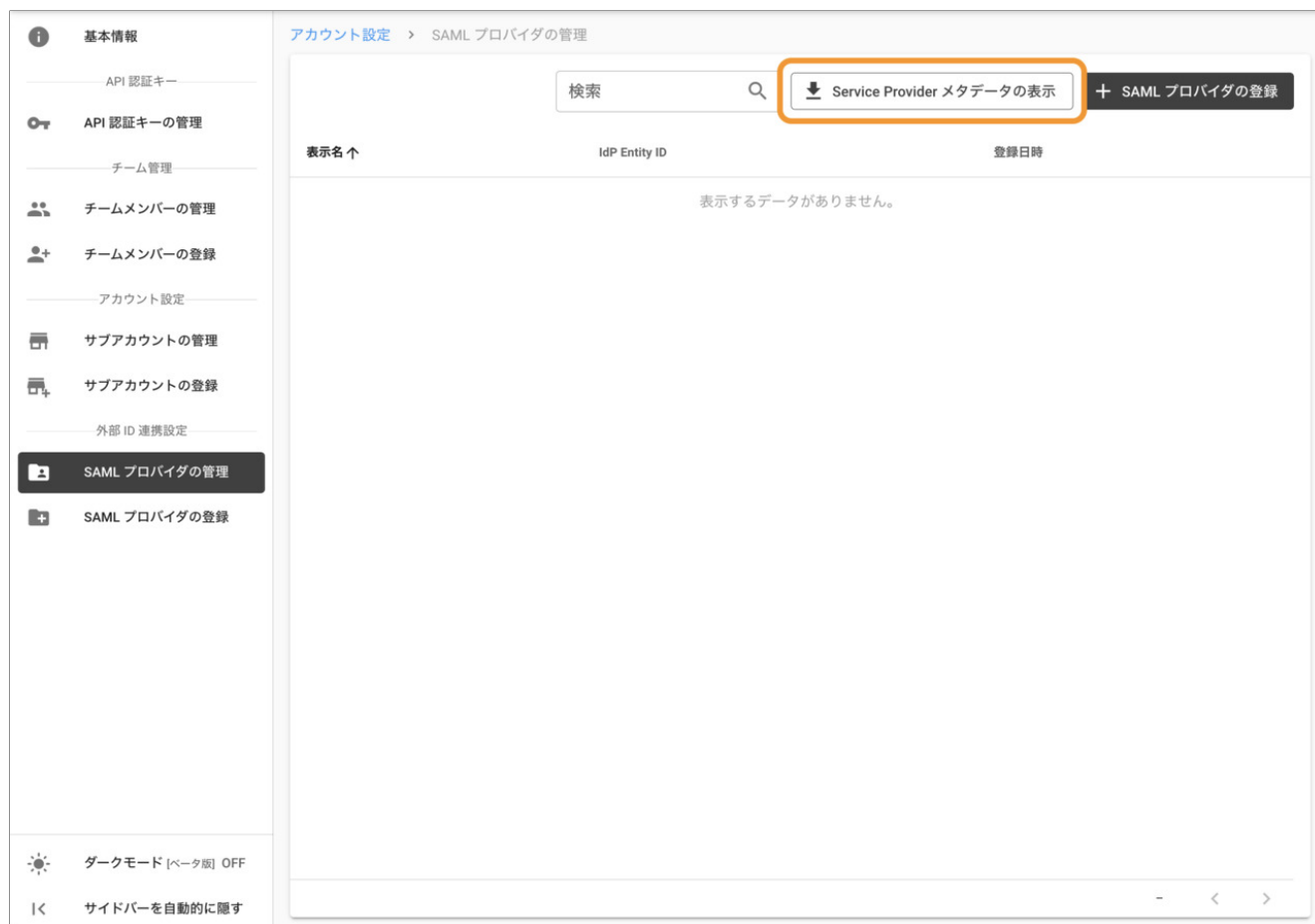
SPメタデータを取得する

1. ULIZAのアカウント設定から「SAMLプロバイダの管理」画面を開きます。

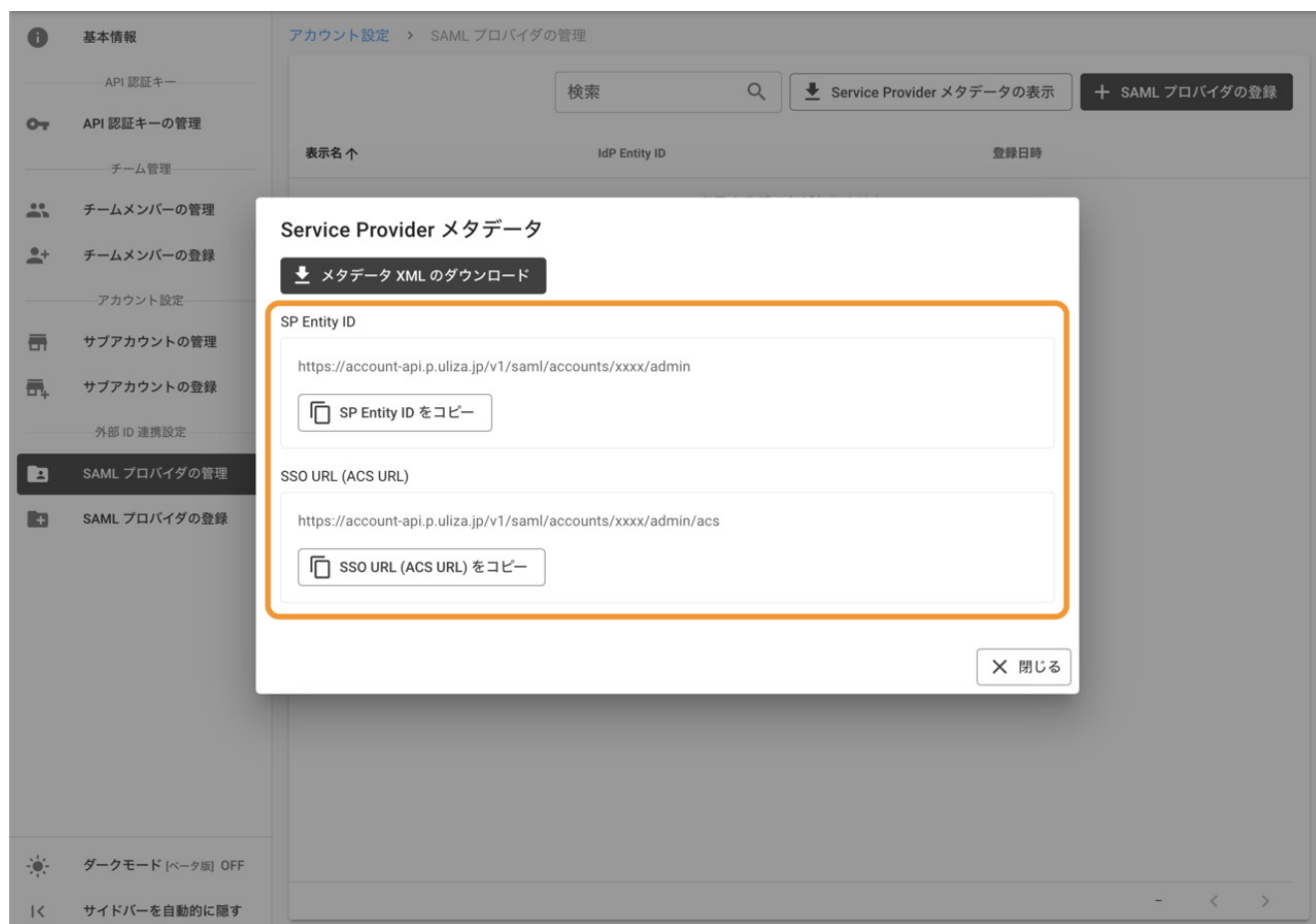
注意

SAML認証の利用可否は契約により異なります。サイドバーに「SAMLプロバイダの管理」メニューが表示されていない場合は、SAML認証は利用できません。弊社までお問い合わせください。

2. 「Service Providerメタデータの表示」ボタンをクリックします。

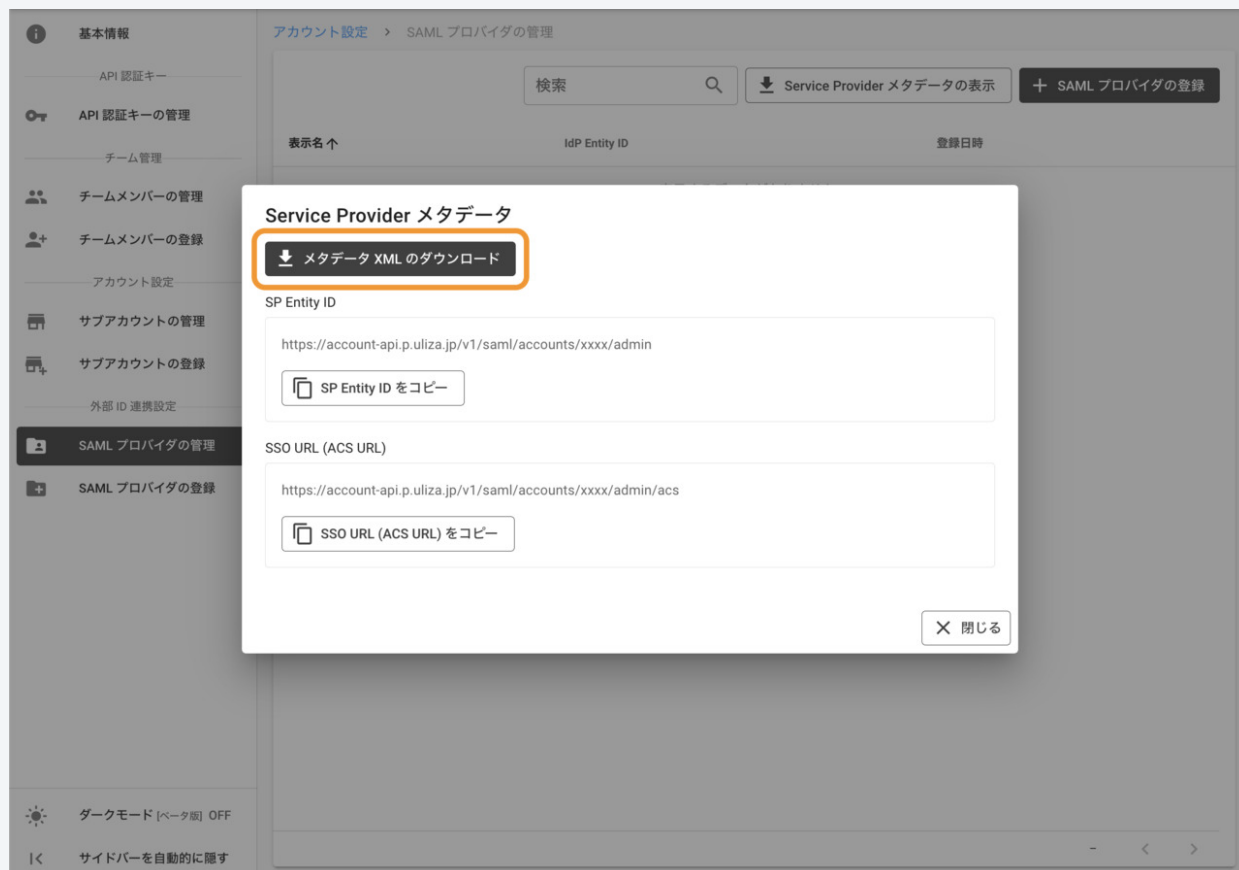


3. 表示される「SP Entity ID」および「SSO URL (ACS URL)」の値をメモしておきます。



補足

IdPがメタデータXMLのアップロードに対応している場合（Azure Active Directoryなど）は、上記の値をメモしておく代わりに「メタデータXMLのダウンロード」ボタンをクリックして、設定値をXMLファイルとしてダウンロードできます。



IdPにULIZAを登録する

以下の設定例を参考に設定を行います。

- Auth0の場合
- Azure Active Directoryの場合
- CloudGate UNOの場合
- Oktaの場合
- OneLoginの場合

ULIZAにIdPを登録する

1. ULIZAのアカウント設定から「SAMLプロバイダの管理」画面を開きます。

注意

SAML認証の利用可否は契約により異なります。サイドバーに「SAMLプロバイダの管理」メニューが表示されていない場合は、SAML認証は利用できません。弊社までお問い合わせください。

2. 「SAMLプロバイダの登録」ボタンをクリックします。
3. 「基本情報」セクションについて、以下のように設定します。

項目	設定値
表示名	任意の名前（例：「Auth0」「Azure AD」など）を入力
Identity Providerメタデータ	IdPから取得したメタデータXMLをアップロード

基本情報

API 認証キー

API 認証キーの管理

チーム管理

チームメンバーの管理

チームメンバーの登録

アカウント設定

サブアカウントの管理

サブアカウントの登録

外部 ID 連携設定

SAML プロバイダの管理

SAML プロバイダの登録

アカウント設定 > SAML プロバイダの管理 > SAML プロバイダの登録

基本情報

登録する SAML プロバイダの情報を設定します。

表示名 必須

認証プロバイダを識別するための分かりやすい名前を指定します。30 文字以内で指定します。

0 / 30

Identity Provider メタデータ 必須

Identity Provider (IdP) から取得したメタデータを指定します。メタデータは XML 形式 (文字コード UTF-8) である必要があります。

Choose File

No file chosen

× キャンセル

保存

4. 「保存」ボタンをクリックします。

権限制御

IdPにより認証された使用者には、関連付けられているULIZAプロダクトアカウントに付与されているすべての権限（ただし、チームメンバーやサブアカウントの管理権限など、「ULIZAプロダクト共通」グループに含まれる権限は除く）がデフォルトで付与されます。この挙動を変更するには、以下に示すSAML AttributeをSAMLレスポンスに含めることで、権限設定をULIZAに渡すことができます。

- **Name** : `https://account-api.p.uliza.jp/v1/saml/attributes/permissions`
- **Value** : 下表に示す権限表現文字列（コンマ区切りで複数指定可）

権限	権限表現文字列
すべての権限（ULIZAプロダクト共通を含む）	<code>*</code>
ULIZA VMS (Cloud)のすべての権限	<code>manager:*</code>
ULIZA VMS (Cloud)のすべての取得系の権限	<code>manager:GET:*</code>
ULIZA VMS (Cloud)のすべての登録系の権限	<code>manager:POST:*</code>
ULIZA VMS (Cloud)のすべての更新系の権限	<code>manager:PUT:*</code>
ULIZA VMS (Cloud)のすべての削除系の権限	<code>manager:DELETE:*</code>
ULIZA En-Cluster (Cloud)のすべての権限	<code>encoder:*</code>
ULIZA Player (Cloud)のすべての権限	<code>player:*</code>
ULIZA Video Analytics (Cloud)のすべての権限	<code>analyticsv2:*</code>
ULIZA IP Broadcaster (Cloud)のすべての権限	<code>ipb:*</code>
ULIZA Live Event Managerのすべての権限	<code>liveEventManager:*</code>
ULIZA Sidetalkのすべての権限	<code>sidetalk:*</code>

補足

上表に記載のない権限についても設定可能な場合があります。詳しくはお問い合わせください。

IdPの具体的な設定方法については、IdPの提供元にお問い合わせください。

設定例

ULIZA VMS (Cloud)のすべての権限とULIZA Sidetalkのすべての権限を付与するには、SAMLレスポンスに以下のようなSAML Attributeを含める必要があります。

```
<Attribute Name="https://account-api.p.uliza.jp/v1/saml/attributes/permissions">
  <AttributeValue>manager:*,sidetalk:*</AttributeValue>
</Attribute>
```

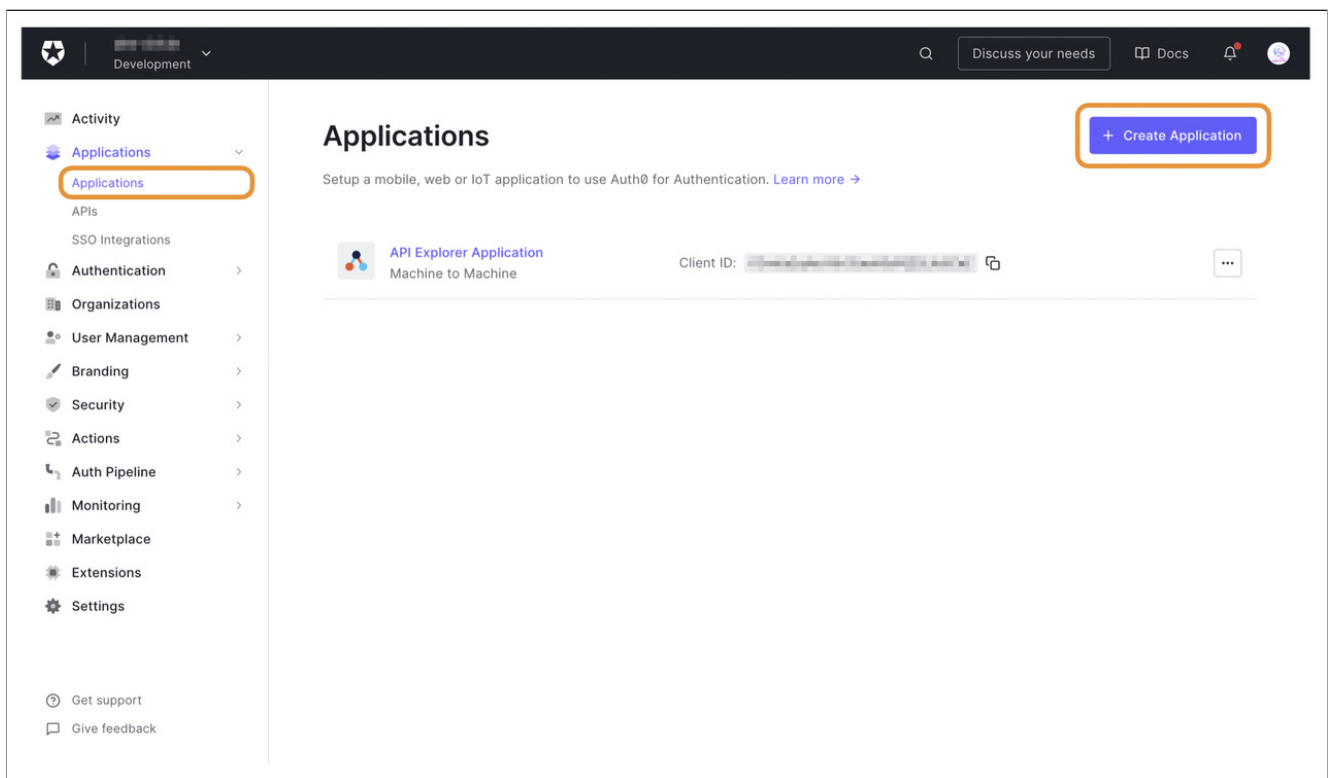
IdP設定例

注意

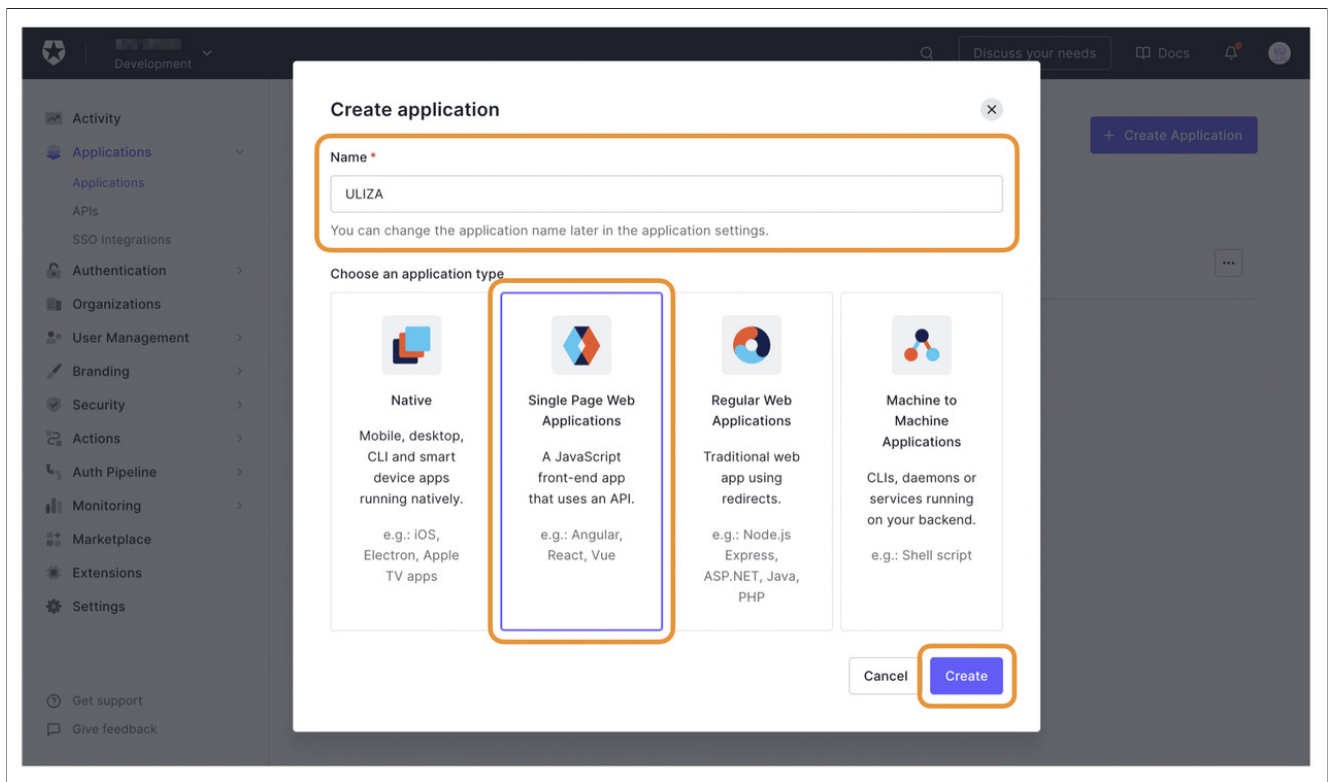
IdP設定例は2022年8月時点の情報に基づき作成しています。

Auth0の場合

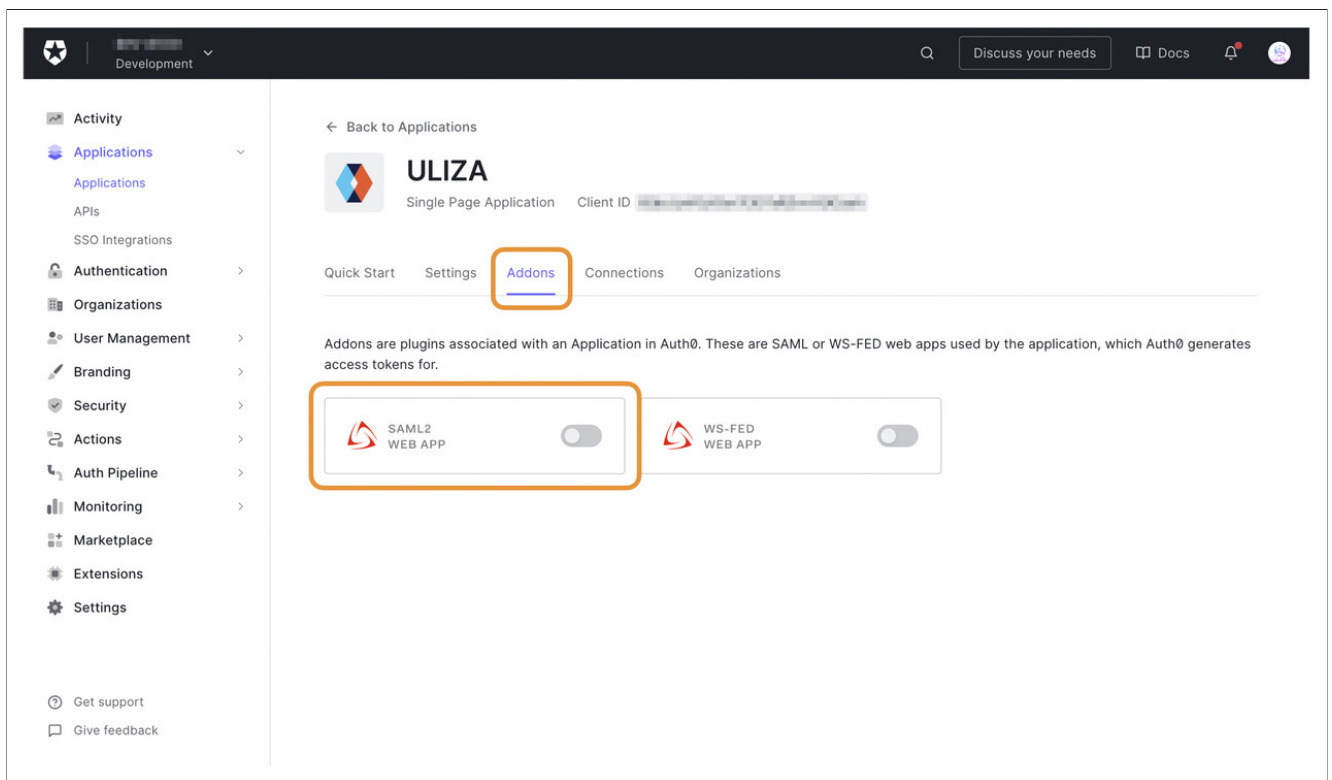
1. Auth0 Dashboard を開きます。
2. 左側のメニューから「Applications>Applications」をクリックしてアプリケーション一覧画面を開きます。
3. 「Create Application」 ボタンをクリックします。



4. 「Name」に任意のアプリケーション名（例：「ULIZA」）を入力し、「Single Page Web Applications」を選択して「Create」ボタンをクリックします。



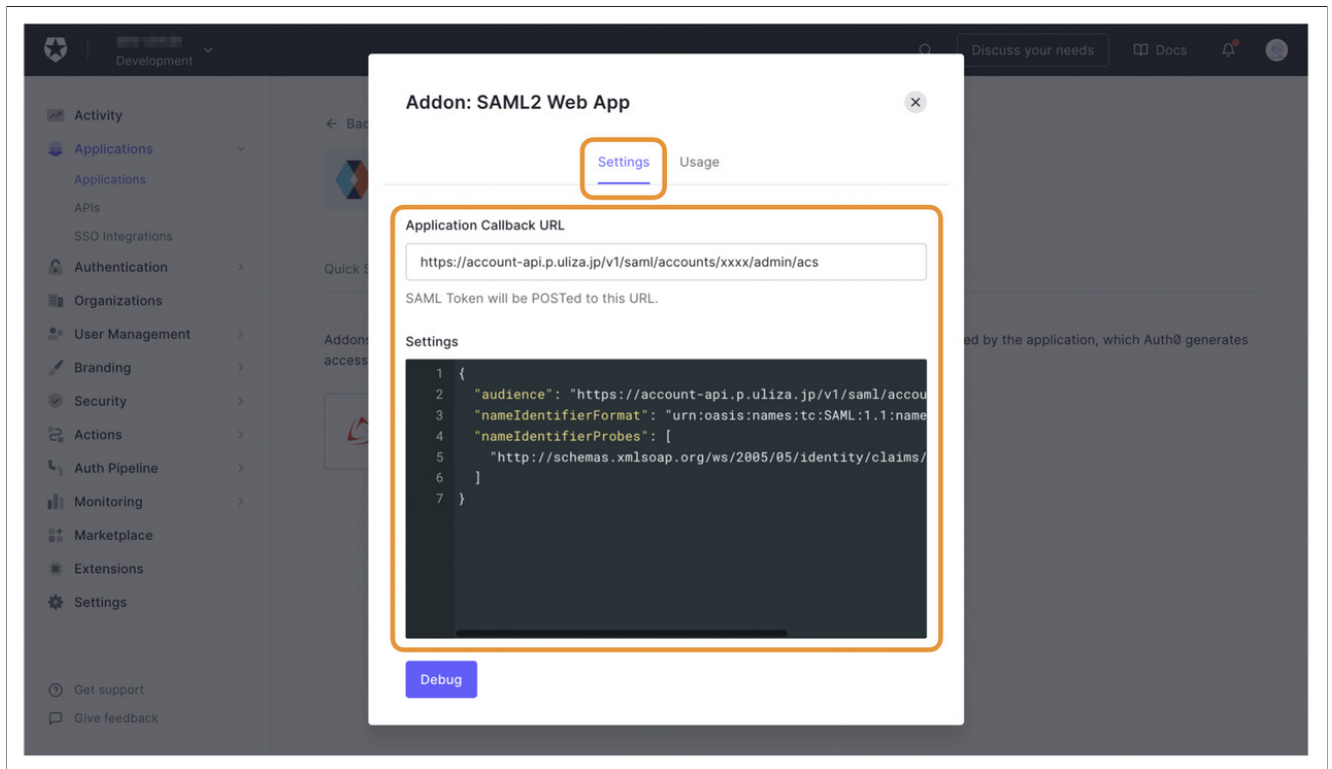
5. 「Addons」タブを開き、「SAML2 WEB APP」をクリックします。



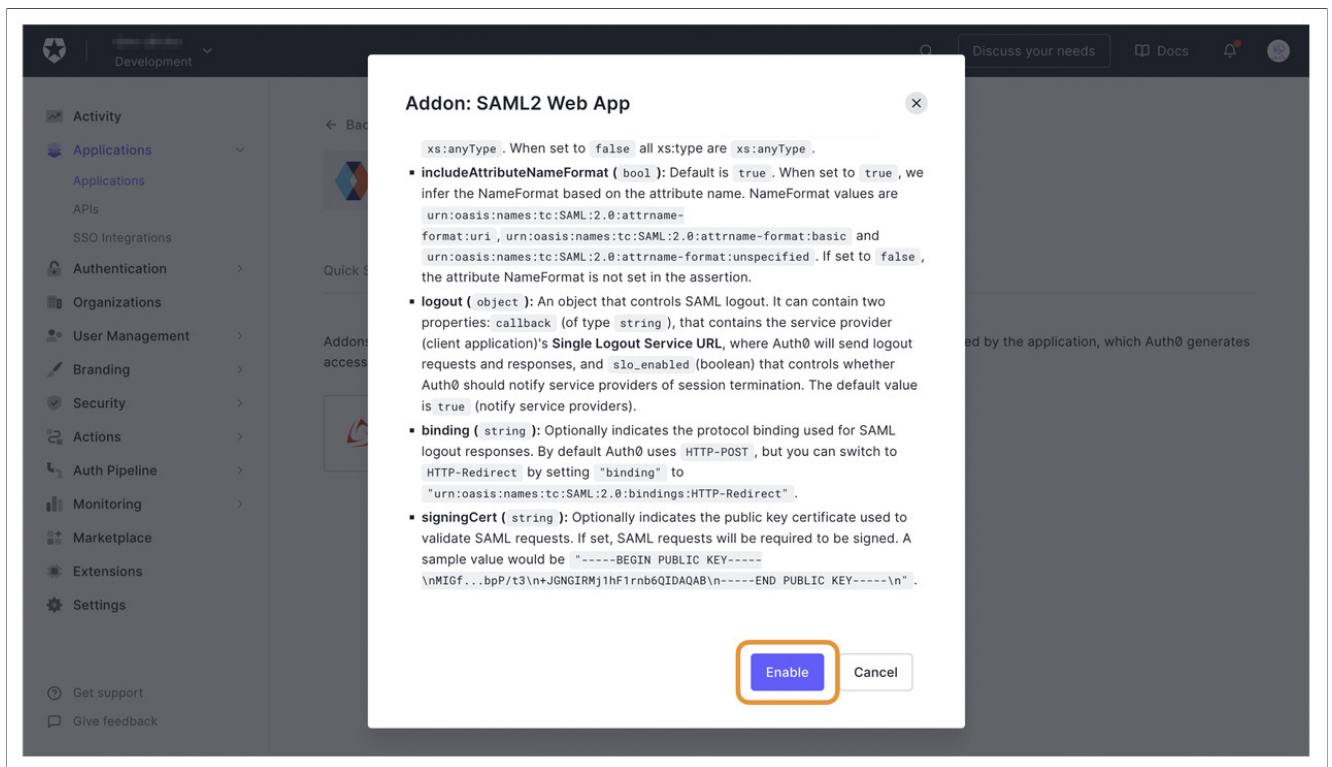
6. 「Settings」タブを開き、「Application Callback URL」にこちらでメモしておいた「SSO URL (ACS URL)」の値を入力します。また、「Settings」には以下のようなJSON文字列を入力します。ただし、`audience`の値はこちらでメモしておいた「SP Entity ID」の値に書き換える必要があります。

```
{
  "audience": "https://account-api.p.uliza.jp/v1/saml/accounts/xxxx/admin", // 書き換えが必要
  "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
  "nameIdentifierProbes": [
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
  ]
}
```

json

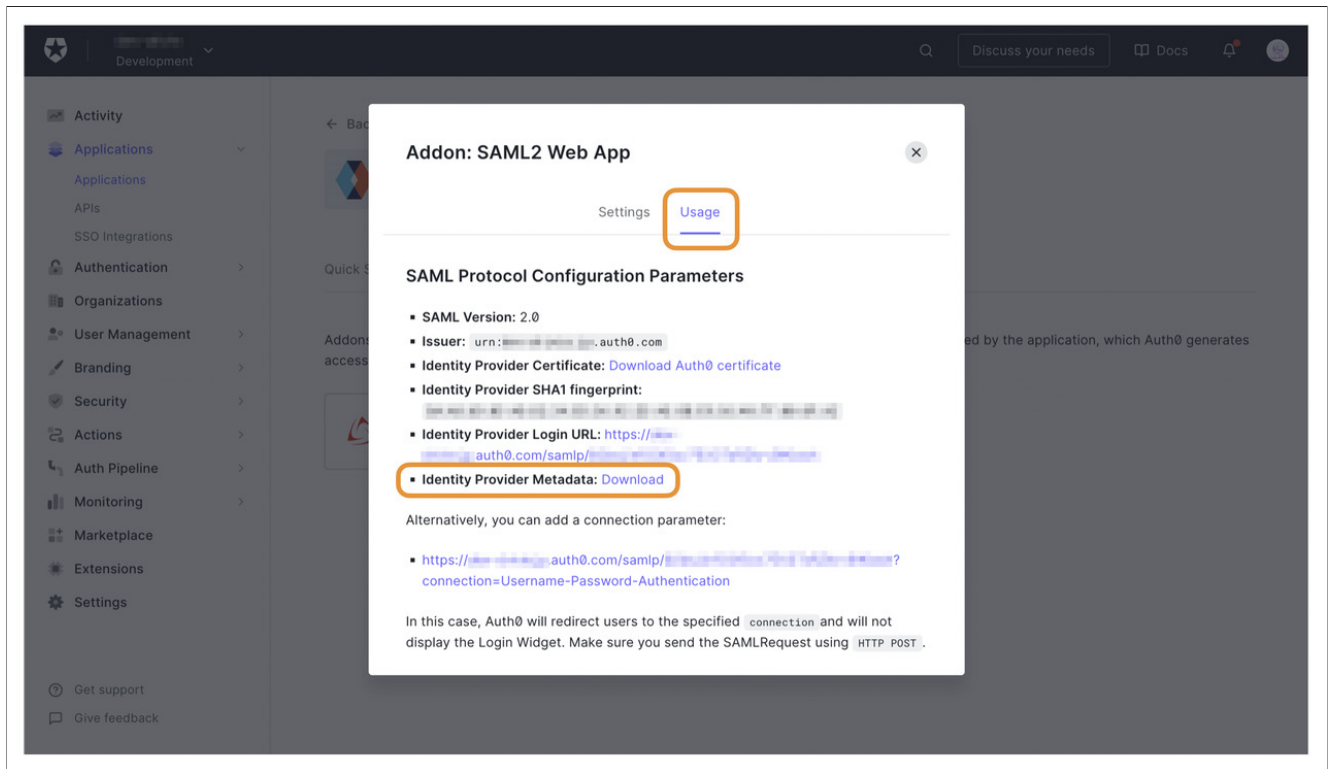


7. ダイアログボックス最下部にある「Enable」ボタンをクリックします。



8. 「Usage」タブをクリックします。

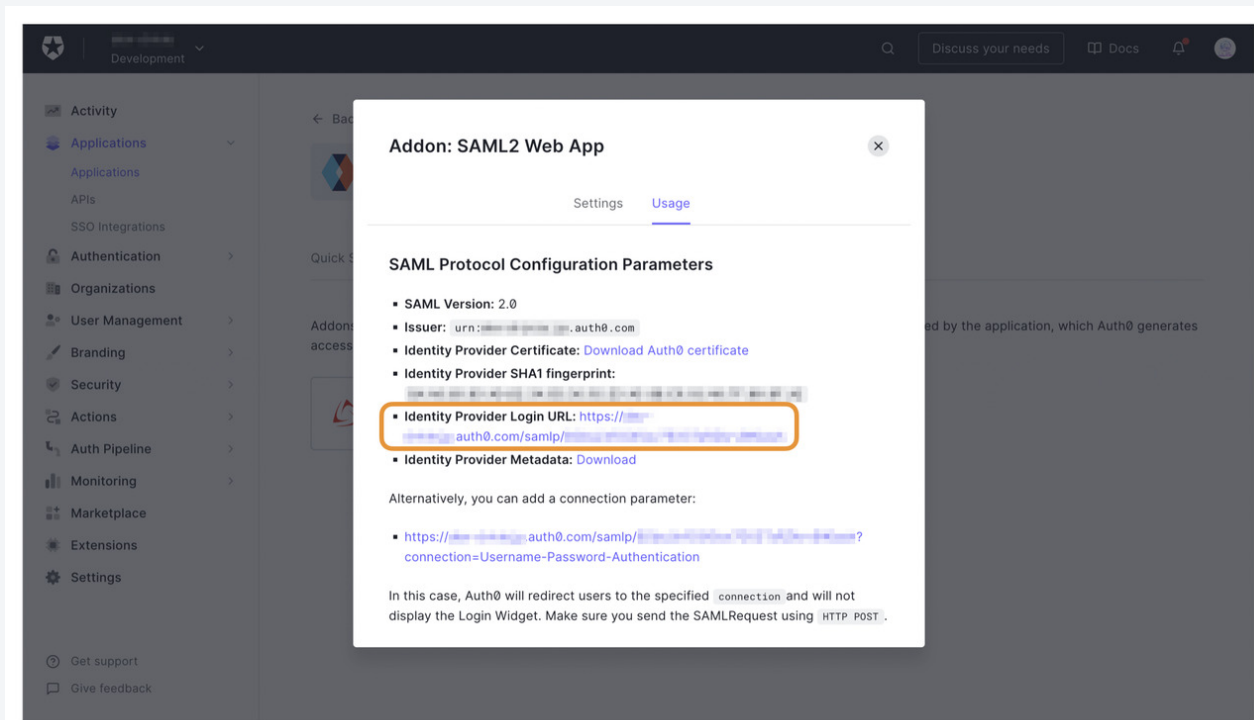
9. 「Identity Provider Metadata」の右にある「Download」をクリックして、メタデータXMLをダウンロードしておきます。



引き続きULIZA側での設定を行います。

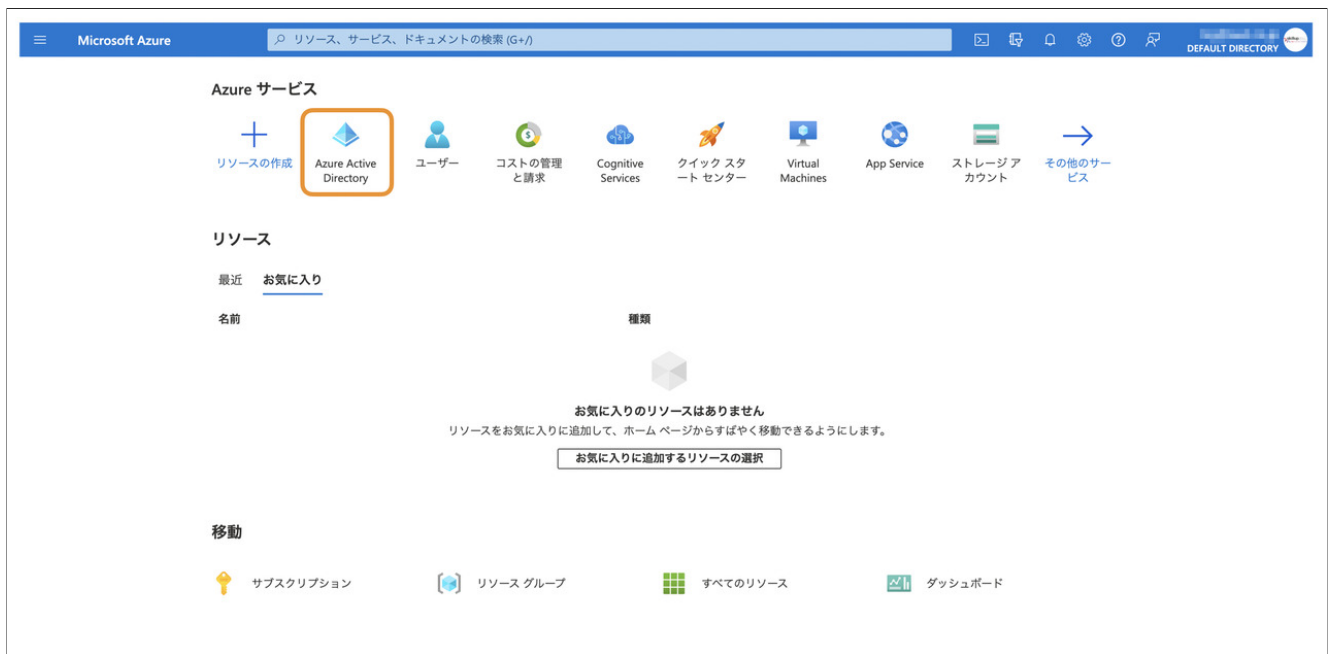
補足

ULIZA側での設定が完了すると「Identity Provider Login URL」にアクセスすることでULIZA管理画面にシングルサインオンできるようになります。

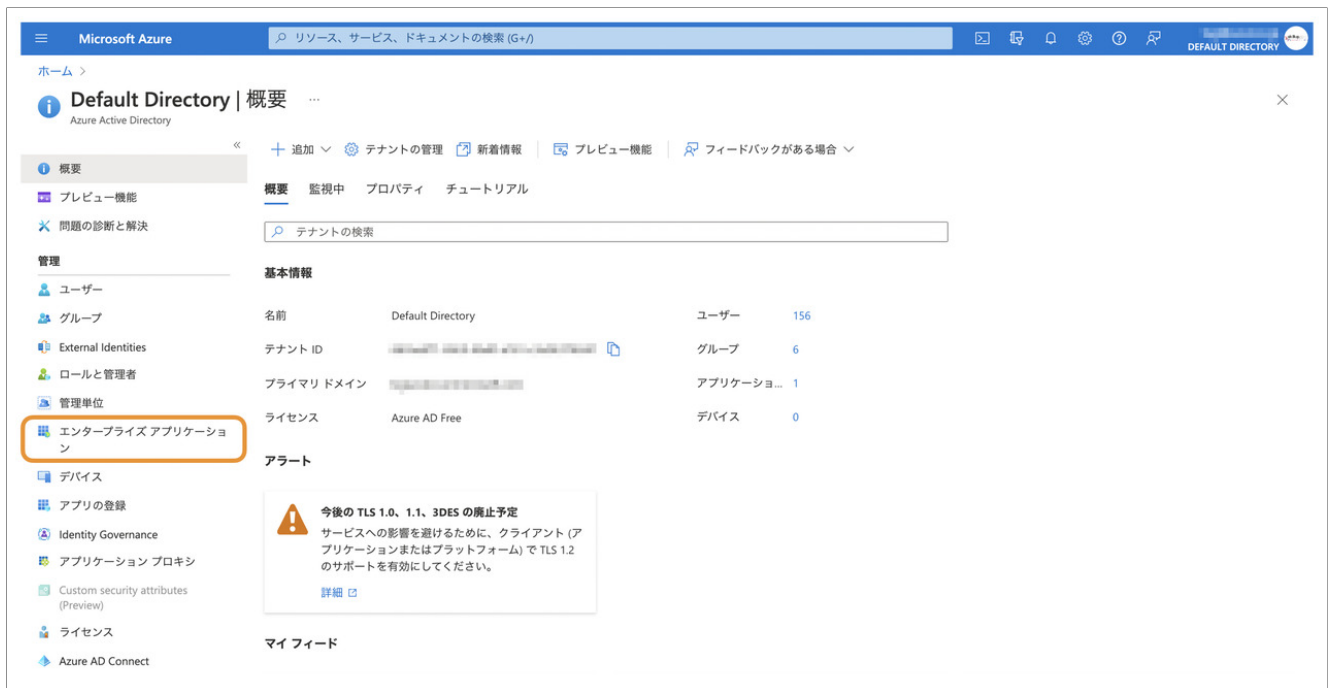


Azure Active Directoryの場合

1. Azureポータル にサインインします。
2. 「Azure Active Directory」をクリックします。



3. 左側のメニューから「エンタープライズ アプリケーション」をクリックします。



4. 左側のメニューから「すべてのアプリケーション」をクリックし、画面上部にある「新しいアプリケーション」をクリックします。



5. 「独自のアプリケーションの作成」をクリックします。

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+/J)

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | すべてのアプリケーション >

Azure AD ギャラリーの参照


+ 独自のアプリケーションの作成 | フィードバックがある場合

Azure AD アプリ ギャラリーは、シングルサインオン (SSO) と自動ユーザー プロビジョニングの展開と構成を簡単にする数千のアプリのカatalogです。アプリ ギャラリーからアプリをデプロイするときに、事前に構築されたテンプレートを活用して、ユーザーをより安全にアプリに接続することができます。ここで独自のアプリケーションを参照または作成してください。他の組織が検出して使用できるように、開発したアプリケーションを Azure AD ギャラリーに公開する場合は、次に説明されているプロセスを使用して要求を提出できます。 [この記事](#)


アプリケーションを検索 | シングル サインオン: **すべて** | ユーザー アカウントの管理: **ALL** | カテゴリ: **すべて**

クラウド プラットフォーム


Amazon Web Services (AWS)




Google Cloud Platform



Oracle



SAP



オンプレミスのアプリケーション

オンプレミスのアプリケーションの追加

Azure AD アプリケーション プロキシを構成し、セキュアなリモートアクセスを実現します。

アプリケーション プロキシの詳細情報

アプリケーション プロキシを使用してオンプレミスのアプリケーションへの安全なリモートアクセスを提供する方法について説明します。

アプリケーション プロキシ コネクタの管理

コネクタは、オンプレミスの軽量エージェントであり、アプリケーション プロキシ サービスへの通信接続を容易にします。

フェデレーション SSO | プロビジョニング中

6. 任意のアプリケーション名（例：「ULIZA」）を入力し「作成」ボタンをクリックします。

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+/J)

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | すべてのアプリケーション >

Azure AD ギャラリーの参照

+ 独自のアプリケーションの作成 | フィードバックがある場合

Azure AD アプリ ギャラリーは、シングルサインオン (SSO) と自動ユーザー プロビジョニングの展開と構成を簡単にする数千のアプリのカatalogです。アプリ ギャラリーからアプリをデプロイするときに、事前に構築されたテンプレートを活用して、ユーザーをより安全にアプリに接続することができます。ここで独自のアプリケーションを参照または作成してください。他の組織が検出して使用できるように、開発したアプリケーションを Azure AD ギャラリーに公開する場合は、次に説明されているプロセスを使用して要求を提出できます。 [この記事](#)

アプリケーションを検索 | シングル サインオン: **すべて** | ユーザー アカウントの管理: **ALL** | カテゴリ: **すべて**

クラウド プラットフォーム

Amazon Web Services (AWS)



Google Cloud Platform



Oracle



オンプレミスのアプリケーション

オンプレミスのアプリケーションの追加

Azure AD アプリケーション プロキシを構成し、セキュアなリモートアクセスを実現します。

アプリケーション プロキシの詳細情報

アプリケーション プロキシを使用してオンプレミスのアプリケーションへの安全なリモートアクセスを提供する方法について説明します。

フェデレーション SSO | プロビジョニング中

独自のアプリケーションの作成

フィードバックがある場合

独自のアプリケーションを開発している場合、アプリケーション プロキシを使用している場合、またはギャラリーにないアプリケーションを統合する必要がある場合は、ここで独自のアプリケーションを作成できます。

お使いのアプリの名前は何か?

ULIZA

アプリケーションでどのような操作を行いたいですか?

- ☐ オンプレミスのアプリケーションへのセキュリティで保護されたリモート アクセス用のアプリケーション プロキシを構成します
- ☐ アプリケーションを登録して Azure AD と統合します (開発中のアプリ)
- ☒ ギャラリーに見つからないその他のアプリケーションを統合します (ギャラリー以外)

作成

7. 「シングル サインオンの設定」をクリックします。

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+)

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | すべてのアプリケーション > Azure AD ギャラリーの参照 >

ULIZA | 概要

エンタープライズ アプリケーション

概要

デプロイ計画

管理

- プロパティ
- 所有者
- ロールと管理者
- ユーザーとグループ
- シングルサインオン
- プロビジョニング
- アプリケーション プロキシ
- セルフサービス
- カスタム セキュリティ属性 (プレビュー)

セキュリティ

- 条件付きアクセス
- アクセス許可
- トークンの暗号化

アクティビティ

- サインイン ログ
- 使用状況と分析情報

プロパティ

名前 ○
ULIZA

アプリケーション ID ○
[アプリケーション ID]

オブジェクト ID ○
[オブジェクト ID]

Getting Started

- 1. ユーザーとグループの割り当て**
特定のユーザーおよびグループにアプリケーションへのアクセスを付与
[ユーザーとグループの割り当て](#)
- 2. シングル サインオンの設定**
ユーザーが自分の Azure AD 資格情報を使用して、アプリケーションにサインインできるようにする
[作業の開始](#)
- 3. ユーザー アカウントのプロビジョニング**
アプリケーションでユーザー アカウントを自動的に作成および削除
[作業の開始](#)
- 4. 条件付きアクセス**
カスタマイズ可能なアクセス ポリシーによる、このアプリケーションへの安全なアクセス。
[ポリシーの作成](#)
- 5. セルフ サービス**
ユーザーが Azure AD 資格情報を使用してアプリケーションへのアクセスを要求できるようにする
[作業の開始](#)

8. 「SAML」をクリックします。

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+)

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | すべてのアプリケーション > Azure AD ギャラリーの参照 > ULIZA

ULIZA | シングル サインオン

エンタープライズ アプリケーション

概要

デプロイ計画

管理

- プロパティ
- 所有者
- ロールと管理者
- ユーザーとグループ
- シングルサインオン
- プロビジョニング
- アプリケーション プロキシ
- セルフサービス
- カスタム セキュリティ属性 (プレビュー)

セキュリティ

- 条件付きアクセス
- アクセス許可
- トークンの暗号化

アクティビティ

- サインイン ログ
- 使用状況と分析情報

シングルサインオン (SSO) により、組織内のユーザーが、自分が使用しているすべてのアプリケーションに、1つのアカウントでサインインできるようになるため、ユーザーが Azure Active Directory のアプリケーションにサインオンするときのセキュリティと利便性を向上します。一度ユーザーがアプリケーションにログインすると、その資格情報は、そのユーザーがアクセスする必要がある他のすべてのアプリケーションに使用されます。[詳細については、こちらをご覧ください。](#)

シングル サインオン方式の選択

判断に役立つヘルプの表示

- 無効**
シングルサインオンが有効になっていません。ユーザーは、[マイアプリ] からアプリを起動できません。
- SAML**
SAML (Security Assertion Markup Language) プロトコルを使用した、アプリケーションに対する多機能かつセキュリティで保護された認証。
- パスワードベース**
Web ブラウザーの拡張機能またはモバイルアプリを使用したパスワードの保存と再生。
- リンク**
マイアプリや Office 365 アプリケーション起動プログラム内のアプリケーションへのリンク。

9. 「メタデータ ファイルをアップロードする」をクリックします。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | すべてのアプリケーション > Azure AD ギャラリーの参照 > ULIZA >

ULIZA | SAML ベースのサインオン

エンタープライズ アプリケーション

概要 | デプロイ計画 | 管理 | プロパティ | 所有者 | ロールと管理者 | ユーザーとグループ | シングルサインオン | プロビジョニング | アプリケーション プロキシ | セルフサービス | カスタム セキュリティ属性 (プレビュー) | セキュリティ | 条件付きアクセス | アクセス許可 | トークンの暗号化 | アクティビティ | サインイン ログ | 使用状況と分析情報

メタデータ ファイルをアップロードする | シングルサインオン モードの変更 | このアプリケーションをテスト | フィードバックがある場合

SAML によるシングル サインオンのセットアップ

フェデレーション プロトコルに基づく SSO 実装により、セキュリティ、信頼性、エンド ユーザー エクスペリエンスが向上し、実装が容易になります。OpenID Connect または OAuth が使用されていない既存のアプリケーションの場合は、できるだけ SAML シングル サインオンを選択してください。詳細については、[こちらをご覧ください](#)。

以下をお読みください [構成ガイド](#)。ULIZA を統合するためのヘルプ。

- 基本的な SAML 構成** [編集](#)

識別子 (エンティティ ID)	必須
応答 URL (Assertion Consumer Service URL)	必須
サインオン URL	省略可能
リレー状態 (省略可能)	省略可能
ログアウト URL (省略可能)	省略可能
- 属性とクレーム**

⚠ 手順 1 で必須フィールドを入力してください

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
一意のユーザー ID	user.userprincipalname
- SAML 署名証明書**

⚠ 手順 1 で必須フィールドを入力してください

10. こちらでダウンロードしておいたメタデータXMLファイルを選択して「追加」ボタンをクリックします。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | すべてのアプリケーション > Azure AD ギャラリーの参照 > ULIZA >

ULIZA | SAML ベースのサインオン

エンタープライズ アプリケーション

概要 | デプロイ計画 | 管理 | プロパティ | 所有者 | ロールと管理者 | ユーザーとグループ | シングルサインオン | プロビジョニング | アプリケーション プロキシ | セルフサービス | カスタム セキュリティ属性 (プレビュー) | セキュリティ | 条件付きアクセス | アクセス許可 | トークンの暗号化 | アクティビティ | サインイン ログ | 使用状況と分析情報

メタデータ ファイルをアップロードする | シングルサインオン モードの変更 | このアプリケーションをテスト | フィードバックがある場合

メタデータ ファイルをアップロードします。

以下のフィールドの値は ULIZA によって提供されます。値を手動で入力することもできますし、構成済みの SAML メタデータ ファイルが ULIZA によって提供されている場合にはそれをアップロードすることもできます。

[追加](#) [キャンセル](#)

- 基本的な SAML 構成** [編集](#)

識別子 (エンティティ ID)	必須
応答 URL (Assertion Consumer Service URL)	必須
サインオン URL	省略可能
リレー状態 (省略可能)	省略可能
ログアウト URL (省略可能)	省略可能
- 属性とクレーム**

⚠ 手順 1 で必須フィールドを入力してください

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
一意のユーザー ID	user.userprincipalname
- SAML 署名証明書**

⚠ 手順 1 で必須フィールドを入力してください

11. 「保存」ボタンをクリックします。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | ULIZA | SAML ベースのサインオン

基本的な SAML 構成

保存 フィードバックがある場合

SAML 構成エクスペリエンスのこのプレビューを終了しますか? ここをクリックすると、プレビューが終了します。 →

識別子 (エンティティ ID) * ①

Azure Active Directory に対してアプリケーションを識別する一意の ID。この値は、Azure Active Directory テナント内のすべてのアプリケーションで一意である必要があります。既定の識別子は、IDP で開始された SSO の SAML 応答の対象ユーザーになります。

https://account-api.p.uliza.jp/v1/saml/accounts/xxxx/admin

識別子の追加

応答 URL (Assertion Consumer Service URL) * ②

応答 URL は、アプリケーションが認証トークンを受け取る場所です。これは、SAML では "Assertion Consumer Service" (ACS) とも呼ばれます。

https://account-api.p.uliza.jp/v1/saml/accounts/xxxx/admin/acs

応答 URL の追加

サインオン URL (省略可能)

サービス プロバイダーによって開始されたシングル サインオンを実行する場合は、サインオン URL が使用されます。この値は、アプリケーションのサインイン ページの URL です。ID プロバイダーによって開始されたシングル サインオンを実行する場合、このフィールドは不要です。

サインオン URL を入力してください

SAML によるシングル サインオンのセットアップ

フェデレーション プロトコルに基づく SSO 実装により、セキュリティ、信頼性、エンド ユーザー エクスペリエンスが向上し、実装が容易になります。OpenID Connect または OAuth が使用されていない既存のアプリケーションの場合は、できるだけ SAML シングル サインオンを選択してください。詳細については、こちらをご覧ください。

以下をお読みください 構成ガイド ULIZA を統合するためのヘルプ。

- 基本的な SAML 構成
 - 識別子 (エンティティ ID) 必須
 - 応答 URL (Assertion Consumer Service URL) 必須
 - サインオン URL 省略可
 - リレー状態 (省略可能) 省略可
 - ログアウト URL (省略可能) 省略可
- 属性とクレーム
 - 手順 1 で必須フィールドに入力してください
 - givenname user.givenname
 - surname user.surname
 - emailaddress user.mail
 - name user.userprincipalname
 - 一意のユーザー ID user.userprincipalname
- SAML 署名証明書
 - 手順 1 で必須フィールドに入力してください

12. 「フェデレーション メタデータXML」の右にある「ダウンロード」をクリックして、メタデータXMLをダウンロードしておきます。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | ULIZA | SAML ベースのサインオン

ULIZA | SAML ベースのサインオン

メタデータファイルをアップロードする シングル サインオン モードの変更 このアプリケーションをテスト フィードバックがある場合

SAML によるシングル サインオンのセットアップ

フェデレーション プロトコルに基づく SSO 実装により、セキュリティ、信頼性、エンド ユーザー エクスペリエンスが向上し、実装が容易になります。OpenID Connect または OAuth が使用されていない既存のアプリケーションの場合は、できるだけ SAML シングル サインオンを選択してください。詳細については、こちらをご覧ください。

以下をお読みください 構成ガイド ULIZA を統合するためのヘルプ。

- 基本的な SAML 構成 [編集](#)
 - 識別子 (エンティティ ID) https://account-api.p.uliza.jp/v1/saml/accounts/xxx/admin
 - 応答 URL (Assertion Consumer Service URL) https://account-api.p.uliza.jp/v1/saml/accounts/xxx/admin/acs
 - サインオン URL 省略可能
 - リレー状態 (省略可能) 省略可能
 - ログアウト URL (省略可能) 省略可能
- 属性とクレーム [編集](#)
 - givenname user.givenname
 - surname user.surname
 - emailaddress user.mail
 - name user.userprincipalname
 - 一意のユーザー ID user.userprincipalname
- SAML 署名証明書 [編集](#)
 - 状態 アクティブ
 - 封印
 - 有効期限 2027/5/23 5:02:49
 - 通知用メール
 - アプリのフェデレーション メタデータ URL https://login.microsoftonline.com/
 - 証明書 (Base64) [ダウンロード](#)
 - 証明書 (未加工) [ダウンロード](#)
 - フェデレーション メタデータ XML [ダウンロード](#)
- ULIZA のセットアップ

続いて、ULIZAにユーザーを割り当てます。

1. 左側のメニューから「ユーザーとグループ」をクリックします。
2. 画面上部にある「ユーザーまたはグループの追加」をクリックします。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | すべてのアプリケーション > Azure AD ギャラリーの参照 > ULIZA

ULIZA | ユーザーとグループ

エンタープライズ アプリケーション

概要

デプロイ計画

管理

- プロパティ
- 所有者
- ロールと管理者
- ユーザーとグループ**
- シングルサインオン
- プロビジョニング
- アプリケーション プロキシ
- セルフサービス
- カスタム セキュリティ属性 (プレビュー)

セキュリティ

- 条件付きアクセス
- アクセス許可

ユーザーまたはグループの追加

編集 削除 資格情報の更新 列 フィードバックがある場合

アプリケーションは、割り当てられたユーザーのマイ アプリ内に表示されます。これを表示しないするには、プロパティの中で [ユーザーに表示しますか?] を [いいえ] に設定します。 →

ここで、アプリケーションのアプリのロールにユーザーとグループを割り当てます。このアプリケーションの新しいアプリのロールを作成するには、[アプリケーション登録](#)を使用します。

最初の 200 件を表示しています。すべてのユーザーとグループを検索するには、表示名を入力してください。

表示名	オブジェクトの種類	割り当てられたロール
アプリケーションの割り当てが見つかりませんでした		

3. 「ユーザー」の下にある「選択されていません」をクリックします。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | すべてのアプリケーション > Azure AD ギャラリーの参照 > ULIZA | ユーザーとグループ >

割り当ての追加

Default Directory

お客様の Active Directory プラン レベルでは、グループを割り当てることはできません。個々のユーザーをアプリケーションに割り当てることはできます。

ユーザー

選択されていません

ロールを選択してください

User

割り当て

4. ULIZAへのアクセス権限を割り当てるユーザーをクリックして「選択」ボタンをクリックします。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | すべてのアプリケーション > Azure AD

割り当ての追加

Default Directory

お客様の Active Directory プラン レベルでは、グループを割り当てることはできません。個々のユーザーをアプリケーションに割り当てることはできます。

ユーザー

選択されていません

ロールを選択してください

User

割り当て

ユーザー

検索

	選択済み
	選択済み
	選択済み

選択したアイテム

	削除
	削除

選択

5. 「割り当て」 ボタンをクリックします。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Default Directory | エンタープライズ アプリケーション > エンタープライズ アプリケーション | すべてのアプリケーション > Azure AD ギャラリーの参照 > ULIZA | ユーザーとグループ >

割り当ての追加

Default Directory

お客様の Active Directory プラン レベルでは、グループを割り当てることはできません。個々のユーザーをアプリケーションに割り当てることはできます。

ユーザー

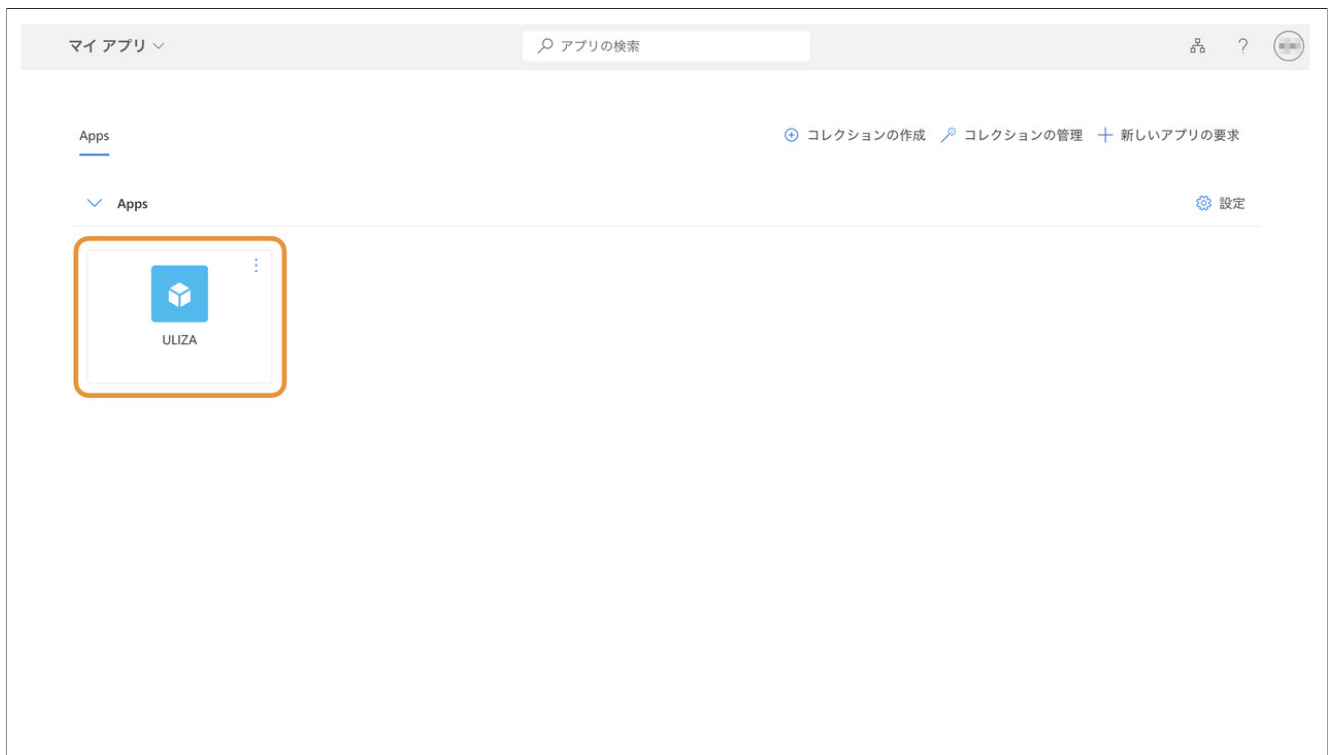
2 人のユーザーが選択されました。

ロールを選択してください

User

割り当て

6. 割り当てられたユーザーのマイ アプリ にULIZAへのリンクが表示されることを確認します。



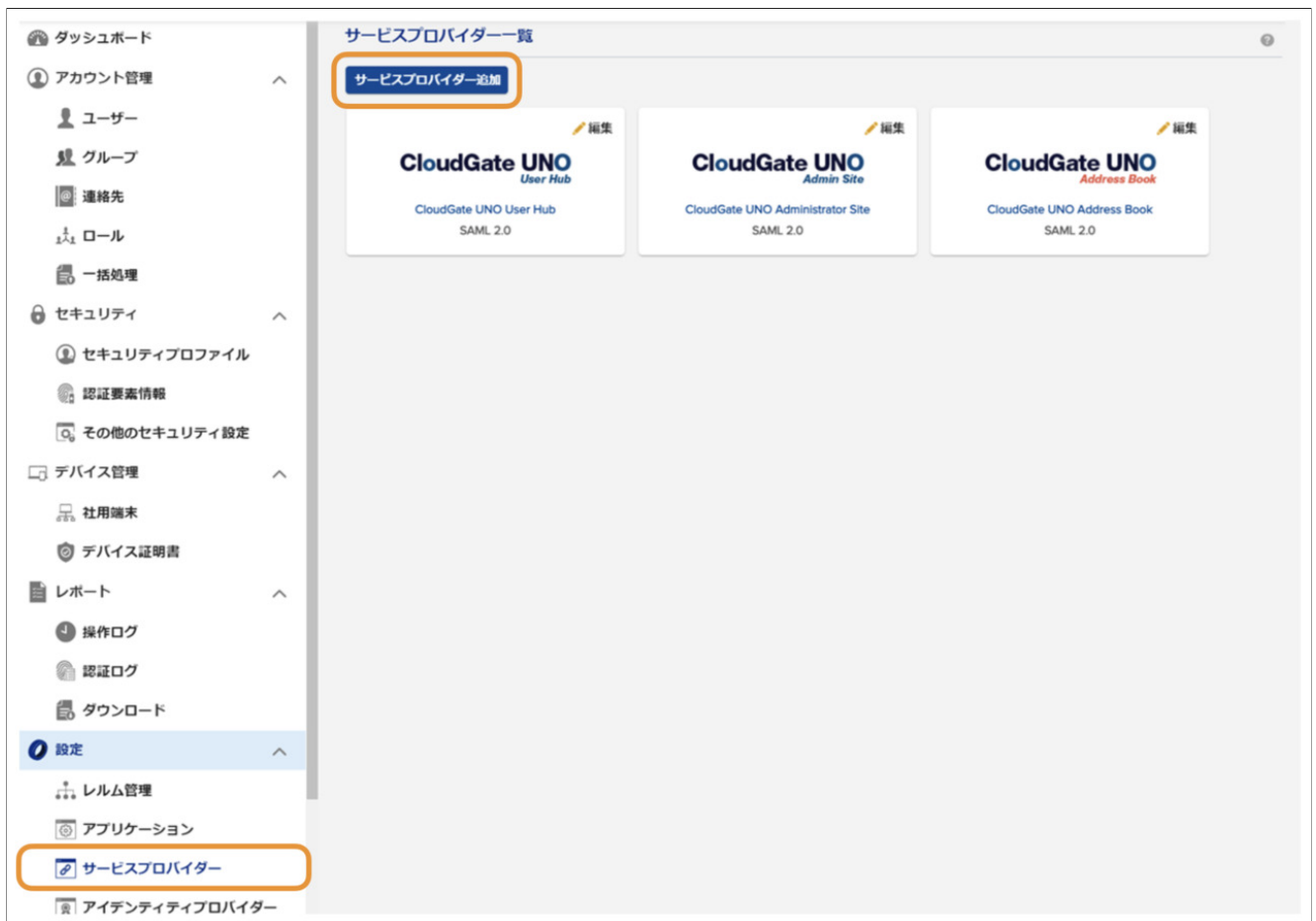
注意

この時点ではULIZA側での設定が完了していないため、ULIZAへのリンクをクリックするとエラーが発生します。

引き続きULIZA側での設定を行います。

CloudGate UNOの場合

1. CloudGate UNO管理者サイト（CloudGate UNO Admin Site）を開きます。
2. 左側のメニューから「設定＞サービスプロバイダー」をクリックしてサービスプロバイダー一覧画面を開きます。
3. 一覧画面上部にある「サービスプロバイダー追加」ボタンをクリックします。



4. 検索ボックスに「xxxxxxForSaml」と入力して「検索」ボタンをクリックし、表示されたCustom Serviceの右上にある「追加」をクリックします。



5. 任意の表示名（例：「ULIZA」）を入力して「追加」ボタンをクリックします。



6. サービスプロバイダの「一般設定」画面が表示されます。必要に応じて「サービスの選択状態」や「ロゴ画像」などを設定し、「保存」ボタンをクリックします。

サービスプロバイダー一覧 ▶ ULIZA

一般設定 シングルサインオン設定 プロビジョニング設定

基本情報

サービス名 xxxxxxForSaml

表示名* ULIZA

管理サイトURL


ユーザー管理設定

サービスの選択状態 ☐ On 新規ユーザー作成画面が表示されたときに ULIZA は未選択

デバイスの設定


サポートデバイス ☒ PC ☐ スマートデバイス

ロゴ

 ファイルを選択 選択されていません [プレビュー](#) [デフォルトに戻す](#)

i ロゴの変更を適用するには、保存をクリックしてください。

アイコン

 ファイルを選択 選択されていません [プレビュー](#) [デフォルトに戻す](#)

i アイコンの変更を適用するには、保存をクリックしてください。

◀ サービスプロバイダー一覧へ **保存** 削除 履歴

7. 「シングルサインオン設定」タブをクリックします。

サービスプロバイダー一覧 ▶ ULIZA

一般設定 **シングルサインオン設定** プロビジョニング設定

基本情報

8. 「シングルサインオンの設定」および「シングルサインオフの設定」セクションについて、以下のように設定します。

項目	設定値
IdP-initiated SSO	「On」に設定
SP-initiated SSO	「On」に設定
Issuer / Provider name / Entity ID	こちらでメモしておいた「SP Entity ID」の値を入力
Assertion consumer service URL	こちらでメモしておいた「SSO URL (ACS URL)」の値を入力
RelayState	何も入力しない
Name IDの形式	「urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress」を選択
リクエストへの署名	「Off」に設定（変更できません）

項目	設定値
レスポンスへの署名	「On」に設定
アサーションへの署名	「On」に設定
サインオフ方法	「なし」を選択

サービスプロバイダー一覧 ▶ **ULIZA**

一般設定 シングルサインオン設定 プロビジョニング設定

SAML 2.0のIdP情報

プロバイダー名	https://echizen.cloudgate.jp/sso/...	コピー
ログインURL	https://echizen.cloudgate.jp/sso/...	コピー
ログアウトURL	https://echizen.cloudgate.jp/sso/...	コピー
パスワード変更画面URL	https://echizen.cloudgate.jp/user-hub/...	コピー
証明書	ダウンロード	
証明書のフィンガープリント (SHA1)	コピー	
証明書のフィンガープリント (SHA256)	コピー	
証明書のフィンガープリント (MD5)	コピー	
SAML 2.0 メタデータ	ダウンロード	

シングルサインオンの設定

サインオンメソッド	SAML 2.0
IdP-initiated SSO	<input checked="" type="checkbox"/> On
SP-initiated SSO	<input checked="" type="checkbox"/> On
Issuer / Provider name / Entity ID	https://account-api.p.uliza.jp/v1/saml/accounts/xxxx/admin
Assertion consumer service URL*	https://account-api.p.uliza.jp/v1/saml/accounts/xxxx/admin/acs
RelayState	
Name IDの形式	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress ▼
リクエストへの署名	<input type="checkbox"/> Off
レスポンスへの署名	<input checked="" type="checkbox"/> On
アサーションへの署名	<input checked="" type="checkbox"/> On

[さらに表示する](#)

シングルサインオフの設定

サインオフ方法	なし ▼
---------	------

◀ サービスプロバイダー一覧へ

[保存](#) [履歴](#)

9. 「保存」ボタンをクリックします。

10. 「SAML 2.0メタデータ」の右にある「ダウンロード」をクリックして、メタデータXMLをダウンロードしておきます。

サービスプロバイダー一覧 ▶ **ULIZA**

一般設定 **シングルサインオン設定** プロビジョニング設定

SAML 2.0のIdP情報

プロバイダー名	https://echizen.cloudgate.jp/sso/	📄 コピー
ログインURL	https://echizen.cloudgate.jp/sso/	📄 コピー
ログアウトURL	https://echizen.cloudgate.jp/sso/	📄 コピー
パスワード変更画面URL	https://echizen.cloudgate.jp/user-hub/	📄 コピー
証明書	📄 ダウンロード	
証明書のフィンガープリント (SHA1)		📄 コピー
証明書のフィンガープリント (SHA256)		📄 コピー
証明書のフィンガープリント (MD5)		📄 コピー
SAML 2.0 メタデータ	📄 ダウンロード	

続いて、ULIZAにユーザーを割り当てます。

1. 左側のメニューから「アカウント管理>ユーザー」をクリックしてユーザー管理画面を開きます。
2. ULIZAへのアクセス権限を割り当てるユーザーのユーザーIDをクリックします。

🏠 ダッシュボード **ユーザー管理**

👤 アカウント管理 **ユーザー** 組織 役割 カスタムフィールド

👤 ユーザー

👥 グループ

📧 連絡先

👤 ロール

📁 一括処理

🔒 セキュリティ

🔒 セキュリティプロファイル

🔒 認証要素情報

🔒 その他のセキュリティ設定

ユーザー管理

🔍 ユーザー検索

全てのセキュリティプロファイル 全ての利用可能サービス 全てのステータス

🔍 検索

現在の階層 株式会社PLAY ▶

🟢 作成 🚫 削除 🔄 移動 ⚙️ その他の操作 ▼

ユーザーID	表示名	サービス	プロファイル	ステータス
①		🔵	デフォルト	
②		🔵	デフォルト	
③		🔵	デフォルト	

3. 「サービス」セクションで「ULIZA」にチェックを入れ、任意のアカウントIDを入力し「保存」ボタンをクリックします。



4. 割り当てられたユーザーのユーザーハブ（CloudGate UNO User Hub）にULIZAへのリンクが表示されることを確認します。



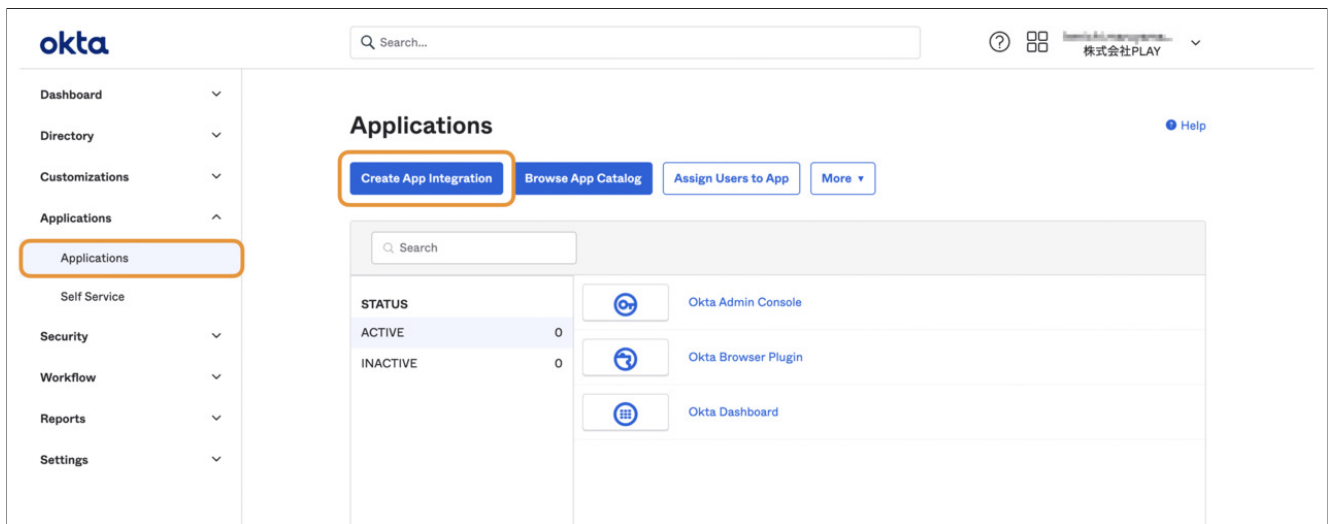
注意

この時点ではULIZA側での設定が完了していないため、ULIZAへのリンクをクリックするとエラーが発生します。

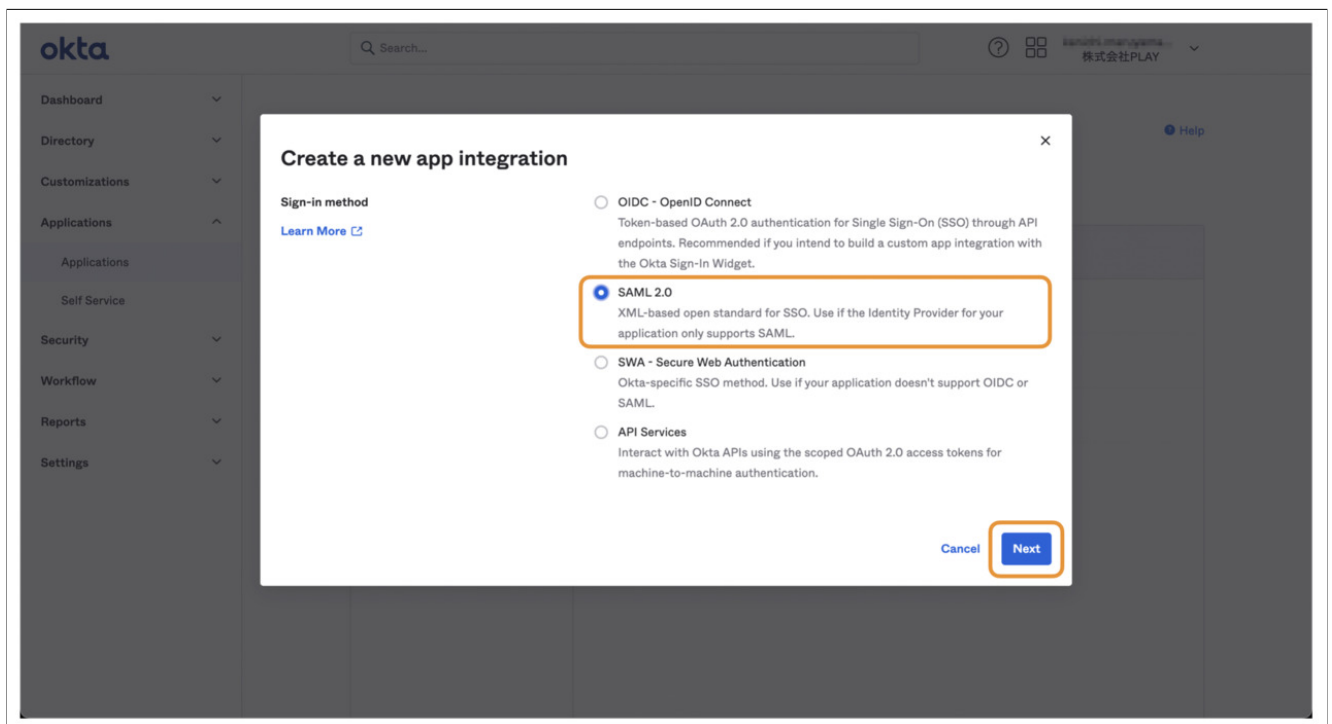
引き続きULIZA側での設定を行います。

Oktaの場合

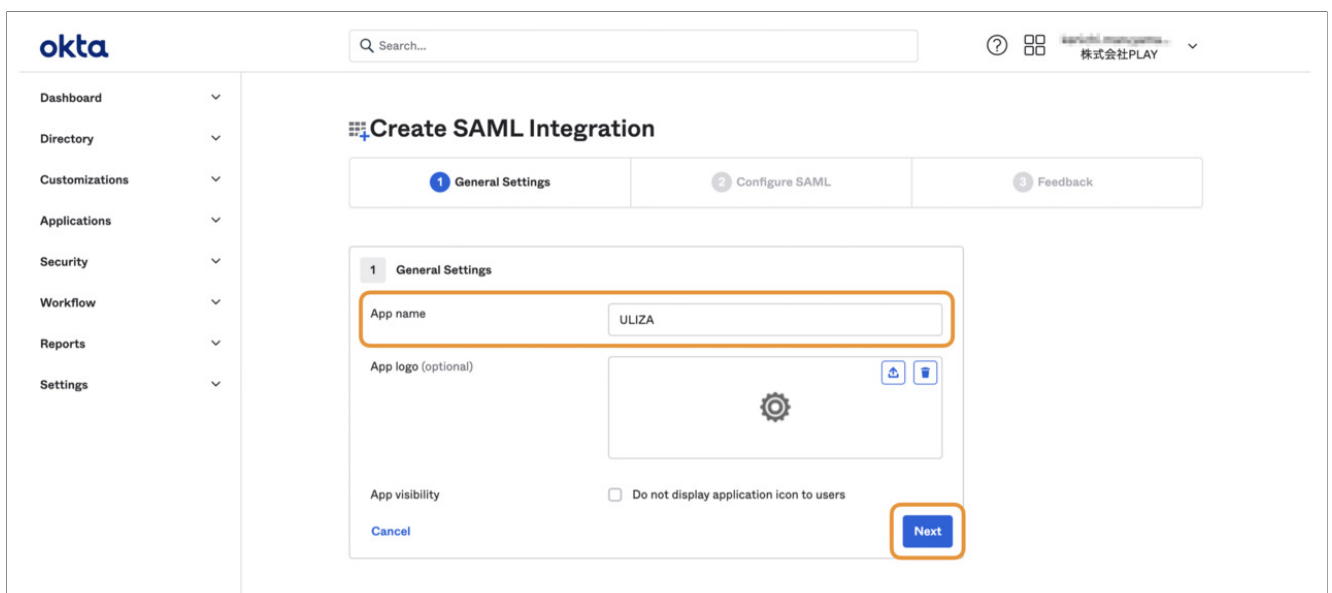
1. Okta Admin Consoleを開きます。
2. 左側のメニューから「Applications>Applications」をクリックしてアプリケーション一覧画面を開きます。
3. 画面上部にある「Create App Integration」ボタンをクリックします。



4. 「SAML 2.0」を選択して「Next」ボタンをクリックします。



5. 「App Name」に任意のアプリケーション名（例：「ULIZA」）を入力します。必要に応じてロゴ画像などを設定し「Next」ボタンをクリックします。



6. 「General」セクションについて、以下のように設定します。

項目	設定値
Single sign on URL	こちらでメモしておいた「SSO URL (ACS URL)」の値を入力
Audience URI (SP Entity ID)	こちらでメモしておいた「SP Entity ID」の値を入力
Default RelayState	何も入力しない
Name ID format	「EmailAddress」を選択
Application username	「Oktaユーザー名」を推奨
Update application username on	「作成と更新」を選択

okta Search... ? 株式会社PLAY

Create SAML Integration

- General Settings
- Configure SAML**
- Feedback

A SAML Settings

General

Single sign on URL
☒ Use this for Recipient URL and Destination URL
☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState
If no value is set, a blank RelayState is sent

Name ID format

Application username

Update application username on

[Show Advanced Settings](#)

Attribute Statements (optional) [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text"/>

[Add Another](#)

Group Attribute Statements (optional)

Name	Name format (optional)	Filter
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text" value="先頭"/>

[Add Another](#)

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

7. 「Next」 ボタンをクリックします。

okta

Search...

?

Basic Management

株式会社PLAY

Dashboard

Directory

Customizations

Applications

Applications

Self Service

Security

Workflow

Reports

Settings

← Back to Applications

ULIZA

Active

View Logs

Monitor Imports

General

Sign On

Import

Assignments

Settings

Edit

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

Credentials Details

Application username formatOktaユーザー名

Update application username on作成と更新

Update Now

Password reveal

☐ Allow users to securely see their password (Recommended)

SAML Signing Certificates

Generate new certificate

Type	Type	Type	Created	Expires	Status	Actions
SHA-1	SHA-1	SHA-1	Today	Aug 2032	Inactive	Actions
SHA-2	SHA-2	SHA-2	Today	Aug 2032	Active	Actions

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

View SAML setup instructions

How to Configure SAML 2.0 for ULIZA Application

Note: These setup instructions include certificate information for this app's most recently created SAML signing certificate. For users to get access to the app using these instructions, that certificate must be active.

The following is needed to configure ULIZA

- 1 Identity Provider Single Sign-On URL:
`https://[redacted].okta.com/app/[redacted]`
- 2 Identity Provider Issuer:
`http://www.okta.com/[redacted]`
- 3 X.509 Certificate:
-----BEGIN CERTIFICATE-----
[redacted]
-----END CERTIFICATE-----
[Download certificate](#)

Optional

- 1 Provide the following IDP metadata to your SP provider.
`<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor entityID="http://www.okta.com/[redacted]"`

注意

IDP metadataは複数行にまたがる長い文字列です。テキストボックスを右クリックして「すべて選択」をクリックするか、Ctrl+Aキーを使用して、IDP metadataの内容全体が確実にコピーされていることを確認してください。

続いて、ULIZAにユーザーを割り当てます。

1. アプリケーション詳細画面で「Assignments」タブをクリックします。
2. 「Assign」ボタンをクリックし、表示されるメニューから「Assign to People」を選択します。

ULIZA Active View Logs Monitor Imports

General Sign On Import **Assignments**

Assign Convert assignments Search... People

Assign to People Assign to Groups

Groups	Type
	01101110
	01101111
	01101100
	01101100
	01101101
	01101110
	01100111

No users found

REPORTS

- Current Assignments
- Recent Unassignments

SELF SERVICE

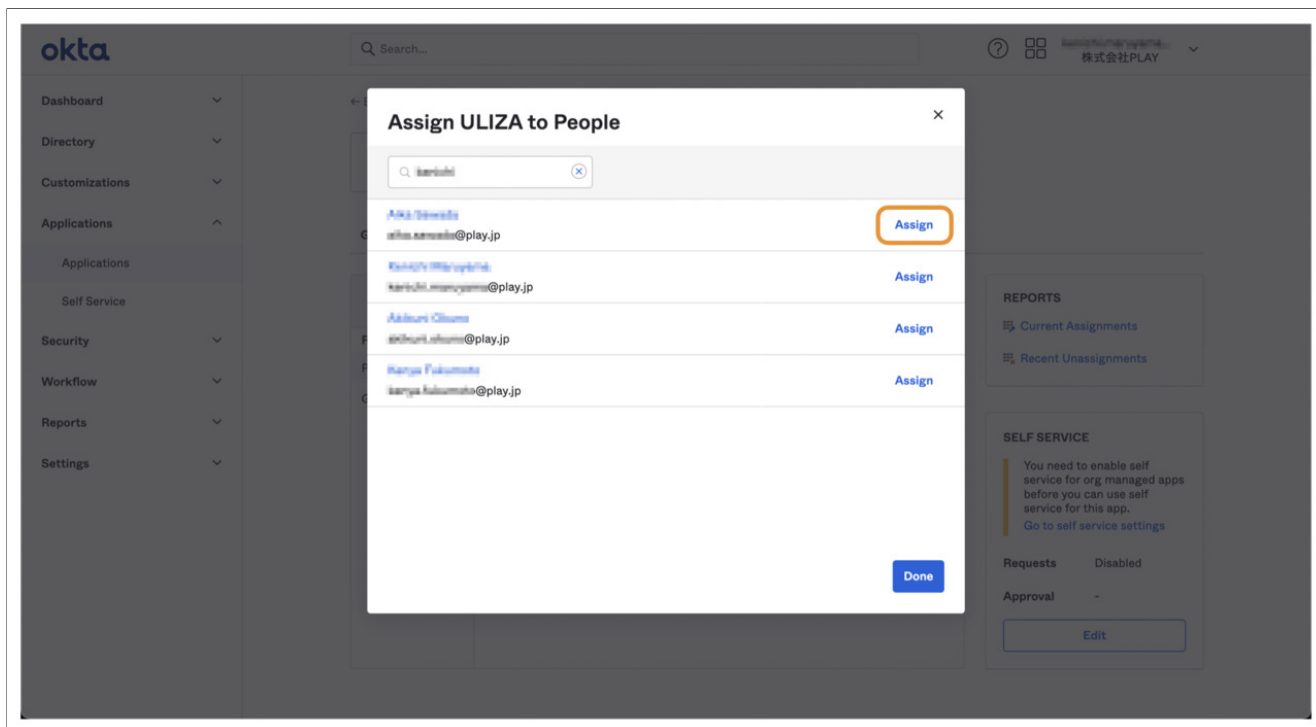
You need to enable self service for org managed apps before you can use self service for this app. [Go to self service settings](#)

Requests Disabled

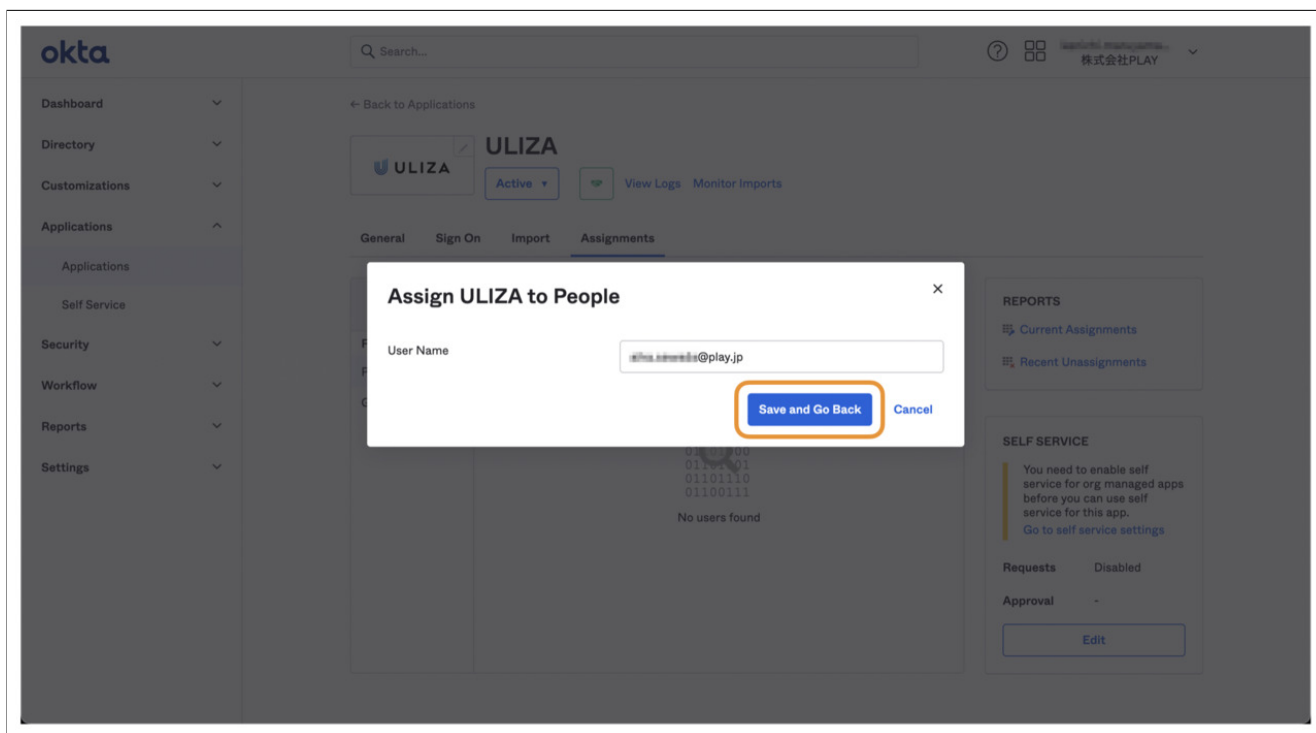
Approval -

[Edit](#)

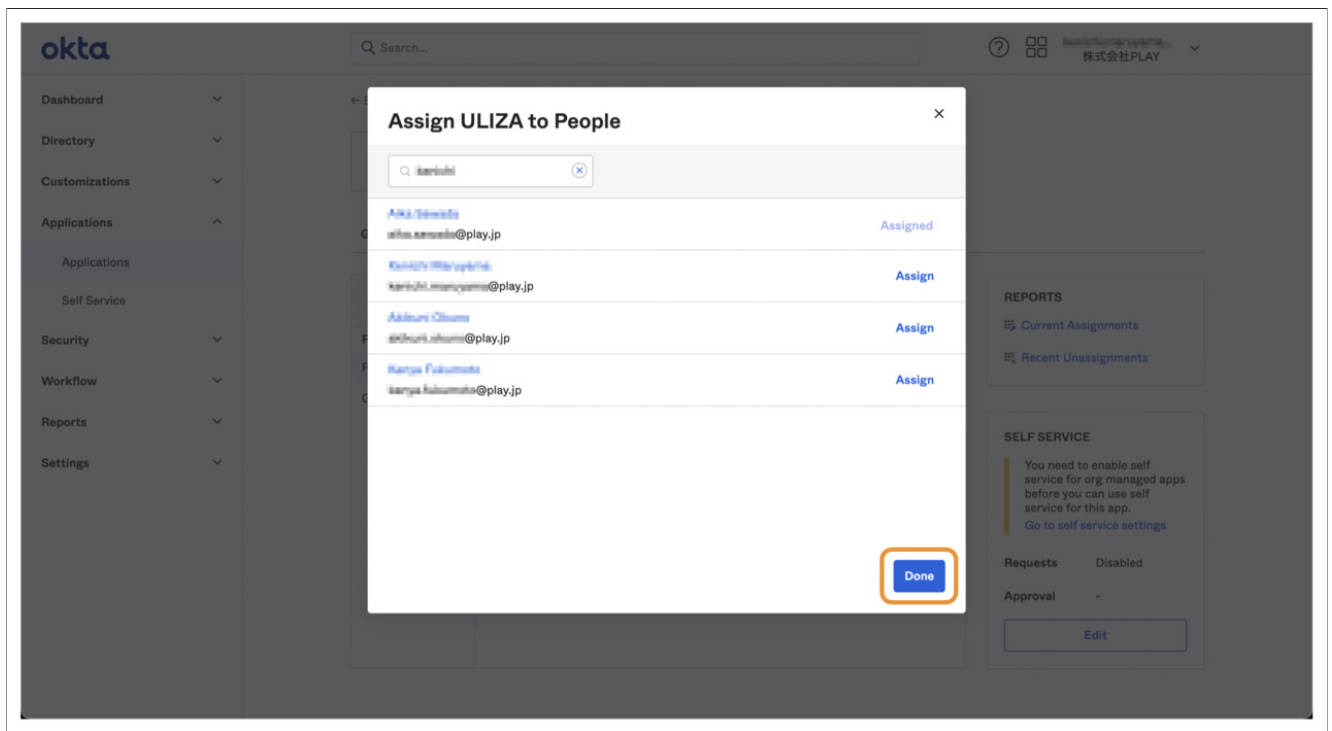
3. ULIZAへのアクセス権限を割り当てるユーザーの右にある「Assign」をクリックします。



4. 「Save and Go Back」ボタンをクリックします。



5. 引き続きユーザーの割り当てを行います。終わったら「Done」ボタンをクリックします。



6. 割り当てられたユーザーのダッシュボードにULIZAへのリンクが表示されることを確認します。



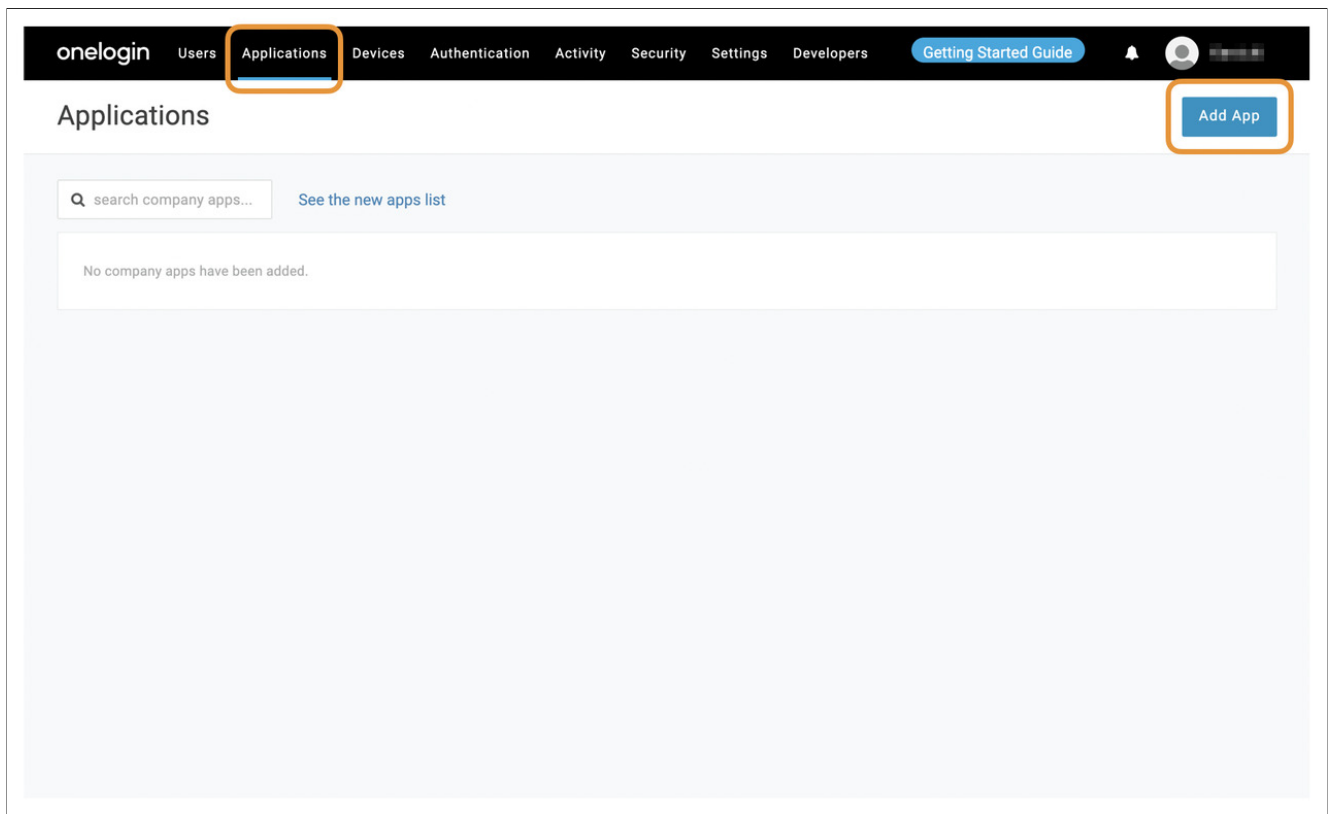
注意

この時点ではULIZA側での設定が完了していないため、ULIZAへのリンクをクリックするとエラーが発生します。

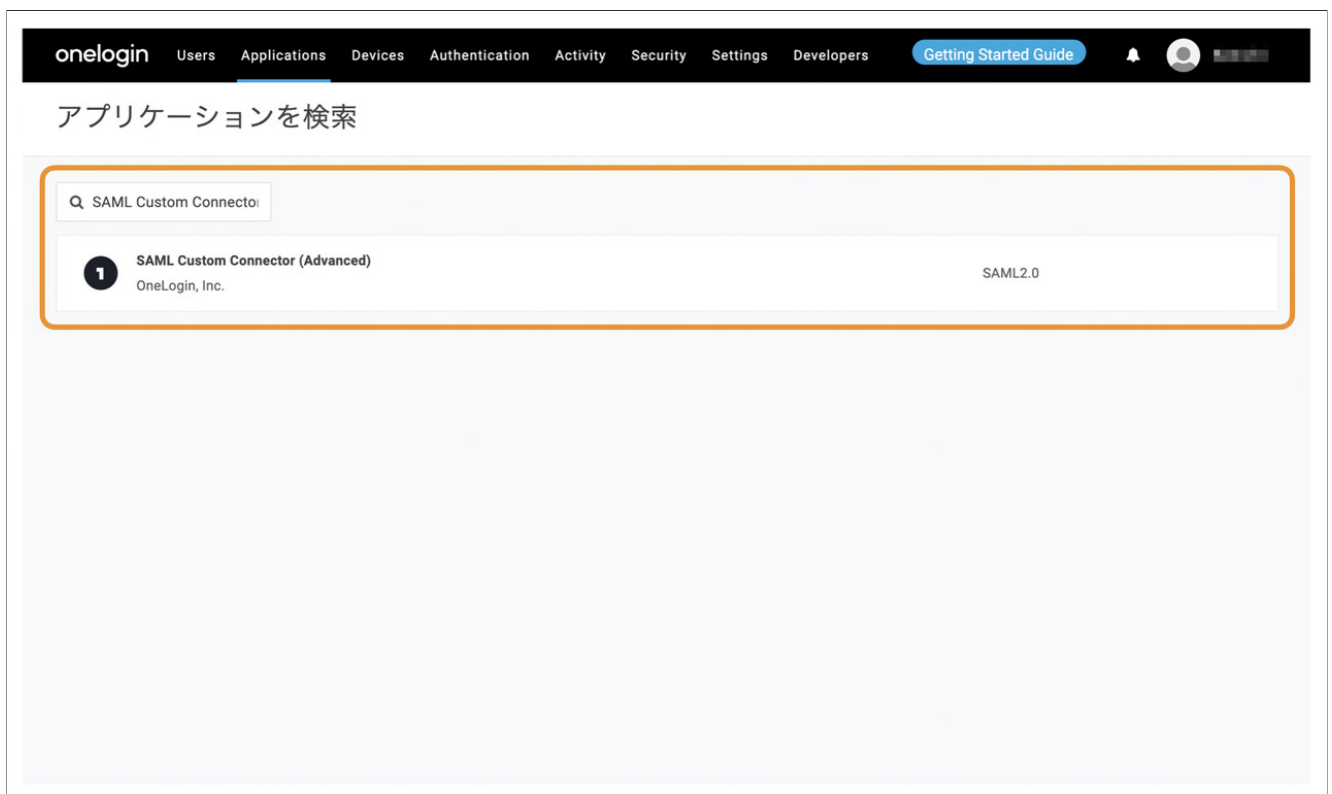
引き続きULIZA側での設定を行います。

OneLoginの場合

1. OneLogin管理コンソールを開きます。
2. 画面上部のメニューから「Applications」をクリックしてアプリケーション一覧画面を開きます。
3. 「Add App」 ボタンをクリックします。



4. 検索ボックスに「SAML Custom Connector (Advanced)」と入力し、表示された「SAML Custom Connector (Advanced)」をクリックします。



5. 「Display Name」に任意の表示名（例：「ULIZA」）を入力します。必要に応じてロゴ画像などを設定し「Save」ボタンをクリックします。

onelogin
Users
Applications
Devices
Authentication
Activity
Security
Settings
Developers
Getting Started Guide

App Listing /
Add SAML Custom Connector (Advanced)
キャンセル
Save

Configuration

Portal

Display Name
ULIZA

Visible in portal
☒

Rectangular Icon

Square Icon

Upload an icon with an aspect-ratio of 2.64:1 as either a transparent .PNG or .SVG

Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

Description
200 characters

6. 左側のメニューから「Configuration」をクリックします。

7. 各項目について、以下のように設定します。特に指定のない項目については、変更する必要はありません。

項目	設定値
RelayState	何も入力しない
Audience (EntityID)	こちらでメモしておいた「SP Entity ID」の値を入力
ACS (Consumer) URL Validator	こちらでメモしておいた「SSO URL (ACS URL)」の先頭に <code>^</code> を、末尾に <code>\$</code> を連結し、 <code>.</code> を <code>\.</code> に、 <code>/</code> を <code>\/</code> に置換した文字列を入力
ACS (Consumer) URL	こちらでメモしておいた「SSO URL (ACS URL)」の値を入力

onelogin Users Applications Devices Authentication Activity Security Settings Developers Getting Started Guide

Applications / SAML Custom Connector (Advanced) More Actions Save

Info Configuration Parameters Rules SSO Access Users Privileges Setup

Application details

RelayState

Audience (EntityID)
https://account-api.p.uliza.jp/v1/saml/accounts/xxxx/admin

Recipient

ACS (Consumer) URL Validator*
*https://account-api.p.uliza.jp/v1/saml/accounts/xxxx/admin/acs\$
*Required.

ACS (Consumer) URL*
https://account-api.p.uliza.jp/v1/saml/accounts/xxxx/admin/acs
*Required

Single Logout URL

8. 「Save」 ボタンをクリックします。

9. 画面右上にある「More actions」メニューから「SAML metadata」をクリックし、メタデータXMLをダウンロードしておきます。

onelogin Users Applications Devices Authentication Activity Security Settings Developers Getting Started Guide

Applications / SAML Custom Connector (Advanced) More Actions Save

Info Configuration Parameters Rules SSO Access Users Privileges Setup

Portal

Display Name
ULIZA

Tab
PLAY, inc.

Visible in portal
✓

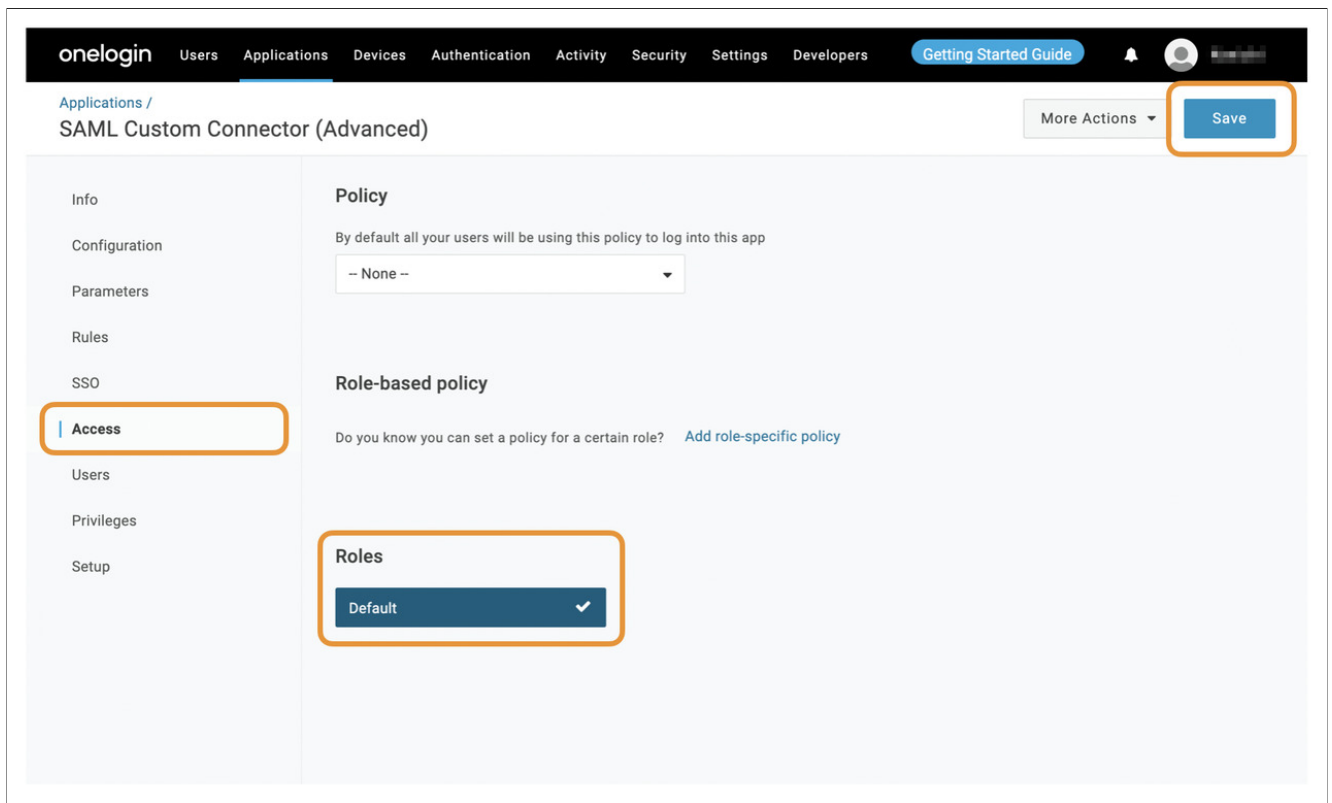
Rectangular Icon
Upload an icon with an aspect-ratio of 2.64:1 as either a transparent .PNG or .SVG

Square Icon
Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

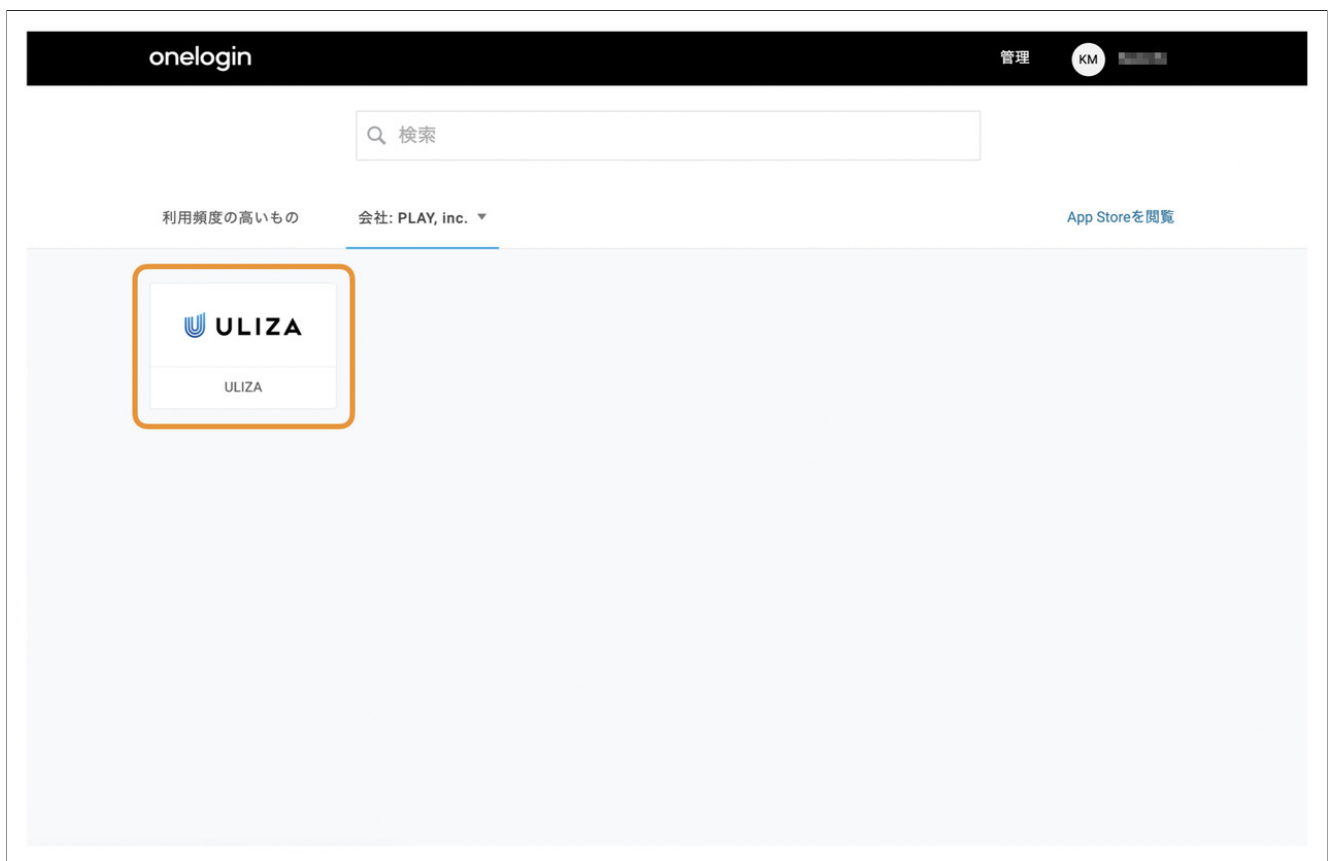
More Actions
Vendor Homepage
Reapply entitlement mappings
SAML Metadata
Delete

10. 左側のメニューから「Access」をクリックします。

11. ULIZAへのアクセス権限を割り当てるロールを選択して「Save」 ボタンをクリックします。



12. 割り当てられたロールを持つユーザーのポータルにULIZAへのリンクが表示されることを確認します。



注意

この時点ではULIZA側での設定が完了していないため、ULIZAへのリンクをクリックするとエラーが発生します。

引き続きULIZA側での設定を行います。

お問い合わせ

サービス利用制限の緩和や選択可能な権限の変更が必要な場合、または解決できないエラーが発生した場合は、弊社までお問い合わせください。

改版履歴

版	改版日	改版内容
1.2.0	2022/8/30	SAML認証に関する記述を追加しました。
1.1.0	2021/2/22	チーム機能、2段階認証、およびIPアドレス制限に関する記述を追加しました。
1.0.1	2020/6/15	アカウント設定画面の改修に伴い一部の文言を修正しました。
1.0.0	2018/8/20	初版