Safie Manager
SSO・ディレクトリ連携設定マニュアル

Microsoft Entra ID編

セーフィー株式会社

safie

はじめに

- 本書はSafie ManagerでMicrosoft Entra IDとのシングルサインオン（SSO）およびディレクトリ連携の設定に関するマニュアルです。
- 本設定には**Safie Managerは全体管理者**、**Microsoft Entra IDは管理者相当の権限**を持つアカウントが必要です。
- 多くの手順でMicrosoft Azure ADとSafie Managerを行き来しながら設定します。両方の画面を開いた状態で作業してください。
- 設定に際しては**必ず本書の手順通りに行ってください**。異なる手順で行った場合、連携に失敗する場合があります。

目次

- シングルサインオン
  - 設定の流れ
  - Safie Managerの初期設定
  - Microsoft Entra IDの設定
  - Safie Managerの設定
  - 動作確認

目次

- ディレクトリ連携
  - 設定の流れ
  - Safie Managerの初期設定
  - Microsoft Entra IDの設定
  - 動作確認

目次

シングルサインオン

設定の流れ

シングルサインオンの設定は以下の手順で行います。

1. Safie Managerの初期設定
   1.1. Safie Managerに「全体管理者」のアカウントでログイン
   1.2. 管理設定 > SSO設定タブから「企業別認証ID」を発行
2. Microsoft Entra IDの設定
   2.1. Microsoft Azureに管理者アカウントでログインし、Microsoft Entra ID設定画面へ
   2.2. エンタープライズアプリケーションの作成
   2.3. シングルサインオンの設定
   2.4. ユーザーの割り当て
3. Safie Managerの設定
   3.1. Microsoft Entra ID側情報の入力
   3.2. SAML署名証明書のアップロード
   3.3. SSO有効化
4. SSOの動作テスト

Safie Managerの初期設定

Safie Managerにログイン

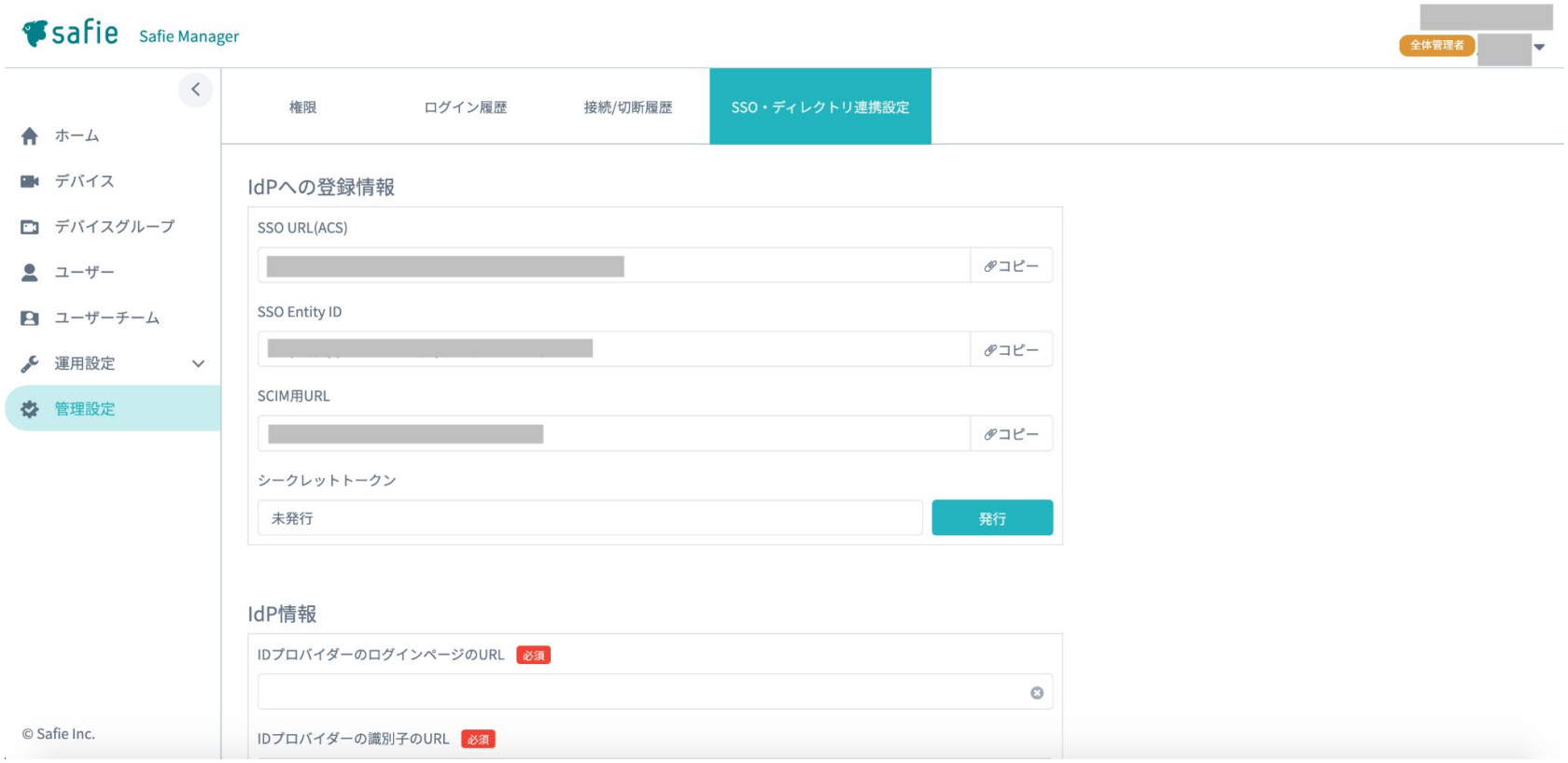
- 以下のURLにアクセスし、Safie Managerにログインしてください
  https://safie.link/manager/#/login
- ログイン後、画面右上の赤枠部が「全体管理者」であることを確認してください
  ※「管理者」となっている場合、以降の手順が行えません

企業別認証IDの発行

- サイドメニューの管理設定の画面からSSO・ディレクトリ連携設定タブをクリック
- 「企業別認証IDの発行」をクリック
- 確認のダイアログが表示されるので「続行」をクリック

初期設定の完了

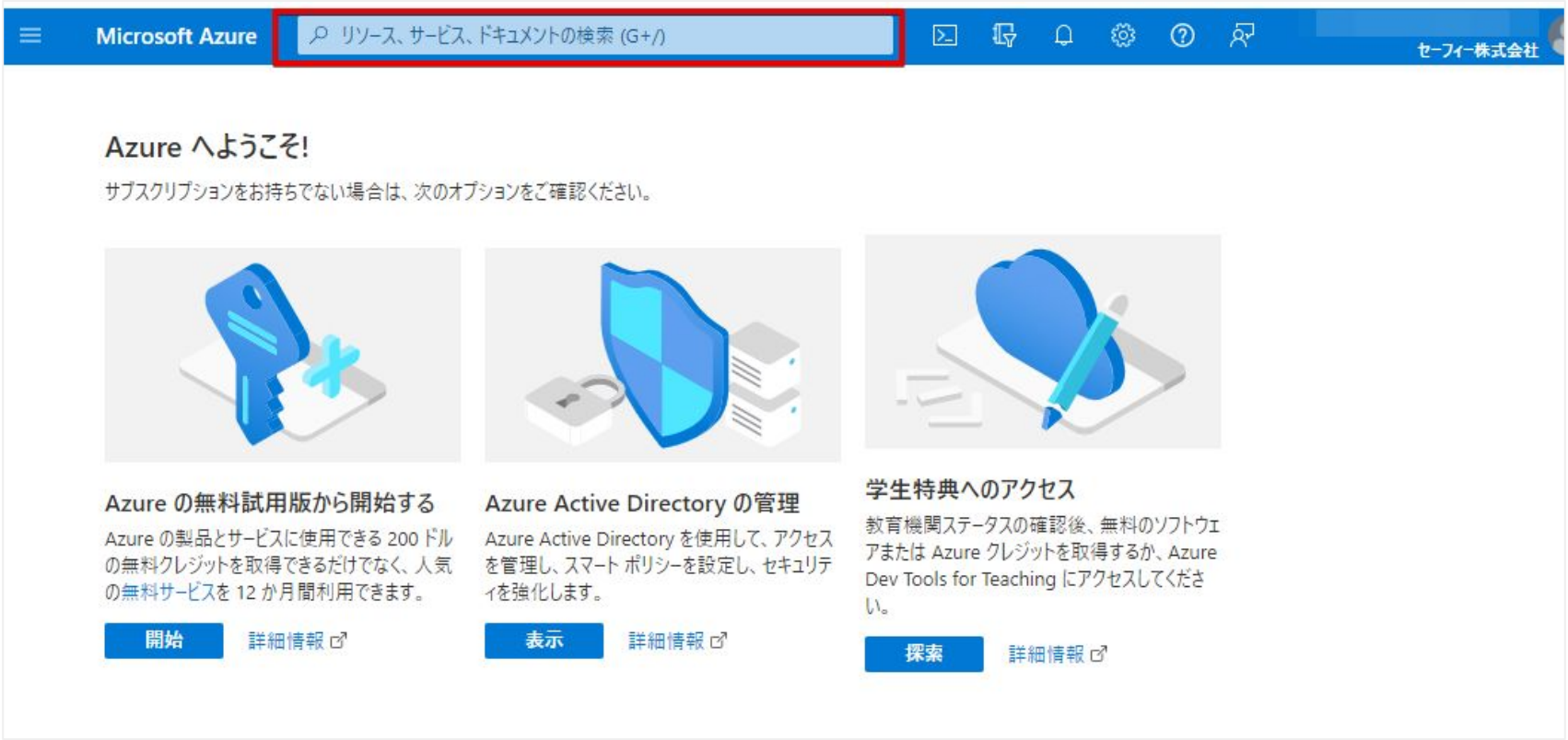
- 以下の画面が表示されたらSafie Managerのシングルサインオン初期設定は完了です。
- 本画面は以降の手順でも参照するので<u>画面を閉じずに</u>次の手順に進んでください。



Microsoft Entra IDの設定

Microsoft Azureにログイン

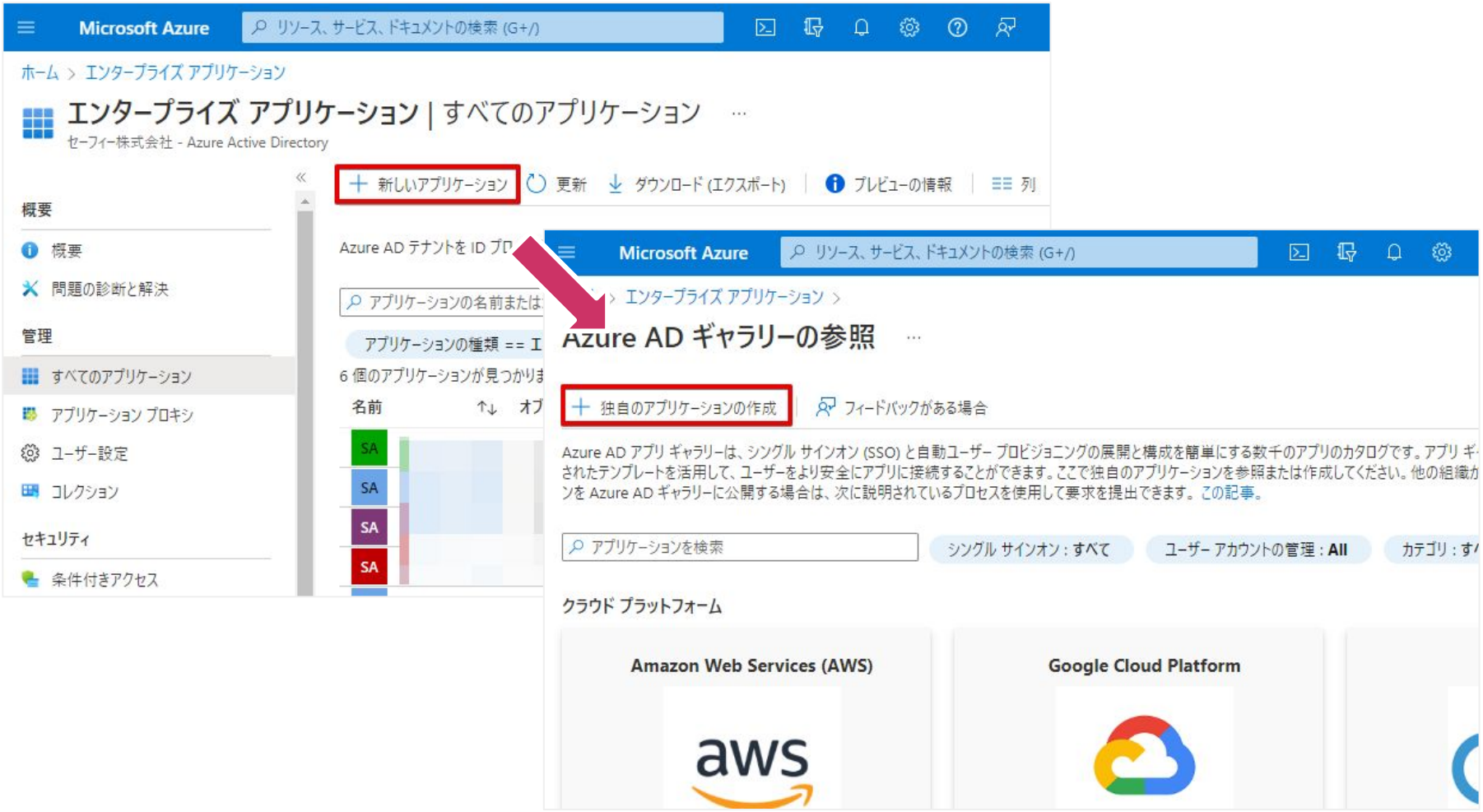
- 以下のURLにアクセスし、Azureにログインしてください
  https://portal.azure.com/#home
- 上部の検索フォームに「エンタープライズ」と入力し、「エンタープライズアプリケーション」のメニューに遷移してください



エンタープライズアプリケーションの作成（1/3）

safie

- 画面上部の「新しいアプリケーション」をクリック
- 遷移先の画面で「独自のアプリケーションの作成」をクリック



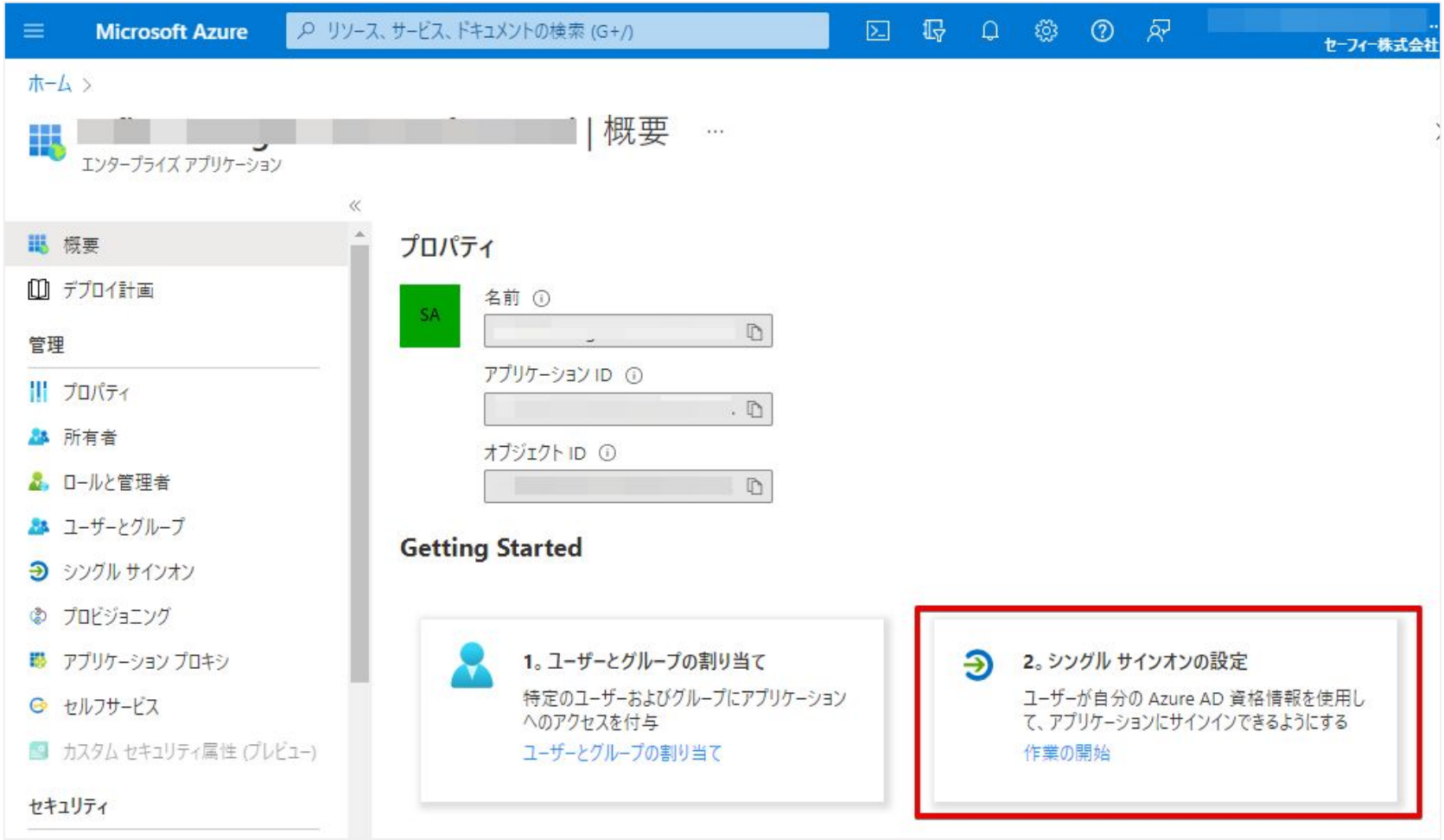
エンタープライズアプリケーションの作成（2/3）

- 画面右に作成画面が表示されるので、以下の情報を入力
  - アプリケーション名：任意の文字列を入力
  - 操作の種類：一番下を選択
- 入力が終わったら「作成」をクリック

エンタープライズアプリケーションの作成（3/3）

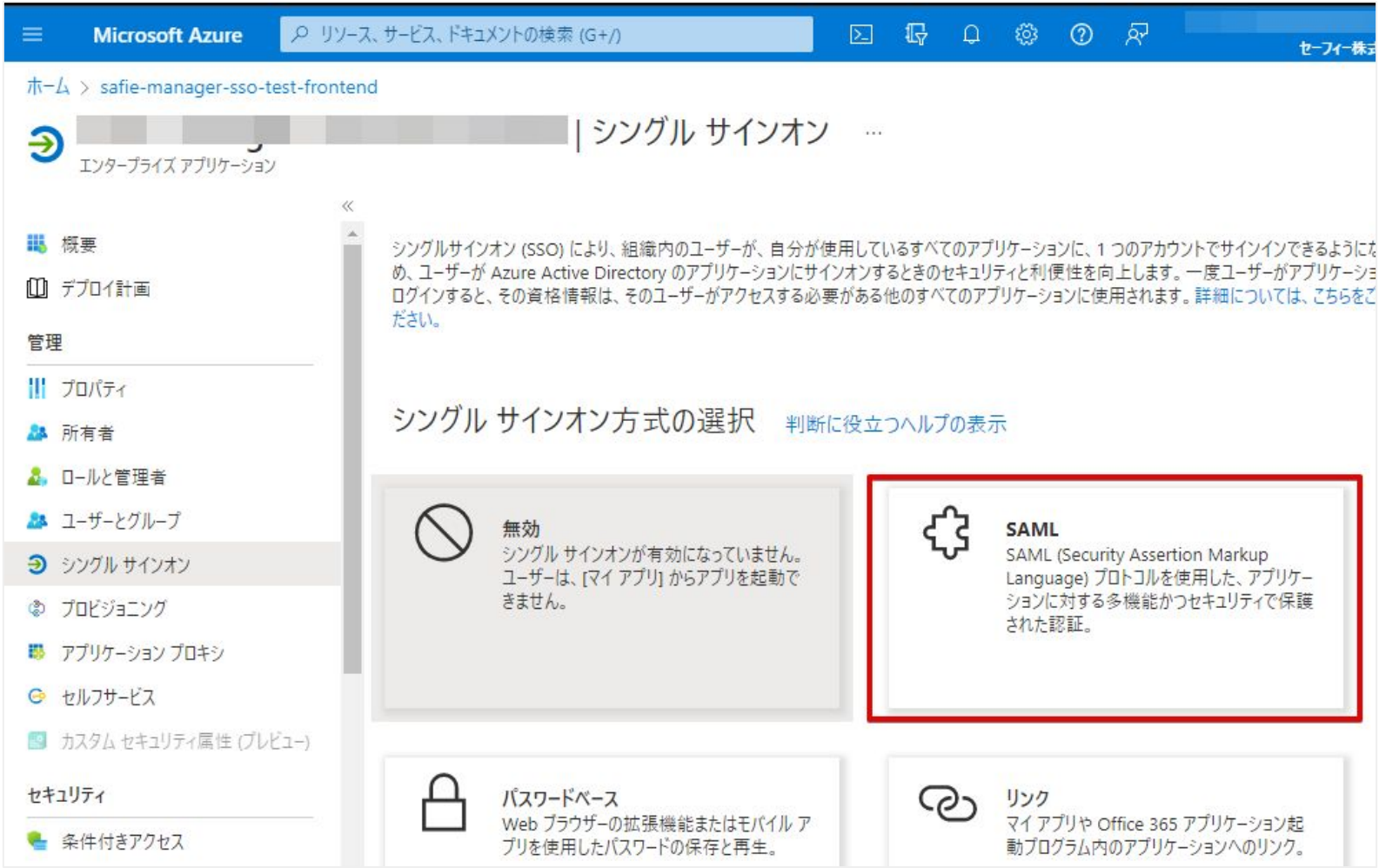
safie

- 作成が無事に完了すると以下の画面に遷移します
- 下部のメニューから「2.シングルサインオンの設定」をクリック



シングルサインオンの設定（1/6）

- シングルサインオン方式の設定画面が表示されます
- 下部の選択欄の中から「SAML」をクリック



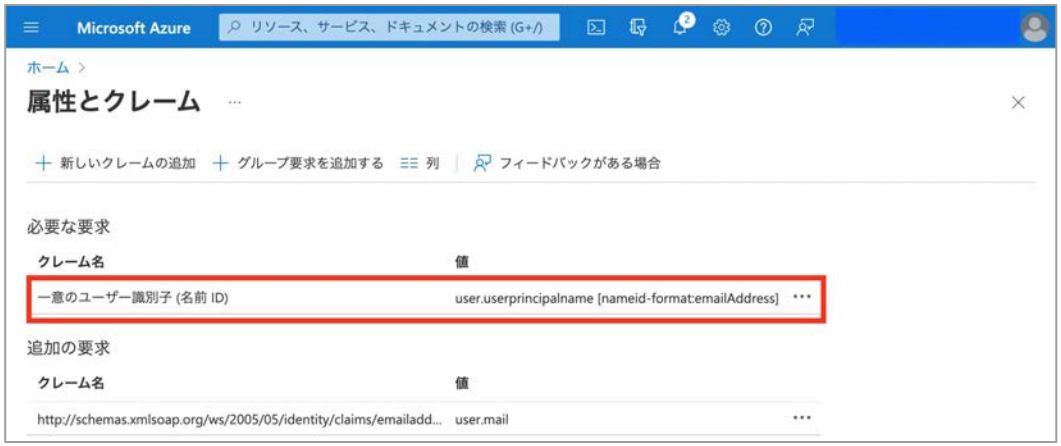
- 基本的なSAML構成の右上にある編集ボタンをクリックして編集画面を表示します

シングルサインオンの設定（3/6）

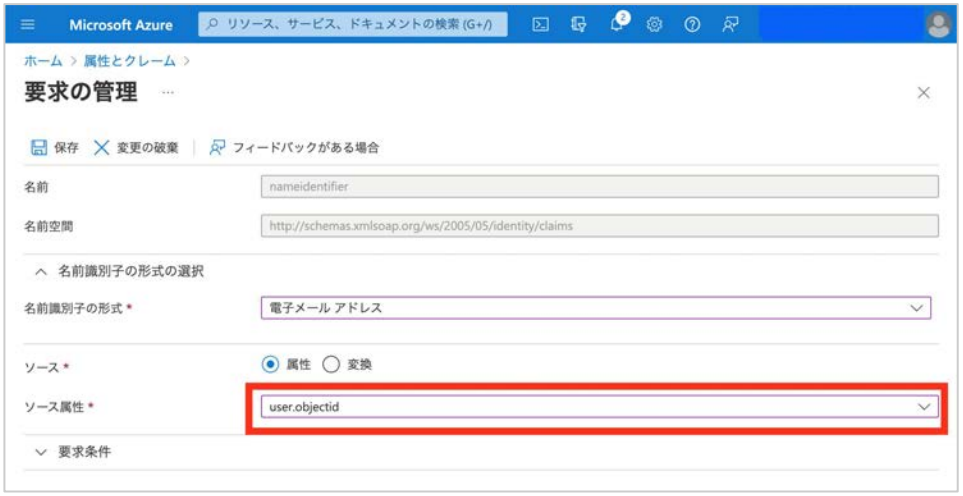
- 識別子（エンティティID）と応答URL（Assertion Consumer Service URL）にSafie Manager側の情報を転記します
- 入力が完了したら画面上部の「保存」ボタンをクリックしてください

- シングルサインオン設定から「属性とクレーム」の画面の編集ボタンをクリックしてください

- 画面中央の「一意のユーザー識別子（名前 ID）」をクリック



- 「ソース属性」を[user.objectid]に変更し、画面上部の「保存」ボタンをクリックしてください



- 右上の「新しいクレームの追加」をクリック

- 下表の２項目を新たに追加します

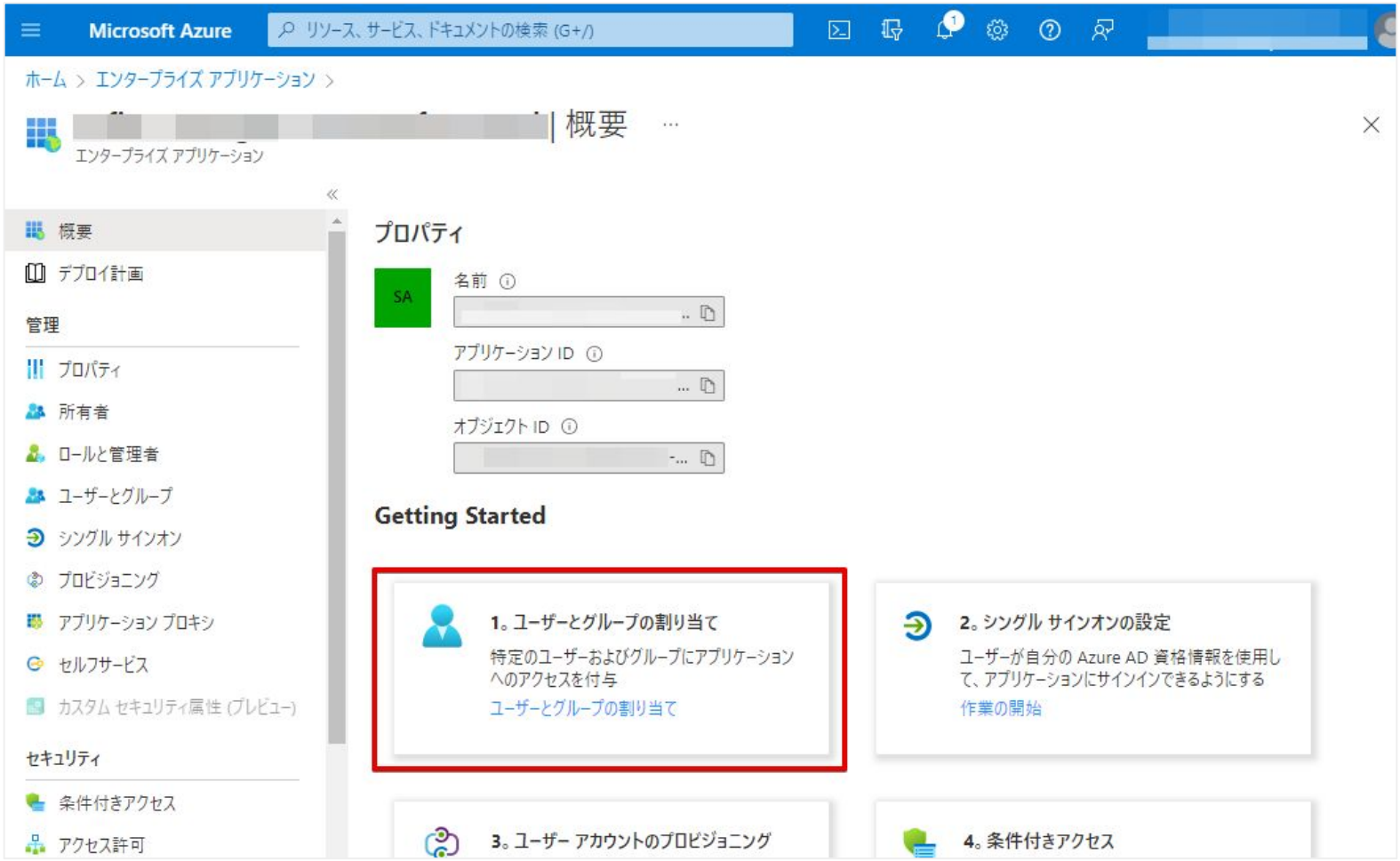
名前	名前空間	ソース	ソース属性
mail_address	なし	属性	user.mail
user_name	なし	属性	user.displayname

※要求条件は設定不要です。

ユーザーの割り当て（1/2）

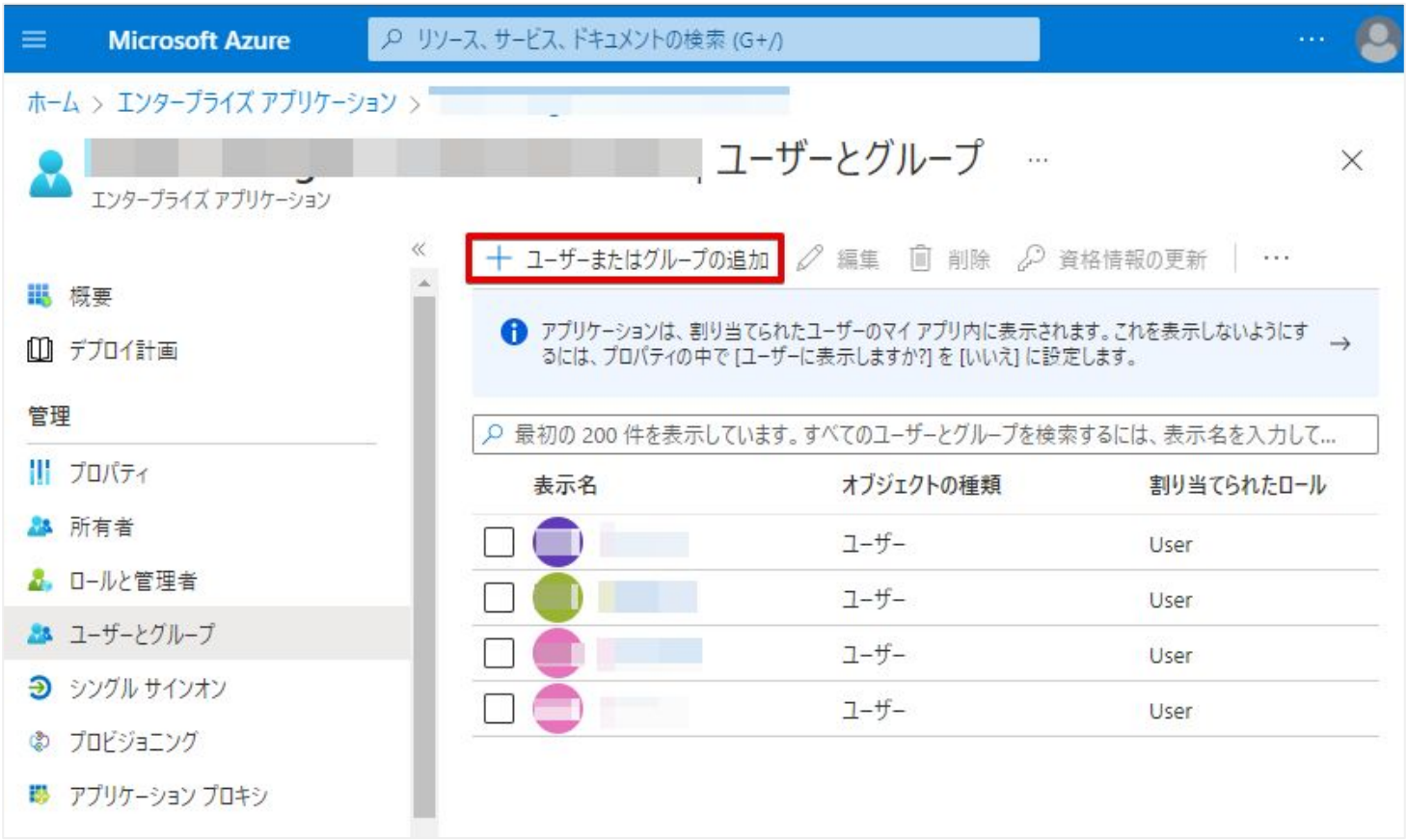
safie

- アプリケーションのトップに戻って「ユーザーとグループの割り当て」を選択します



ユーザーの割り当て（1/2）

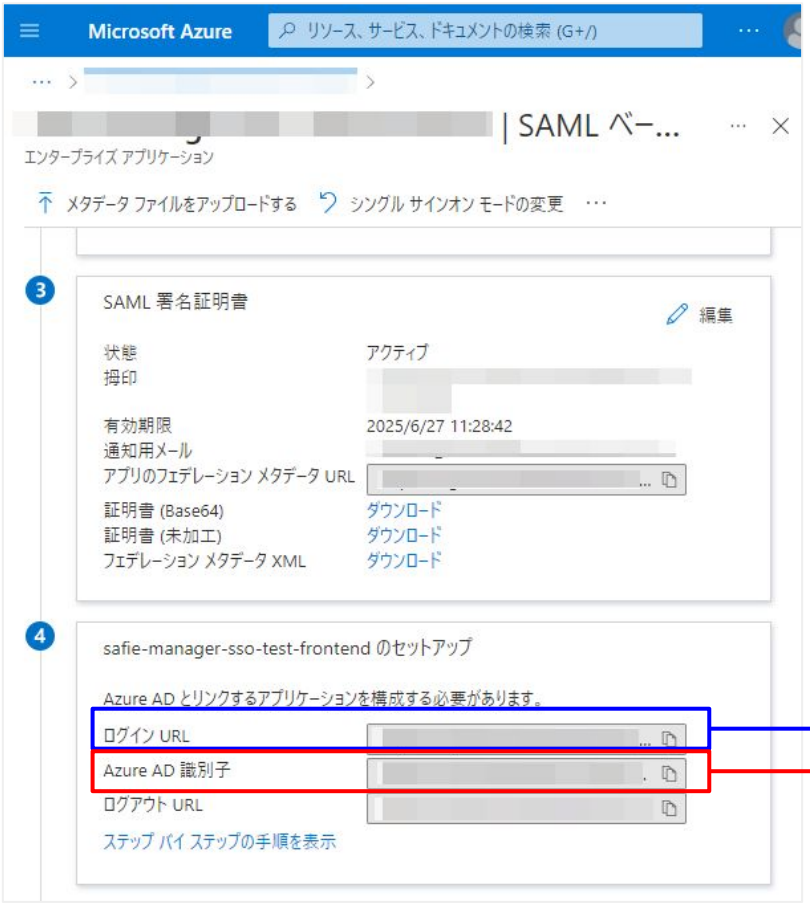
- 「ユーザーまたはグループの追加」をクリックし、ユーザーを追加します
- ここで追加したアカウントがSSOでセーフィーのサービスを利用できるようになります



Safie Managerの設定

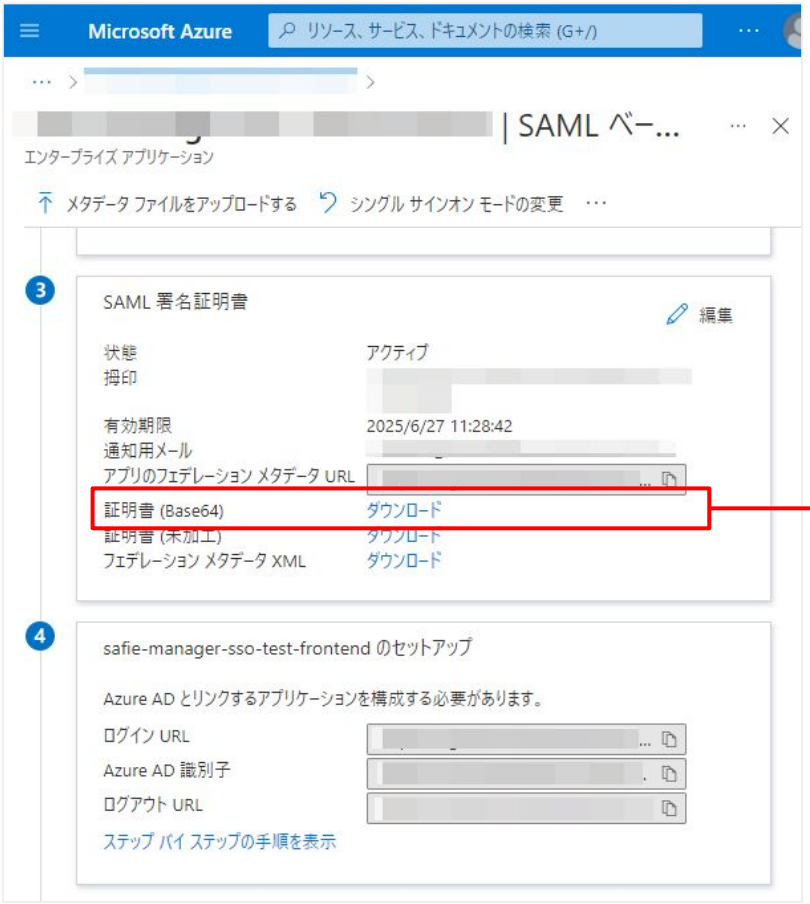
Azure AD側の情報の入力

- Safie ManagerのSSO設定画面で以下の通りAzure AD側のログインURL、識別子情報を入力します



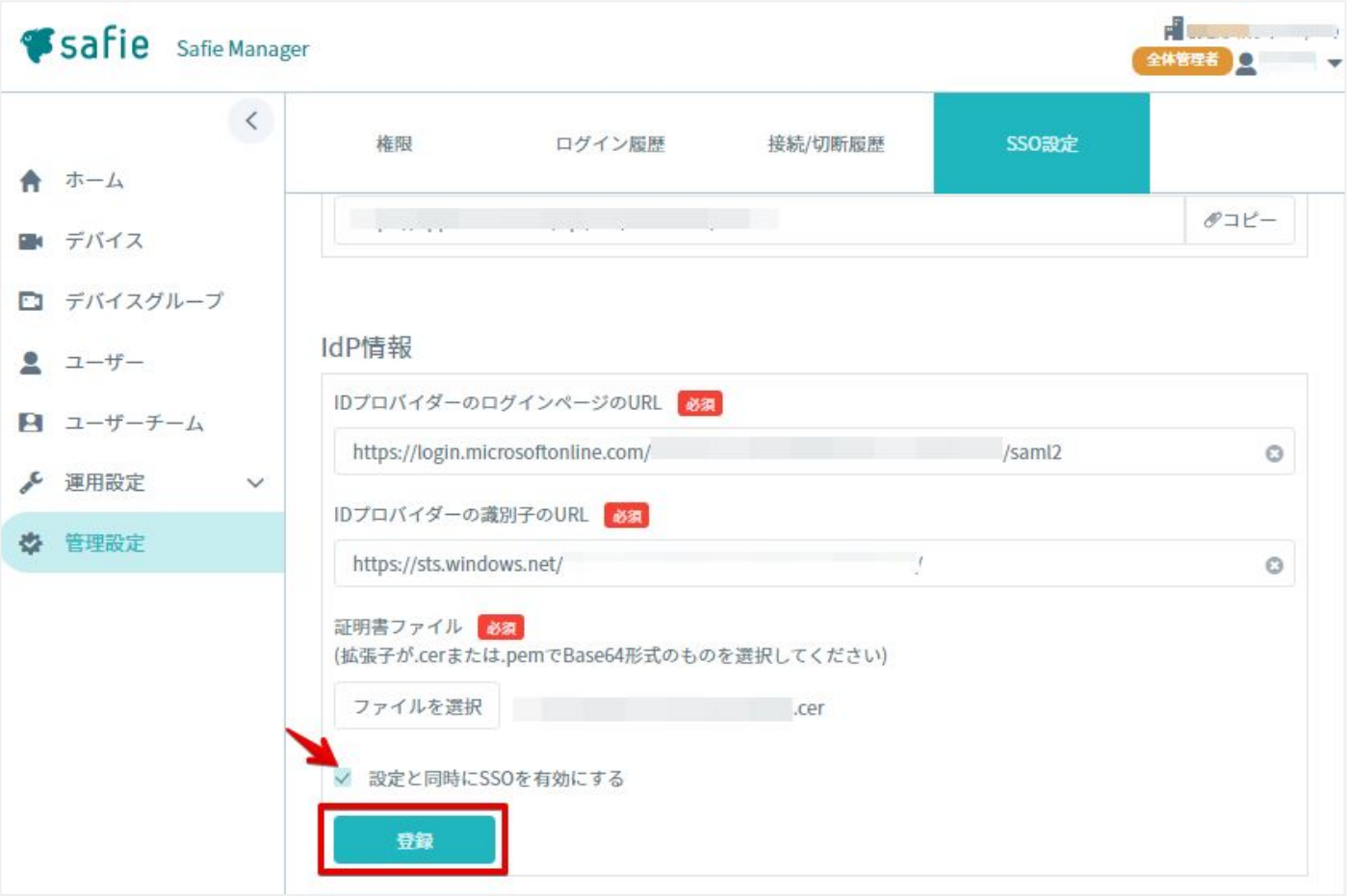
SAML署名証明書のアップロード

- Azure ADからSAML署名証明書のファイルをダウンロードして、Safie ManagerのSSO設定画面で同ファイルをアップロードします



設定の完了

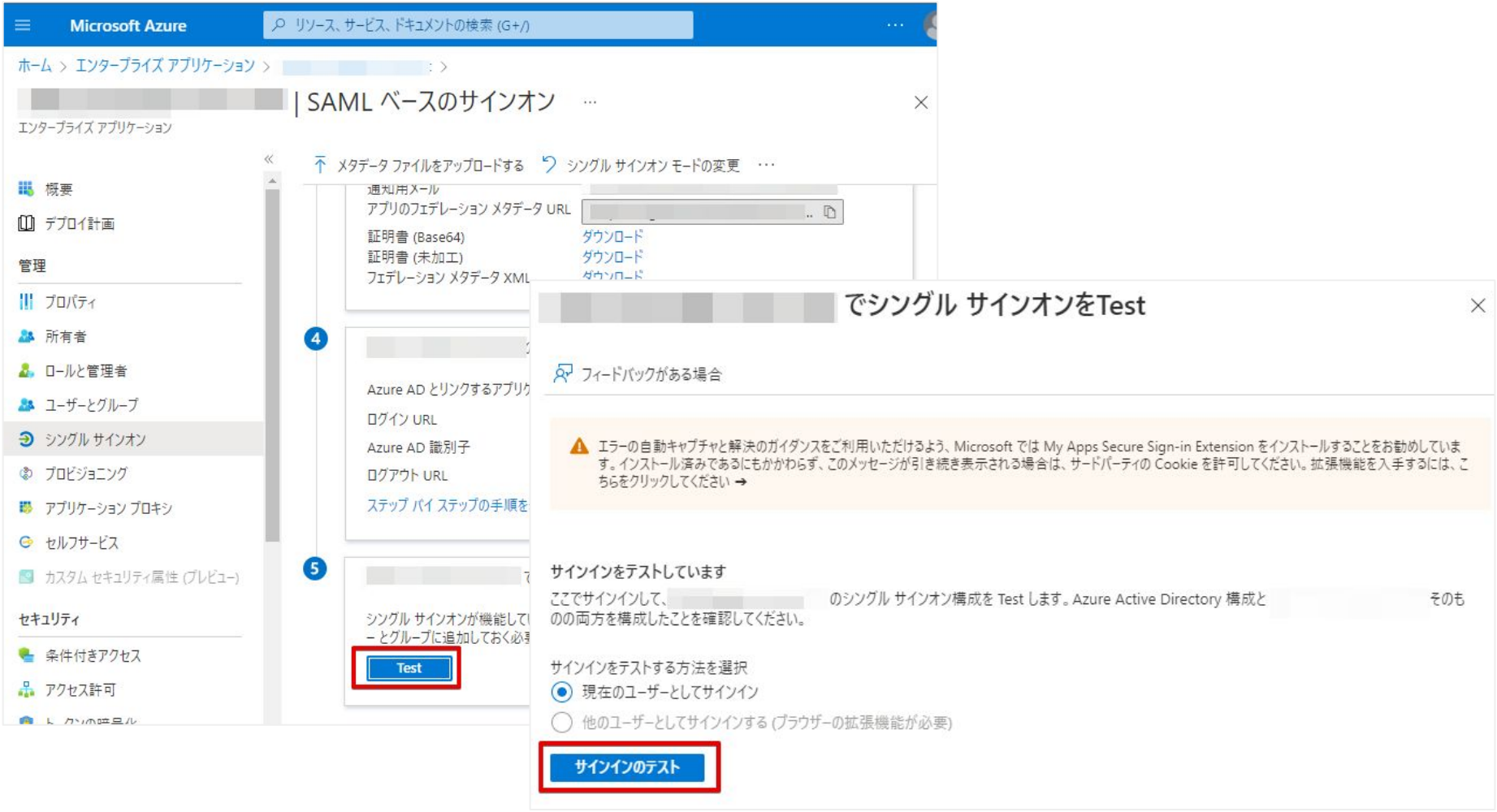
- Azure AD側の情報や証明書ファイルが正しいことを確認したら、「設定と同時にSSOを有効にする」にチェックを入れて「登録」をクリックしてください



SSOの動作テスト

SSOの動作テスト（1/2）

- 画面下部のテストのエリアにある「Test」のボタンをクリック遷移後の画面にある「サインインのテスト」をクリックしてください。



SSOの動作テスト（2/2）

- しばらくたって、Safie Viewerの利用規約画面（またはログイン後のトップページ）に遷移したら設定は正常に完了しています。
- エラーが表示された場合は入力したURL情報や証明書情報に誤りがないか確認して再度お試しください。

目次

ディレクトリ連携

前提

シングルサインオンの機能のみをご利用されたい場合、ディレクトリ連携設定については必須ではありません。
P30までの設定を行なっていただければご利用いただけるため、これ以降の設定は不要となります。

逆に、ディレクトリ連携の設定を行うにはシングルサインオンの設定は必須となるため、P5-P30までの設定は完了いただくようお願いいたします。

設定の流れ

ディレクトリ連携の設定は以下の手順で行います。

1. Safie Managerの初期設定
   1.1. Safie Managerに「全体管理者」のアカウントでログイン
   1.2. 管理設定 > SSO設定タブから「企業別認証ID」を発行
   1.3. シークレットトークンの発行
2. Microsoft Entra IDの設定
   2.1. Microsoft Azureに管理者アカウントでログイン&エンタープライズアプリケーションの作成
   2.2. ディレクトリ連携の設定
   2.3. ユーザーの割り当て
3. 動作確認
4. プロビジョニングの停止

Safie Managerの初期設定

Safie Managerにログイン

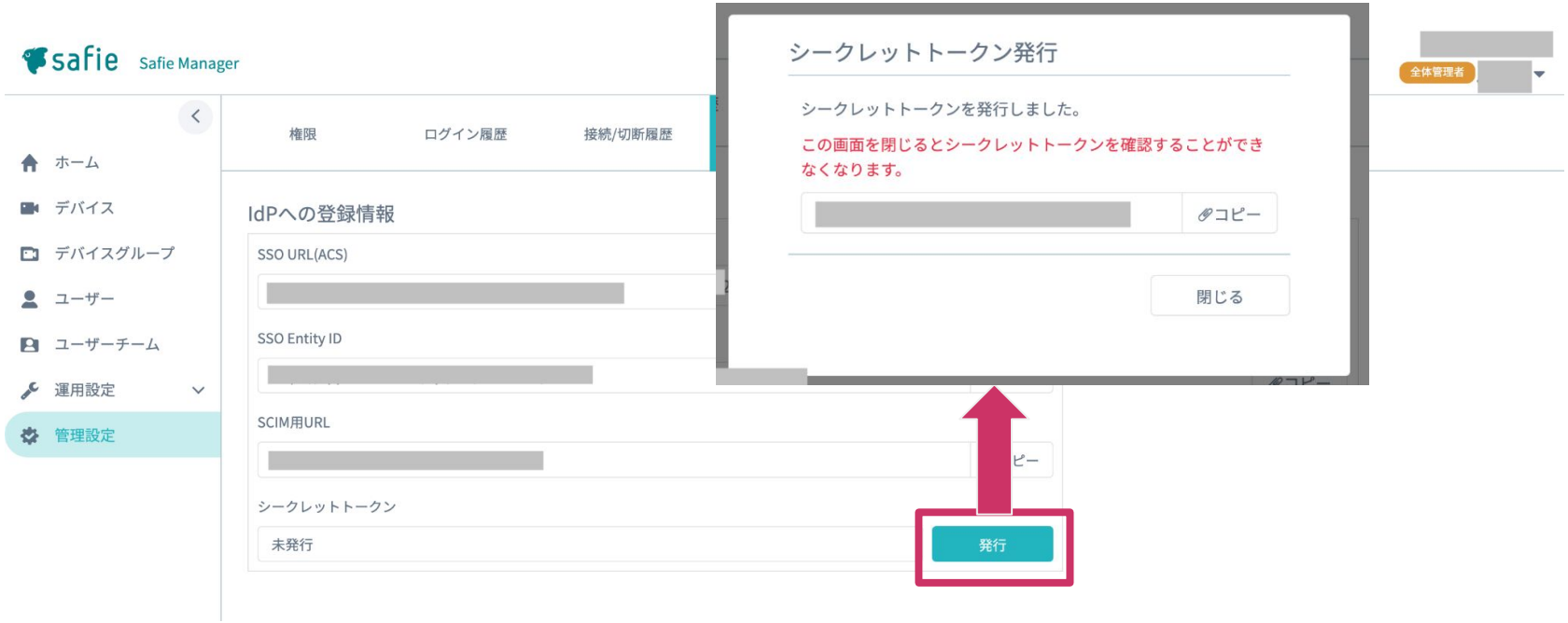
- 以下のURLにアクセスし、Saafie Managerにログインしてください
  https://safie.link/manager/#/login
- ログイン後、画面右上の赤枠部が「全体管理者」であることを確認してください
  ※「管理者」となっている場合、以降の手順が行えません

企業別認証IDの発行

- サイドメニューの管理設定の画面からSSO・ディレクトリ連携設定タブをクリック
- 「企業別認証IDの発行」をクリック
- 確認のダイアログが表示されるので「続行」をクリック

シークレットトークンの発行

- 以下の画面が表示されたら、「IdPへの登録情報」内の「シークレットトークン」蘭の横にある「発行」ボタンをクリック
- 表示されたシークレットトークンを手元に控える **※シークレットトークンはここでしか表示されないため、必ず手元に控えてください**
- 本画面は以降の手順でも参照するので<u>画面を閉じずに</u>次の手順に進んでください。



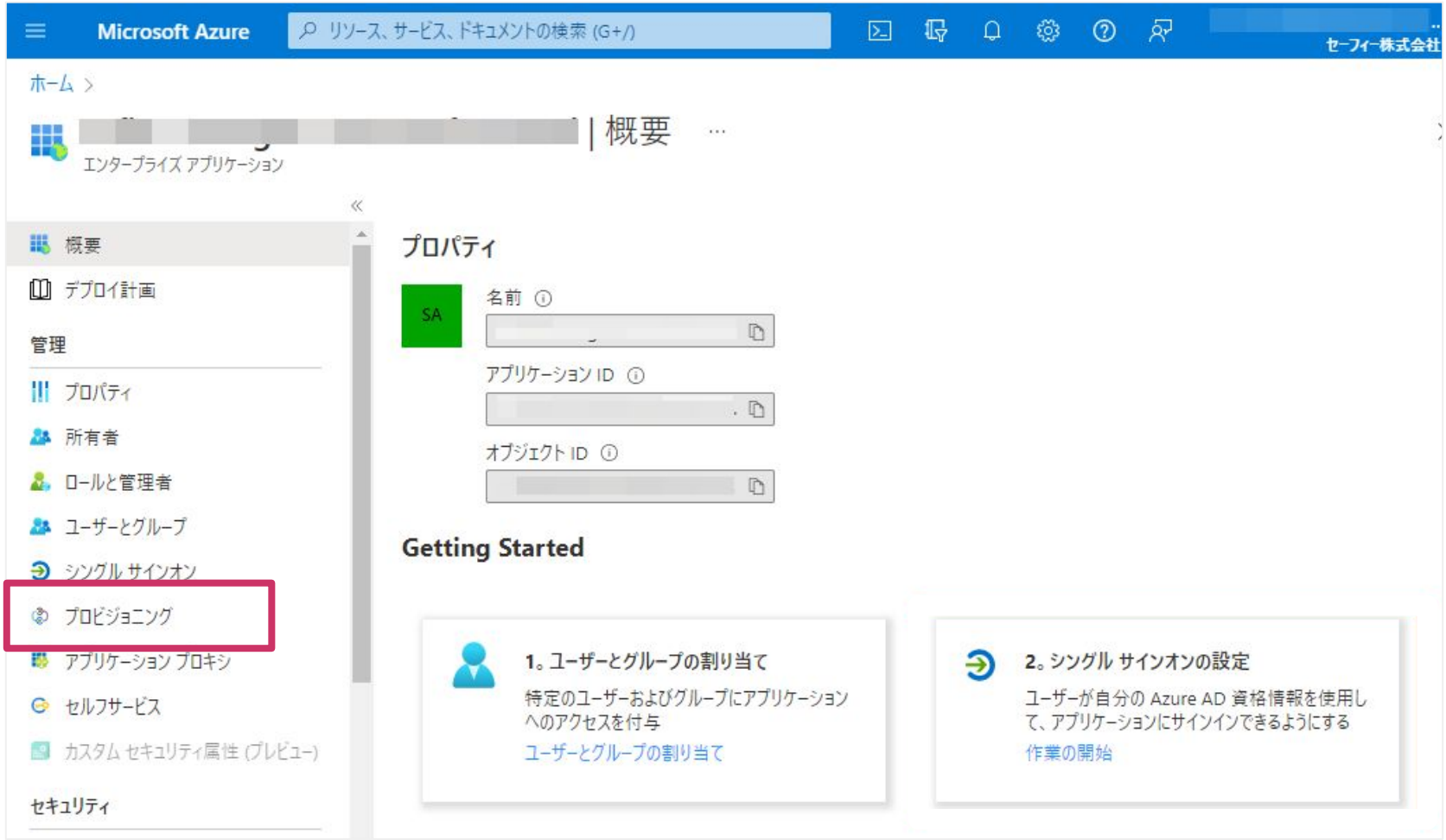
Microsoft Entra IDの設定

Azureにログイン&エンタープライズアプリケーションの作成

- 本マニュアルのP12～P14を参照し、Microsoft Azureへのログインおよびエンタープライズアプリケーションの作成を行います

プロビジョニング設定画面への遷移

- 作成が無事に完了すると以下の画面に遷移します
- サイドメニューから「プロビジョニング」をクリック

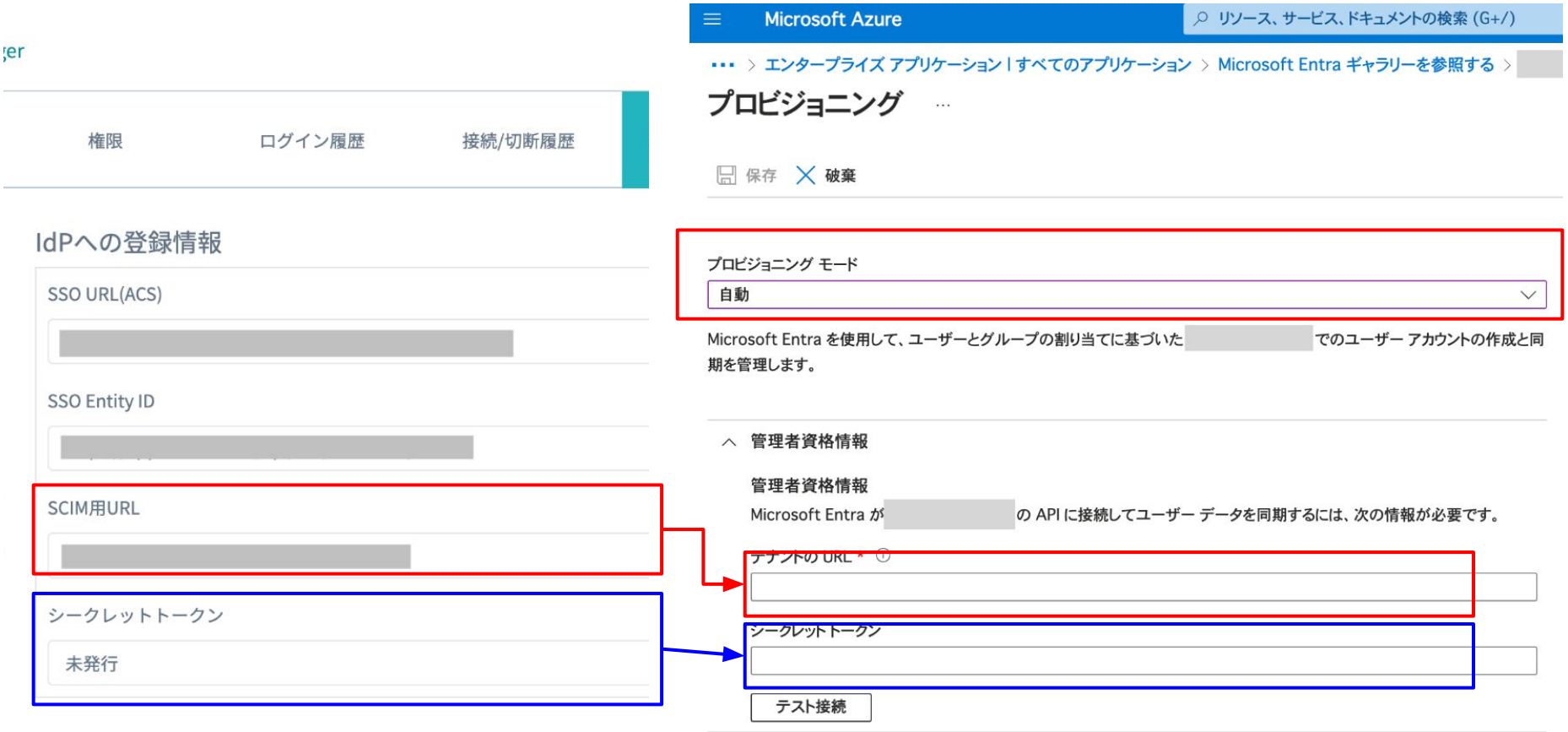


- 「作業の開始」をクリック


Microsoft Azure
リソース、サービス、ドキュメントの検索 (G+/)
ホーム > | 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 > Microsoft Entra ギャラリーを参照する > | プロビジョニング >
| 概要
フィードバックがある場合
概要
オンデマンドでプロビジョニング
管理
プロビジョニング
モニター
プロビジョニング ログ
監査ログ
分析情報
トラブルシューティング
新しいサポート リクエスト
Microsoft Entra を使用して ID ライフサイクル管理を自動化する
ユーザーが組織内で参加、脱退、移動するときに、アカウントを自動的に作成、更新、削除します。詳細情報。
作業の開始
プロビジョニングとは何ですか?
アプリケーションのデプロイを計画します。
自動プロビジョニングを構成します。

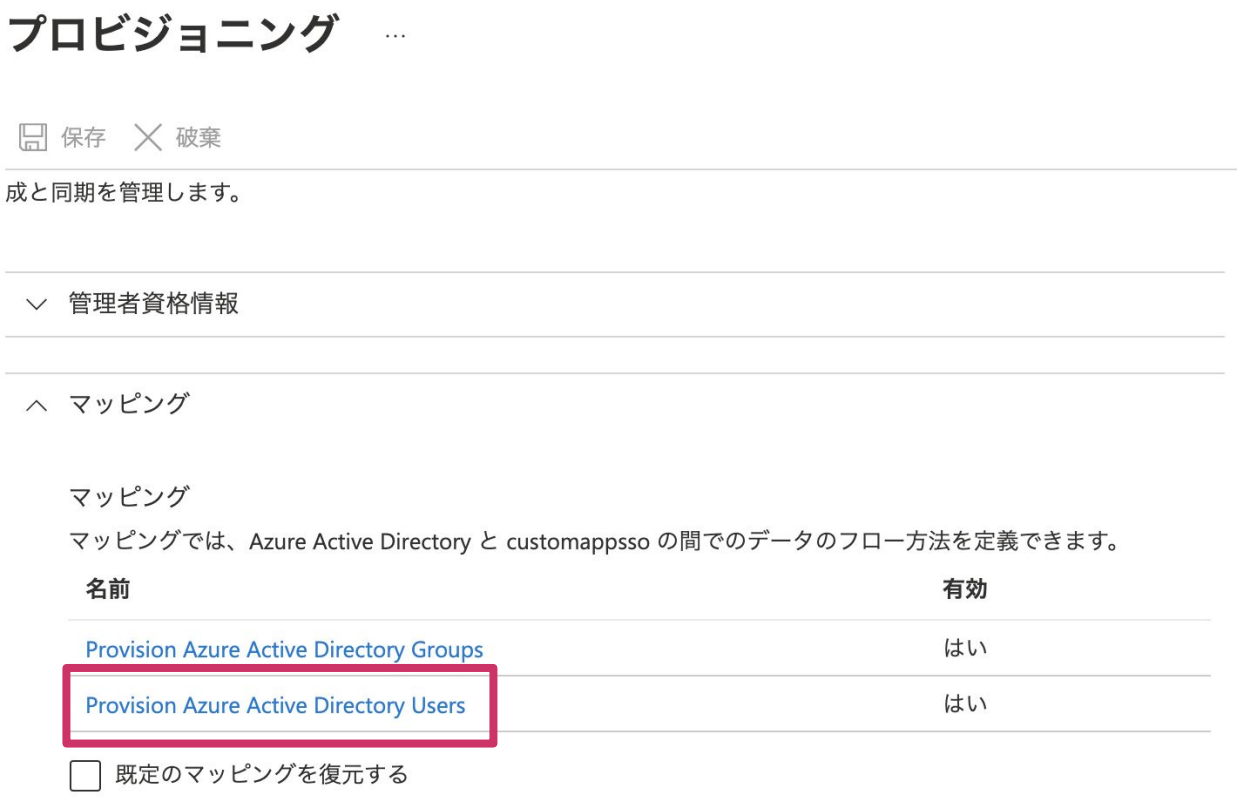
プロビジョニング設定（2/7）

- プロビジョニングモードについて「自動」を選択します。
- 「自動」を選ぶと「管理者資格情報」の中に「テナントのURL」と「シークレットトークン」の入力項目が表示されます。こちらに、Safie Manager側の情報を転記します
- 入力が完了したら画面上部の「保存」ボタンをクリックしてください



プロビジョニング設定（3/7）

- 保存を行うと、「マッピング」という設定項目が表示されるようになります。こちらよりユーザー情報・グループ情報のマッピング設定を行います
- ユーザー情報「Provision Azure Active Directory Users」をクリック



プロビジョニング設定（4/7）

safie

- 「属性マッピング」内の設定をデフォルト設定から変更します
- customappsso属性の「externalId」をMicrosoft Entra ID属性の「objectId」に紐付け、照合の優先順位を1としてください
- 「displayName」を「displayName」に紐付けてください
- 「emails[type eq "work"].value」を「mail」に紐付けてください
- (任意)
  「urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:employeeNumber」を「employeeId」に紐付けてください

属性マッピング

属性マッピングでは、Microsoft Entra ID と customappsso の間で属性をどのように同期するかを定義します

customappsso 属性	Microsoft Entra ID 属性	照合の優先順位	編集	削除
externalId	objectId	1	編集	削除
active	Switch([isSoftDeleted], , False , True , True , False)		編集	削除
displayName	displayName		編集	削除
title	jobTitle		編集	削除
emails[type eq "work"].value	mail		編集	削除
preferredLanguage	preferredLanguage		編集	削除
name.givenName	givenName		編集	削除
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:empl···	employeeId		編集	削除

属性マッピング設定のコツ（1/3）

safie

- 「属性マッピング」内の設定のデフォルト値として、MIcrosoft Entra ID属性の「userPrincipalName」の照合の優先順位が1となっています。本設定ではcustomappsso属性の「externalId」をMIcrosoft Entra ID属性の「objectId」に紐付け、照合の優先順位を1とする必要があるため、以下の手順で設定を行なってください。
- customappsso属性の「externalId」をMIcrosoft Entra ID属性の「objectId」に紐付けた段階で「この属性を使用してオブジェクトを照合する」を「はい」に設定し、照合の優先順位を「2」で設定する

属性マッピング設定のコツ（2/3）

safie

- MIcrosoft Entra ID属性の「userPrincipalName」の「この属性を使用してオブジェクトを照合する」を「いいえ」に設定する

マッピングの種類 ⓘ

直接

ソース属性 * ⓘ

userPrincipalName

null の場合の既定値 (オプション) ⓘ

対象の属性 * ⓘ

userName

この属性を使用してオブジェクトを照合する

いいえ

照合の優先順位 ⓘ

このマッピングを適用する ⓘ

常時

属性マッピング設定のコツ（3/3）

safie

- MIcrosoft Entra ID属性の「objectId」をの照合の優先順位を「1」で設定する

マッピングの種類 ⓘ

直接

ソース属性 * ⓘ

objectId

null の場合の既定値 (オプション) ⓘ

対象の属性 * ⓘ

externalId

この属性を使用してオブジェクトを照合する

はい

照合の優先順位 * ⓘ

1

このマッピングを適用する ⓘ

常時

- 「マッピング」よりグループ情報「Provision Azure Active Directory Groups」をクリック

プロビジョニング設定（6/7）

- 「属性マッピング」内の設定をデフォルト設定から変更します
- customappsso属性の「externalId」をMicrosoft Entra ID 属性の「objectId」に紐付け、照合の優先順位を1としてください
- 「displayName」を「displayName」に紐付けてください
- 「members」を「members」に紐付けてください

属性マッピング

属性マッピングでは、Microsoft Entra ID と customappsso の間で属性をどのように同期するかを定義します

customappsso 属性	Microsoft Entra ID 属性	照合の優先順位	編集	削除
externalId	objectId	1	編集	削除
displayName	displayName		編集	削除
members	members		編集	削除

プロビジョニング設定（7/7）

safie

- プロビジョニング画面に戻り、「プロビジョニングの開始」をクリックすることでプロビジョニングが開始されます

プロビジョニングの編集

safie

- 再度設定を変更したい場合は、「プロビジョニングの編集」をクリックし設定の変更を行なってください

ユーザーの割り当て

- P22、P23を参照し、エンタープライズアプリケーションへのユーザーの割り当てを行います

動作確認

プロビジョニングログの確認

- プロビジョニング画面からプロビジョニングログを確認する画面に遷移することができます
- ユーザー・グループ情報の同期成功・失敗について、こちらのログから確認することができます

現在のサイクルの状態

増分サイクルが停止しました。

0% 完

ユーザー 6,246

グループ 151

プロビジョニング ログの表示

プロビジョニングの管理

資格情報の更新
属性マッピングの編集
スコープ フィルターの追加
要求時にプロビジョニングする

プロビジョニング ログ …

許可された時刻 : **過去 24 時間**　日付を次の基準で表示: : **ローカル**　状態 : **すべて**

許可された時刻	ID	操作
2023/1/25 15:12:12	表示名 gtm_demo ソース ID 61a8e20b-c609-4a37-8e76-6 ターゲット ID 61a8e20b-c609-4a37-8e	Update
2023/1/25 15:12:12	表示名 SafieManager開発 ソース ID 4b5744d4-c135-43d9-98e5- ターゲット ID 4b5744d4-c135-43d9-9	Update
2023/1/25 15:12:12	表示名 SafieManager開発 ソース ID 4b5744d4-c135-43d9-98e5- ターゲット ID 4b5744d4-c135-43d9-9	Update
2023/1/25 15:12:12	表示名 SafieManager開発 ソース ID 4b5744d4-c135-43d9-98e5- ターゲット ID 4b5744d4-c135-43d9-9	Update
2023/1/25 15:12:12	表示名 SafieManager開発 ソース ID 4b5744d4-c135-43d9-98e5- ターゲット ID 4b5744d4-c135-43d9-9	Update

プロビジョニング失敗時の通知

- プロビジョニング画面の「プロビジョニング編集」をクリックし、「設定」よりプロビジョニング失敗時にメール通知を行うことができます

プロビジョニング失敗時のエラー一覧

safie

- プロビジョニング失敗の理由について、プロビジョニングログの「トラブルシューティング」より、SCIMエンドポイントからのエラーレスポンス値を確認することができます。主なエラー内容については下記になります。

error_description	エラー内容
emails is invalid. / Invalid mail address / mail_address is invalid.	AzureADのメールアドレスのマッピング設定が間違っているか、マッピングし取得した情報がメールアドレスの形式となっていない可能性があります。P43を参考に設定を行ってください。
employee_number is invalid. / invalid employee_number	AzureADの社員番号のマッピング設定が間違っているか、社員番号が16文字より大きい情報である、もしくは既に登録されている社員番号である可能性があります。
Max length of displayName is 32	AzureADのユーザー名のマッピング設定が間違っているか、ユーザー名が32文字より大きい情報である可能性があります。

プロビジョニング失敗時のエラー一覧

safie

error_description	エラー内容
Corporation user capacity is full	SafieManagerに登録できるユーザー数の上限を超えています。新たにカメラをご契約いただき上限を増やすか、不要なユーザー情報の削除をご検討ください。
failed to authorize	シークレットトークンによるSCIM用URLでの認証に失敗しています。新たにシークレットトークンを発行しAzureADへの設定を行うことで解決できる可能性があります。
invalid sso_setting_id.	AzureADの管理者資格情報に設定するSCIM用URLの値が間違っているか、同期対象のユーザーが別企業アカウントに所属している可能性があります。

プロビジョニングの停止

プロビジョニングの停止

- プロビジョニング画面から、「プロビジョニングの停止」をクリックすることでプロビジョニングが停止されます

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

ホーム > [redacted] | 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 > [redacted]

[redacted] | プロビジョニング

エンタープライズ アプリケーション

プロビジョニングの開始　プロビジョニングの停止　プロビジョニングの再開　プロビジョニングの編集　要求時にプロビジョニングする　更新

- 概要
- デプロイ計画
- 問題の診断と解決

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

現在のサイクルの状態

増分サイクルが停止しました。

0% 完了

ユーザー 6,246　グループ 151

プロビジョニング ログの表示

プロビジョニングの管理

資格情報の更新
属性マッピングの編集
スコープ フィルターの追加
要求時にプロビジョニングする

現在までの統計情報

プロビジョニングの詳細の表示
技術情報の表示

https://portal.azure.com/#


memory
think
listen
see
speak
映像から未来をつくる
「賢くなるカメラ」が人々の第三の目となり
生き方・働き方を豊かにする情報を提供
気象
交通状況
顔認証
店舗データ
混雑状況
顧客導線

safie