Mist 設定マニュアル

- Settings -

シングルサインオンの設定

ジュニパーネットワークス株式会社

2023年6月 Ver 1.2

JUNIPer driven by Mist AI

はじめに

- 本マニュアルは、『シングルサインオンの設定』について説明します
  シングルサインオンの設定例として Azure AD と Google Cloud Identity を利用した手順を記載しております

- 手順内容は 2023年6月 時点の Mist Cloud にて確認を実施しております
  実際の画面と表示が異なる場合は以下のアップデート情報をご確認下さい
  https://www.mist.com/documentation/category/product-updates/

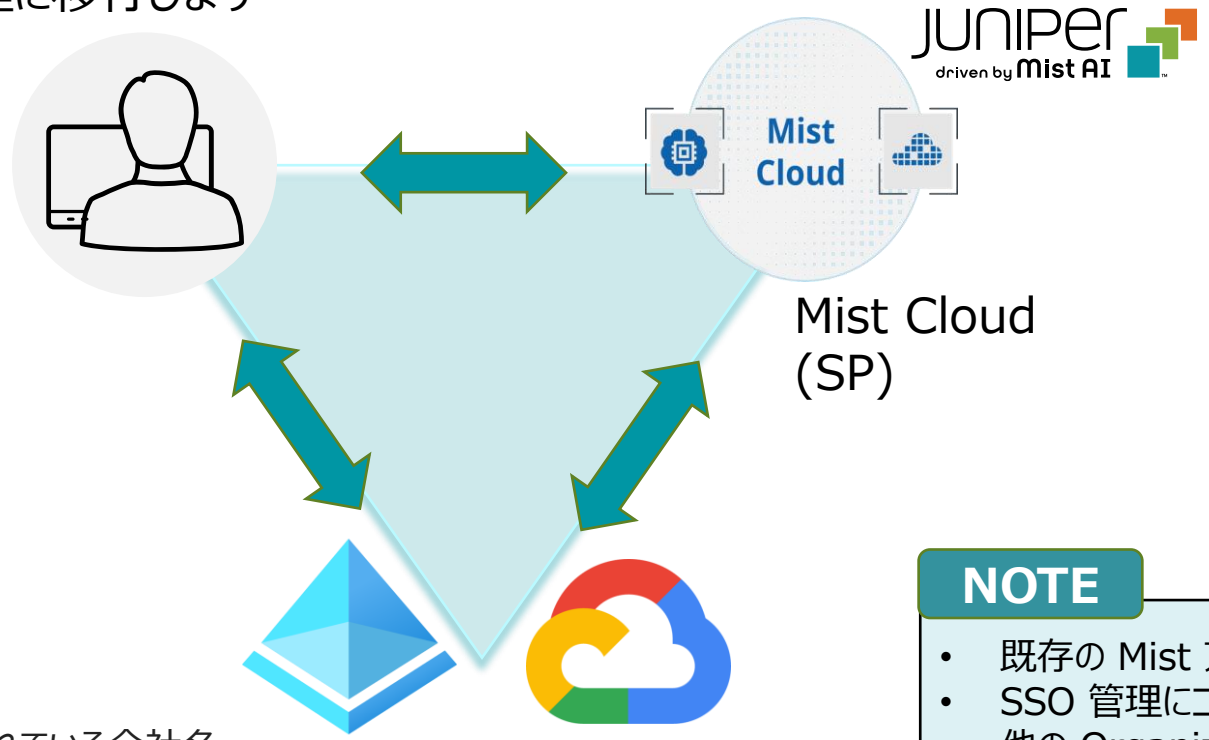
- 設定内容やパラメータは導入する環境や構成によって異なります
  各種設定内容の詳細は下記リンクよりご確認ください
  https://www.mist.com/documentation/

- 他にも多数の Mist 日本語マニュアルを「ソリューション＆テクニカル情報サイト」に掲載しております
  https://www.juniper.net/jp/ja/local/solution-technical-information/mist.html

シングルサインオンの設定

SSO 概要と注意点

本資料では、パスワード管理している既存の Mist アカウントを
Azure AD、または、Google Cloud Identity を IdP、
Mist Cloud を SP とする SAML 認証による SSO を設定し、
SSO 管理に移行します

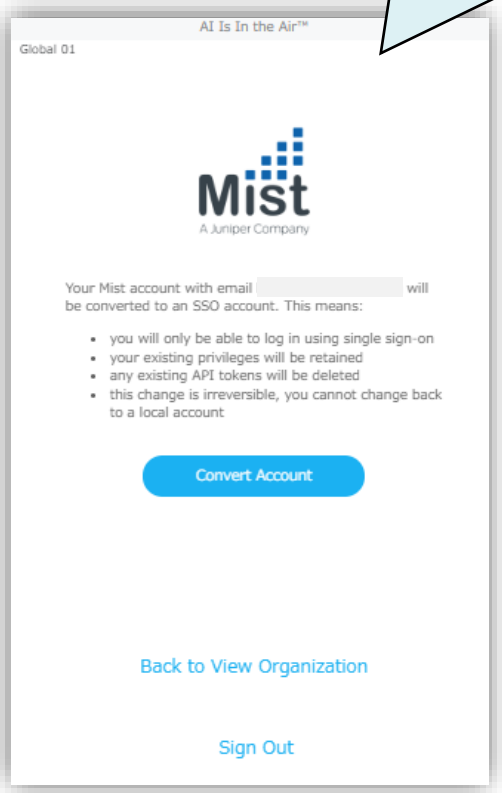


Mist Cloud
(SP)

Azure AD
(IdP)

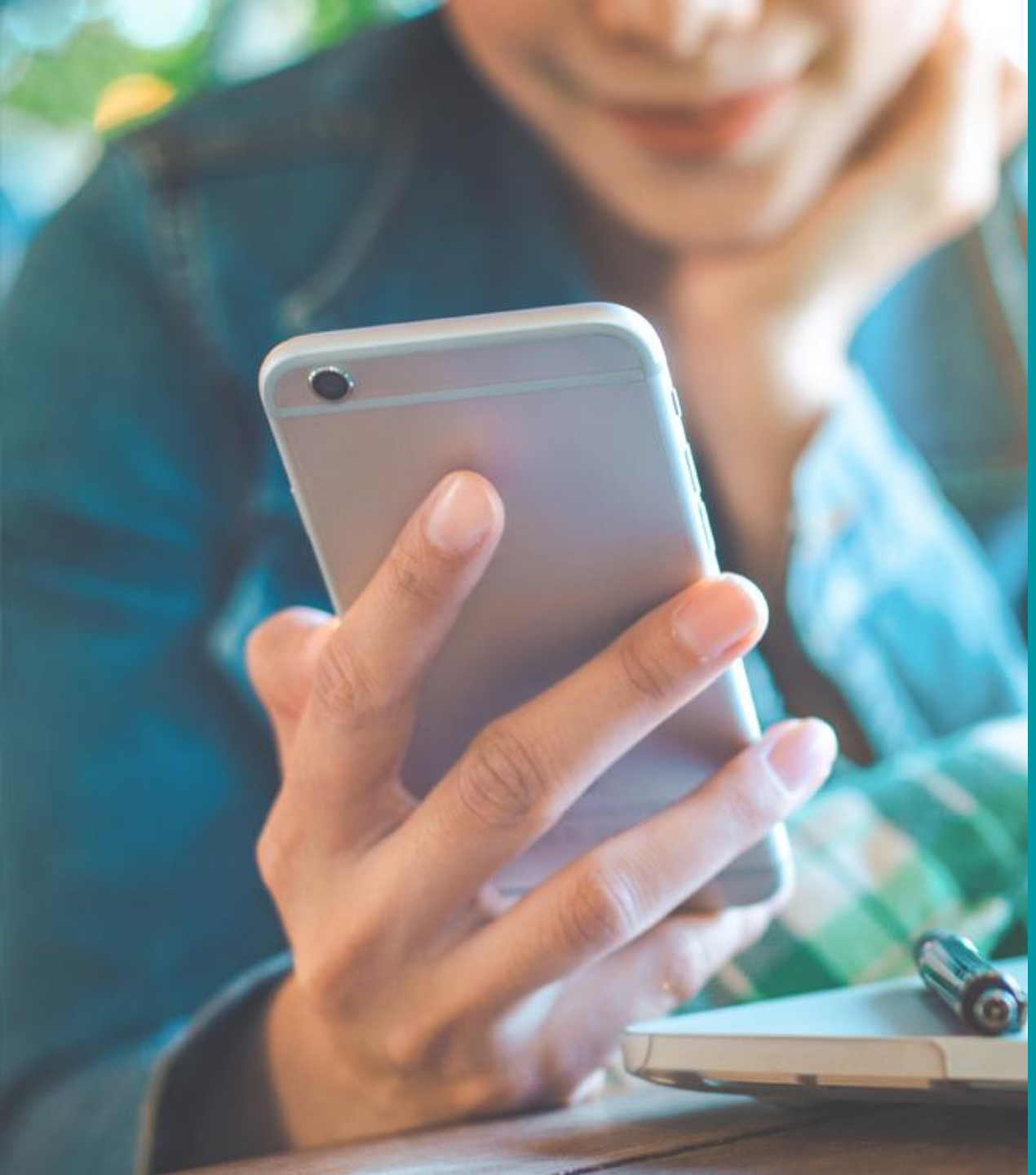
Google Cloud
Identity(IdP)

SSO 管理にコンバートしたときに
表示されるメッセージ



NOTE

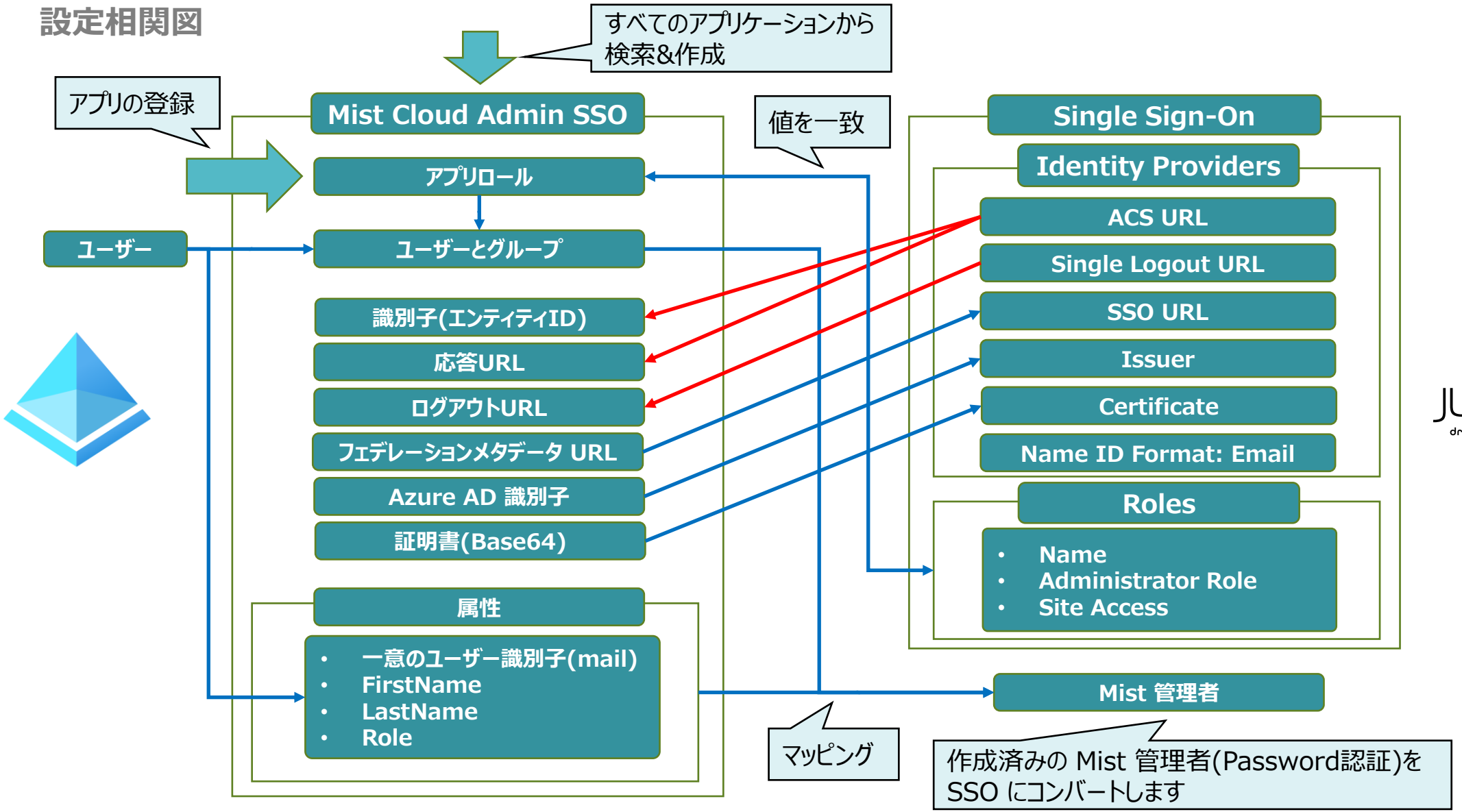
- 既存の Mist アカウントは、パスワード管理から SSO 管理にコンバートされます
- SSO 管理にコンバートしたアカウントをパスワード管理に戻すことはできません
- 他の Organization へ Invite した際に設定した Role が、SSOで指定した Role よりも優先されます



Azure AD

シングルサインオンの設定

設定相関図



シングルサインオンの設定

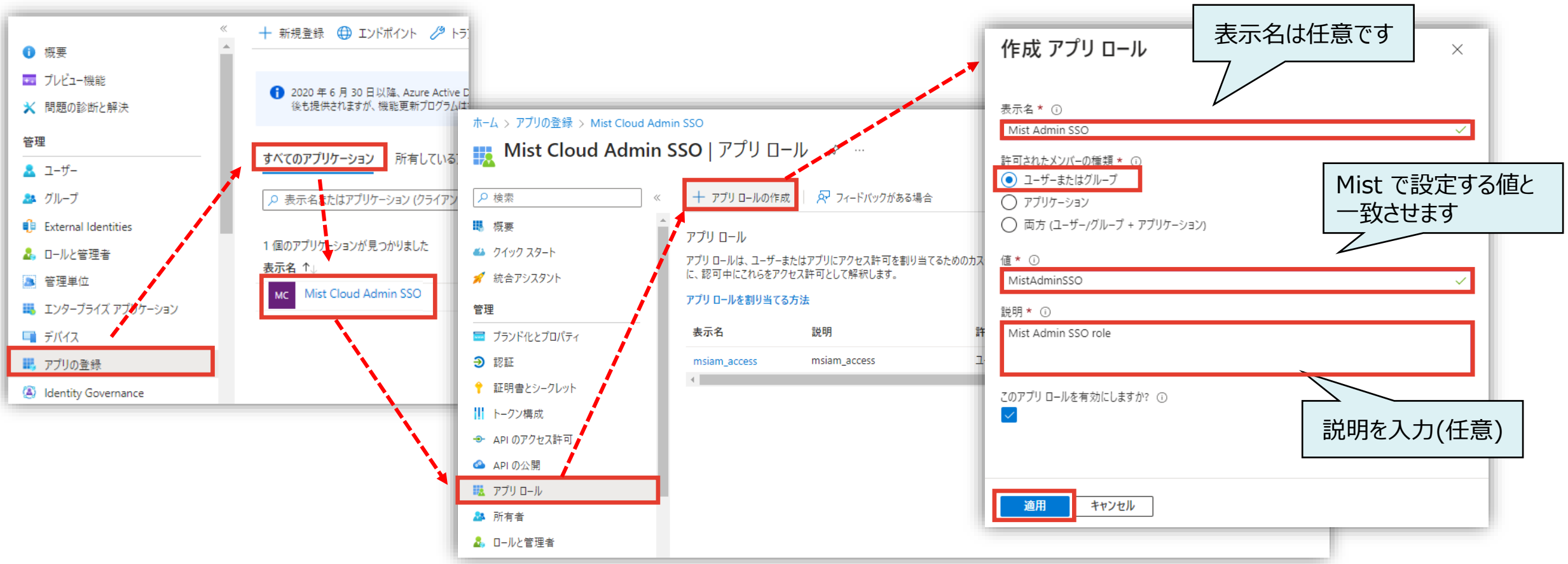
Azure AD - Mist Cloud Admin SSO の作成

1. [Azure Active Directory] エンタープライズアプリケーションを開き、 [すべてのアプリケーション] から
   [新しいアプリケーション] をクリックします
   検索バーで Mist Cloud などで検索し、[Mist Cloud Admin SSO] をクリック、次いで [作成] をクリックします

シングルサインオンの設定

Azure AD – アプリの登録 > アプリロールの作成

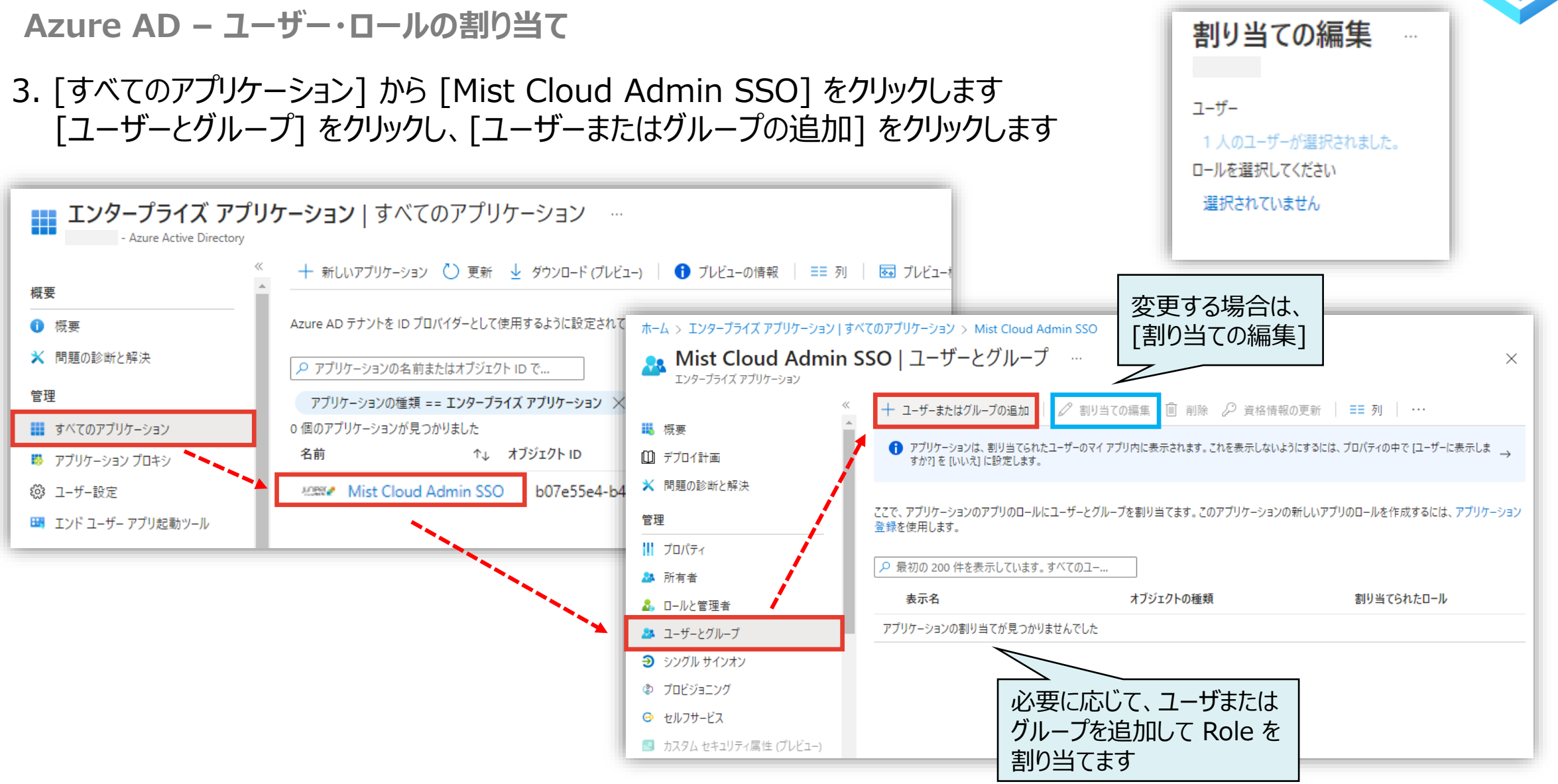
2. [アプリの登録]、[すべてのアプリケーション]、[Mist Cloud Admin SSO] を順にクリックしします
[アプリロール] で [アプリロールの作成] をクリックし、[表示名](任意) を入力、[ユーザーまたはグループ] を選択、
値に [MistAdminSSO](後述する Mist の設定と一致させます)、[説明](任意) を入力し適用をクリックします



シングルサインオンの設定

Azure AD – ユーザー・ロールの割り当て

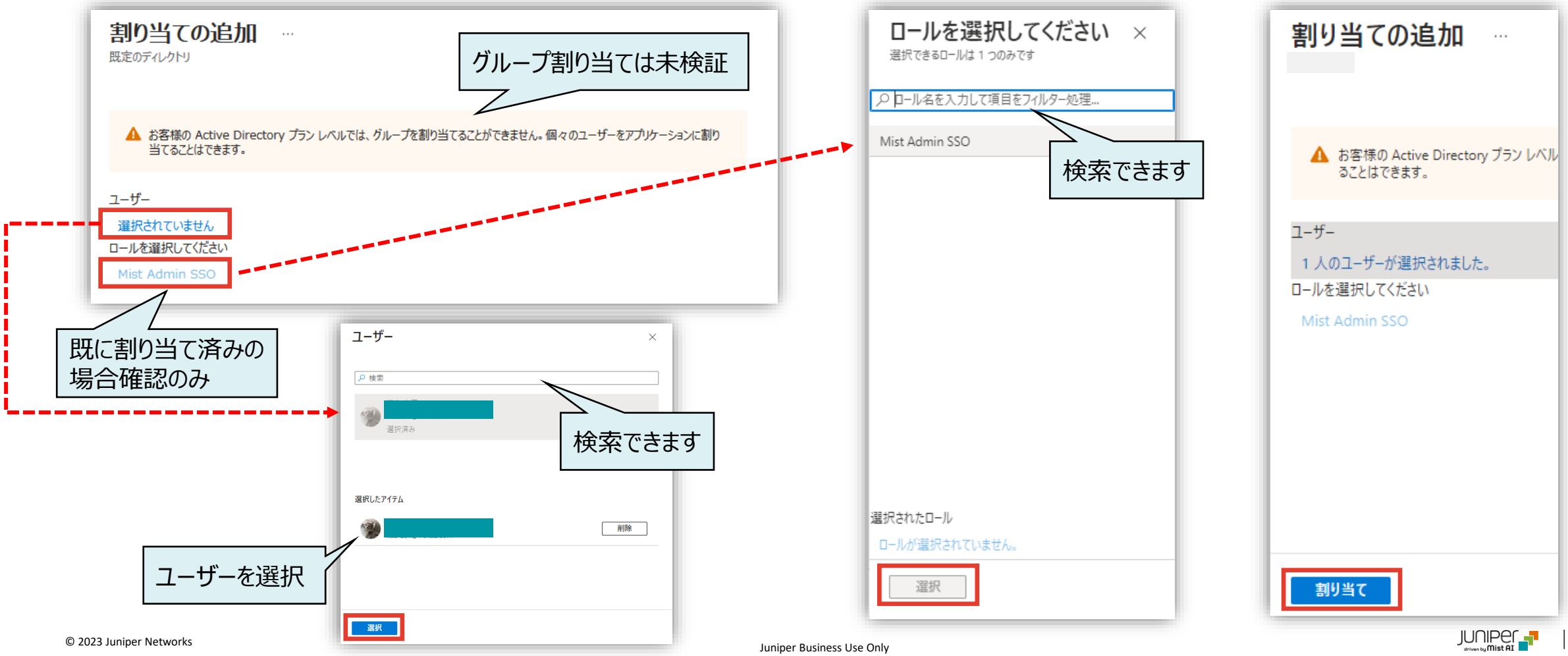
3. [すべてのアプリケーション] から [Mist Cloud Admin SSO] をクリックします
   [ユーザーとグループ] をクリックし、[ユーザーまたはグループの追加] をクリックします



シングルサインオンの設定

Azure AD – ユーザー・ロールの割り当て

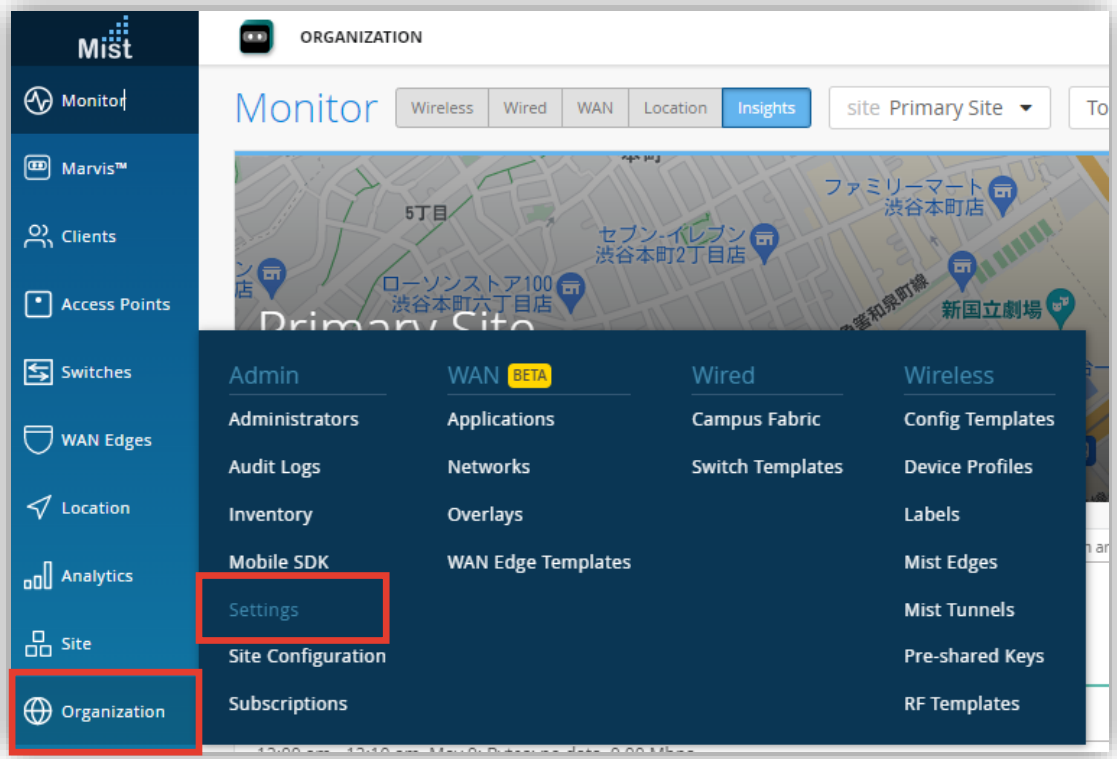
4. [割り当ての追加]で、[選択されていません] をクリックして、ユーザーを選択します
   次いで、ロール [Mist Admin SSO](アプリロールで作成した表示名) を選択し、[割り当て] をクリックします



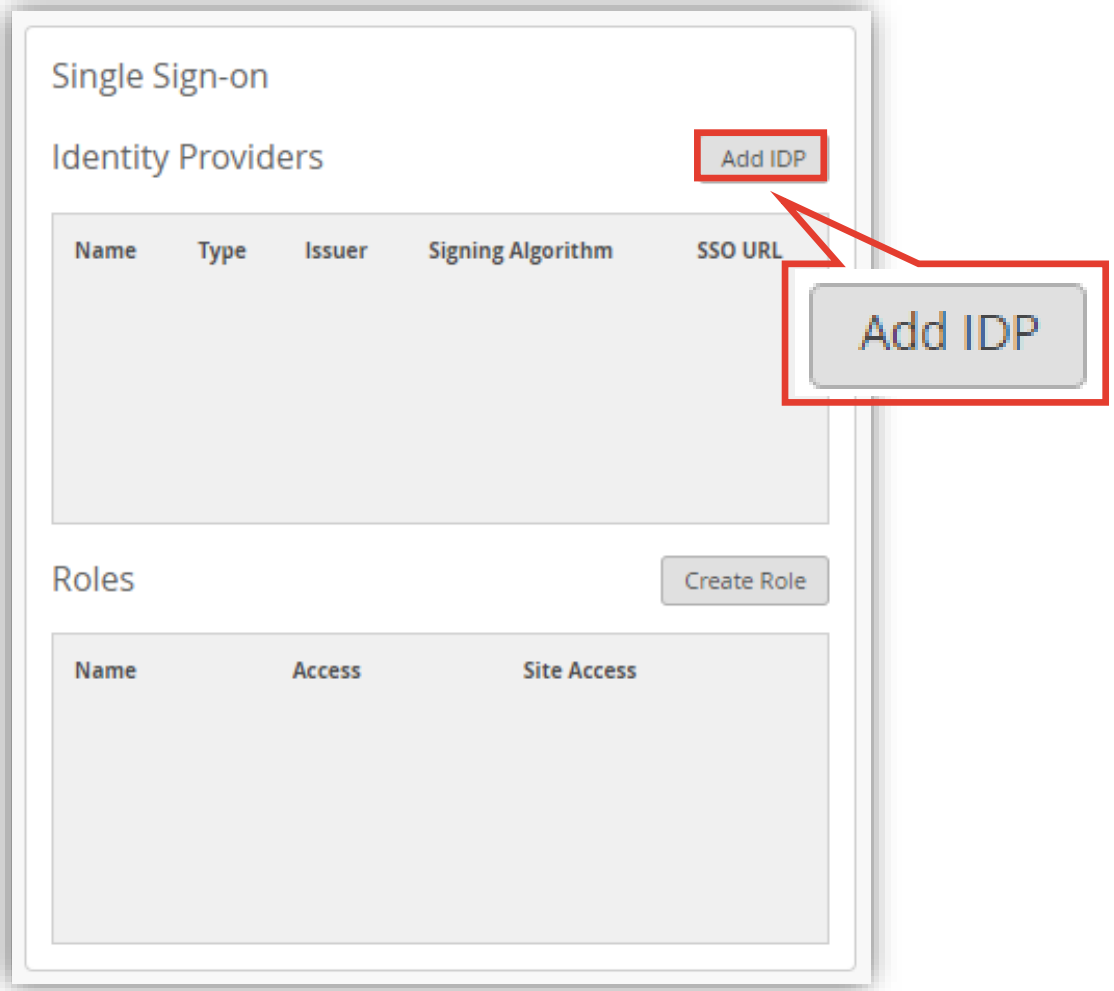
シングルサインオンの設定

Mist Cloud – SSO (IDP) の設定

5. [Organization] から [Settings] を選択します



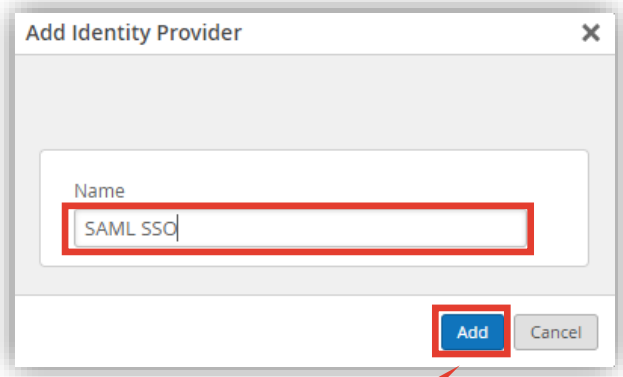
6.「Single Sign-on」の [Add IDP] をクリックします

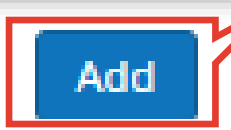


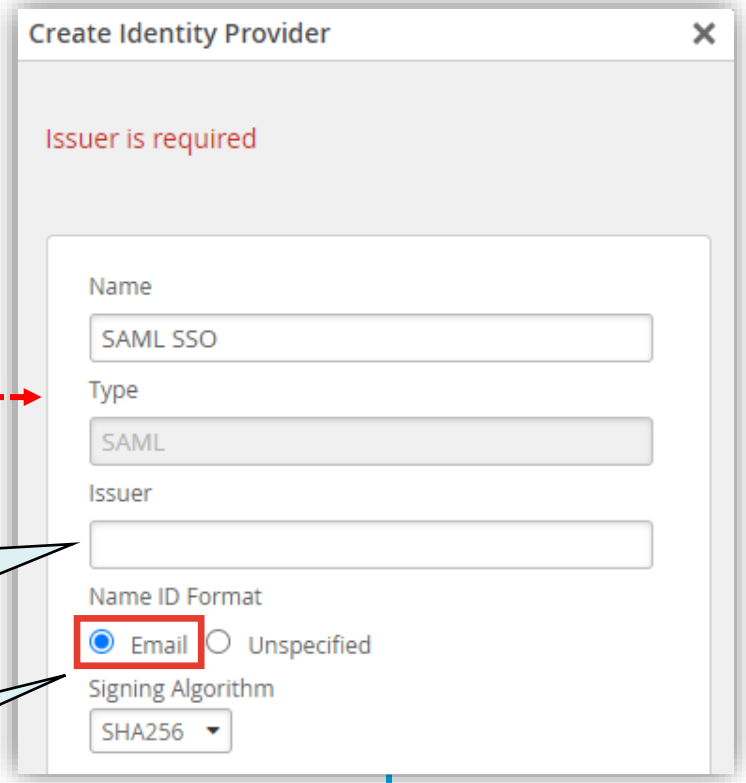
シングルサインオンの設定

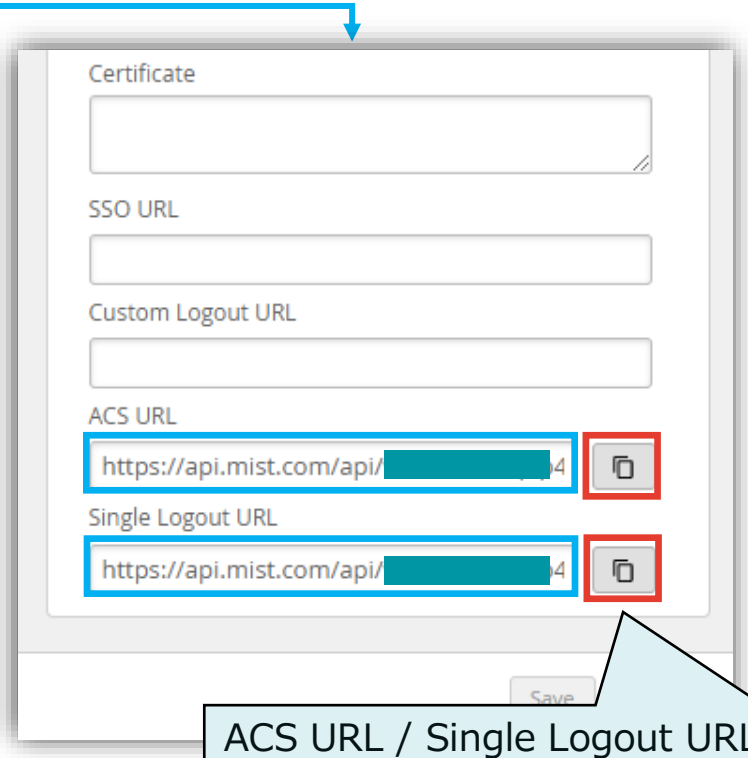
Mist Cloud – SSO (IDP) の設定

7. [Add Identity Provider] にて [Name] を入力し、[Add] をクリックします
   Name ID Format が [Email](デフォルト) であることを確認し、[Create Identity Provider] 下部に表示される [ACS URL] と [Single Logout URL] を控えます









Issuer / Certificate / SSO URL は、後述の Azure AD で設定した値を貼り付けます(p.19)

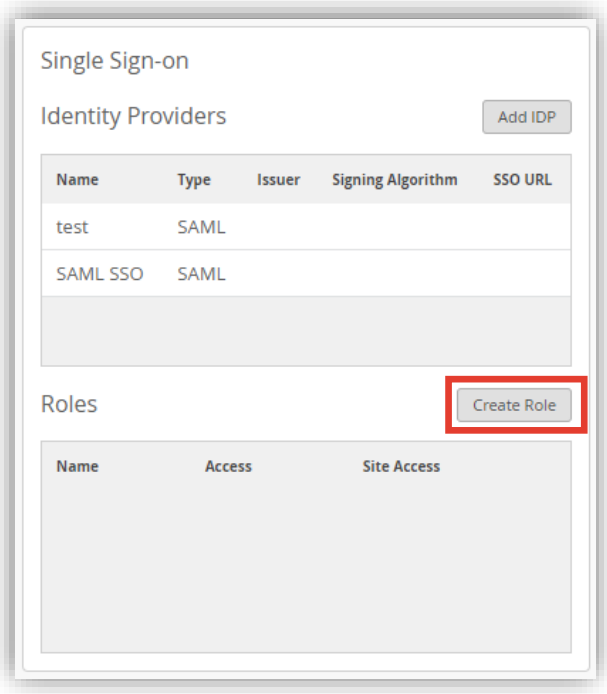
Name ID Format は Email(デフォルト)

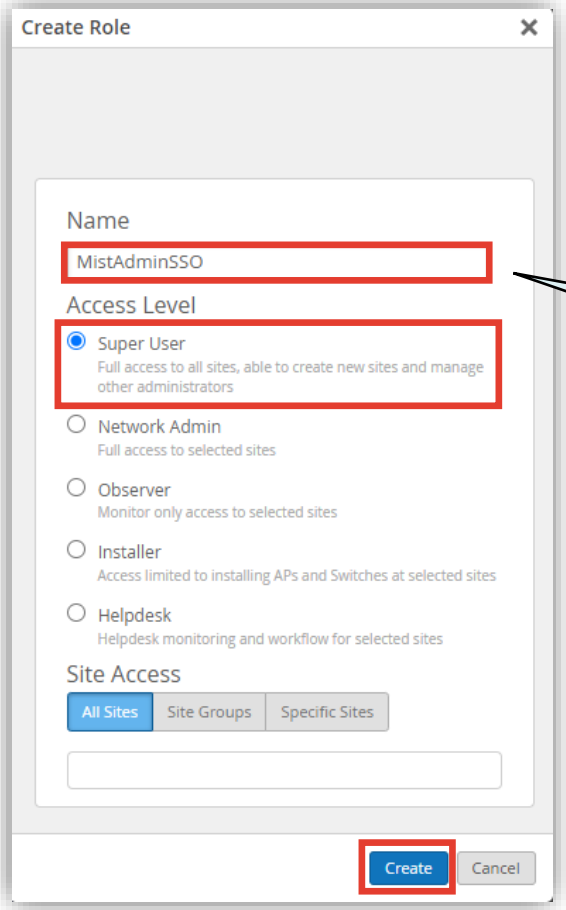
ACS URL / Single Logout URL は、Azure AD の SAML 設定で使用します(p.15)

シングルサインオンの設定

Mist Cloud – SSO (IDP) の設定 / Create Role

8. [Create Role] をクリックします
   [Name] に User、[Access Level] は Super User を選択し、[Create] をクリックします





Role 名は、Azure AD で設定する Role と一致させます(p.7)

シングルサインオンの設定

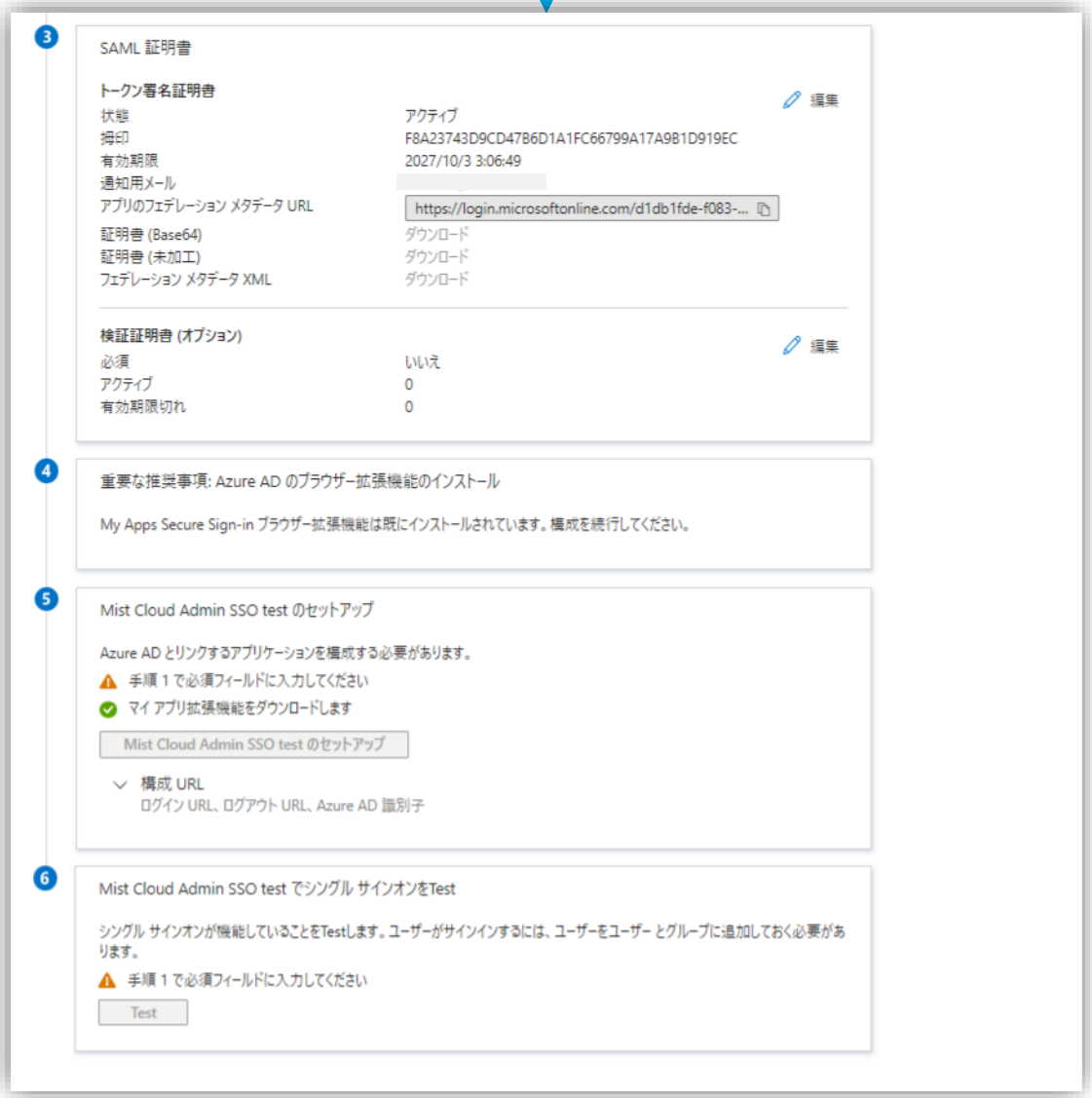
Azure AD - SAML 設定

9. [Mist Admin SSO] の [シングルサインオンの設定] をクリック、 [SAML] をクリックします

シングルサインオンの設定

Azure AD - SAML 設定

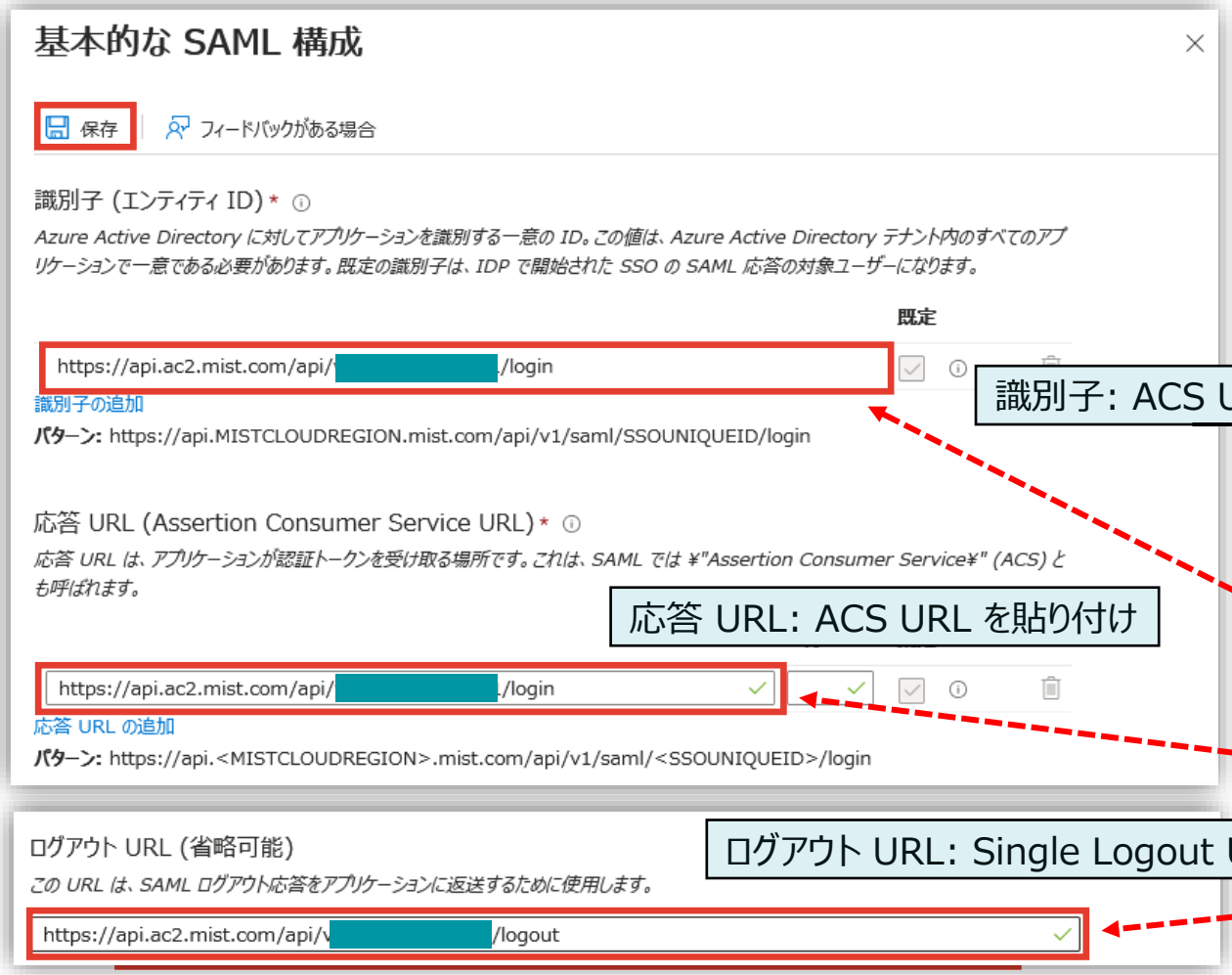
10. SAML 設定の手順の全体の流れ(①～⑥)を確認します



シングルサインオンの設定

Azure AD - SAML 設定 ① 基本的な SAML 構成

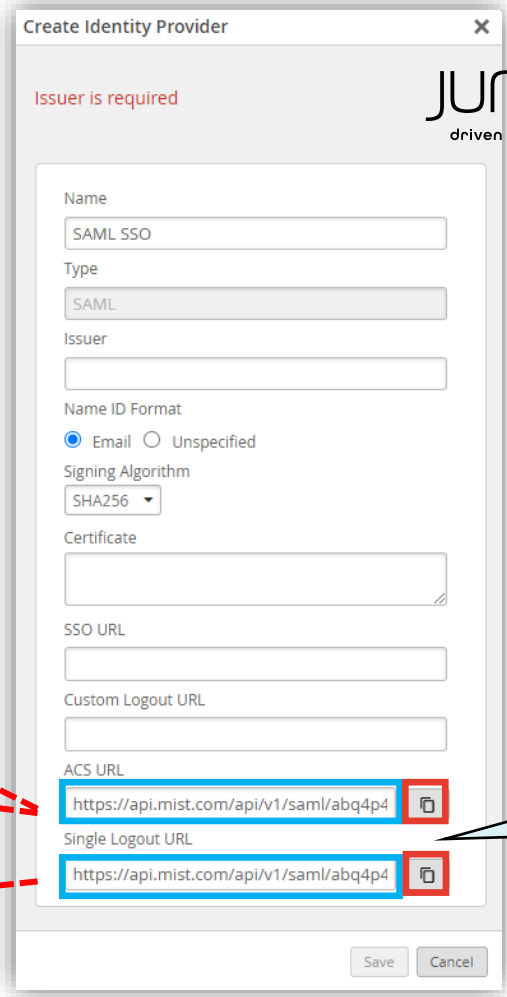
11. 「基本的な SAML 構成」の編集をクリックし、[識別子]、[応答 URL]、[ログアウト URL] を入力し保存をクリックします



識別子: ACS URL を貼り付け

応答 URL: ACS URL を貼り付け

ログアウト URL: Single Logout URL を貼り付け

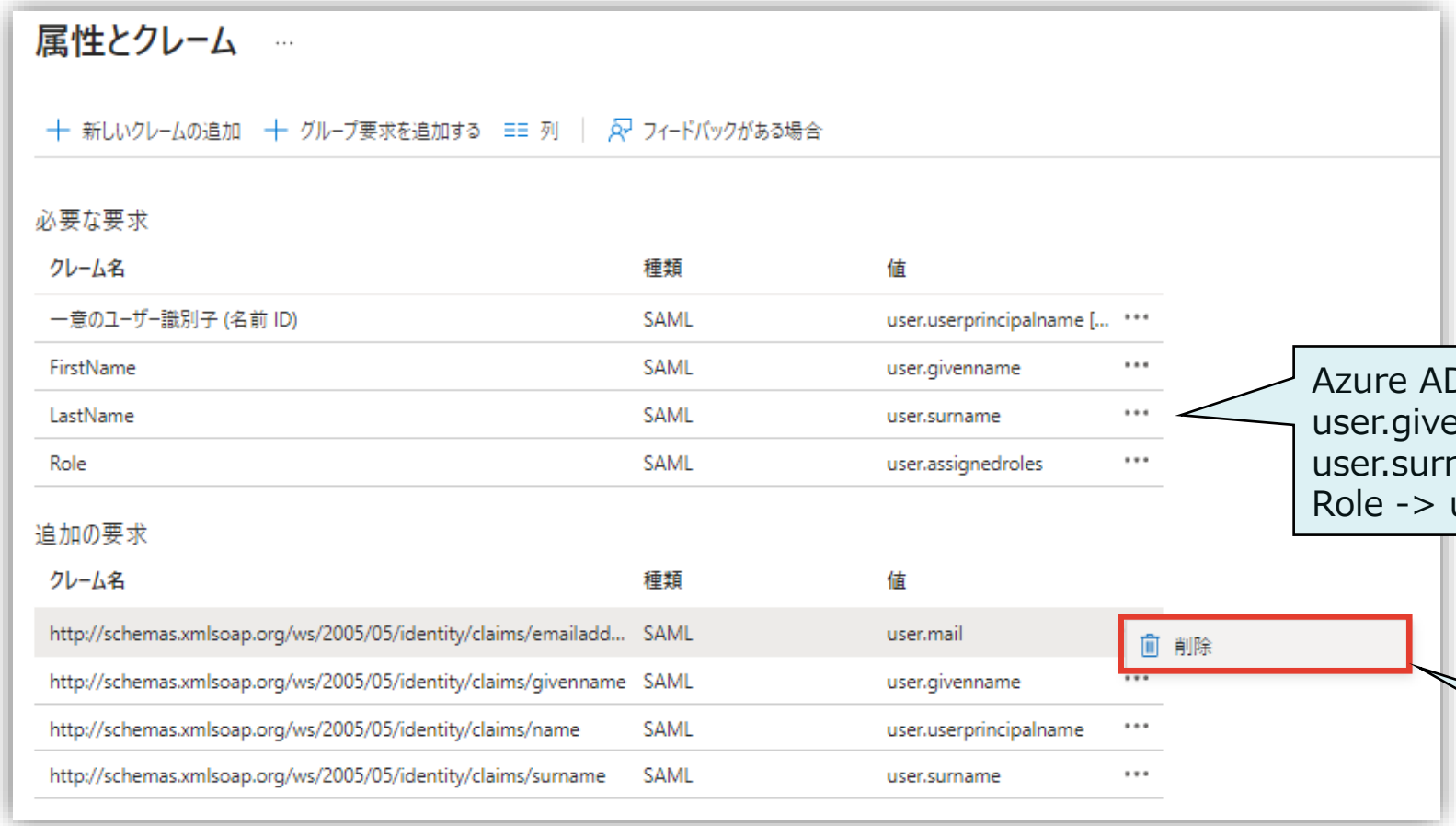


コピー

シングルサインオンの設定

Azure AD - SAML 設定 ② 属性とクレーム

12. [属性とクレーム] の [編集] をクリックし、追加の要求のクレーム名から値 [user.mail]、[user.givenname]、[user.userprincipalname]、[user.surname] を削除します



Azure AD に登録してある値をマッピングします
user.givenname (名) -> FirstName
user.surname (姓) -> LastName
Role -> user.assignedroles

追加の要求のクレーム名を
4 つ削除します

シングルサインオンの設定

Azure AD - SAML 設定 ② 属性とクレーム

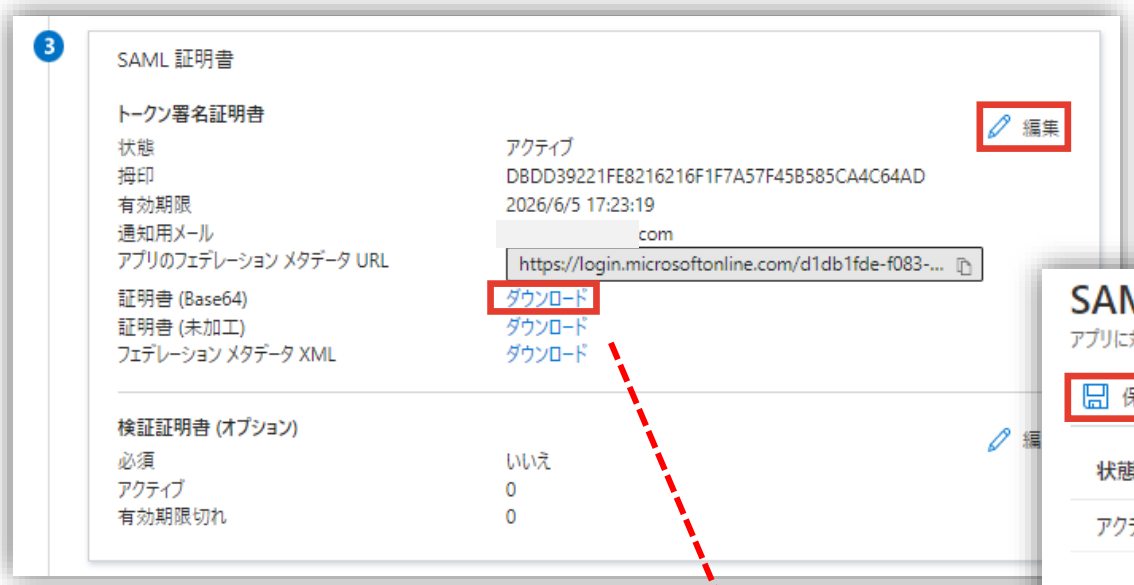
13. 必要な要求で「一意のユーザー識別子(名前ID)」をクリックし、ソース属性を [user.mail] に変更して保存します

デフォルトは、user.userprincipalname です
メールアドレスを UPN(User Principal Name) としている場合、
変更しなくても問題ありません
それ以外の場合、user.mail に変更します

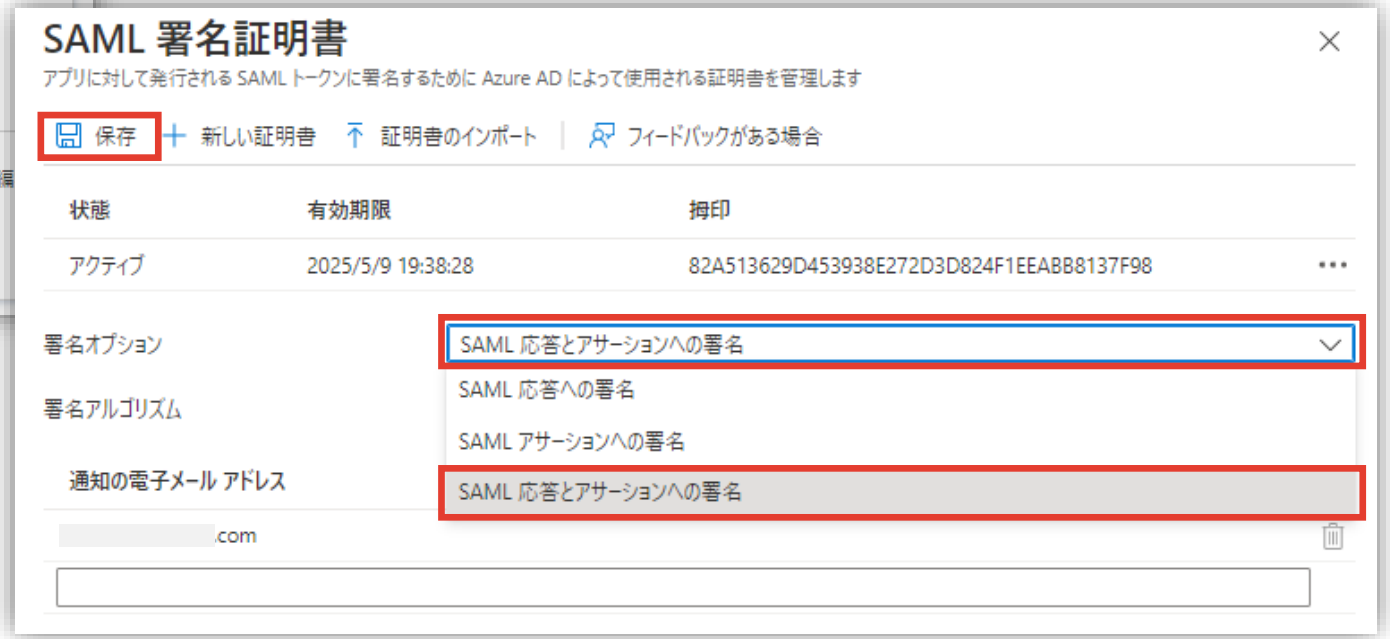
シングルサインオンの設定

Azure AD - SAML 設定 ③ SAML 署名証明書

14.「証明書 (Base64)」をダウンロードし、保存します
　　SAML署名証明書の編集をクリックし、「署名オプション」を [SAML応答とアサーションへの署名](デフォルト) を確認します



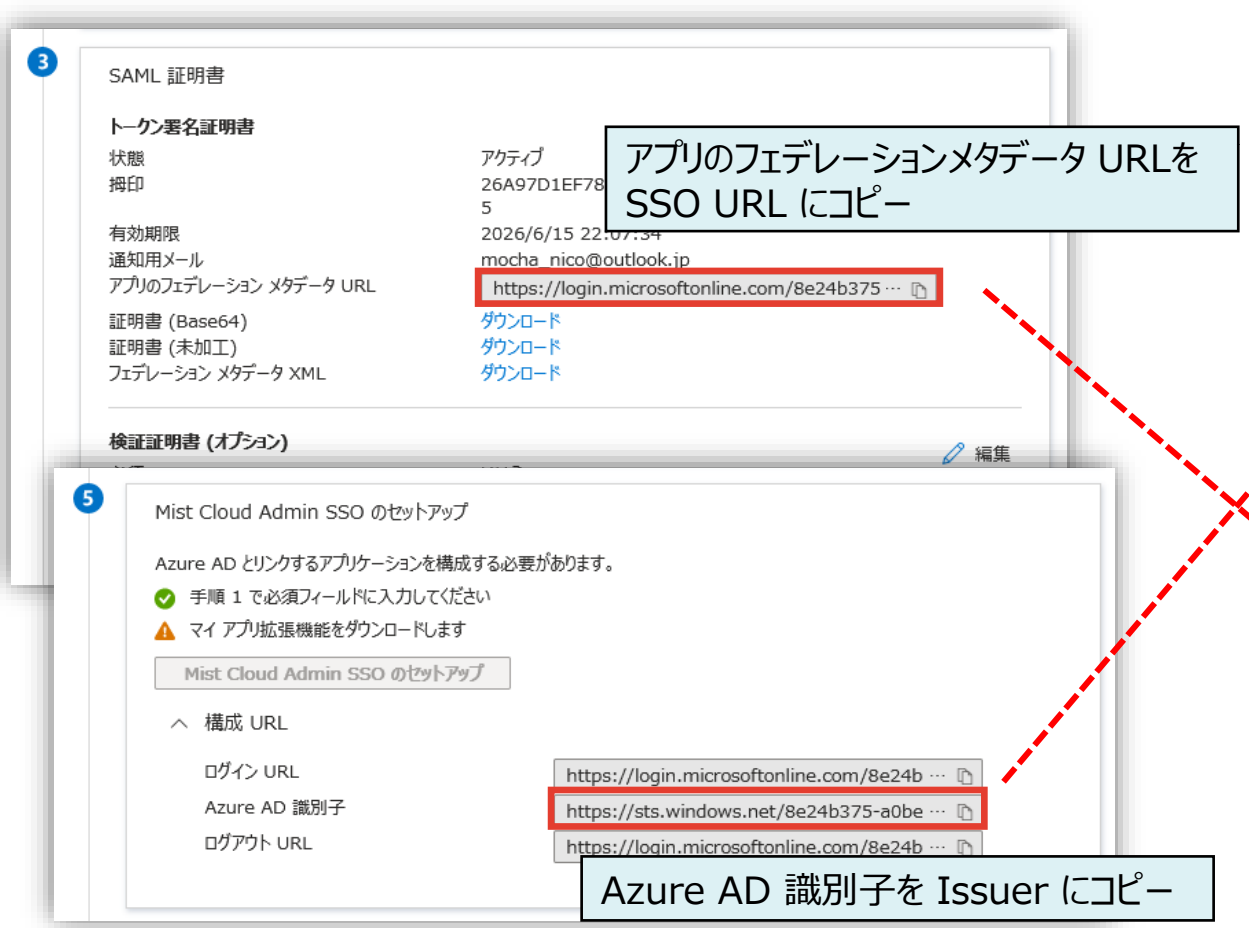
証明書 (Base64)



シングルサインオンの設定

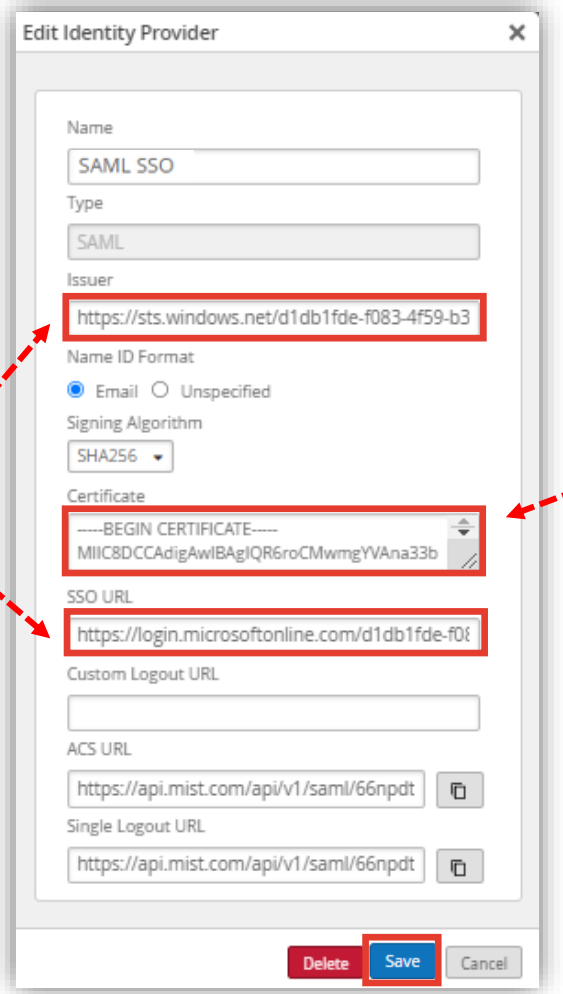
Azure AD - SAML 設定 各パラメータを Mist Cloud の IdP 設定に転記

15. [アプリのフェデレーションメタデータ URL] と [Azure AD 識別子] をコピー、Mist の IdP 設定の [SSO URL] と [Issuer] にそれぞれ貼り付け、証明書 (Base64) の内容を Certificate にコピーして、Save します

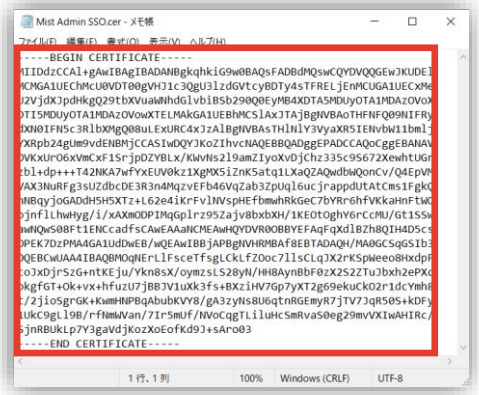


アプリのフェデレーションメタデータ URLを SSO URL にコピー

Azure AD 識別子を Issuer にコピー



証明書 (Base64)

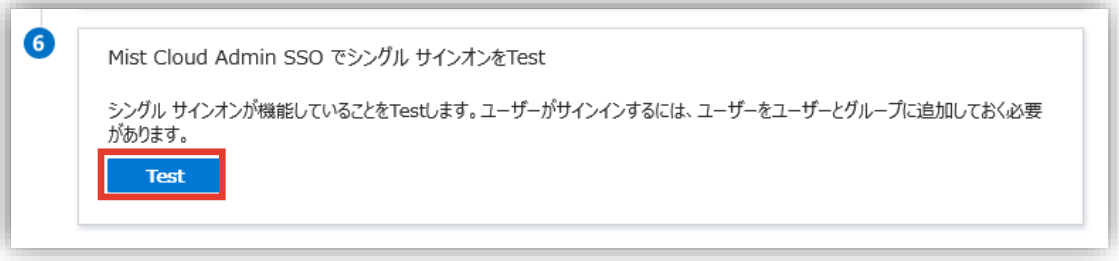


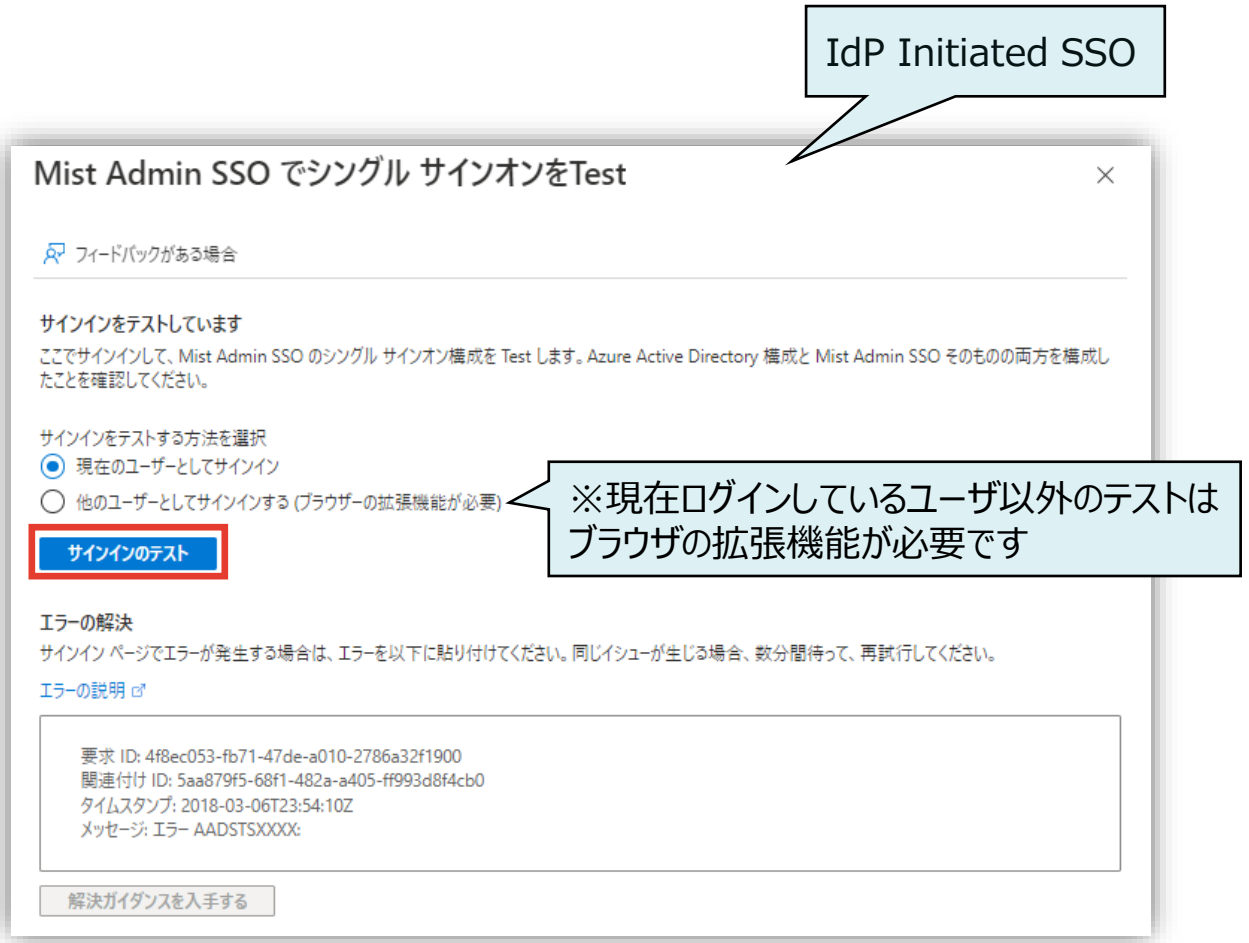
証明書(Base64) をテキストエディタで開き、コピー

シングルサインオンの設定

Azure AD - SAML 設定 シングルサインオンを Test

16. シングルサインオンをテストします
[Test] をクリックし、[サインインのテスト]をクリックします

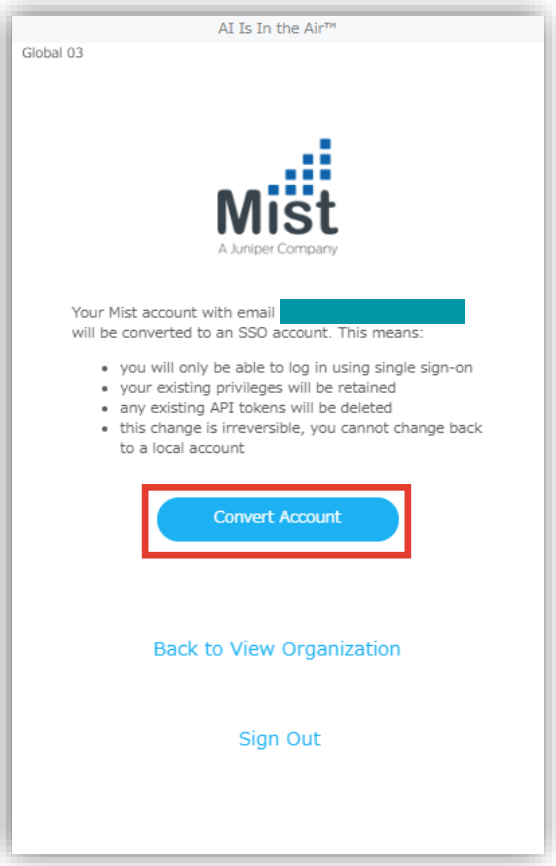


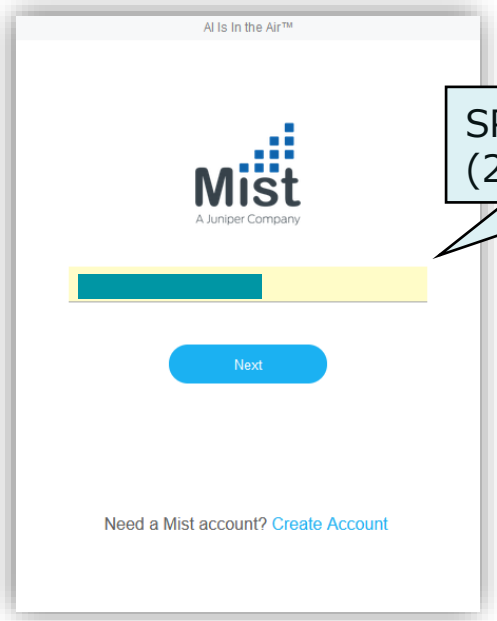


シングルサインオンの設定

Mist Cloud - SSO コンバート

17. Mist の管理画面に遷移するので、注意事項を確認し、[Convert Account] をクリックして、SSO ログインに移行します

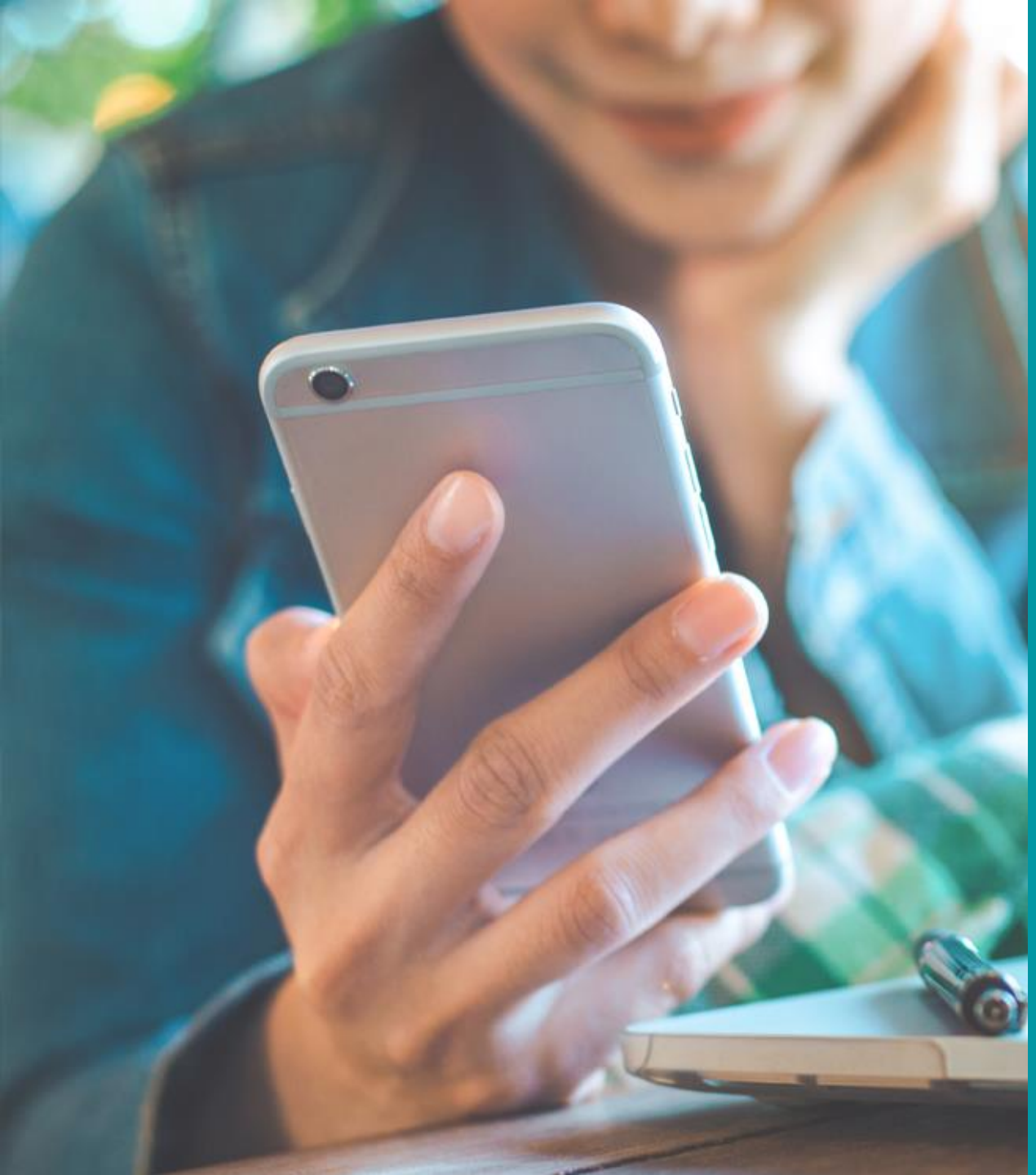




SP Initiated SSO
(2回目以降)

NOTE

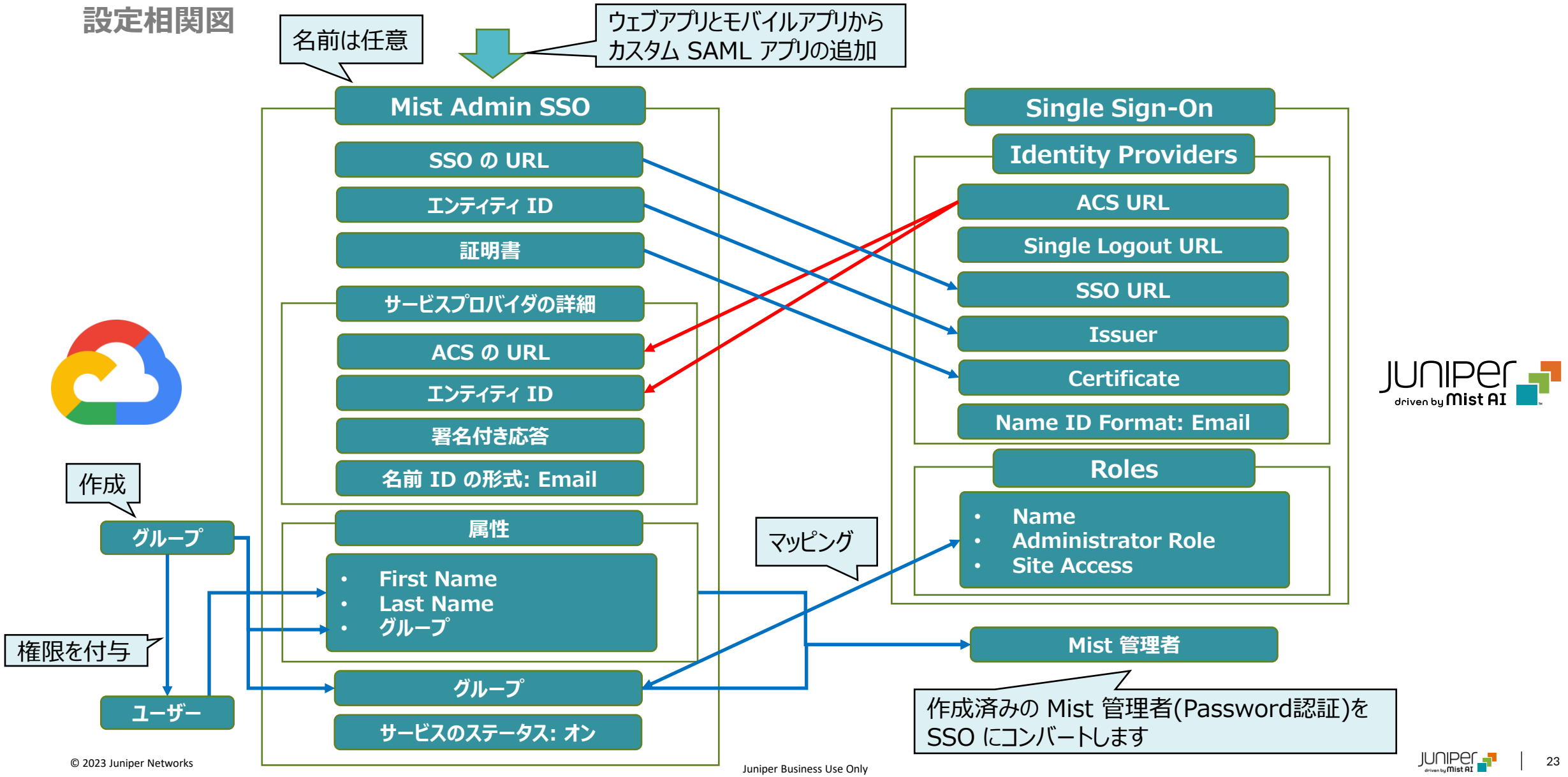
初回ログインは、IdP を起点とする SSO ログイン(IdP Initiated SSO) を実施します
以降のログインは、SP 起点の SSO ログイン(SP initiated SSO) も可能です



Google Cloud Identity

シングルサインオンの設定

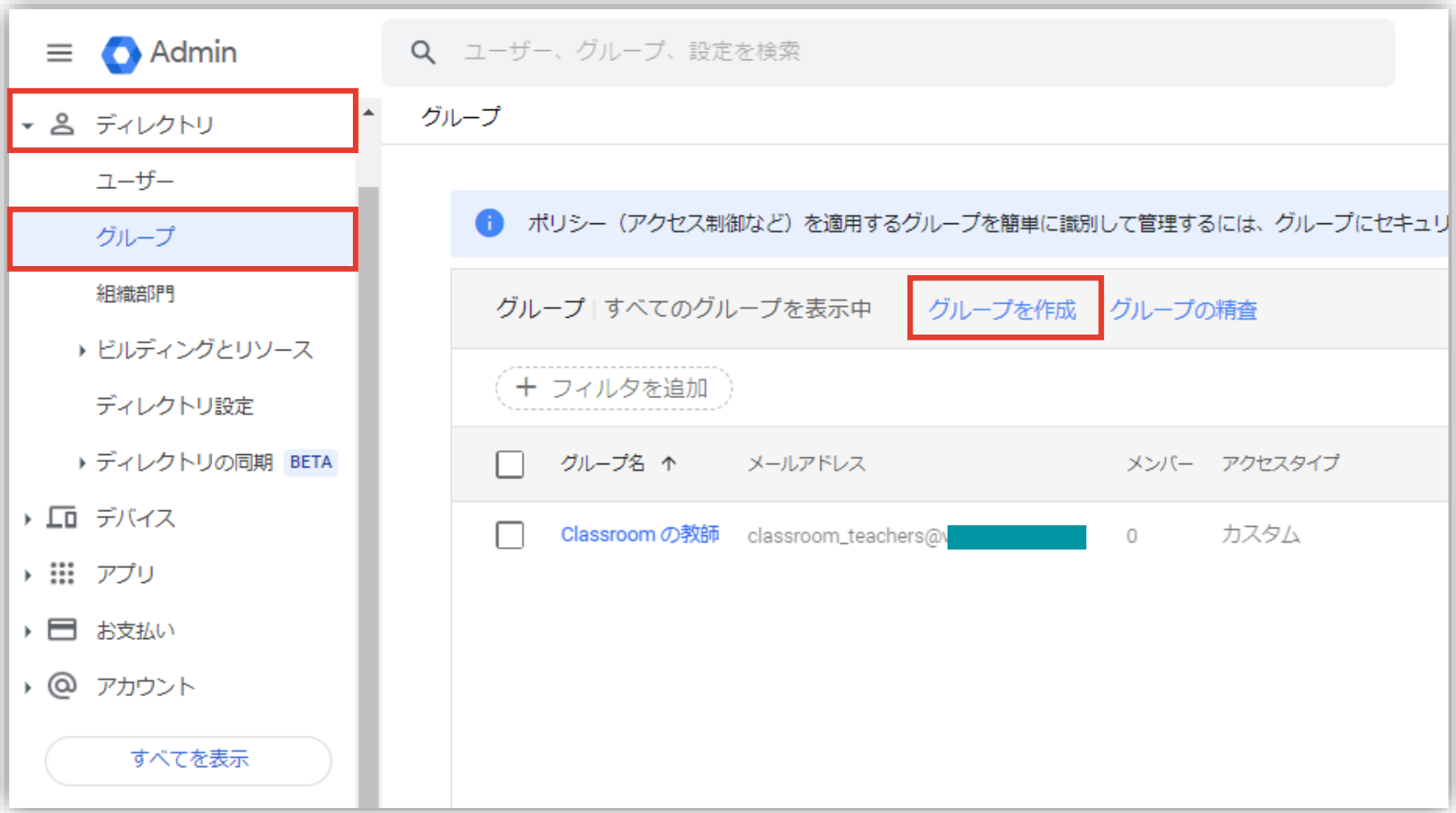
設定相関図



シングルサインオンの設定

Google Cloud Identity – グループの作成

1. Google の管理コンソール(https://admin.google.com/) に 管理者アカウントでログインします (一般アカウント不可)
   [ディレクトリ] より、[グループ]、 [グループの作成] をクリックしてグループを作成します



シングルサインオンの設定

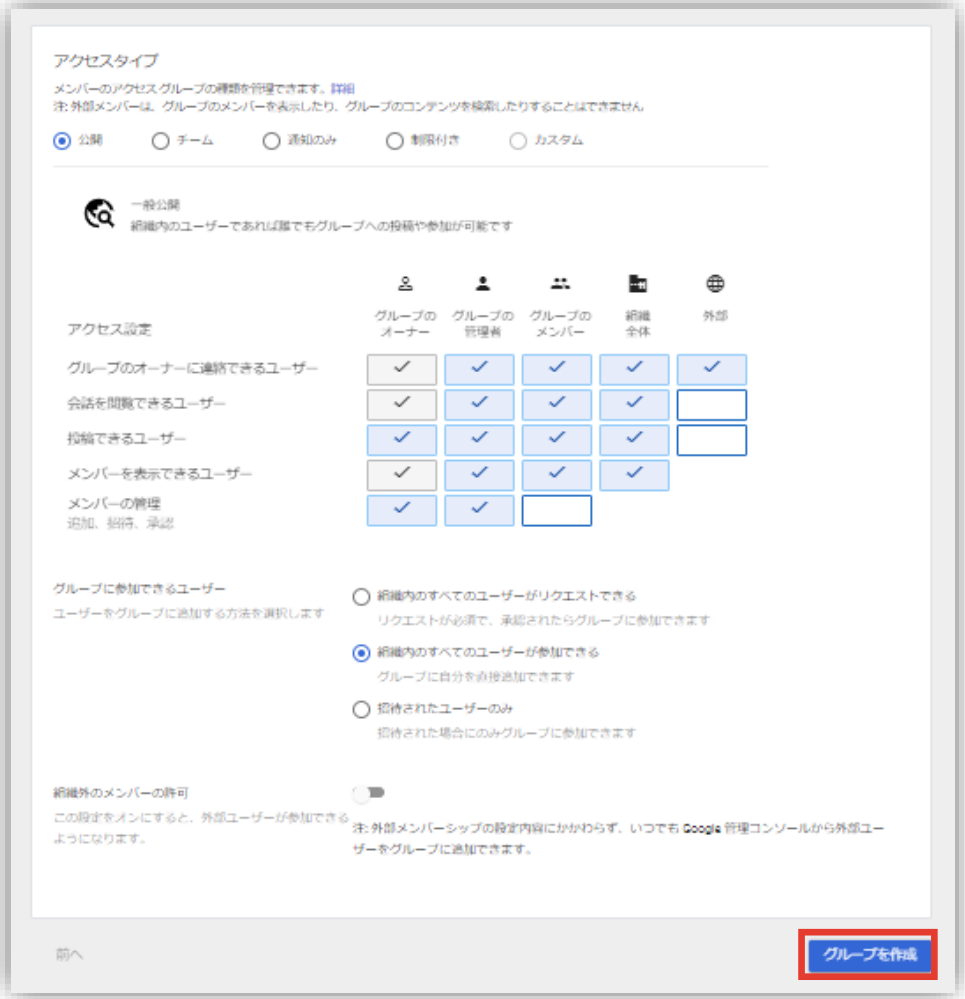
Google Cloud Identity – グループの作成

2. [グループ名]、[グループのメールアドレス]、[グループの説明](オプション)を入力、[グループのオーナー]を選択、[セキュリティ]ラベルにチェックを入れ、[次へ] をクリックします

シングルサインオンの設定

Google Cloud Identity – グループの作成

3. 各パラメータを確認し、[グループを作成] をクリック、次の確認画面で [完了] をクリックします



シングルサインオンの設定

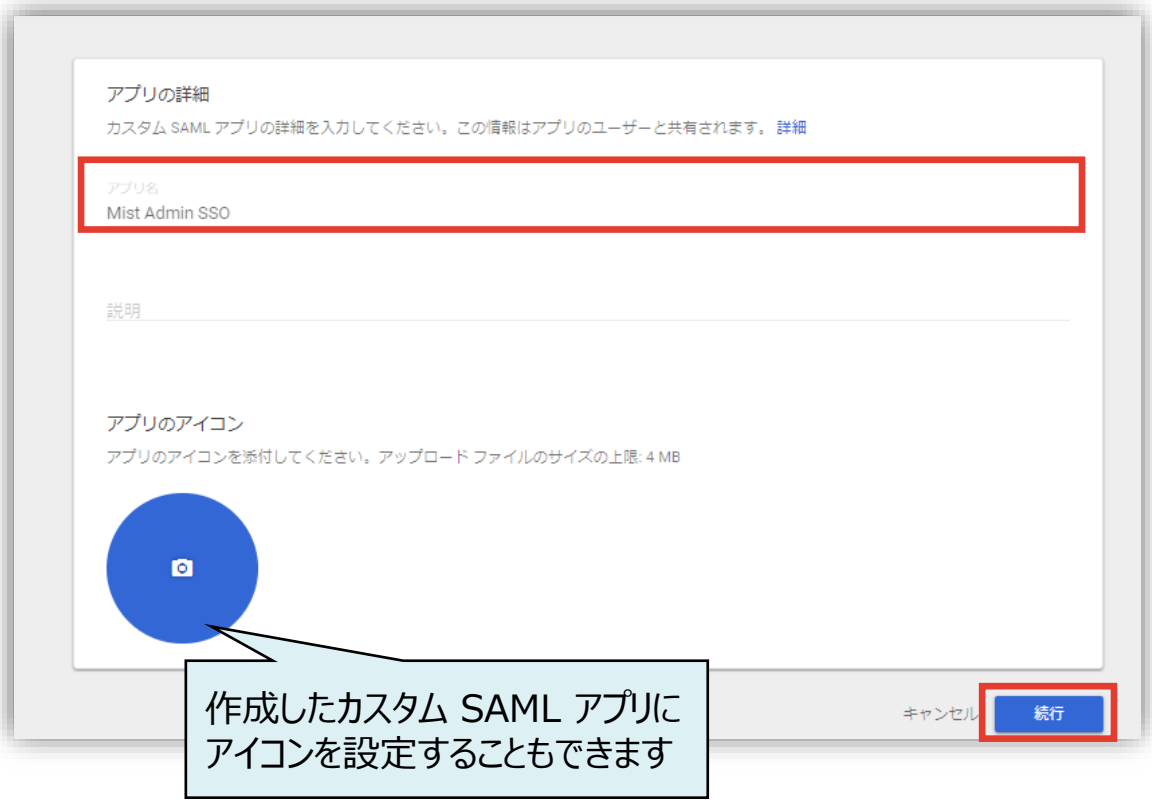
Google Cloud Identity – カスタム SAML アプリの追加

1. Google の管理コンソール(https://admin.google.com/) に 管理者アカウントでログインします (一般アカウント不可)
2. [アプリ] の [ウェブアプリとモバイルアプリ] から [アプリを追加]、[カスタムSAMLアプリの追加] をクリックします

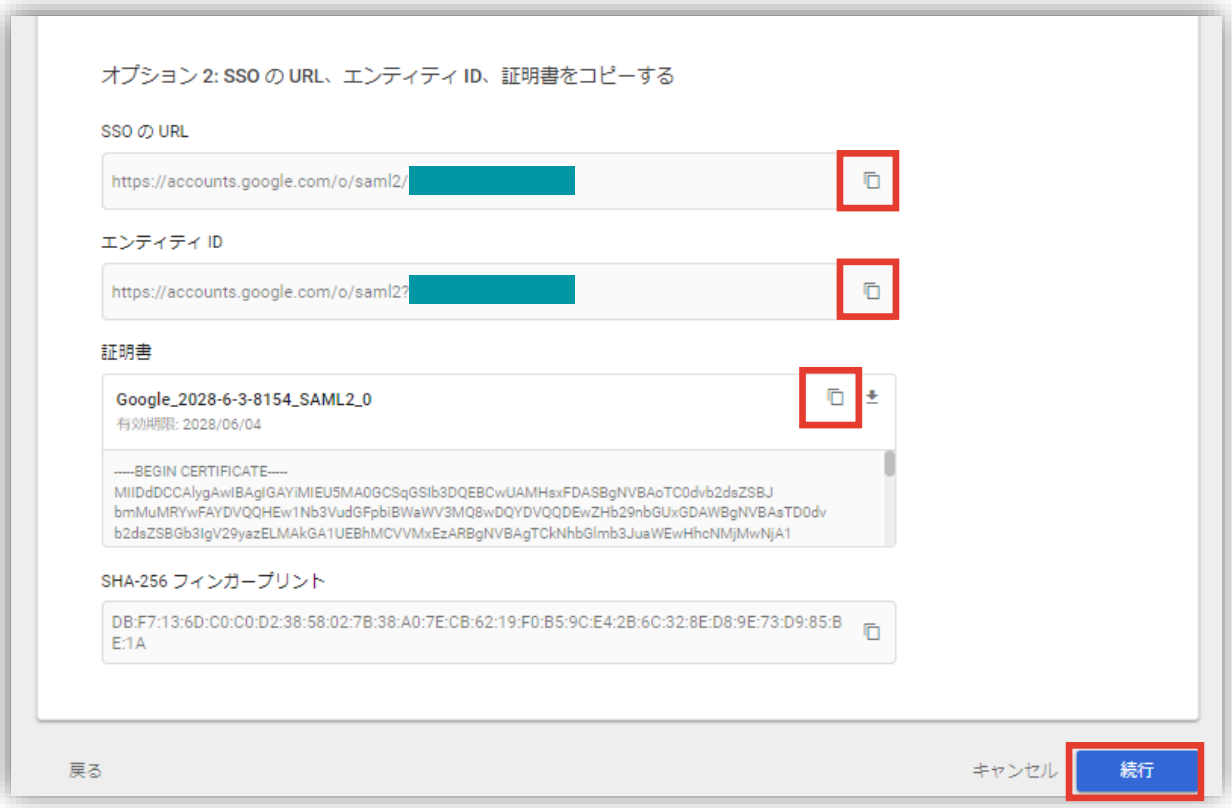
シングルサインオンの設定

Google Cloud Identity – カスタム SAML アプリの追加

3. [アプリ名] を入力して、[続行] をクリックします



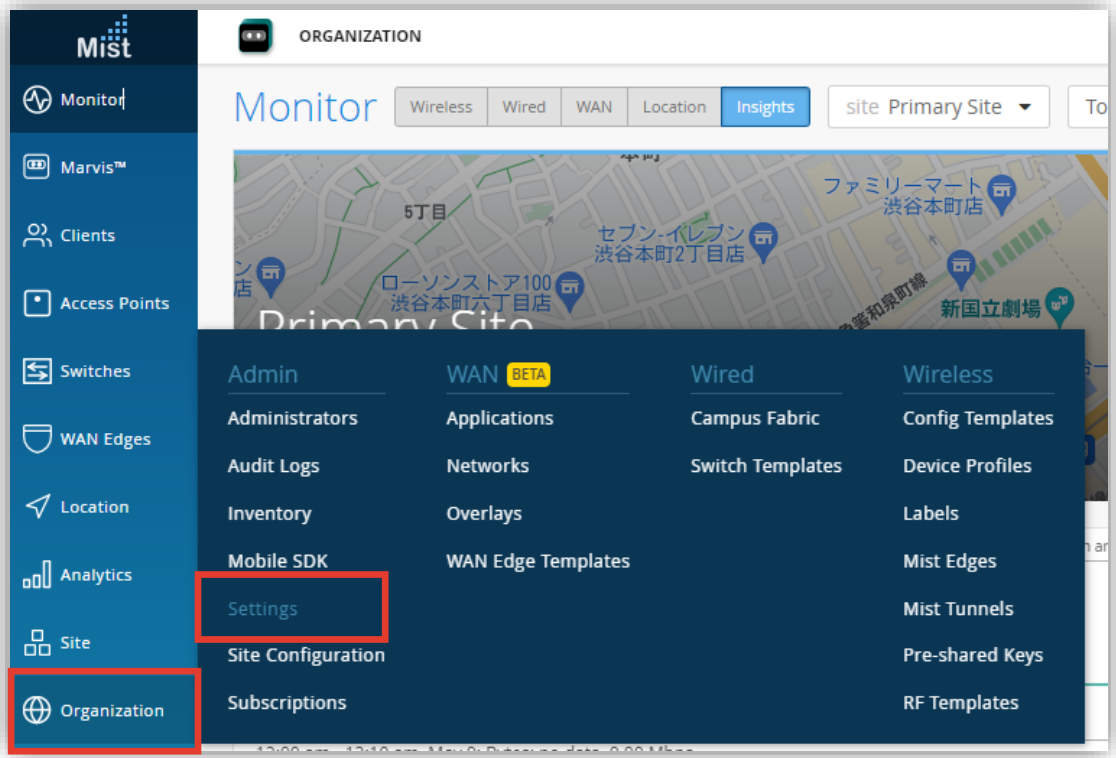
4. 「SSO の URL」、[エンティティ ID]、[証明書] をそれぞれコピーし情報を控え、[続行] をクリックします



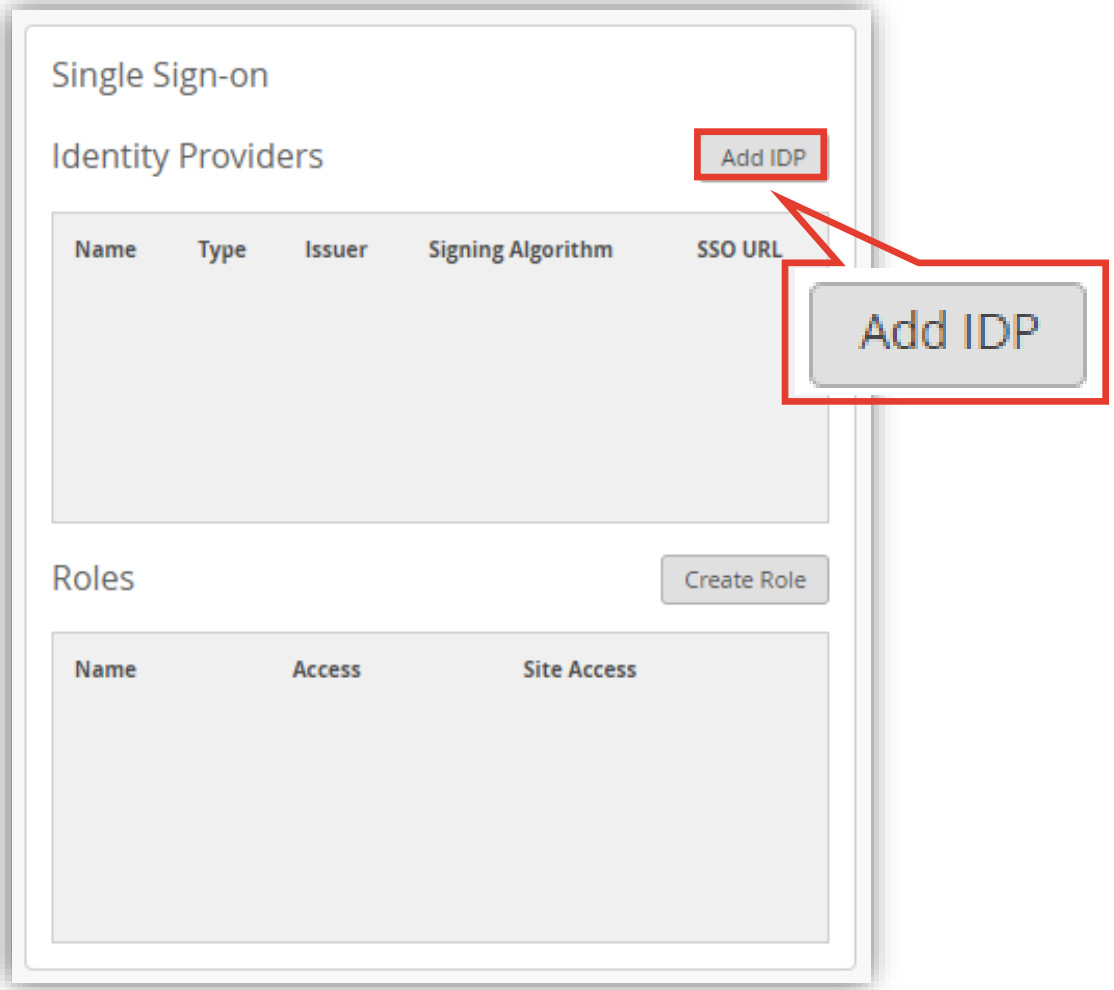
シングルサインオンの設定

Mist Cloud – SSO (IDP) の設定

5. [Organization] から [Settings] を選択します



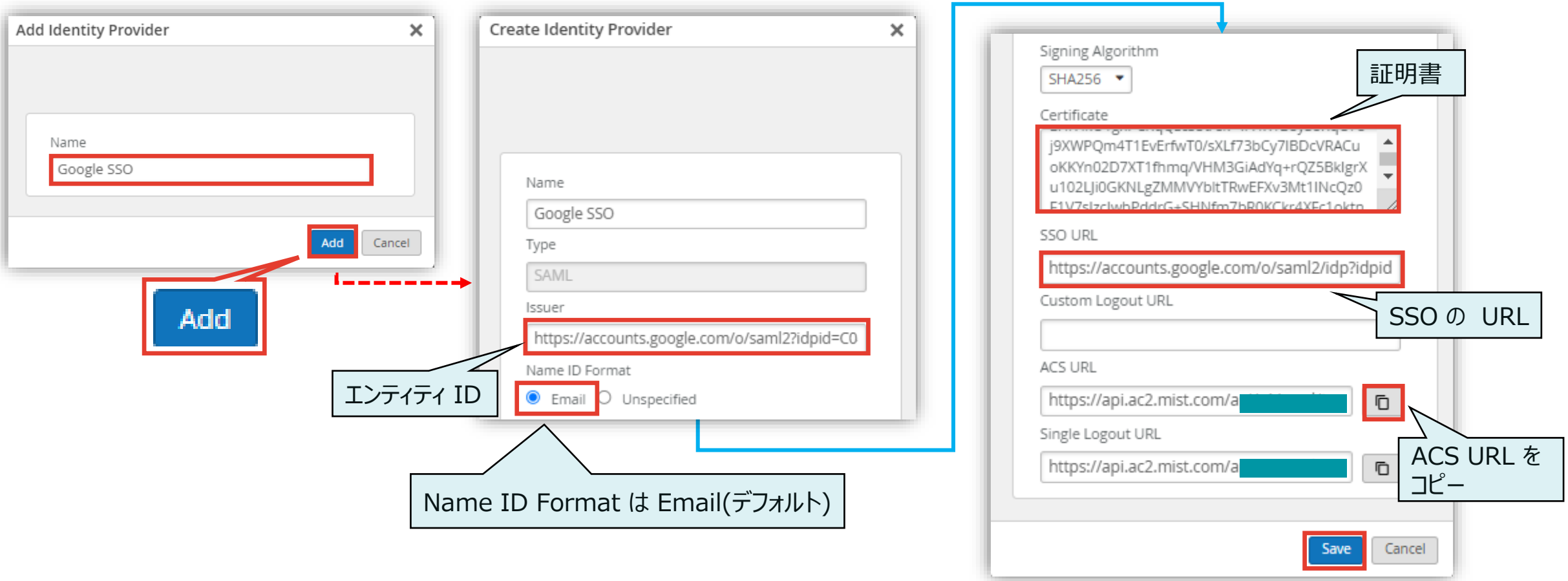
6.「Single Sign-on」の [Add IDP] をクリックします



シングルサインオンの設定

Mist Cloud – SSO (IDP) の設定

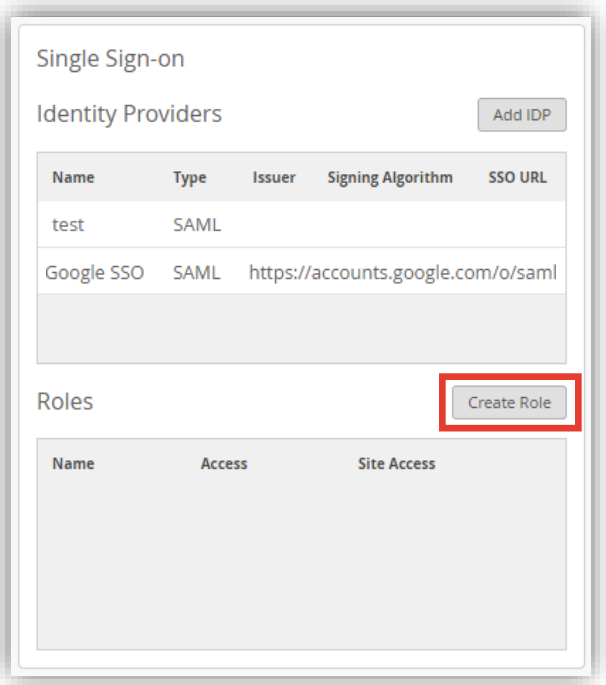
7. Google Cloud Identity で作成した「SSO の URL」、[エンティティ ID]、[証明書] をそれぞれ、[SSO URL]、[Issuer]、[Certificate] にコピーします
8. [ACS URL] をコピーして控え、[Save] をクリックします

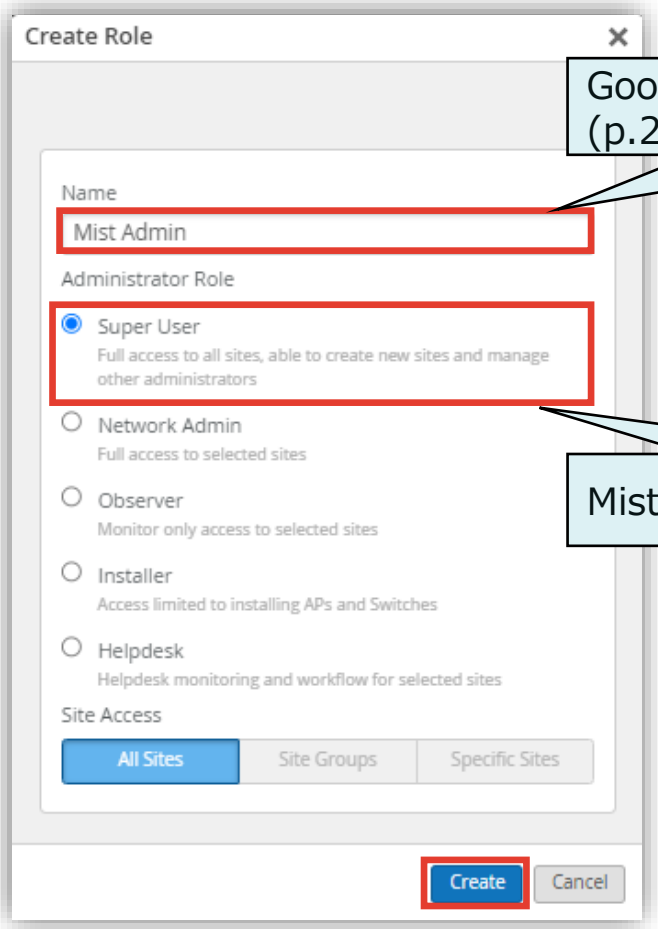


シングルサインオンの設定

Mist Cloud – SSO (IDP) の設定

9. [Create Role] をクリックします
   [Name] に User、[Access Level] は Super User を選択し、[Create] をクリックします





Google グループで作成した名前と一致させます (p.25)

Mist 管理者に割り当てる Role を設定します

シングルサインオンの設定

Google Cloud Identity – カスタム SAML アプリの追加

10. Google の管理コンソールに戻り、Mist の IdP で設定した [ACS URL] を [ACS の URL] と [エンティティ ID] にコピー、[署名付き応答] をチェック、名前 ID の形式で [EMAIL] を選択し、[続行]をクリックします

ID はメールアドレスを使用

シングルサインオンの設定

Google Cloud Identity – カスタム SAML アプリの追加

11. [マッピングを追加] をクリックして、Google Directory の属性 [First name]、[Last name] をプルダウンから選択し、それぞれアプリの属性に、[FirstName]、 [LastName] を入力します
Google グループから割り当てるグループを選択し、アプリ属性に [Role] を入力、[完了]をクリックします

Google Directory に登録してある姓・名を、SSO でログインする Mist 管理者の姓・名にマッピングします

Google グループ(任意)を、Mist 管理者の Role にマッピングします

シングルサインオンの設定

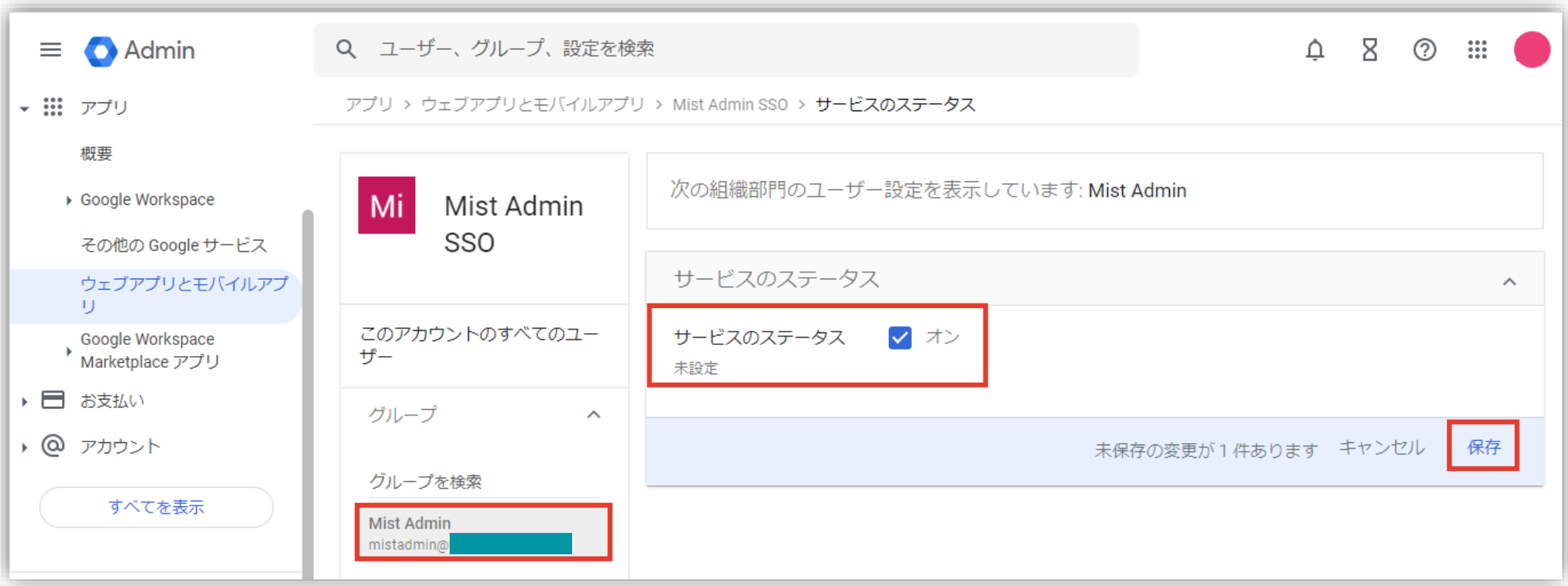
Google Cloud Identity – カスタム SAML アプリの追加

12. [アプリ] の [ウェブアプリとモバイルアプリ] から作成したカスタム SAML を選択し、[ユーザーアクセス] をクリックします

シングルサインオンの設定

Google Cloud Identity – カスタム SAML アプリの追加

13. グループを検索からマッピングするグループを選択、サービスのステータスを [オン] をチェック、[保存] をクリックします



シングルサインオンの設定

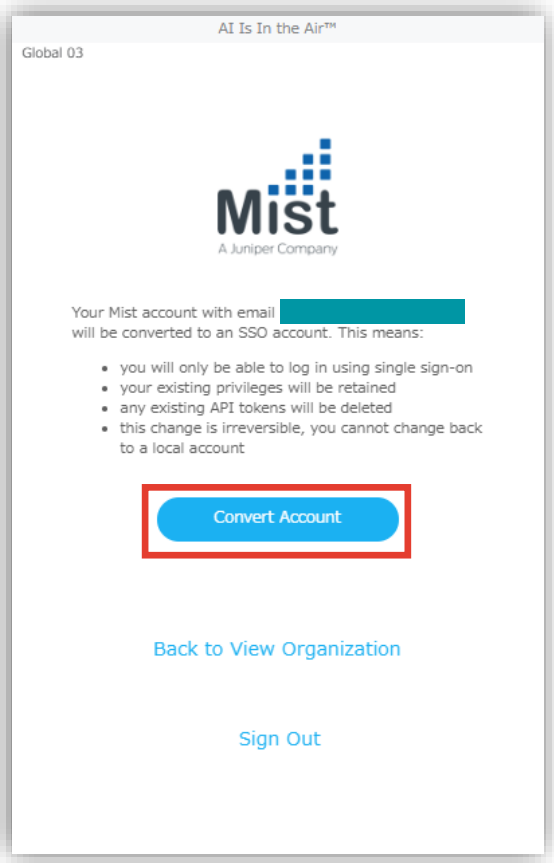
Google Cloud Identity – 動作テスト

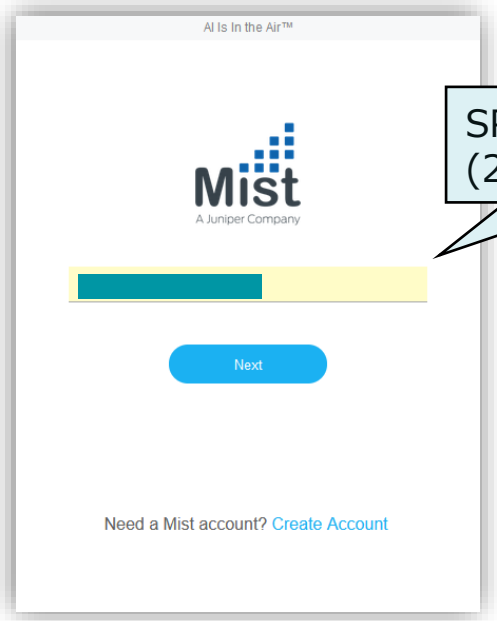
14. 画面右上の Google アプリから追加されたカスタム SAML アプリをクリックして、SSO を実行します

シングルサインオンの設定

Mist Cloud - SSO コンバート

14. Mist の管理画面に遷移するので、注意事項を確認し、[Convert Account] をクリックして、SSO ログインに移行します





SP Initiated SSO
(2回目以降)

NOTE

初回ログインは、IdP を起点とする SSO ログイン(IdP Initiated SSO) を実施します
以降のログインは、SP 起点の SSO ログイン(SP initiated SSO) も可能です


Thank you
JUNIPER
driven by Mist AI