

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

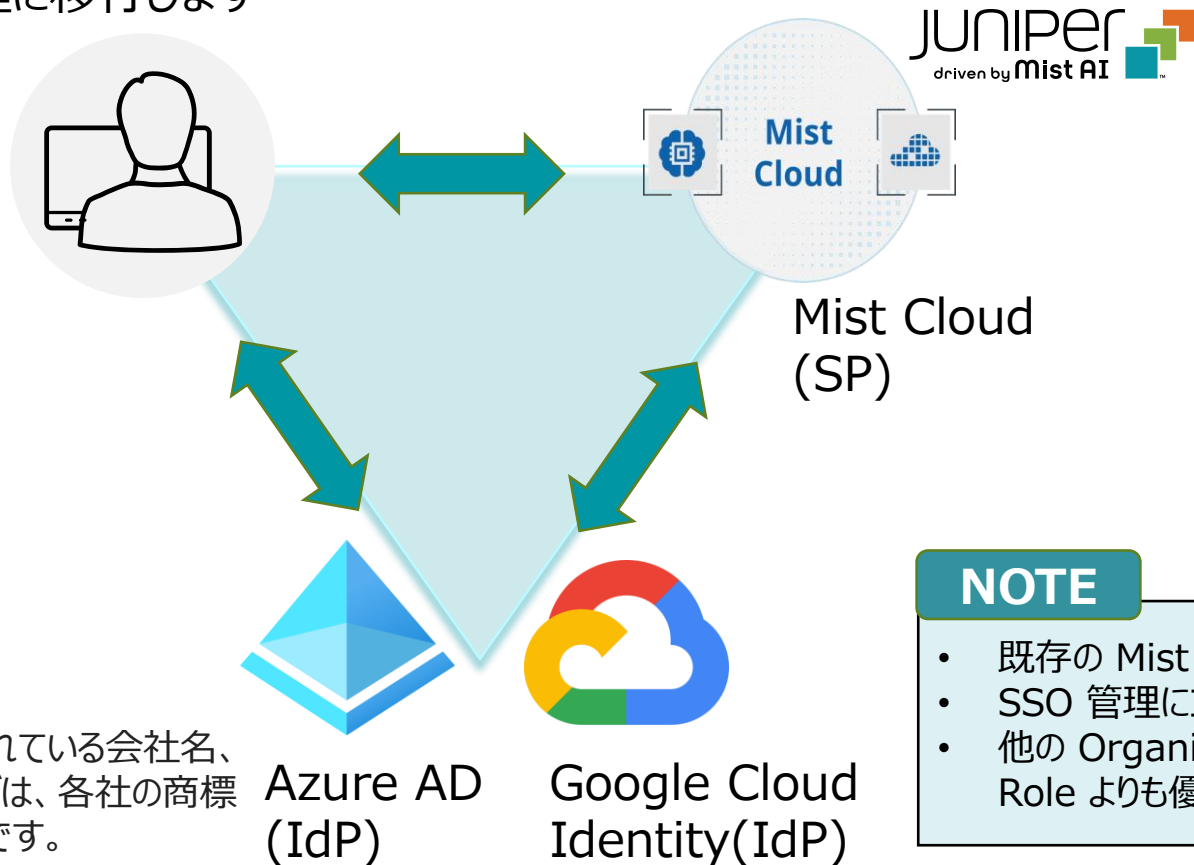
はじめに

- ❖ 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>

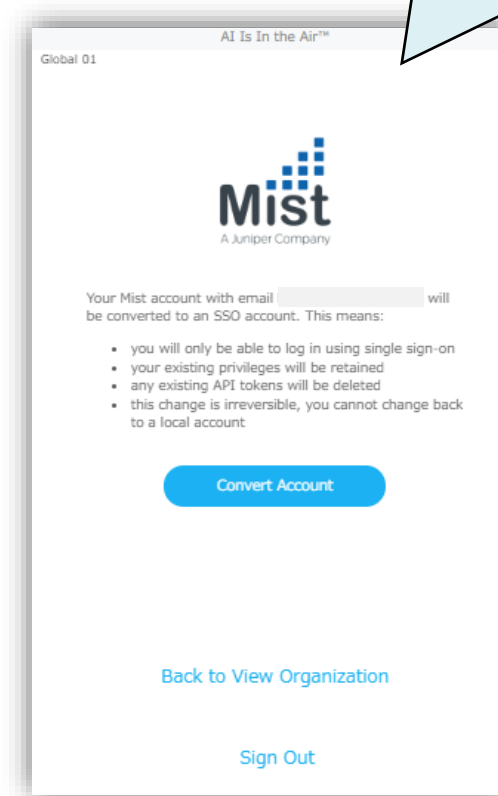
シングルサインオンの設定

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



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

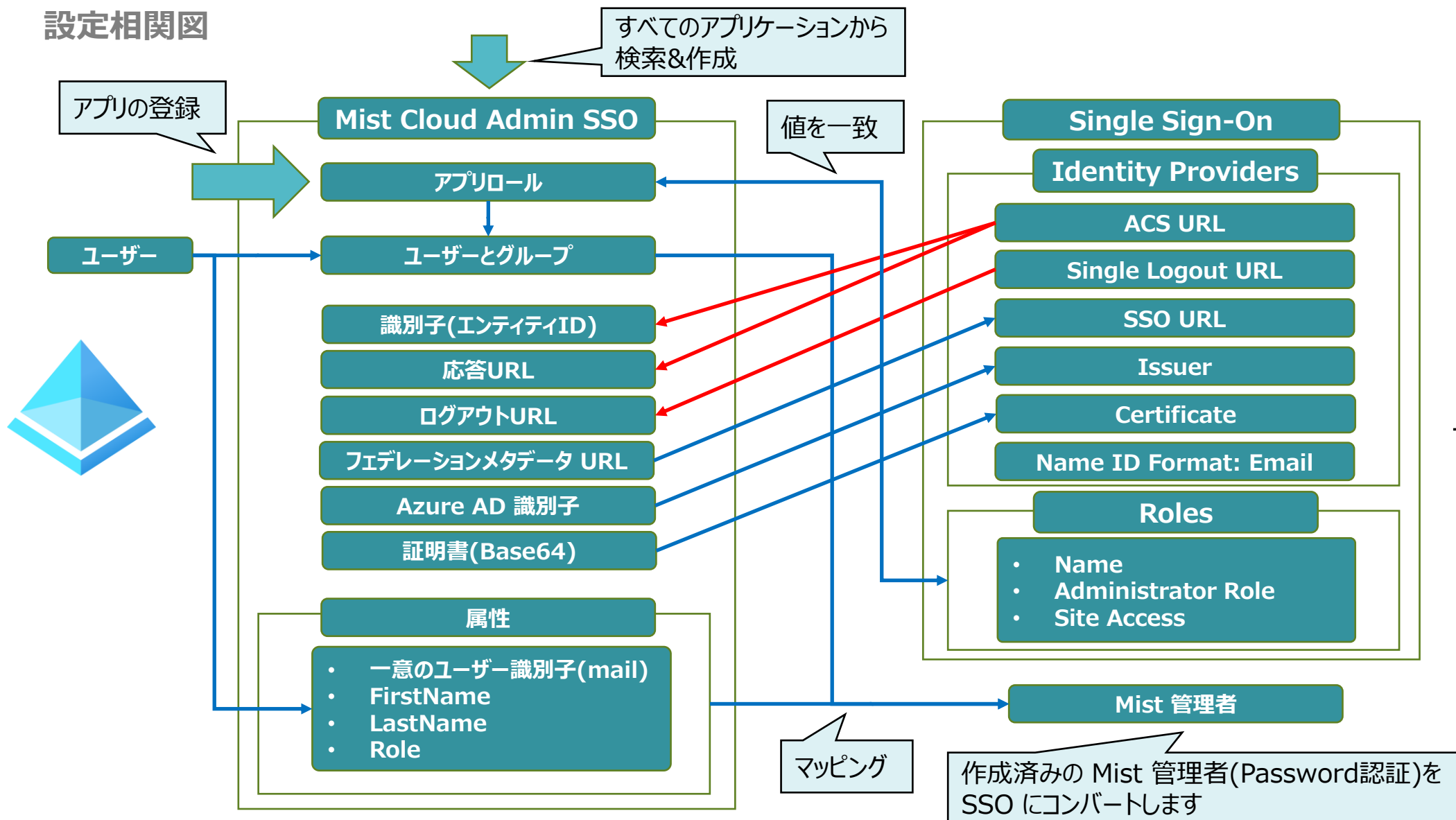
※本資料に記載されている会社名、製品名およびロゴは、各社の商標または登録商標です。



Azure AD

シングルサインオンの設定

設定関連図





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

The screenshot illustrates the process of creating a single sign-on (SSO) for Mist Cloud Admin SSO in Azure AD. It is divided into three main panels:

- Left Panel (Azure AD Enterprise Applications):** Shows the 'すべてのアプリケーション' (All Applications) view. A red dashed arrow points from the '+ 新しいアプリケーション' (New Application) button to the search bar in the middle panel.
- Middle Panel (Azure AD Gallery Reference):** Shows the search results for 'Mist Cloud'. A red dashed arrow points from the search bar to the 'Mist Cloud Admin SSO' application card. Below the card, a red dashed arrow points to the '作成' (Create) button in the right panel.
- Right Panel (Mist Cloud Admin SSO Configuration):** Shows the configuration page for the 'Mist Cloud Admin SSO' application. The '名前' (Name) field is filled with 'Mist Cloud Admin SSO'. The '発行元' (Issuer) is 'Juniper Networks'. The 'シングルサインオンモード' (Single Sign-On Mode) is set to 'SAML ベースのサインオン リンクされたサインオン' (SAML-based sign-on linked sign-on). The 'URL' is 'https://www.mist.com'. A red dashed arrow points from the '作成' (Create) button in this panel to the '作成' (Create) button in the bottom right corner of the overall screenshot.



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

The screenshot shows the Azure AD portal interface. The navigation path is highlighted with red dashed arrows:

- Start at the 'App Registrations' link in the left sidebar.
- Click on 'All Applications' in the main content area.
- Click on the 'Mist Cloud Admin SSO' application.
- Click on the '+ Create Application Role' button.

The 'Create Application Role' dialog box is shown with the following fields and callouts:

- 表示名 ***: Mist Admin SSO (Callout: 表示名は任意です)
- 許可されたメンバーの種類 ***: ユーザーまたはグループ (Callout: Mist で設定する値と一致させます)
- 値 ***: MistAdminSSO (Callout: Mist で設定する値と一致させます)
- 説明 ***: Mist Admin SSO role (Callout: 説明を入力(任意))
- このアプリ ロールを有効にしますか?**:
- Buttons: 適用 (Apply), キャンセル (Cancel)



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

変更する場合は、**[割り当ての編集]**

必要に応じて、ユーザーまたはグループを追加して Role を割り当てます

割り当ての編集 ...

ユーザー

1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

選択されていません

概要

Azure AD テナントを ID プロバイダーとして使用するよう設定された

アプリケーションの種類 == エンタープライズ アプリケーション

0個のアプリケーションが見つかりました

名前	オブジェクト ID
Mist Cloud Admin SSO	b07e55e4-b4...

ホーム > 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 > Mist Cloud Admin SSO

Mist Cloud Admin SSO | ユーザーとグループ ...

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

セルフサービス

カスタム セキュリティ属性 (プレビュー)

+ ユーザーまたはグループの追加

割り当ての編集

削除

資格情報の更新

列

...

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。これを表示しないようにするには、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...

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		



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

割り当ての追加 ...
既定のディレクトリ

グループ割り当ては未検証

お客様の Active Directory プランレベルでは、グループを割り当てるできません。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

Mist Admin SSO

既に割り当て済みの場合確認のみ

ユーザーを選択

検索

検索できます

検索

選択されたアイテム

削除

選択

ロールを選択してください ×
選択できるロールは 1 つのみです

検索

検索できます

Mist Admin SSO

選択されたロール

ロールが選択されていません。

選択

割り当ての追加 ...

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。

ユーザー

1 人のユーザーが選択されました。

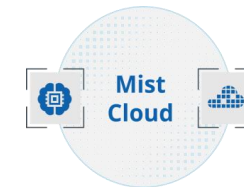
ロールを選択してください

Mist Admin SSO

割り当て

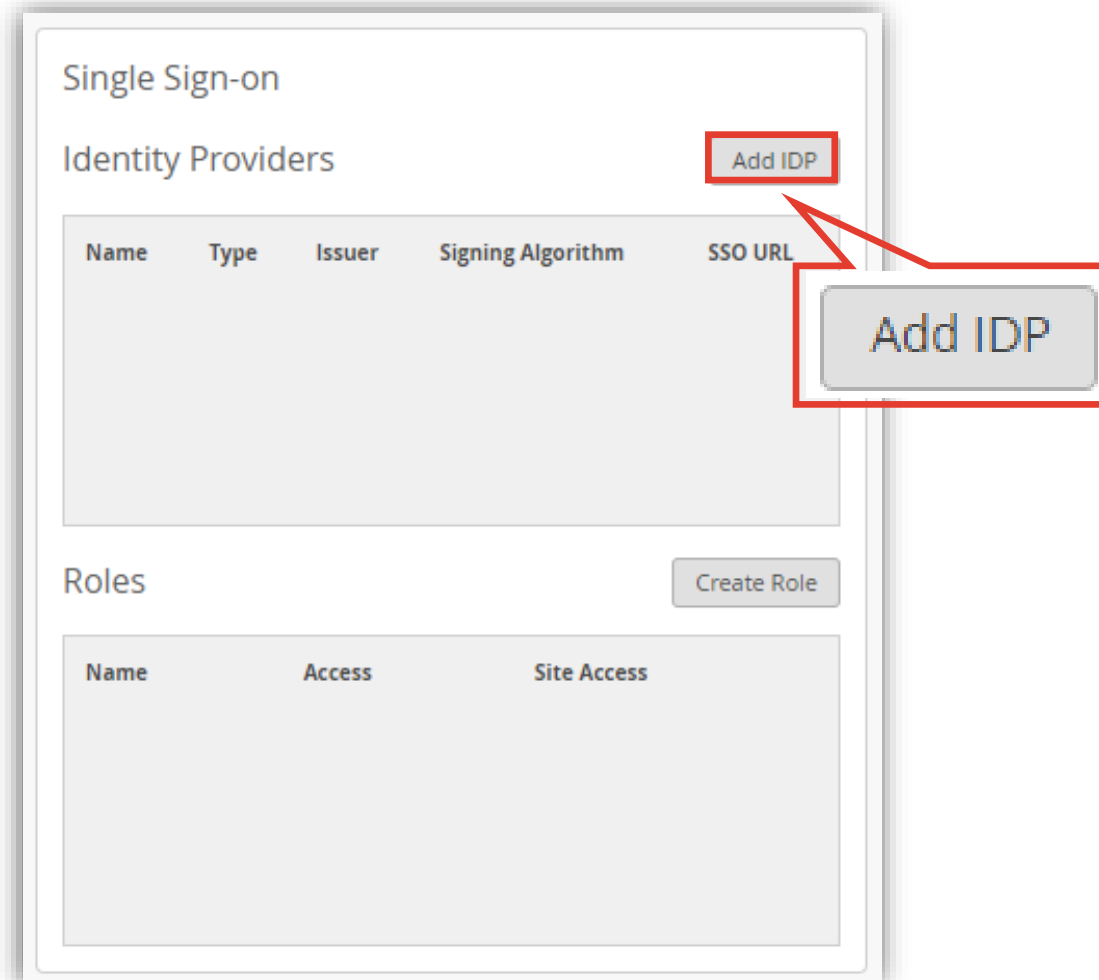
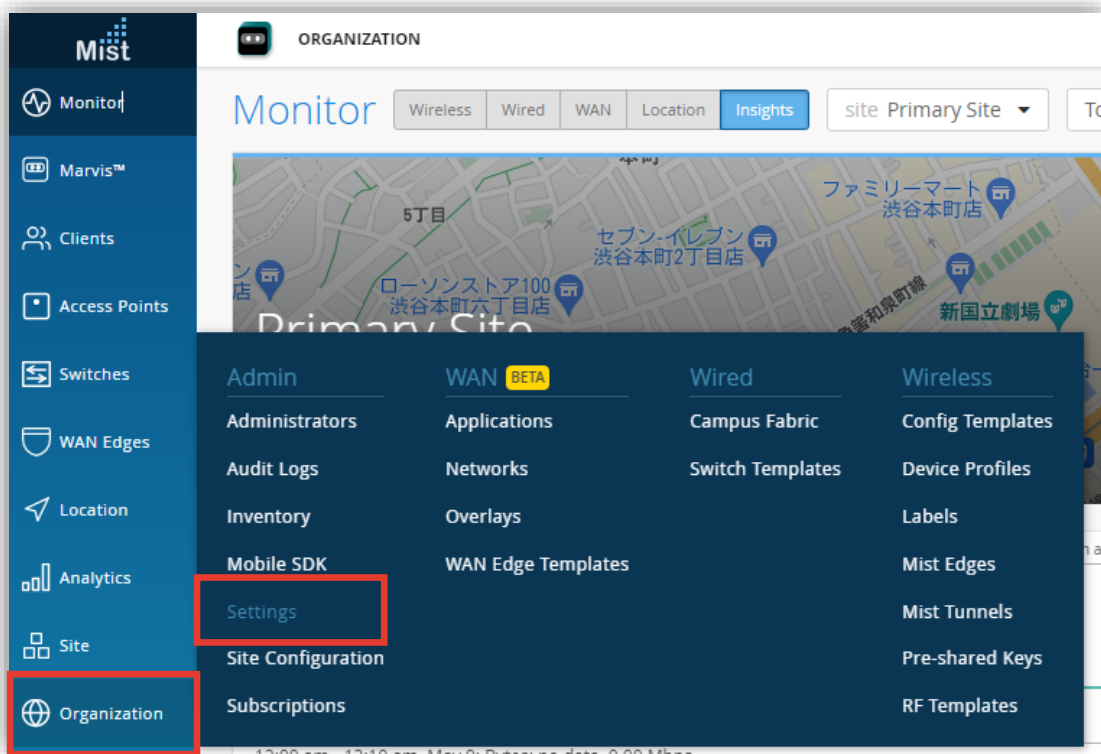
シングルサインオンの設定

Mist Cloud – SSO (IDP) の設定



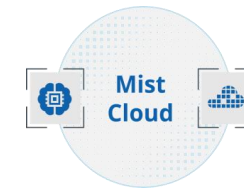
5. [Organization] から [Settings] を選択します

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

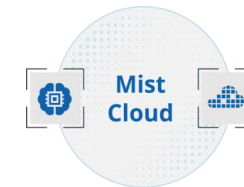
Issuer / Certificate / SSO URL は、
後述の Azure AD で設定した値を貼り付
けます(p.19)

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

Single Sign-on

Identity Providers Add IDP

Name	Type	Issuer	Signing Algorithm	SSO URL
test	SAML			
SAML SSO	SAML			

Roles Create Role

Name	Access	Site Access
------	--------	-------------

Create Role

Name
MistAdminSSO

Access Level

Super User
Full access to all sites, able to create new sites and manage other administrators

Network Admin
Full access to selected sites

Observer
Monitor only access to selected sites

Installer
Access limited to installing APs and Switches at selected sites

Helpdesk
Helpdesk monitoring and workflow for selected sites

Site Access

All Sites Site Groups Specific Sites

Create Cancel

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

ホーム > Mist Cloud Admin SSO

Mist Cloud Admin SSO | 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
- 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
 - 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

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。
- 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。



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

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](#) Mist Cloud Admin SSO test を統合するためのヘルプ。

- 1** 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
- 2** 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
FirstName	user.givenname
LastName	user.surname
Role	user.assignedroles
一意のユーザー ID	user.userprincipalname

- 3** SAML 証明書
トークン署名証明書 編集

状態	アクティブ
拇印	F8A23743D9CD4786D1A1FC66799A17A9B1D919EC
有効期限	2027/10/3 3:06:49
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/d1db1fde-f083-...
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

検証証明書 (オプション) 編集

必須	いいえ
アクティブ	0
有効期限切れ	0
- 4** 重要な推奨事項: Azure AD のブラウザー拡張機能のインストール
My Apps Secure Sign-in ブラウザー拡張機能は既にインストールされています。構成を続けてください。
- 5** Mist Cloud Admin SSO test のセットアップ
Azure AD とリンクするアプリケーションを構成する必要があります。
⚠ 手順 1 で必須フィールドに入力してください
✅ マイアプリ拡張機能をダウンロードします
[Mist Cloud Admin SSO test のセットアップ](#)
▼ 構成 URL
ログイン URL、ログアウト URL、Azure AD 識別子
- 6** Mist Cloud Admin SSO test でシングル サインオンを Test
シングル サインオンが機能していることを Test します。ユーザーがサインインするには、ユーザーをユーザー とグループに追加しておく必要があります。
⚠ 手順 1 で必須フィールドに入力してください
[Test](#)



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

基本的な SAML 構成

保存 フィードバックがある場合

識別子 (エンティティ ID) * ⓘ
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。

既定
https://api.ac2.mist.com/api/[redacted]/login

識別子の追加
パターン: https://api.MISTCLOUDREGION.mist.com/api/v1/saml/SSOUNIQUEID/login

応答 URL (Assertion Consumer Service URL) * ⓘ
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) と呼ばれます。

https://api.ac2.mist.com/api/[redacted]/login

応答 URL の追加
パターン: https://api.<MISTCLOUDREGION>.mist.com/api/v1/saml/<SSOUNIQUEID>/login

ログアウト URL (省略可能)
この URL は、SAML ログアウト応答をアプリケーションに返送するために使用します。

https://api.ac2.mist.com/api/[redacted]/logout

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

Create Identity Provider

Issuer is required

JUNIPER
driven by Mist AI

Name
SAML SSO

Type
SAML

Issuer

Name ID Format
 Email Unspecified

Signing Algorithm
SHA256

Certificate

SSO URL

Custom Logout URL

ACS URL
https://api.mist.com/api/v1/saml/abq4p4

Single Logout URL
https://api.mist.com/api/v1/saml/abq4p4

Save Cancel

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

属性とクレーム ...

+ 新しいクレームの追加 + グループ要求を追加する ≡ 列 | フィードバックがある場合

必要な要求

クレーム名	種類	値
一意のユーザー識別子 (名前 ID)	SAML	user.userprincipalname [...]
FirstName	SAML	user.givenname
LastName	SAML	user.surname
Role	SAML	user.assignedroles

追加の要求

クレーム名	種類	値	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail	🗑️ 削除
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname	⋮
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname	⋮
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname	⋮

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

属性とクレーム ...

+ 新しいクレームの追加 + グループ要求を追加する ≡ 列 | 🔍 フィードバックがある場合

必要な要求

クレーム名	種類	値
一意のユーザー識別子 (名前 ID)	SAML	user.userprincipalname [...]
FirstName	SAML	user.givenname ...
LastName	SAML	user.surname ...
Role	SAML	user.assignedroles ...

追加の要求

クレーム名	種類	値
-------	----	---

要求の管理 ...

📁 保存 ✕ 変更の破棄 | 🔍 フィードバックがある場合

名前

名前空間

名前識別子の形式の選択

名前識別子の形式 *

ソース * 属性 変換 ディレクトリスキーマ拡張 (プレビュー)

ソース属性 *

要求条件

SAML クレームの詳細オプション

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

3 SAML 証明書

トークン署名証明書

状態 アクティブ 編集

拇印 DBDD39221FE8216216F1F7A57F45B585CA4C64AD

有効期限 2026/6/5 17:23:19

通知用メール com

アプリのフェデレーション メタデータ URL <https://login.microsoftonline.com/d1db1fde-f083-...>

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

検証証明書 (オプション)

必須 いいえ

アクティブ 0

有効期限切れ 0



証明書 (Base64)

SAML 署名証明書

アプリに対して発行される SAML トークンに署名するために Azure AD によって使用される証明書を管理します

保存 + 新しい証明書 ↑ 証明書のインポート | フィードバックがある場合

状態	有効期限	拇印
アクティブ	2025/5/9 19:38:28	82A513629D453938E272D3D824F1EEABB8137F98

署名オプション SAML 応答とアサーションへの署名

署名アルゴリズム

- SAML 応答への署名
- SAML アサーションへの署名
- SAML 応答とアサーションへの署名**

通知の電子メール アドレス

.com



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

3 SAML 証明書

トークン署名証明書

状態: アクティブ

押印: 26A97D1EF785

有効期限: 2026/6/15 22:07:34

通知用メール: mocha_nico@outlook.jp

アプリのフェデレーションメタデータ URL: <https://login.microsoftonline.com/8e24b375...>

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

検証証明書 (オプション): 編集

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

5 Mist Cloud Admin SSO のセットアップ

Azure AD とリンクするアプリケーションを構成する必要があります。

- 手順 1 で必須フィールドに入力してください
- マイ アプリ拡張機能をダウンロードします

Mist Cloud Admin SSO のセットアップ

構成 URL

- ログイン URL: <https://login.microsoftonline.com/8e24b...>
- Azure AD 識別子: <https://sts.windows.net/8e24b375-a0be...>
- ログアウト URL: <https://login.microsoftonline.com/8e24b...>

Azure AD 識別子を Issuer にコピー

Edit Identity Provider

Name: SAML SSO

Type: SAML

Issuer: <https://sts.windows.net/d1db1fde-f083-4f59-b3...>

Name ID Format: Email (selected)

Signing Algorithm: SHA256

Certificate: -----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQR6roCMwmgYVAna33b

SSO URL: <https://login.microsoftonline.com/d1db1fde-f0...>

Custom Logout URL:

ACS URL: <https://api.mist.com/api/v1/saml/66npdt>

Single Logout URL: <https://api.mist.com/api/v1/saml/66npdt>

Buttons: Delete, Save, Cancel

JUNIPER driven by Mist AI

証明書 (Base64)

Mist Admin SSO.cer - メモ帳

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQR6roCMwmgYVAna33b
-----END CERTIFICATE-----
```

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

6 Mist Cloud Admin SSO でシングル サインオンをTest

シングル サインオンが機能していることをTestします。ユーザーがサインインするには、ユーザーをユーザーとグループに追加しておく必要があります。

Test

Mist Admin SSO でシングル サインオンをTest

フィードバックがある場合

サインオンをテストしています
ここでサインインして、Mist Admin SSO のシングル サインオン構成を Test します。Azure Active Directory 構成と Mist Admin SSO そのものの両方を構成したことを確認してください。

サインオンをテストする方法を選択

現在のユーザーとしてサインイン

他のユーザーとしてサインインする (ブラウザの拡張機能が必要)

サインインのテスト

エラーの解決
サインイン ページでエラーが発生する場合は、エラーを以下に貼り付けてください。同じ 이슈が生じる場合、数分間待って、再試行してください。

エラーの説明

要求 ID: 4f8ec053-fb71-47de-a010-2786a32f1900
関連付け ID: 5aa879f5-68f1-482a-a405-ff993d8f4cb0
タイムスタンプ: 2018-03-06T23:54:10Z
メッセージ: エラー AADSTSXXXX

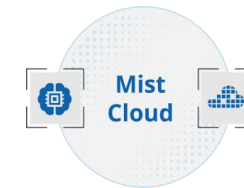
解決ガイドンスを入手する

IdP Initiated SSO

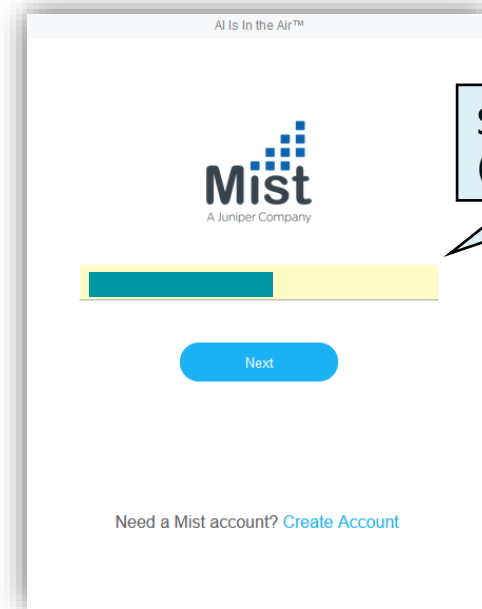
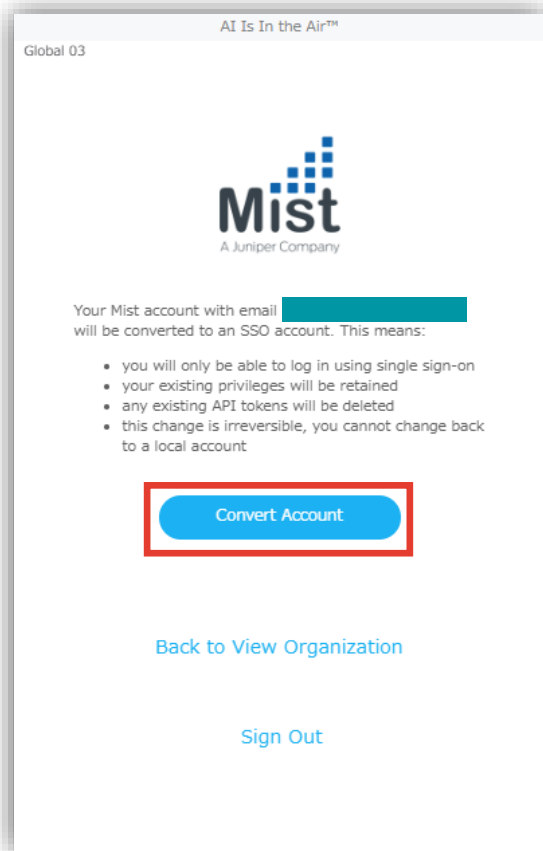
※現在ログインしているユーザ以外のテストはブラウザの拡張機能が必要です

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



NOTE

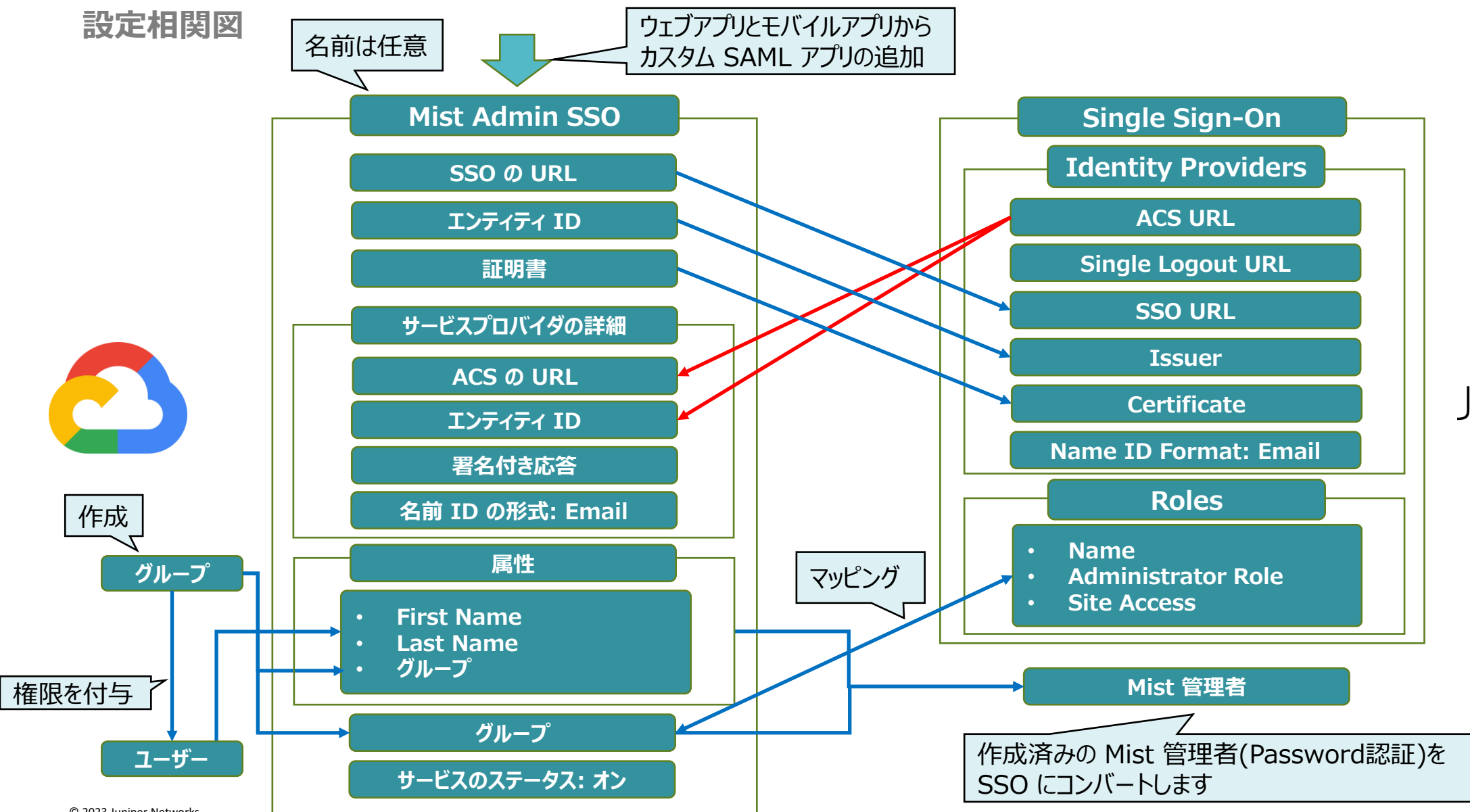
初回ログインは、IdP を起点とする SSO ログイン(IdP Initiated SSO) を実施します
以降のログインは、SP 起点の SSO ログイン(SP initiated SSO) も可能です



Google Cloud Identity

シングルサインオンの設定

設定関連図





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

The screenshot shows the Google Admin console interface. On the left sidebar, the 'Admin' menu is open, and 'ディレクトリ' (Directory) is selected. Under 'ディレクトリ', 'グループ' (Groups) is highlighted. The main content area shows the 'グループ' (Groups) page. At the top, there is a search bar and a notification. Below that, there are buttons for 'グループを作成' (Create Group) and 'グループの精査' (Audit Groups). A table below shows a list of groups with columns for 'グループ名' (Group Name), 'メールアドレス' (Email Address), 'メンバー' (Members), and 'アクセスタイプ' (Access Type). One group is listed: 'Classroom の教師' (Classroom Teachers) with email 'classroom_teachers@...', 0 members, and 'カスタム' (Custom) access type.



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

グループの詳細

グループ名*

Mist Admin

リストおよびメッセージでグループを識別するための名前を入力します。

グループのメールアドレス*

mistadmin @ [redacted]

グループのメールアドレスを入力します。

グループの説明

Mist Admin SSO Role

グループの目的や用途を入力します。

グループのオーナー

このグループのオーナーのロールを付与するユーザー。

[redacted] ユーザーの名前やメールアドレスを検索

ラベル NEW

セキュリティ

ポリシー（アクセス制御など）を適用するグループを簡単に識別して管理するには、グループにセキュリティ ラベルを追加します。[セキュリティグループの詳細](#)

⚠ 機密情報やリソースへのアクセスを制御するために使用します。このラベルを削除することはできません。

[次へ](#)



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

アクセスタイプ

メンバーのアクセスグループの権限を管理できます。詳細
注: 外部メンバーは、グループのメンバーを表示したり、グループのコンテンツを検索したりすることはできません。

公開 チーム 通知のみ 制限付き カスタム

一般公開
組織内のユーザーであれば誰でもグループへの投稿や参加が可能です

アクセス設定	グループの オーナー	グループの 管理者	グループの メンバー	組織 全体	外部
グループのオーナーに連絡できるユーザー	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
会話を閲覧できるユーザー	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
投稿できるユーザー	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
メンバーを表示できるユーザー	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
メンバーの管理 追加、招待、承認	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

グループに参加できるユーザー
ユーザーをグループに追加する方法を選択します

組織内のすべてのユーザーがリクエストできる
リクエストが必須で、承認されたらグループに参加できます

組織内のすべてのユーザーが参加できる
グループに自分を直接追加できます

招待されたユーザーのみ
招待された場合にのみグループに参加できます

組織外のメンバーの許可
この設定をオンにすると、外部ユーザーが参加できるようになります。
注: 外部メンバーシップの設定内容にかかわらず、いつでも Google 管理コンソールから外部ユーザーをグループに追加できます。

前へ **グループを作成**

✔ Mist Admin を作成しました

✔ 設定を保存しました

✔ オーナーを追加しました

次の操作

+ Mist Admin へのメンバーの追加

Mist Admin のグループの詳細を表示
詳細ページでは、グループのメンバーや設定などを確認できます

+ 別のグループを作成

完了



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

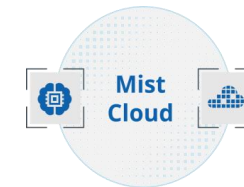
Google Cloud Identity – カスタム SAML アプリの追加

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

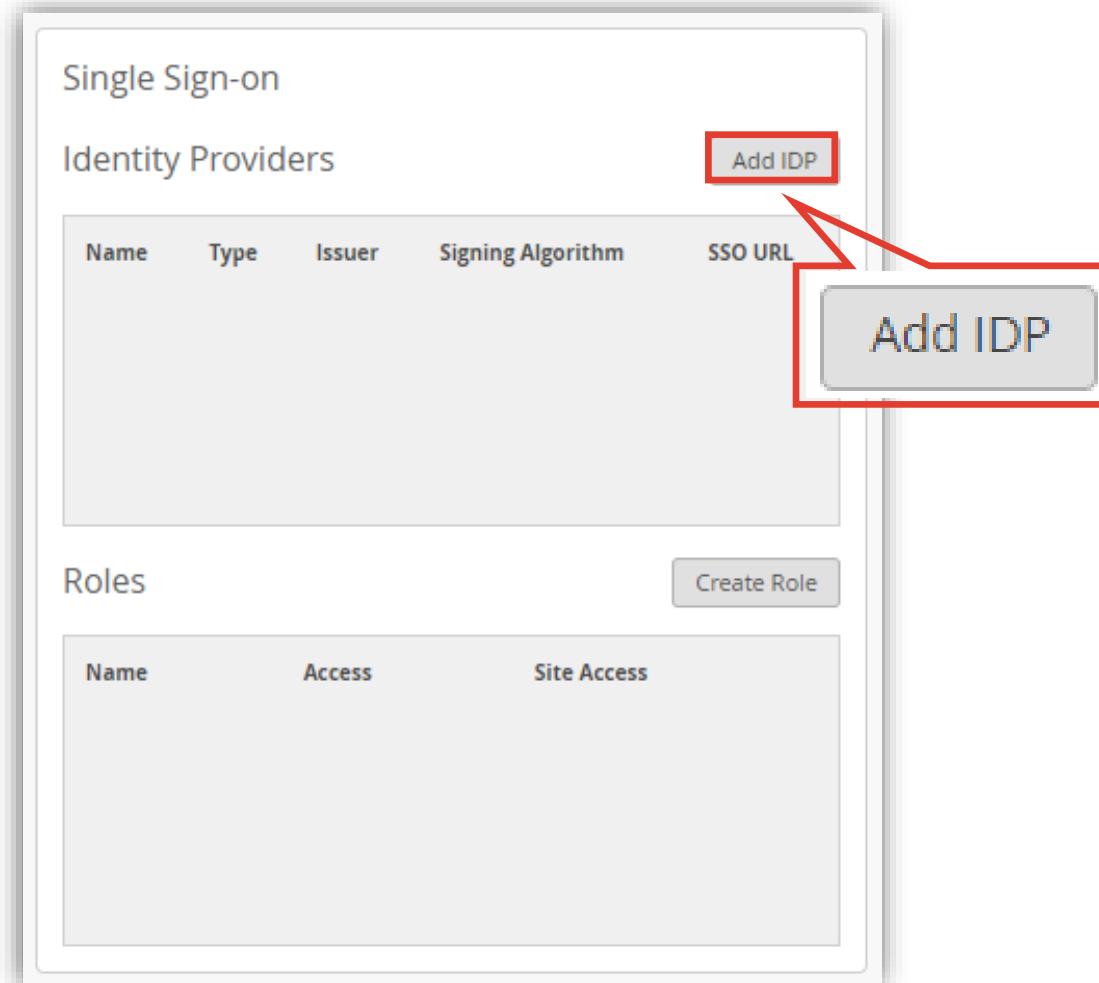
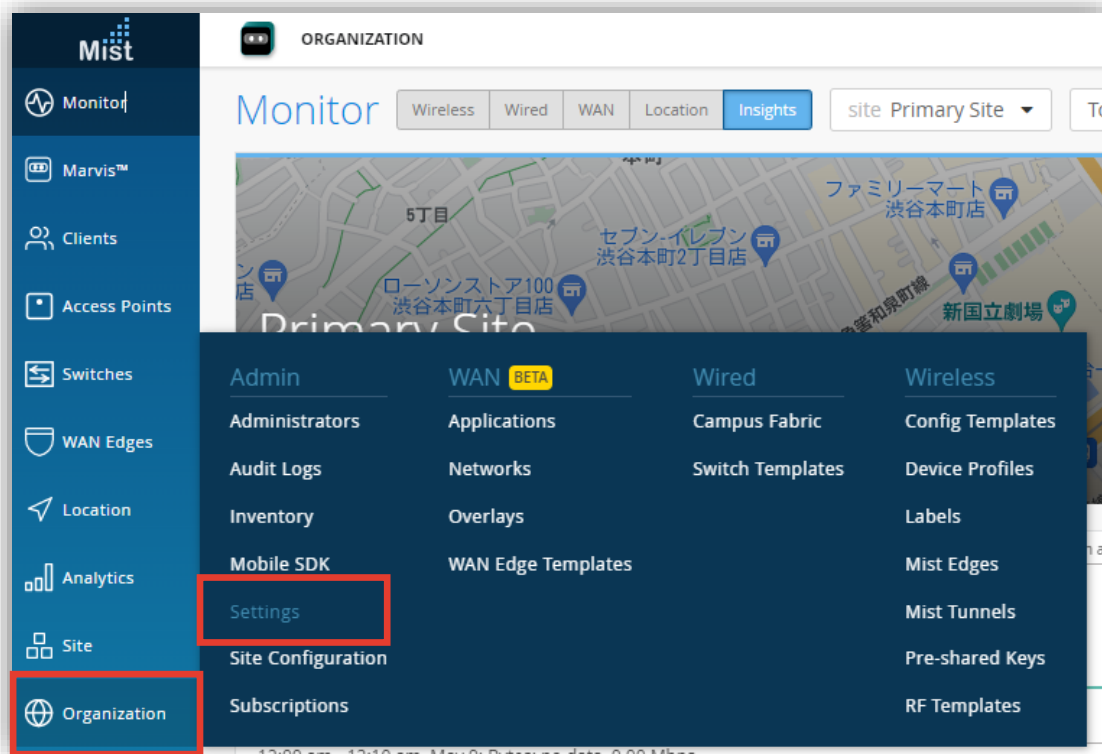
シングルサインオンの設定

Mist Cloud – SSO (IDP) の設定



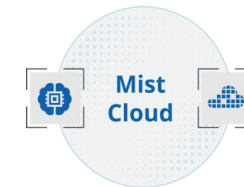
5. [Organization] から [Settings] を選択します

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



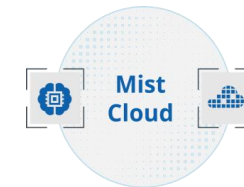
7. Google Cloud Identity で作成した「SSO の URL」、[エンティティ ID]、[証明書] をそれぞれ、[SSO URL]、[Issuer]、[Certificate] にコピーします
8. [ACS URL] をコピーして控え、[Save] をクリックします

The image shows a three-step process for configuring SSO in Mist Cloud:

- Step 1: Add Identity Provider**
 - Field: Name (Google SSO)
 - Buttons: Add, Cancel
 - Annotation: A blue box labeled "Add" points to the "Add" button.
- Step 2: Create Identity Provider**
 - Field: Name (Google SSO)
 - Field: Type (SAML)
 - Field: Issuer (https://accounts.google.com/o/saml2?idpid=C0) - Annotation: "エンティティ ID" (Entity ID)
 - Field: Name ID Format (Email selected) - Annotation: "Name ID Format は Email(デフォルト)" (Name ID Format is Email (default))
 - Buttons: Add, Cancel
- Step 3: Save Configuration**
 - Field: Signing Algorithm (SHA256)
 - Field: Certificate (j9XWPQm4T1EvErfwT0/sXLf73bCy7IBDcVRACu...oKKYn02D7XT1fhnmq/VHM3GiAdYq+rQZ5BklgrXu102LjI0GKNLgZMMVYbitTRwEFXv3Mt1INcQz0E1V7szclwbPddrG+SHNfm7bR0KCr4XFc1oktp) - Annotation: "証明書" (Certificate)
 - Field: SSO URL (https://accounts.google.com/o/saml2/idp?idpid) - Annotation: "SSO の URL" (SSO URL)
 - Field: Custom Logout URL
 - Field: ACS URL (https://api.ac2.mist.com/a...) - Annotation: "ACS URL をコピー" (Copy ACS URL)
 - Field: Single Logout URL (https://api.ac2.mist.com/a...)
 - Buttons: Save, Cancel

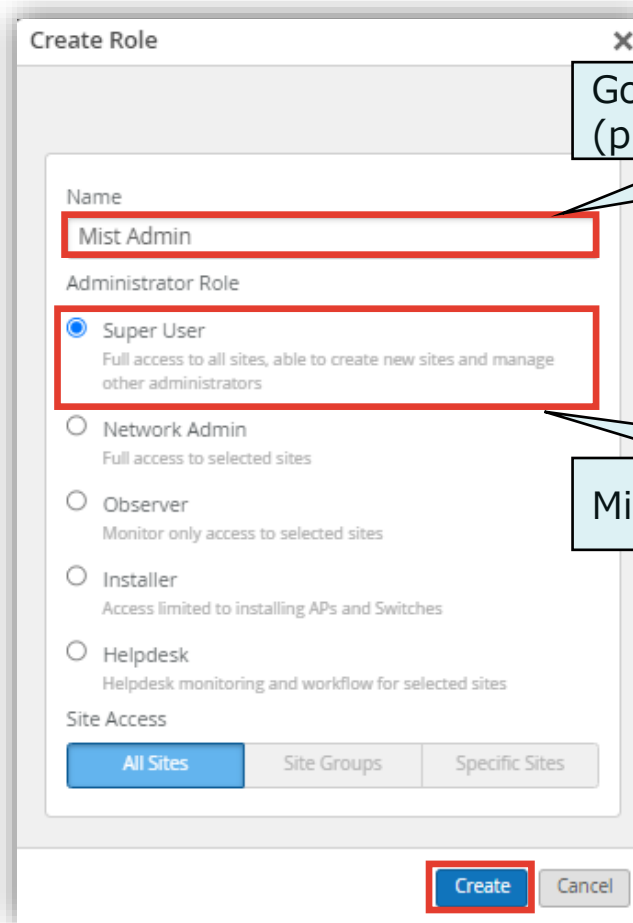
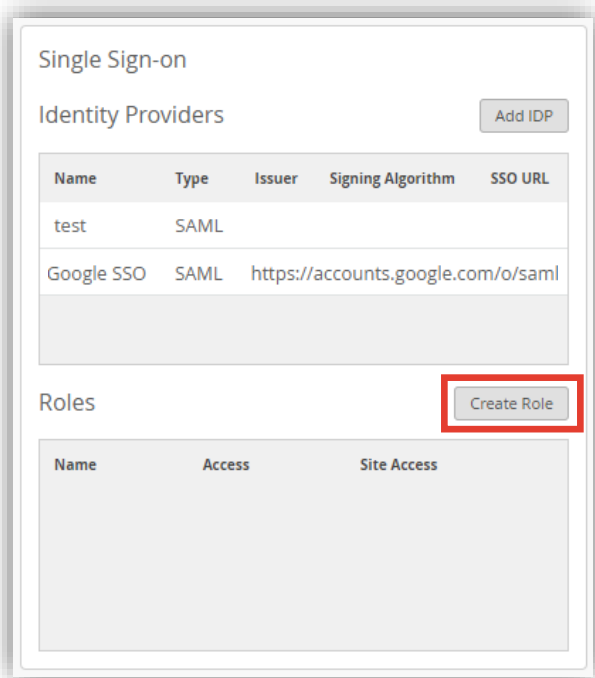
シングルサインオンの設定

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

- 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

サービスプロバイダの詳細
シングルサインオンを設定するには、サービスプロバイダの詳細情報（ACS の URL やエンティティ ID など）の入力が必要です。 [詳細](#)

ACS の URL
https://api.ac2.mist.com/api/v1/saml/tsza9ll0/login

エンティティ ID
https://api.ac2.mist.com/api/v1/saml/tsza9ll0/login

開始 URL（省略可）

署名付き応答

名前 ID
ID プロバイダでサポートされる名前の形式を定義します。 [詳細](#)

名前 ID の形式
EMAIL

名前 ID
Basic Information > Primary email

戻る キャンセル

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

属性

Google Directory のユーザー フィールドを追加および選択し、サービスプロバイダの属性にマッピングしてください。*の付いた属性は必須です。 [詳細](#)

Google Directory の属性	アプリの属性
Basic Information > First name	FirstName
Basic Information > Last name	LastName

マッピングを追加

グループメンバー (省略可)

ここで追加したいいずれかのグループにユーザーが属している場合は、グループメンバー情報を SAML レスポンスで送信できます。

Google グループ	アプリ属性
Mist Admin	Role

戻る キャンセル 完了

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

The screenshot shows the Google Cloud Identity Admin console interface. The left sidebar contains navigation options: Home, Directory, Devices, **アプリ** (Applications), Summary, Google Workspace, Other Google Services, **ウェブアプリとモバイルアプリ** (Web and mobile apps), Google Workspace Marketplace apps, and Billing. The main content area is titled 'アプリ > ウェブアプリとモバイルアプリ > Mist Admin SSO'. It displays the application's SAML configuration, including a 'ユーザーアクセス' (User Access) section with a dropdown arrow, a 'サービスプロバイダの詳細' (Service provider details) section, and a table of configuration parameters.

証明書	ACS の URL	エンティティ ID
Google_2028-6-3-8154_SAML2_0 (有効期限: 2028/06/04)	https://api.ac2.mist.com/api/v1/saml/	https://api.ac2.mist.com/api/v1/saml/



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

The screenshot shows the Google Cloud Identity Admin console interface. The left sidebar contains navigation options like 'Admin', 'アプリ', '概要', 'Google Workspace', and 'ウェブアプリとモバイルアプリ'. The main content area displays the 'Mist Admin SSO' service configuration. The 'サービスのステータス' (Service Status) section is highlighted with a red box, showing the status as 'オン' (On) with a checked checkbox. The 'グループ' (Groups) section is also highlighted with a red box, showing a search result for 'Mist Admin' with the email address 'mistadmin@'. A '保存' (Save) button is highlighted with a red box at the bottom right of the page.



シングルサインオンの設定

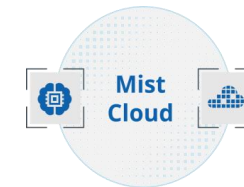
Google Cloud Identity – 動作テスト

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

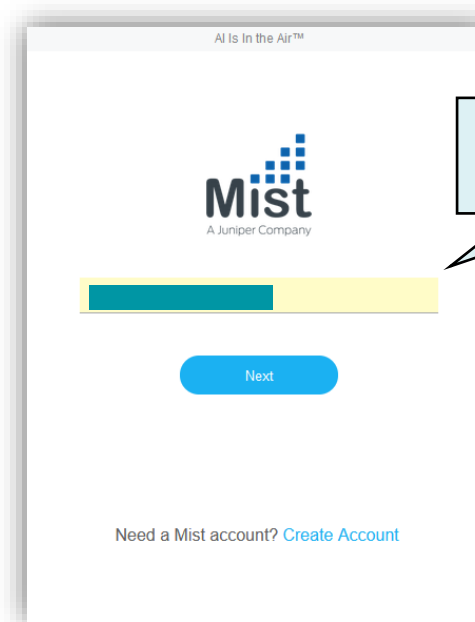
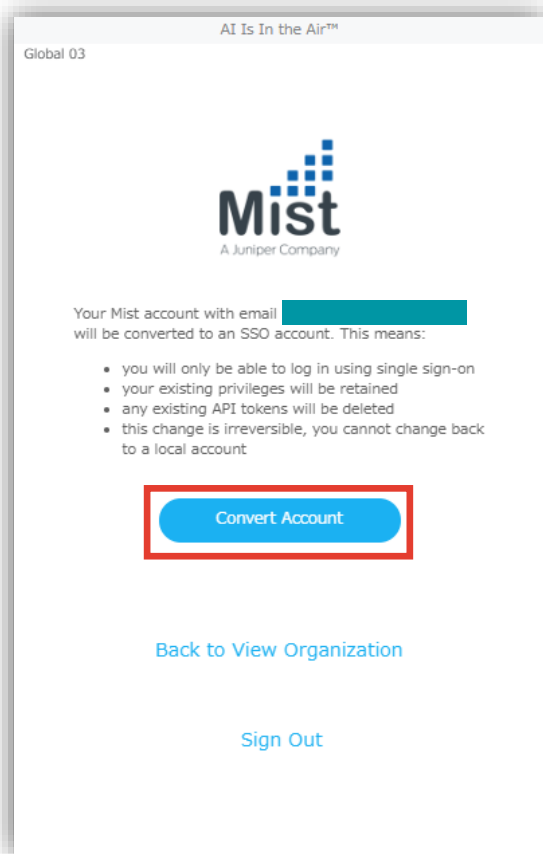


シングルサインオンの設定

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



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 