



JCCH・セキュリティ・ソリューション・システムズ

プライベート認証局Gléas ホワイトペーパー

シングルサインオンによるGléas UAログイン (Azure AD 連携)

Ver.1.1

2022 年 9 月

- ・ JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
- ・ その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
- ・ Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

目次

1. はじめに	5
1.1. 本書について	5
1.2. 本書における環境	5
1.3. 本書における構成	7
2. AD の設定	8
2.1. SSL 証明書をインポート	8
3. Gléas アカウントの登録	11
3.1. AD ユーザ情報をインポート	11
4. SAML SP 署名用証明書の発行	14
5. AzureAD の設定	16
5.1. AD ユーザ情報を同期	16
5.2. エンタープライズ アプリケーションの登録	17
5.3. エンタープライズ アプリケーションの割り当て	26
6. Gléas の管理者設定 (Windows 向け)	27
7. クライアントからのアクセス (Windows)	30

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

7.1.	シングルサインオンで UA にログイン	30
7.2.	クライアント証明書のインポート	32
8.	Gléas の管理者設定 (iPhone 向け)	34
9.	クライアントからのアクセス (iPhone)	38
9.1.	シングルサインオンで UA にログイン	38
9.2.	クライアント証明書のインポート	40
10.	Gléas の管理者設定 (Android 向け)	43
11.	クライアントからのアクセス (Android)	48
11.1.	シングルサインオンで UA にログイン	48
11.2.	クライアント証明書のインポート	50
12.	問い合わせ	53

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベート認証局 Gléas」のユーザ申込局 UA を、Azure Active Directory のエンタープライズ アプリケーションとして登録し、シングルサインオンで UA にログインする環境の設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、最終項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

- SAML IDP : Microsoft Azure Active Directory

※以後「Azure AD」と記載します

- SAML SP : JS3 プライベート認証局 Gléas (バージョン 2.6.0) UA

※以後「UA」と記載します

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

➤ ドメインコントローラ : Microsoft Windows Server 2019

※以後「AD」と記載します

➤ JS3 プライベート認証局 Gléas (バージョン 2.6.0)

※以後「Gléas」と記載します

➤ クライアント : Windows 10 Pro (21H1) / Microsoft Edge 104.0.1293.70

※以後「Windows」と記載します

➤ クライアント : iPhone X (iOS 16) / Safari

※以後「iPhone」と記載します

➤ クライアント : Google Pixel5 (Android 13) / Chrome

※以後「Android」と記載します

以下については、本書では説明を割愛します。

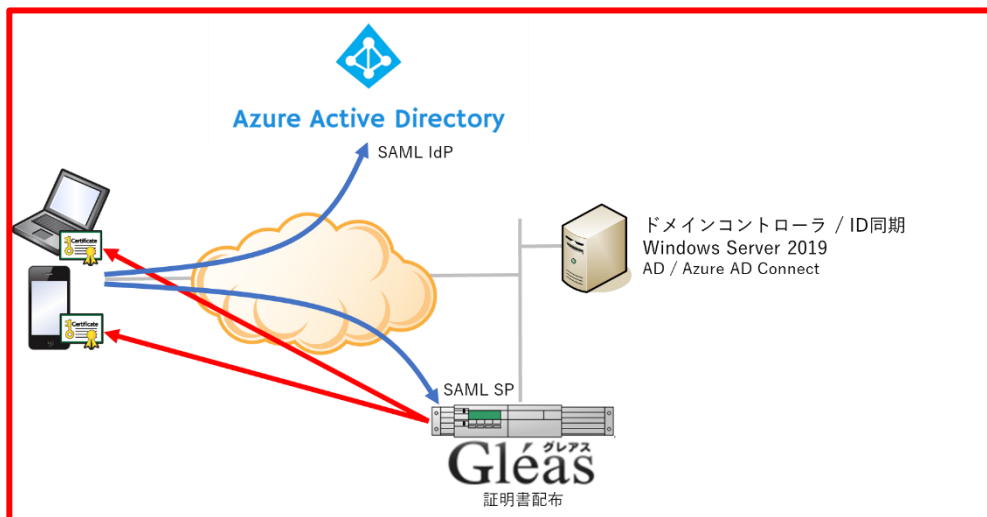
- Azure ADの基本設定
- Azure AD ConnectによるADユーザの同期操作
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作
- Windows、iPhone での UA へのログイン方法

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている

販売店にお問い合わせください。

1.3. 本書における構成

本書では、以下の構成で検証を行っています。



1. Windowsでは、EdgeブラウザからUAへアクセス試行する
2. 認証連携先のAzure ADのログイン画面に画面遷移。Azure ADはパスワードを要求し、認証成功するとUAにログインした状態になる
3. iPhoneでは、SafariブラウザからUAへアクセス試行する
4. 認証連携先のAzure ADのログイン画面に画面遷移。Azure ADはパスワードを要求し、認証成功するとUAにログインした状態になる
5. Androidでは、ChromeブラウザからUAへアクセス試行する
6. 認証連携先のAzure ADのログイン画面に画面遷移。Azure ADはパスワードを要求し、認証成功するとUAにログインした状態になる

2. AD の設定

2.1. SSL 証明書をインポート

ADにSSL証明書をインポートして、LDAPSを有効化します。

ADサーバのFQDNが記載されたSSL証明書を準備します。

※SSL証明書はGléasから発行することも可能です。詳しくはお問い合わせください。

PKCS#12(.pfx)形式の SSL 証明書を AD サーバにコピーします。

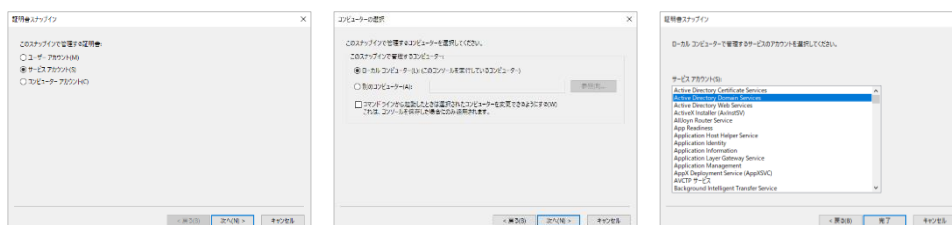
MMC を開き、メニューの[ファイル(F)] > [スナップインの追加と削除(N)]より[証明書]を追加します。

「証明書のスナップイン」では、[サービス アカウント(S)]を選択し、

次の「コンピューターの選択」では、[ローカルコンピューター(L)]を選択し、

次の「証明書スナップイン」では、[Active Directory Domain Services]]を選択し、

[完了]をクリックします。



プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

スナップインが追加されたら左ペインより[証明書-ローカルコンピューター上のサービス] > [NTDS ¥ 個人]と展開し、中央ペインで右クリックして、[すべてのタスク(K)] > [インポート(I)]をクリックします。

「証明書のインポートウィザード」が開始されるので、SSL 証明書をインポートします。



ページ	設定
証明書のインポートウィザードの開始	[次へ(N)]をクリック
インポートする証明書ファイル	SSL 証明書ファイル (拡張子 : p12/pfx) を指定して、[次へ(N)]をクリック
秘密キーの保護	SSL 証明書のパスフレーズを入力して、[次へ(N)]をクリック
証明書ストア	[証明書をすべて次のストアに配置する(P)]を選択し、[証明書ストア]に[NTDS ¥ 個人]が指定されていることを確認し、[次へ(N)]をクリック
証明書インポートウィザードの終了	[完了(F)]をクリック

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

中央ペインで右クリックして、[最新の情報に更新(F)]をクリックします。

左ペインより[証明書-ローカルコンピューター上のサービス] > [NTDS¥個人] > [証明書] と展開すると、インポートされた証明書が確認できます。

※中央ペインにルート証明書がある場合には、ルート証明書を選択し、左ペインの[証明書-ローカルコンピューター上のサービス] > [NTDS¥信頼されたルート証明機関] > [証明書] に移動してください。

3. Gléas アカウントの登録

3.1. AD ユーザ情報をインポート

AD のユーザ情報を LDAPS で Gléas のアカウントとしてインポートします。

GléasのRA (登録局) にログインします。

[アカウント]>[アカウント新規作成]メニューから[上級者向け設定] をクリックします。

The screenshot shows the 'アカウント情報' (Account Information) form in the Gléas management console. The '種類' (Type) is set to 'LDAP'. The '指定方法' (Designation Method) is set to 'ホスト名' (Host Name). The 'ホスト名' (Host Name) field is populated with 'gléas.local'. The 'ポート番号' (Port Number) is '389'. The 'Base DN' is 'OU=gléas,DC=gléas,DC=local'. The '管理者DN' (Administrator DN) is 'CN=admin,CN=gléas,DC=gléas,DC=local'. The 'パスワード' (Password) is masked with '*****'. The '検索フィルタ' (Search Filter) is '(objectClass=person)'. The 'グループメンバー属性' (Group Member Attribute) is 'memberOf'. The '前回のインポート' (Previous Import) checkbox is checked. The '属性のマッピング' (Attribute Mapping) is set to 'カスタム設定' (Custom Setting). The 'Gléasの属性' (Gléas Attributes) table shows 'アカウント名' (Account Name) mapped to 'userPrincipalName', '名前(姓)' (Name (Last Name)) mapped to 'sn', '名前(名)' (Name (First Name)) mapped to 'givenName', 'メールアドレス' (Email Address) mapped to 'mail', 'パスワード' (Password) is a text field, and 'プリンシパル名' (Principal Name) mapped to 'userPrincipalName'. The 'LDAPの属性' (LDAP Attributes) table is empty. A '作成' (Create) button is at the bottom.

Gléasの属性	LDAPの属性
アカウント名	userPrincipalName
名前(姓)	sn
名前(名)	givenName
メールアドレス	mail
パスワード	
プリンシパル名	userPrincipalName

- [種類]から[LDAP]を選択
- [指定方法]に[ホスト名]を選択
- [ホスト名]に AD のホスト名を入力

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

- [ポート番号]に “636” を入力
- [BaseDN]にユーザ情報の検索対象となるベース DN を入力
- [管理者 DN]に BaseDN 以下にアクセスできる AD 管理者の DN を入力
- [パスワード]に AD 管理者のパスワードを入力
- [検索フィルタ]に “(objectClass=person)” を入力
- [属性のマッピング]に[カスタム設定]を入力
- [Gléas の属性]に Gléas のアカウントと LDAP 属性の紐づけを入力

Gléas の属性	LDAP の属性
アカウント名	userPrincipalName
名前 (姓)	sn
名前 (名)	givenName
メールアドレス	mail
パスワード	空欄
プリンシパル名	userPrincipalName

- [作成]をクリック

※[証明書を作成する]をチェックすると、インポートと一緒に証明書の発行が行われます。

インポート内容の確認

指定したファイルの内容

指定されたファイルの最初の4件を表示しています。
下部の「実行」ボタンを押すと、以下のファイルの内容がアカウント登録申請者一覧に反映されます。

指定されたファイルの最初の4件

アカウント名	姓	名	メールアドレス	プリンシパル名
XXXXXXXXXXXXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXXXXXXXXXXXX@XXXXXXXXXX	XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXXXXXXXXXXXX@XXXXXXXXXX	XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXXXXXXXXXXXX@XXXXXXXXXX	XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXXXXXXXXXXXX@XXXXXXXXXX	XXXXXXXXXXXXXXXXXXXX

全 4件

このファイルで間違いない場合は「実行」ボタンを押してください。

実行

- 内容を確認し[実行]をクリック

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

[アカウント]>[登録申請者一覧]メニューを選択します。

※しばらくするとアップロードしたユーザ情報がアカウント登録申請として登録されます。



- [すべて許可する] をクリック
- [実行]をクリック

これで AD のユーザ情報が Gléas のアカウントとしてインポートされました。

4. SAML SP 署名用証明書の発行

SAML SPとして使用する署名用証明書をGléasから発行します。

GléasのRA（登録局）にログインします。

[アカウント]>[アカウント新規作成]からアカウント `saml_sp` を作成します。

新規アカウント作成

アカウント情報の入力

このページではアカウントの新規作成を行います。
アカウントは証明書を発行する対象(エンドエンティティ)のことで、このページで指定したアカウント名が証明書の発行先となります。
★の付いている項目は入力必須項目です。

アカウント情報

アカウント名 ★

名前(姓) ★

名前(名) ★

メールアドレス

パスワード

パスワード(確認)

パスワード(自動生成)

プリンシパル名

[証明書発行]で `saml_sp` アカウントに対し証明書を発行します。

saml_sp

証明書発行

この画面では証明書要求の作成を行います。
左側の「サブジェクト」と「属性」の内容で証明書要求を作成します。
右側のテンプレートの中から必要なものを選択して「発行」を押してください。

証明書発行

下記の内容で証明書を発行します。よろしければ「発行」を押してください。

サブジェクト

CN=saml_sp
O=JCCH Security Solution Systems
DC=local, jcch-sss

属性

発行局:
暗号アルゴリズム: RSA暗号
鍵長: 2048bit
ダイジェストアルゴリズム: SHA256
有効日数: 1年
鍵用途: 電子署名, 鍵の暗号化
拡張鍵用途: SSLクライアント認証
Netscape 拡張: 有効
CRL 配布点:

選択されているテンプレート

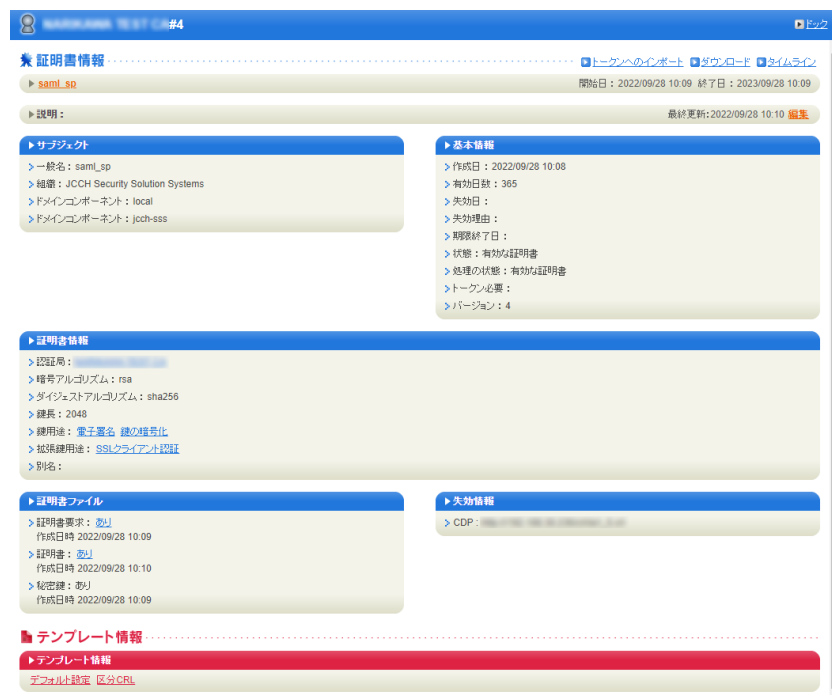
必須 デフォルト設定
必須 区分CRL

選択可能なテンプレート

なし

プライベート認証局 Gléas ホワイトペーパー シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

証明書詳細画面から[ダウンロード]をクリックし証明書をダウンロードします。



※ダウンロード時に証明書、秘密鍵を取り出す際のパスフレーズを指定します。

ダウンロードした.p12ファイルからPEM形式の証明書を取り出します。

※OpenSSLで行なう例 (パスフレーズの入力が必要となります)

```
openssl pkcs12 -in saml_sp.p12 -nokeys -clcerts | openssl x509 out saml_sp.crt
```

※取得した証明書ファイル saml_sp.crt を保存します。

ダウンロードした.p12ファイルからPEM形式の秘密鍵を取り出します。

※OpenSSLで行なう例 (パスフレーズの入力が必要となります)

```
openssl pkcs12 -in saml_sp.p12 -nodes -nocerts | openssl rsa -out saml_sp.key
```

※取り出した秘密鍵ファイル saml_sp.key を保存します。

5. AzureAD の設定

5.1. AD ユーザ情報を同期

Azure AD Connect を使用して AD のユーザ情報を Azure AD に同期します。

Azure Active Directory 管理センター にログインします。

メニュー [カスタムドメイン名] を選択します。

[カスタムドメイン名] をクリックし、同期するドメイン名を入力します。

DNSに指定されたTXTレコードを登録します。

[確認] をクリックして、Azureからドメインの登録確認します。

[Azure AD Connect のダウンロード] をクリックします。

リンク先から Azure AD Connect のインストーラをダウンロードします。

カスタムドメイン登録したドメイン名のAD で Azure AD Connect のインストーラを
実行します。

インストールウィザードを進め、ADに登録したユーザをAzure AD に同期します。

Azure Active Directory 管理センターのメニュー [ユーザー] > [すべてのユーザー] か
らADユーザー情報が登録されていることを確認します。

5.2. エンタープライズ アプリケーションの登録

Gléas UA をエンタープライズ アプリケーションとして登録します。

Azure Active Directory 管理センター にログインします。

メニュー [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] を選択
します。

[新しいアプリケーション] をクリックします。

Azure AD ギャラリーの参照で[独自のアプリケーションの作成] をクリックします。

- [お使いのアプリの名前は何か?] に任意の名前を入力
- [アプリケーションでどのような操作を行いたいですか?] に [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)] を選択
- [作成] をクリック

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?

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

プライベート認証局 Gléas ホワイトペーパー シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

アプリケーションの概要画面に遷移します。



[シングルサインオンの設定] の [作業の開始] をクリックします。

- [シングル サインオン方式の選択] で [SAML] をクリック



SAML によるシングル サインオンのセットアップに遷移します。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

[①基本的な SAML 構成] の [編集] をクリックします。

- [識別子 (エンティティ ID)] の [識別子の追加] をクリック

- [エンティティ ID] を入力

※[https://\[UAのFQDN\]/ua/\[UAの名前\]/saml](https://[UAのFQDN]/ua/[UAの名前]/saml)

- [応答 URL (Assertion Consumer Service URL)] の[応答 URL の追加]をクリック

- [Assertion Consumer Service] を入力

※[https://\[UAのFQDN\]/ua/\[UAの名前\]/saml/acs](https://[UAのFQDN]/ua/[UAの名前]/saml/acs)

- [サインオン URL (省略可能)] を入力

※[https://\[UAのFQDN\]/ua/\[UAの名前\]/saml/sso](https://[UAのFQDN]/ua/[UAの名前]/saml/sso)

- [リレー状態 (省略可能)] は入力しない

- [ログアウト URL (省略可能)] を入力

※[https://\[UAのFQDN\]/ua/\[UAの名前\]/saml/logout](https://[UAのFQDN]/ua/[UAの名前]/saml/logout)

- [保存] をクリック

プライベート認証局 Gléas ホワイトペーパー

シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

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) * ⓘ

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:// /ua/ /saml

✓

✓ ⓘ

🗑

識別子の追加

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) とも呼ばれます。

イン... 既定

https:// /ua/ /saml/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。

https:// /ua/ /saml/sso

✓

リレー状態 (省略可能) ⓘ

リレー状態は、認証が完了した後にユーザーのリダイレクト先となるアプリケーションを指示します。通常、値は、ユーザーをアプリケーション内の特定の場所に移動する URL または URL パスです。

リレー状態を入力してください

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:// /ua/ /saml/logout

✓

[X] をクリックして閉じます。

※エンタープライズ アプリケーションのシングルサインオンのテスト確認が表示されたら [いいえ] をクリックします。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

[②属性とクレーム] の[編集]をクリックします。

- [必要な要求] の[一意のユーザー識別子(名前 ID)]の値をクリック
- [名前識別子の形式]に[指定なし]を選択
- [ソース] に [属性] を選択
- [ソース属性] に [user.userprincipalname] を選択
- [保存] をクリック

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 nameidentifier

名前空間 http://schemas.xmlsoap.org/ws/2005/05/identity/claims

名前識別子の形式の選択

名前識別子の形式 * 指定なし

ソース * 属性 変換

ソース属性 * user.userprincipalname

要求条件

[X] をクリックして閉じます。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

- [追加の要求] に以下を設定

名前	名前空間	ソース	ソース属性
cn	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	属性	user.userprincipalname
sn	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	属性	user.surname
givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	属性	user.givenname
mail	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	属性	user.mail

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	値
一意のユーザー識別子 (名前 ID)	user.userprincipalname [nameid-format:unspecified] ***

追加の要求

クレーム名	値
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/cn	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mail	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/sn	user.surname ***

詳細設定 (プレビュー)

[X] をクリックして閉じます。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

[③SAML 証明書] の [トークン署名証明書]の[編集]をクリックします。

- アクティブな証明書の[⋮] をクリックし [PEM 証明書のダウンロード] をクリックして、IdP 署名用証明書ファイルとして保存
- [署名オプション] に [SAML 応答とアサーションへの署名]を選択
- [署名アルゴリズム] に [SHA-256] を選択
- [通知の電子メールアドレス] は未使用
- [保存] をクリック

[X] をクリックして閉じます。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

[③SAML 証明書] の [検証証明書 (省略可能)] の [編集] を クリックします。

- [検証証明書を必須とする] をチェック
- [RSA-SHA1 で署名された要求を許可する] はチェックしない
- [証明書のアップロード] をクリックして SAML SP 署名用証明書をアップロード
- に[SAML 応答とアサーションへの署名]を選択
- [署名アルゴリズム] に [SHA-256] を選択
- [保存] をクリック

検証証明書 (プレビュー)

① 検証証明書を必須にすると、シングルサインオンテスト機能や、マイ アプリと M365 アプリ ランチャーのエクスペリエンスなど、特定の管理者とエンドユーザーのエクスペリエンスに影響します。
[詳細](#)

検証証明書は、このアプリケーションから Azure Active Directory への要求を検証するために使用されます。
[詳細](#)

検証証明書を必須とする ① ☐

RSA-SHA1 で署名された要求を許可する ☐

①

↑ 証明書のアップロード

拇印	キー ID	開始日付	有効期限	
...	...			...

保存

破棄

[X] をクリックして閉じます。

プライベート認証局 Gléas ホワイトペーパー

シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

[↑](#) 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 Test [🗨](#) 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](#) 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)	https:// /ua/ /saml
応答 URL (Assertion Consumer Service URL)	https:// /ua/ /saml/acs
サインオン URL	https:// /ua/ /saml/sso
リレー状態 (省略可能)	省略可能
ログアウト URL (省略可能)	https:// /ua/ /saml/logout

2

属性とクレーム

編集

cn	user.userprincipalname
sn	user.surname
givenname	user.givenname
mail	user.mail
一意のユーザー ID	user.userprincipalname

3

SAML 証明書

編集

トークン署名証明書	
状態	アクティブ
拇印	
有効期限	
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

検証証明書 (省略可能) (プレビュー)

編集

必須	はい
アクティブ	1
有効期限切れ	0

4

/ 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。

ログイン URL	https://login.microsoftonline.com/ /...
Azure AD 識別子	https://sts.windows.net/ /...
ログアウト URL	https://login.microsoftonline.com/ /...

[X] をクリックして閉じます。

5.3. エンタープライズ アプリケーションの割り当て

登録したエンタープライズ アプリケーションをユーザーに割り当てて、利用できるようにします。

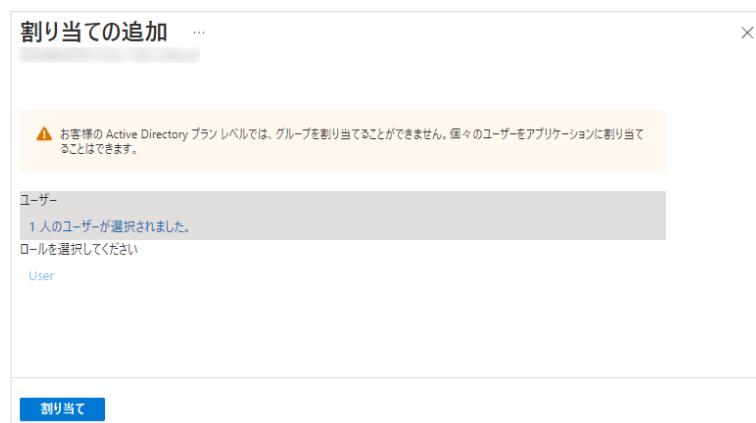
Azure Active Directory 管理センター にログインします。

メニュー [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] を選択します。

登録したアプリケーションを選択して、アプリケーションの概要画面に遷移します。

[ユーザーとグループの割り当て] をクリックします

- [ユーザーまたはグループの追加] をクリック
- エンタープライズ アプリケーションを割り当てるユーザーを選択
- [割り当て]をクリック



※エンタープライズ アプリケーションは、UA 毎に登録、割り当て、を行う必要があります。PC と iOS などデバイス種類ごとに複数の UA を利用している場合などは、それぞれエンタープライズ アプリケーションを登録する必要があります。

6. Gléas の管理者設定 (Windows 向け)

GléasのWindows向けUA (申込局) をAzure ADのエンタープライズ アプリケーションとして動作するように設定します。

※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

GléasのRA (登録局) にログインします。

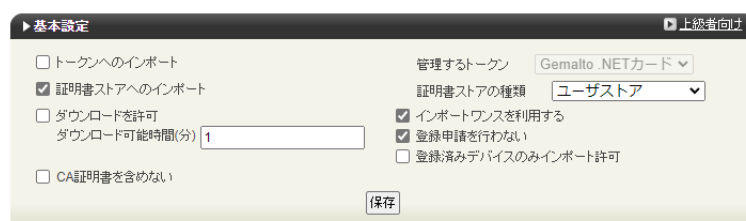
画面上部より[認証局]をクリックし認証局一覧画面に移動し、設定を行うUA (申込局)をクリックします。

※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します



申込局詳細画面が開くので、基本設定で以下の設定を行います。

- [証明書ストアへのインポート]をチェック
- 証明書ストアの選択で、[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック



[上級者向け]をクリックします。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力
 - ※ <https://myapps.microsoft.com/>
- [ログアウト URL]を入力
 - ※ <https://myapps.microsoft.com/>
- [SP 証明書]に SAML SP 署名用証明書ファイルを指定
- [SP 秘密鍵]に SAML SP 署名用証明書の秘密鍵ファイルを指定
- [IdP エンティティ ID] を入力
 - ※ [https://sts.windows.net/\[テナント ID\]/](https://sts.windows.net/[テナント ID]/)
- [IdP SSO URL] を入力
 - ※ [https://login.microsoftonline.com/\[テナント ID\]/saml2](https://login.microsoftonline.com/[テナント ID]/saml2)
- [IdP SLO URL] を入力
 - ※ [https://login.microsoftonline.com/\[テナント ID\]/saml2](https://login.microsoftonline.com/[テナント ID]/saml2)
- [IdP 署名用証明書]に ダウンロードした IdP 署名用証明書ファイルを指定
 - ※IdP 署名用証明書はフェデレーション メタデータ XML から取得することも可能
- [IdP 暗号用証明書]は指定しない
- [ダイジェストアルゴリズム]に「SHA-256」を選択
- [署名アルゴリズム]に「RSA SHA-256」を選択
- [署名リクエストに署名]をチェック
- [ログアウトリクエストに署名]をチェック
- [ログアウトレスポンスに署名]をチェック

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

- [メタデータに署名する]をチェック
- [署名をメッセージに埋め込む]はチェックしない

ログイン方法

☒ SAML2.0で外部認証する

ホームURL

ログアウトURL

SP Issuer

SP 証明書 ☐ 削除する
🔑 saml_sp
有効期限:

SP 秘密鍵 ☐ 削除する
🔑 あり

SP ACS URL

SP SLO URL

名前ID形式

IdP エンティティID

IdP SSO URL

IdP SLO URL

IdP 署名用証明書 ☐ 削除する
🔑 Microsoft Azure Federated SSO Certificate
有効期限:

IdP 暗号用証明書 ファイルが選択されていません

ダイジェストアルゴリズム

署名アルゴリズム

☒ 認証リクエストに署名 ☒ ログアウトリクエストに署名

☒ ログアウトレスポンスに署名 ☒ メタデータに署名

☐ 署名をメッセージに埋め込む

設定完了後、[保存]をクリックし保存します。

また、認証デバイス設定の以下項目にチェックがないことを確認します。

- iPhone/iPad の設定の、[iPhone / iPad 用 UA を利用する]
- Android の設定の、[Android 用 UA を利用する]

以上でGléasの設定は終了です。

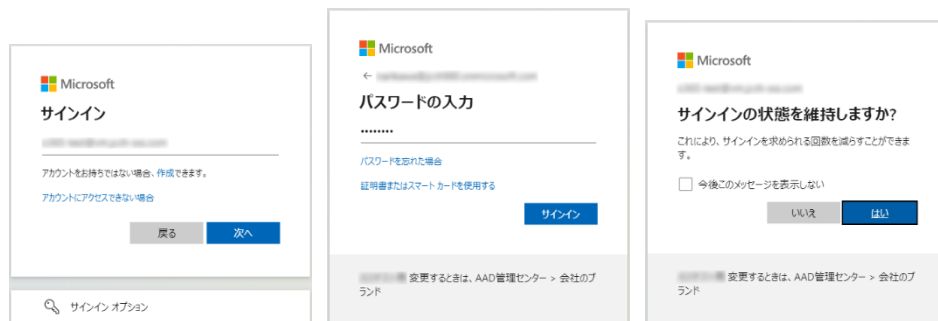
7. クライアントからのアクセス (Windows)

7.1. シングルサインオンで UA にログイン

PCのブラウザ (Edge) で、UAのシングルサインオンURLにアクセスします。

※URL `https://[UAのFQDN]/ua/[UAの名前]/saml/sso`

サインインに遷移します。



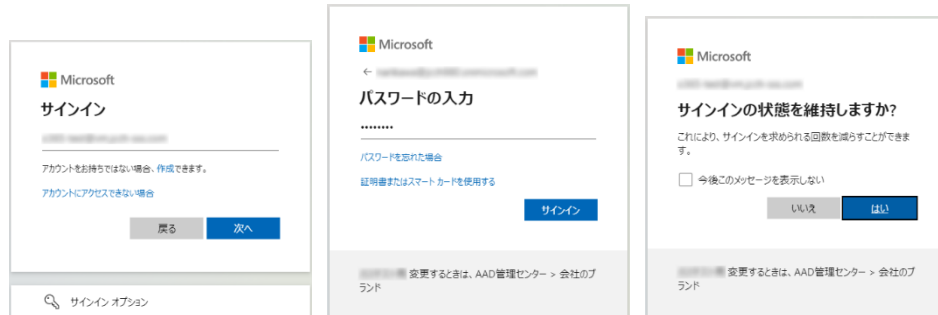
[ユーザー名]、[パスワード]を入力して[サインイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

マイ アプリ ポータルからログインすることもできます。

※URL <https://myapps.microsoft.com/>



[ユーザー名]、[パスワード]を入力して[サインイン]をクリックします。



[アプリ]一覧から登録した「エンタープライズ アプリケーション」をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

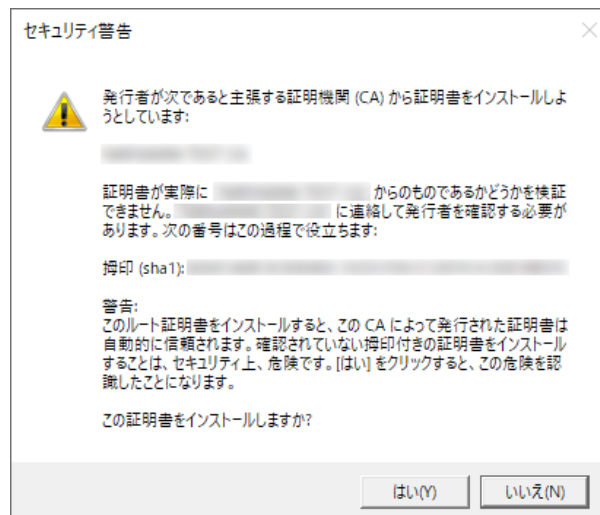
プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

7.2. クライアント証明書のインポート

[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。

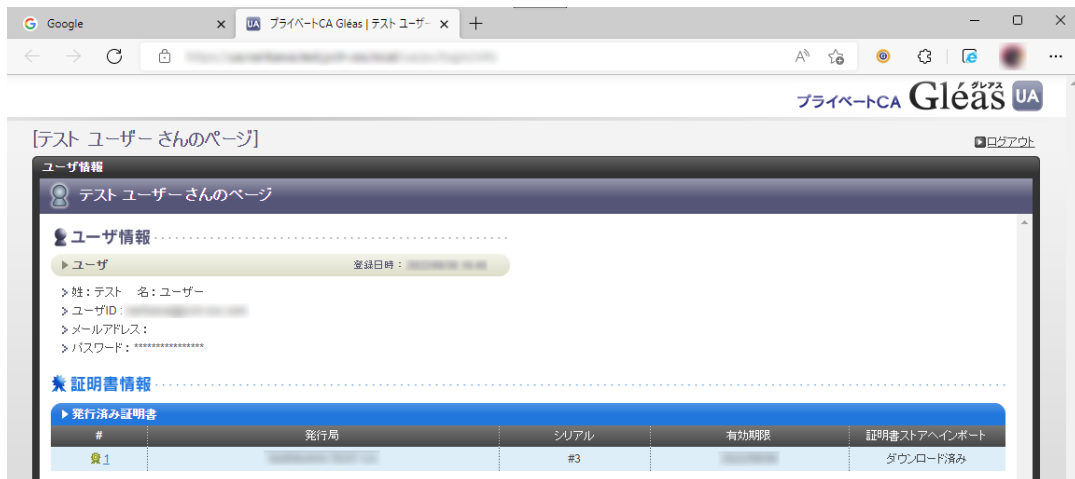


※ 証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印を確認するなど正当性を確認してから[はい]をクリックします



プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

インポートワンス機能を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度ログインしてインポートを行うことはできません。



8. Gléas の管理者設定 (iPhone 向け)

GléasのiPhone向けUA (申込局) をAzure ADのエンタープライズ アプリケーションとして動作するように設定します。

※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

GléasのRA (登録局) にログインします。

画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA (申込局)をクリックします。

※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します



[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック

この設定を行うと、GléasのUAからインポートから指定した時間 (分) を経過した後は、構成プロファイルのダウンロードが不可能になります (インポートロック機能)。これにより複数台のデバイスへの構成プロファイルのインストールを制限することができます。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

基本設定 上級者向け

☐ トークンへのインポート	管理するトークン Gemalto .NETカード
☐ 証明書ストアへのインポート	証明書ストアの種類 ユーザストア
☒ ダウンロードを許可 ダウンロード可能時間(分) 1	☒ インポートワンスを使用する
☐ CA証明書を含まない	☒ 登録申請を行わない
	☐ 登録済みデバイスのみインポート許可

保存

[上級者向け]をクリックします。

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力
 - ※ <https://myapps.microsoft.com/>
- [ログアウト URL]を入力
 - ※ <https://myapps.microsoft.com/>
- [SP 証明書]に SAML SP 署名用証明書ファイルを指定
- [SP 秘密鍵]に SAML SP 署名用証明書の秘密鍵ファイルを指定
- [IdP エンティティ ID] を入力
 - ※ [https://sts.windows.net/\[テナント ID\]/](https://sts.windows.net/[テナント ID]/)
- [IdP SSO URL] を入力
 - ※ [https://login.microsoftonline.com/\[テナント ID\]/saml2](https://login.microsoftonline.com/[テナント ID]/saml2)
- [IdP SLO URL] を入力
 - ※ [https://login.microsoftonline.com/\[テナント ID\]/saml2](https://login.microsoftonline.com/[テナント ID]/saml2)
- [IdP 署名用証明書]に ダウンロードした IdP 署名用証明書ファイルを指定
 - ※IdP 署名用証明書はフェデレーション メタデータ XML から取得することも可能
- [IdP 暗号用証明書]は指定しない
- [ダイジェストアルゴリズム]に「SHA-256」を選択
- [署名アルゴリズム]に「RSA SHA-256」を選択

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

- [署名リクエストに署名]をチェック
- [ログアウトリクエストに署名]をチェック
- [ログアウトレスポンスに署名]をチェック
- [メタデータに署名する]をチェック
- [署名をメッセージに埋め込む]はチェックしない

The screenshot shows a configuration page titled "ログイン方法" (Login Method). It contains various fields for SAML configuration, including Home URL, Logout URL, SP Issuer, SP Certificate, SP Secret Key, SP ACS URL, SP SLO URL, Name ID Format, IdP Entity ID, IdP SSO URL, IdP SLO URL, IdP Certificate, IdP Private Key Certificate, Digest Algorithm, and Signature Algorithm. There are checkboxes for "SAML 2.0で外部認証する" (checked), "ログアウトリクエストに署名" (checked), "ログアウトレスポンスに署名" (checked), "メタデータに署名" (checked), and "署名をメッセージに埋め込む" (unchecked). The "IdP 署名用証明書" (IdP Signature Certificate) is set to "Microsoft Azure Federated SSO Certificate".

設定完了後、[保存]をクリックし保存します。

[認証デバイス情報]の[iPhone/iPadの設定]までスクロールし、[iPhone/iPad用UAを利用する]をチェックします。

The screenshot shows the "認証デバイス情報" (Authentication Device Information) page. Under the "iPhone / iPadの設定" (iPhone / iPad Settings) section, the checkbox "iPhone/iPad 用 UA を利用する" (Use UA for iPhone/iPad) is checked. A "保存" (Save) button is visible at the bottom right.

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

構成プロファイルに必要な情報の入力画面が展開されるので、以下設定を行います。

【画面レイアウト】

- [iPhone用レイアウトを利用する]をチェック
- [ログインパスワードで証明書を保護]をチェック

【iPhone構成プロファイル基本設定】

- [名前]、[識別子]に任意の文字を入力（必須項目）

認証デバイス情報

▶ iPhone / iPad の設定

☒ iPhone/iPad 用 UA を利用する

画面レイアウト

☒ iPhone 用レイアウトを使用する ☒ ログインパスワードで証明書を保護

☐ Mac OS X 10.7以降の接続を許可

OTA(Over-the-air)

☐ OTAエンロールメントを利用する ☐ 接続する iOS デバイスを認証する

OTA用SCEP URL

OTA用認証局

デフォルトを利用

iPhone 構成プロファイル基本設定

名前(デバイス上に表示)

サンプルプロファイル

識別子(例: com.jcch-sss.profile)

local.jcch-sss.profile

プロファイルの組織名

JCCHセキュリティ・ソリューション・システムズ

説明

サンプル構成プロファイル

各項目の入力が終わったら、[保存]をクリックします。

以上でGléasの設定は終了です。

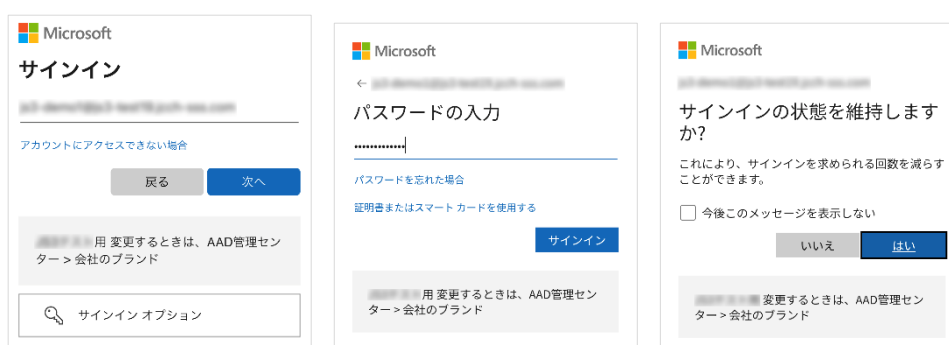
9. クライアントからのアクセス (iPhone)

9.1. シングルサインオンで UA にログイン

iPhoneのブラウザ (Safari) で、UAのシングルサインオンURLにアクセスします。

※URL `https://[UAのFQDN]/ua/[UAの名前]/saml/sso`

サインインに遷移します。



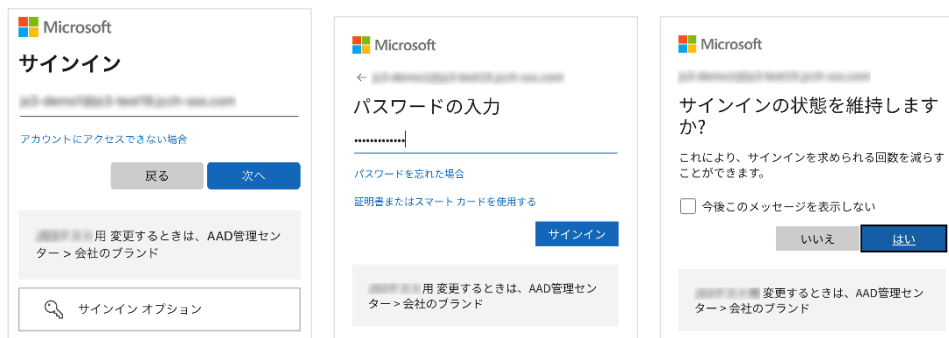
[ユーザー名]、[パスワード]を入力して[サインイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

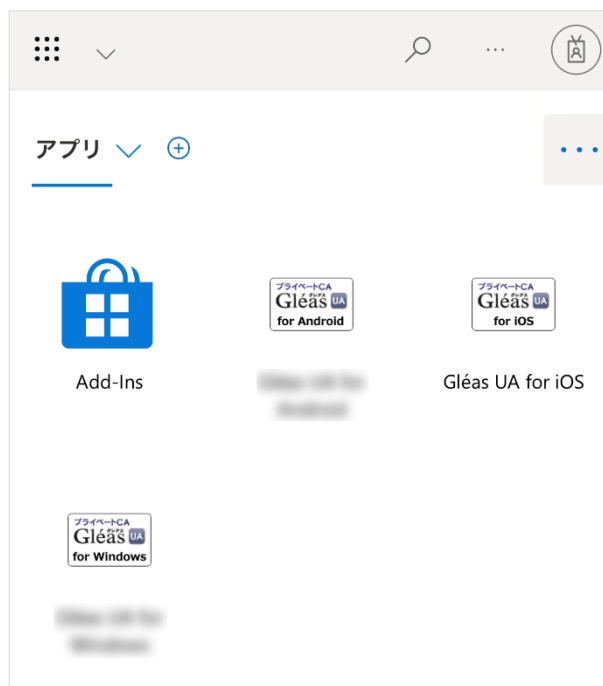
プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

マイ アプリ ポータルからログインすることもできます。

※URL <https://myapps.microsoft.com/>



[ユーザー名]、[パスワード]を入力して[サインイン]をクリックします。



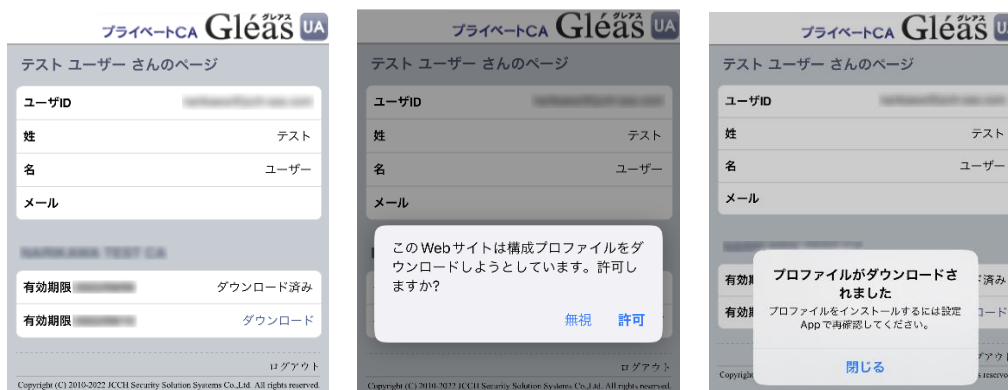
[アプリ]一覧から登録した「エンタープライズ アプリケーション」をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

9.2. クライアント証明書のインポート

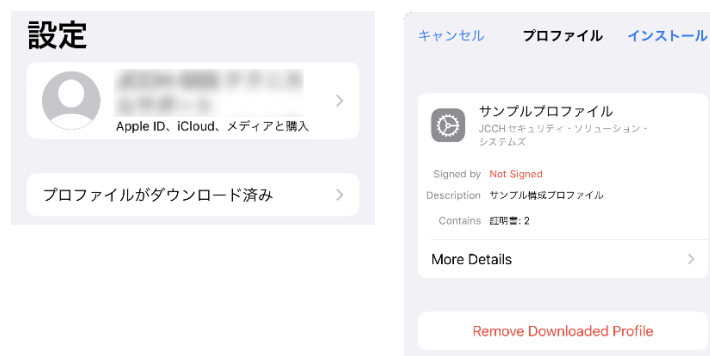
[ダウンロード]をタップし、構成プロファイルのダウンロードをおこないます。



※ インポートロックを有効にしている場合は、この時点からカウントが開始されます

画面の表示にしたがい設定を開くと、プロファイルがダウンロードされた旨が表示され

るので、インストールをおこないます。



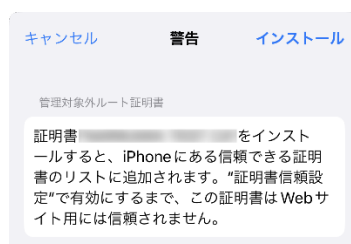
[インストール]をタップして続行してください。

プライベート認証局 Gléas ホワイトペーパー シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

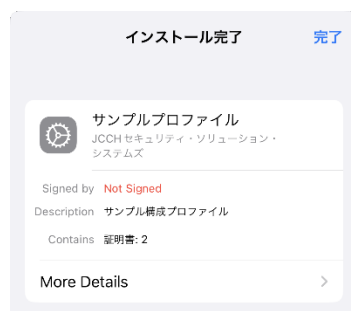
インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し

[インストール]をタップして続行してください。

※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書になります



インストール完了画面になりますので、[完了]をタップして終了します。



なお [More Details]をタップすると、インストールされた証明書情報を見ることがで

きます。必要に応じて確認してください。



Safariに戻り、[ログアウト]をタップしてUAからログアウトします。

以上で、iPhoneでの構成プロファイルのインストールは終了です。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より
管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロ
ード済み」という表記に変わり、以後のダウンロードは一切不可となります。

The screenshot displays the Gléas UA user interface for a test user. At the top, the header reads 'プライベートCA Gléas UA'. Below this, the page title is 'テスト ユーザー さんのページ'. The user profile section includes fields for 'ユーザーID', '姓' (Last Name) with the value 'テスト', '名' (First Name) with the value 'ユーザー', and 'メール' (Email). Below the profile, there are two rows showing '有効期限' (Valid Period) and 'ダウンロード済み' (Downloaded). At the bottom right, there is a 'ログアウト' (Logout) button. The footer contains the copyright notice: 'Copyright (C) 2010-2022 JCCH Security Solution Systems Co., Ltd. All rights reserved.'

10. Gléas の管理者設定 (Android 向け)

GléasのAndroid向けUA (申込局) をAzure ADのエンタープライズ アプリケーションとして動作するように設定します。

※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

GléasのRA (登録局) にログインします。

画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA (申込局)をクリックします。

※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します



[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック

この設定を行うと、GléasのUAからインポートから指定した時間 (分) を経過した後は、証明書ファイルのダウンロードが不可能になります (インポートロック機能) 。これにより複数台のデバイスへの証明書ファイルのインストールを制限することができます。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

基本設定 上級者向け

☐ トークンへのインポート

☐ 証明書ストアへのインポート

☒ ダウンロードを許可
ダウンロード可能時間(分) 1

☐ CA証明書を含まない

管理するトークン Gemalto .NETカード

証明書ストアの種類 ユーザストア

☒ インポートワンスを使用する

☒ 登録申請を行わない

☐ 登録済みデバイスのみインポート許可

保存

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力
※ <https://myapps.microsoft.com/>
- [ログアウト URL]を入力
※ <https://myapps.microsoft.com/>
- [SP 証明書]に SAML SP 署名用証明書ファイルを指定
- [SP 秘密鍵]に SAML SP 署名用証明書の秘密鍵ファイルを指定
- [IdP エンティティ ID] を入力
※ [https://sts.windows.net/\[テナント ID\]/](https://sts.windows.net/[テナント ID]/)
- [IdP SSO URL] を入力
※ [https://login.microsoftonline.com/\[テナント ID\]/saml2](https://login.microsoftonline.com/[テナント ID]/saml2)
- [IdP SLO URL] を入力
※ [https://login.microsoftonline.com/\[テナント ID\]/saml2](https://login.microsoftonline.com/[テナント ID]/saml2)
- [IdP 署名用証明書]に ダウンロードした IdP 署名用証明書ファイルを指定
※IdP 署名用証明書はフェデレーション メタデータ XML から取得することも可能
- [IdP 暗号用証明書]は指定しない
- [ダイジェストアルゴリズム]に「SHA-256」を選択
- [署名アルゴリズム]に「RSA SHA-256」を選択

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

- [署名リクエストに署名]をチェック
- [ログアウトリクエストに署名]をチェック
- [ログアウトレスポンスに署名]をチェック
- [メタデータに署名する]をチェック
- [署名をメッセージに埋め込む]はチェックしない

ログイン方法

☒ SAML2.0で外部認証する

ホームURL

ログアウトURL

SP Issuer

SP 証明書 ☐ 削除する
🔑 saml_sp
有効期限:

SP 秘密鍵 ☐ 削除する
🔑 あり

SP ACS URL

SP SLO URL

名前ID形式

IdP エンティティID

IdP SSO URL

IdP SLO URL

IdP 署名用証明書 ☐ 削除する
🔑 Microsoft Azure Federated SSO Certificate
有効期限:

IdP 暗号用証明書 ファイルが選択されていません

ダイジェストアルゴリズム

署名アルゴリズム

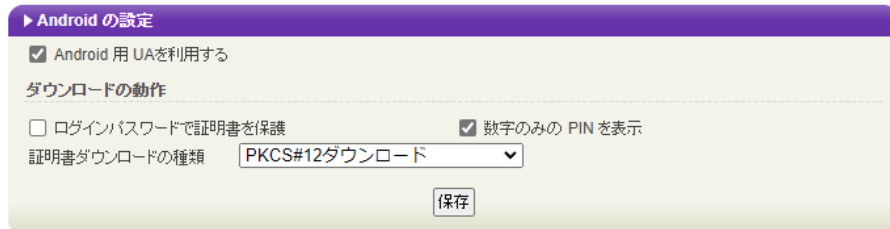
☒ 認証リクエストに署名
☒ ログアウトリクエストに署名
☐ 署名をメッセージに埋め込む

☒ ログアウトリクエストに署名
☒ メタデータに署名

設定完了後、[保存]をクリックし保存します。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

[認証デバイス情報]の[Androidの設定]までスクロールし、[Android用UAを利用する]をチェックします。



証明書のダウンロードに必要なとなる情報の入力画面が展開されるので、以下設定を行います。

- [数字のみのPINを表示]をチェック
- [証明書ダウンロードの種類]]を[PKCS#12ダウンロード]を選択

各項目の入力が終わったら、 [保存]をクリックします。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

証明書インポートアプリ CertImporter for Android を使用する場合は、[証明書インポートアプリ連携の設定] までスクロールし、[証明書インポートアプリを利用する]をチェックします。

▶ 証明書インポートアプリ連携の設定

- ☒ 証明書インポートアプリを利用する
- ☐ インポートボタンを表示
- ☐ 証明書一覧をアプリで表示 (MacOSXのみ)
- ☐ 証明書と一緒にUAマニフェストをダウンロード
- ☐ 証明書PINをGléasで生成

UAマニフェスト

ログインURL

信頼するCA証明書 ファイルが選択されていません

証明書PIN生成シード

[UAマニフェスト要求ファイル](#) をダウンロードして、弊社サポートに送付してください

UAマニフェストのアップロード ファイルが選択されていません

入力が終わったら、[保存]をクリックします。

以上でGléasの設定は終了です。

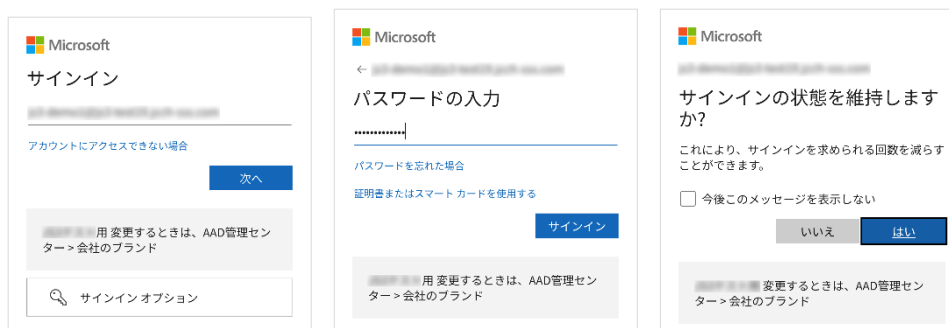
11. クライアントからのアクセス (Android)

11.1. シングルサインオンで UA にログイン

Androidのブラウザ (Chrome) で、UAのシングルサインオンURLにアクセスします。

※URL `https://[UAのFQDN]/ua/[UAの名前]/saml/sso`

サインインに遷移します。



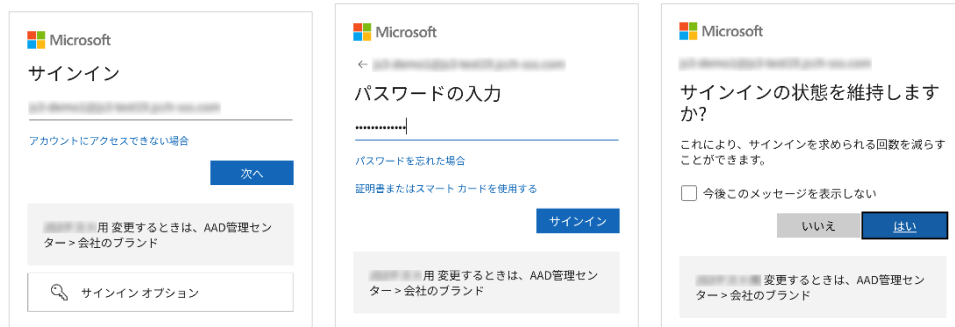
[ユーザー名]、[パスワード]を入力して[サインイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

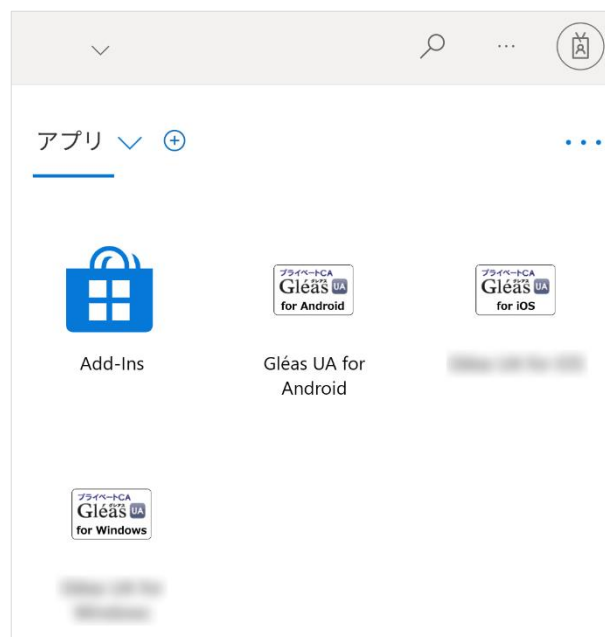
プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

マイ アプリ ポータルからログインすることもできます。

※URL <https://myapps.microsoft.com/>



[ユーザー名]、[パスワード]を入力して[サインイン]をクリックします。



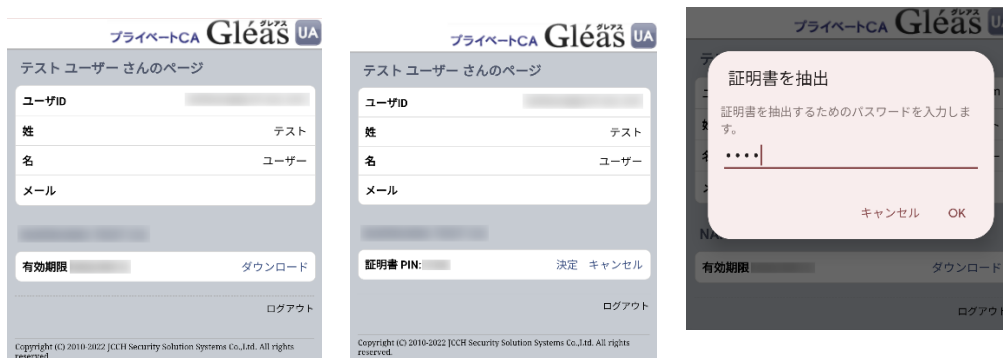
[アプリ]一覧から登録した「エンタープライズ アプリケーション」をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

11.2. クライアント証明書のインポート

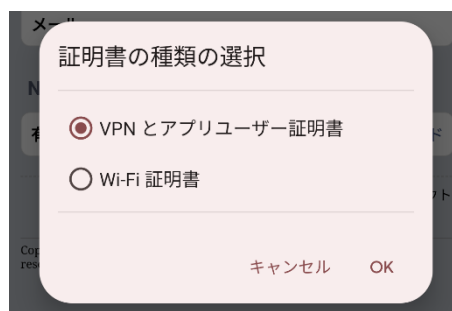
[ダウンロード]をタップし、証明書ファイルのダウンロードをおこないます。



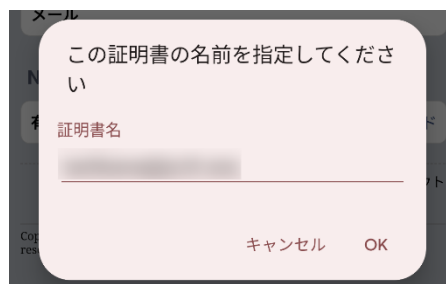
- ※ 「証明書 PIN」の値を「証明書を抽出」のパスワードとして入力します。
- ※ インポートロックを有効にしている場合は、この時点からカウントが開始されます

[OK]をタップして続行してください。

「証明書の種類の用途」のダイアログが出るので、用途を選択します。



[OK]をタップして続行してください。



[OK]をタップします。

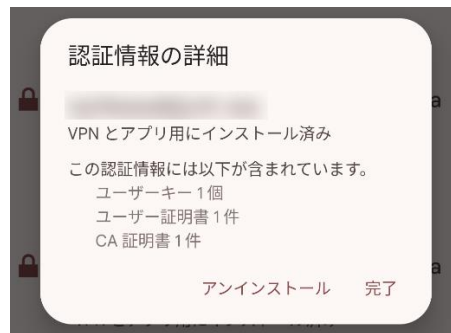
プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

Chromeに戻り、[ログアウト]をタップしてUAからログアウトします。

以上で、Androidでの証明書ファイルのインストールは終了です。

プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Azure AD 連携)

[設定]>[セキュリティ]>[詳細設定]>[暗号化と認証情報]>[ユーザー認証情報]>[証明書
の名前]とタップすると、インストールされた証明書情報を見ることができます。必要
に応じて確認してください。



なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より
管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロ
ード済み」という表記に変わり、以後のダウンロードは一切不可となります。



12.問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■Gléasや本検証内容、テスト用証明書の提供に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ

Tel: 050-3821-2195

Mail: sales@jcch-sss.com