



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 (Keycloak 連携)

Ver.1.0

2023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 (Keycloak 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	5
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. Keycloak の設定	16
5.1. AD ユーザ情報を同期	16
5.2. クライアントの登録	24
6. Gléas の管理者設定 (Windows 向け)	31
7. クライアントからのアクセス (Windows)	34
7.1. シングルサインオンで UA にログイン	34

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 (Keycloak 連携)

7.2. クライアント証明書のインポート	35
8. Gléas の管理者設定 (iPhone 向け)	37
9. クライアントからのアクセス (iPhone)	41
9.1. シングルサインオンで UA にログイン	41
9.2. クライアント証明書のインポート	42
10. Gléas の管理者設定 (Android 向け)	45
11. クライアントからのアクセス (Android)	50
11.1. シングルサインオンで UA にログイン	50
11.2. クライアント証明書のインポート	51
12. 問い合わせ	54

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、Keycloakのクライアントとして登録し、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利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 : Keycloak サーバ

(AlmaLinux 8.7, Keycloak 22.0.1, OpenJDK 17, NGINX 1.24.0, PostgreSQL 15.4)

※以後「Keycloak」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 (Keycloak 連携)

- 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
- 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。

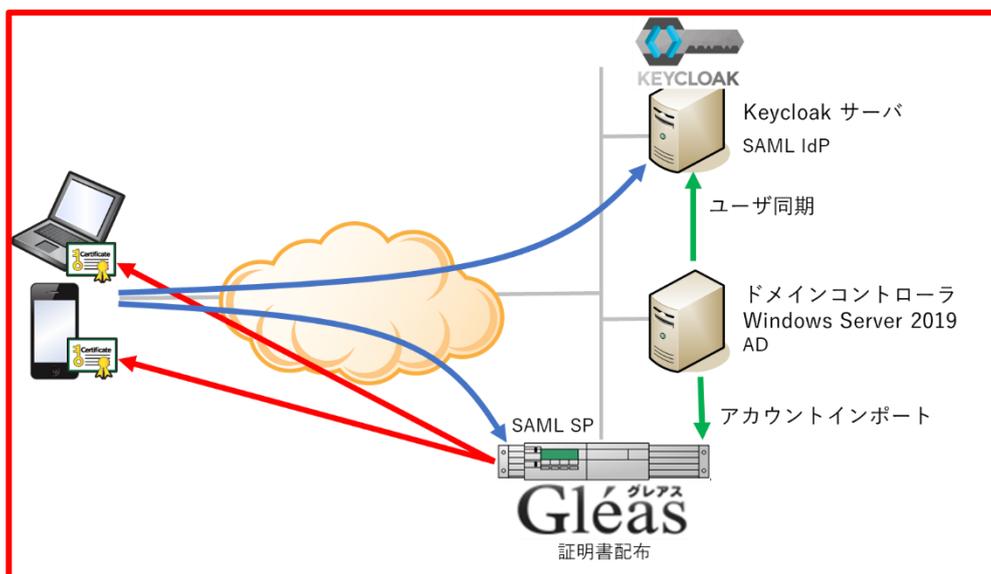
- Keycloakの基本設定
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作
- Windows、iPhone、Android での UA へのログイン方法

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Keycloakのログイン画面に画面遷移。Keycloak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Keycloakのログイン画面に画面遷移。Keycloak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Keycloakのログイン画面に画面遷移。Keycloak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。

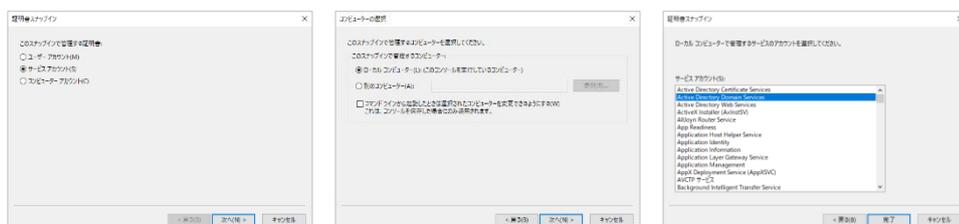
MMC を開き、メニューの[ファイル(F)] > [スナップインの追加と削除(N)]より[証明書]を追加します。

「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 (Keycloak 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 (Keycloak 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) page with the '上級者向け設定' (Advanced Settings) tab selected. 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 'Base DN' is 'OU=,DC=,DC=,DC=' and the '管理者DN' (Administrator DN) is 'CN=,CN=,DC=,DC=,DC='. The '検索フィルタ' (Search Filter) is '(objectClass=person)'. The '属性のマッピング' (Attribute Mapping) is set to 'カスタム設定' (Custom Settings). The mapping table is as follows:

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

A '作成' (Create) button is located at the bottom of the form.

- [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 (Keycloak 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。



- 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 (Keycloak 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。



- [全て許可する] 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。

発行

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

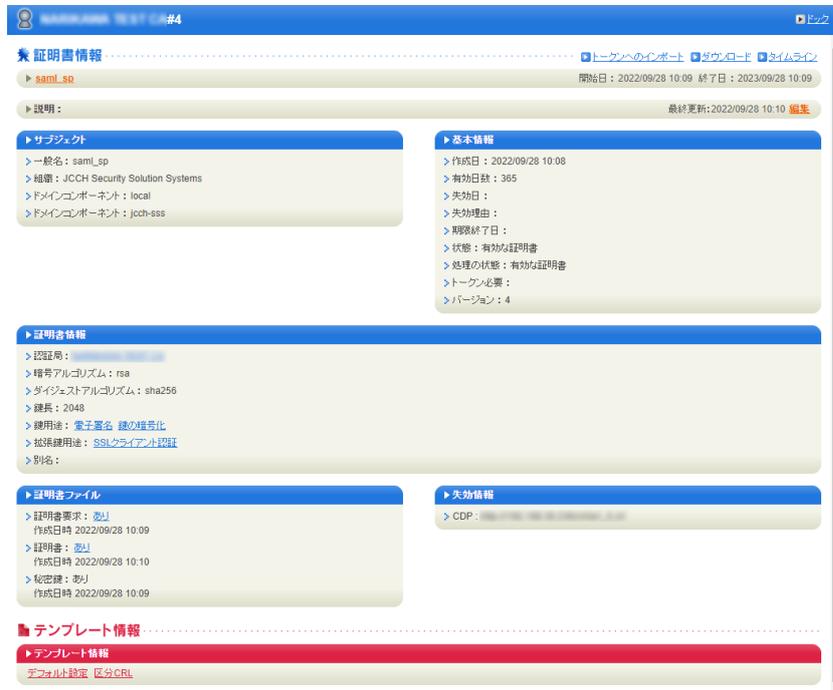
必須 デフォルト設定
必須 区分CRL

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 (Keycloak 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. Keycloak の設定

5.1. AD ユーザ情報を同期

Keycloak のユーザー・フェデレーション機能で AD からユーザ情報を同期します。

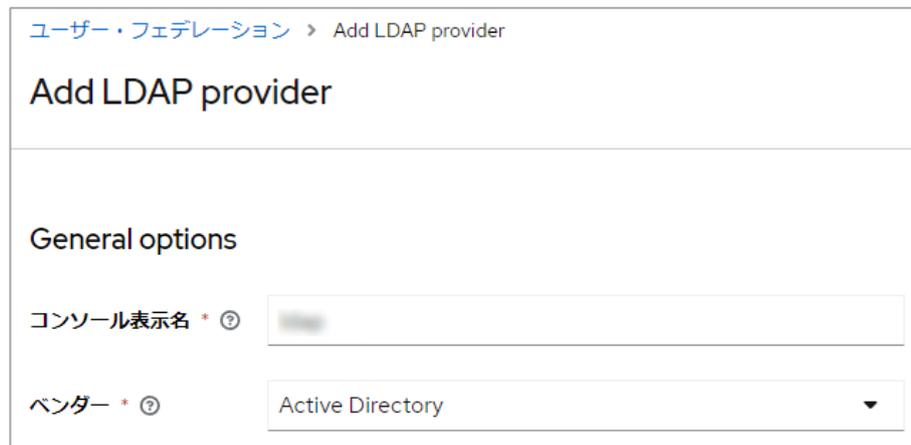
Keycloak 管理コンソール にログインします。

メニュー [ユーザー・フェデレーション] を選択します。

[Add new provider] > [LDAP] をクリックしてLDAP接続設定を入力します。

【General options】

- [コンソール表示名] に任意の名前を入力
- [ベンダー] に [Active Directory] を選択



ユーザー・フェデレーション > Add LDAP provider

Add LDAP provider

General options

コンソール表示名 * ?

ベンダー * ?

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 (Keycloak 連携)

【Connection and authentication settings】

- [接続 URL] に AD の URL を入力
※ Idaps://[AD の FQDN]
- [バインドタイプ] に [simple] を選択
- [バインド DN] にベース DN 以下にアクセスできる AD 管理者の DN を入力
※例) CN=XXX,CN=Users,DC=sample,DC=domain
- [Bind credentials] に AD 管理者のパスワードを入力

Connection and authentication settings

接続URL * ⓘ

StartTLSの有効 ⓘ オフ

トラストストアSPIを使用 ⓘ

接続プーリング ⓘ オフ

接続タイムアウト ⓘ

バインドタイプ * ⓘ

バインドDN * ⓘ

Bind credentials * ⓘ ⓘ

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 (Keycloak 連携)

【LDAP searching and updating】

- [編集モード] に [UNSYNCED] を選択
 - ※ AD から同期するが、Keycloak のユーザ情報変更は AD に反映しない
- [ユーザーDN] にユーザ情報の検索対象となるベース DN を入力
 - ※例) OU=XXX,CN=Users,DC=sample,DC=domain
- [ユーザー名の LDAP 属性] に Keycloak のユーザ名とする LDAP 属性を入力
 - ※例) userPrincipalName
- [UUID LDAP 属性] に “objectGUID” を入力
- [ユーザー・オブジェクト・クラス] に “person, organizationalPerson, user” を
入力
- [User LDAP filter] に検索フィルタを入力
 - ※例) “(! (userAccountControl:1.2.840.113556.1.4.803:=2))” とすると有効化したユーザのみ

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 (Keycloak 連携)

LDAP searching and updating

編集モード * ⓘ UNSYNCED ▼

ユーザーDN * ⓘ OU= ,DC= ,DC= ,DC=

ユーザー名のLDAP属性 * ⓘ userPrincipalName

RDN LDAP属性 * ⓘ cn

UUID LDAP属性 * ⓘ objectGUID

ユーザー・オブジェクト・クラス * ⓘ person, organizationalPerson, user

User LDAP filter ⓘ (!{userAccountControl:1.2.840.113556.1.4.803:=2})

検索スコープ ⓘ One Level ▼

読み取りタイムアウト ⓘ

ページネーション ⓘ オフ

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 (Keycloak 連携)

【Synchronization settings】

- [ユーザーのインポート] に [On] を選択
- [Sync Registrations] に [Off] を選択
 - ※ Keycloak で新規登録したユーザを AD に登録しない
- [定期的なフル同期] に [On] を選択
- [定期的な変更ユーザーの同期] に [On] を選択

Synchronization settings

ユーザーのインポート ?	<input checked="" type="checkbox"/> オン
Sync Registrations ?	<input type="checkbox"/> オフ
バッチサイズ ?	<input type="text"/>
定期的なフル同期 ?	<input checked="" type="checkbox"/> オン
フル同期の周期 ?	<input type="text" value="604800"/>
定期的な変更ユーザー の同期 ?	<input checked="" type="checkbox"/> オン
変更ユーザーの同期周 期 ?	<input type="text" value="86400"/>

- [保存] をクリックして設定を保存

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 (Keycloak 連携)

[マッパー] タブを使用して、AD のLDAP属性とKeycloakのユーザ属性のマッピングを設定します。

以下のようにマッピングします。

Keycloak のユーザ属性	LDAP の属性
ユーザ名	userPrincipalName
名前 (姓)	sn
名前 (名)	givenName
Eメール	mail

Keycloak のデフォルトの設定で、ユーザ名、名前 (姓) 、Eメールは設定済みなので、名前 (名) のマッピングを追加します。

- [Add mapper] をクリック

【Synchronization settings】

- [Name] に "first name" を入力
- [Mapper type] に [user-attribute-ldap-mapper] を選択
- [User Model Attribute] に "firstName" を入力
- [LDAP Attribute] に "givenname" を入力
- [Read Only] に [On] を選択
- [Always Read Value From LDAP] に [On] を選択
- [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 (Keycloak 連携)

[ユーザー・フェデレーション](#) > [設定](#) > [Mapper details](#)

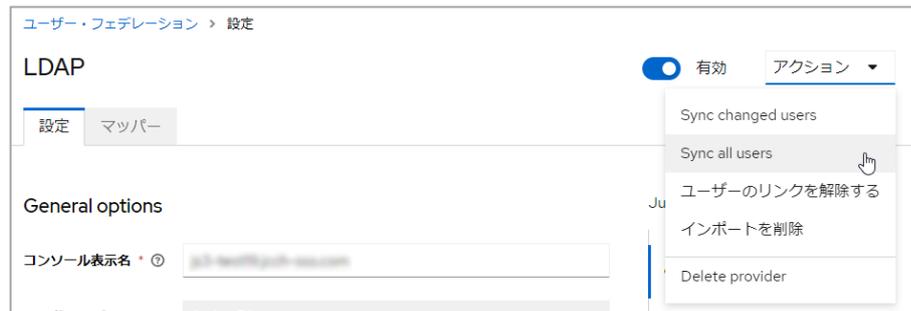
Create new mapper

Name * ⓘ	<input type="text" value="first name"/>
マッパータイプ * ⓘ	<input type="text" value="user-attribute-ldap-mapper"/>
User Model Attribute ⓘ	<input type="text" value="firstName"/>
LDAP Attribute ⓘ	<input type="text" value="givenname"/>
Read Only ⓘ	<input checked="" type="checkbox"/> オン
Always Read Value From LDAP ⓘ	<input checked="" type="checkbox"/> オン
Is Mandatory In LDAP ⓘ	<input type="checkbox"/> オフ
Attribute default value ⓘ	<input type="text"/>
Force a Default Value ⓘ	<input checked="" type="checkbox"/> オン
Is Binary Attribute ⓘ	<input type="checkbox"/> オフ

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 (Keycloak 連携)

[アクション] メニューからユーザ情報の同期を実施します。

- [アクション] > [Sync all users] をクリック



メニュー [ユーザー] から Keycloak にユーザ登録されていることを確認します。

The screenshot shows the 'Users' page in Keycloak. The 'User list' tab is active, and the table displays the following data:

ユーザー名	Eメール	姓	名	ステータス
...	-
...	-
...	-
...	-
...	-
...	-
...	-
...	-
...	-
...	-

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 (Keycloak 連携)

5.2. クライアントの登録

Gléas UA を Keycloak のクライアントとして登録します。

Keycloak 管理コンソール にログインします。

メニュー [クライアント] を選択します。

[Create client] をクリックします。

【① General Settings】

- [Client type] に [SAML] を選択
- [クライアント ID] に SAML SP のエンティティ ID を入力
※ `https://[UA の FQDN]/ua/[UA 名]/saml`
- [次へ] をクリック

The screenshot shows the 'Create client' form in the Keycloak management console. The breadcrumb is 'クライアント > Create client'. The title is 'Create client' with a subtitle 'Clients are applications and services that can request authentication of a user.' The left sidebar shows '1 General Settings' (active) and '2 Login settings'. The main form fields are: 'Client type' (dropdown menu set to 'SAML'), 'クライアントID' (text input with the value 'https://[redacted]/ua/[redacted]/saml'), 'Name' (empty text input), '説明' (empty text area), and '常にコンソールに表示' (checkbox set to 'オフ'). At the bottom, there are three buttons: '次へ' (Next), '戻る' (Back), and 'Cancel'.

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 (Keycloak 連携)

【② Login settings】

- [Home URL] を入力
 - ※ `https://[UA の FQDN]/ua/[UA 名]/saml/sso`
- [有効なリダイレクト URI] を入力
 - ※ `https://[UA の FQDN]/ua/[UA 名]/*`
- [IDP-Initiated SSO URL name] に任意の名前を入力
 - ※ 例えば、“gleas-ua” とすると、
`https://[Keycloak の FQDN]/realms/[レルム名]/protocol/saml/clients/gleas-ua`
の URL で IdP-Initiated SSO が開始されます。
- [保存] をクリック

The screenshot shows the 'Create client' page in Keycloak, specifically the 'Login settings' tab. The page has a breadcrumb 'クライアント > Create client' at the top. Below the title 'Create client', there is a subtitle 'Clients are applications and services that can request authentication of a user.' The main content area is divided into two columns. The left column contains a sidebar with two tabs: '1 General Settings' and '2 Login settings', with 'Login settings' being the active tab. The right column contains several form fields: 'ルートURL' (Root URL) with an empty input field; 'Home URL' with the value 'https://[redacted]/ua/[redacted]/saml/sso'; '有効なリダイレクトURI' (Valid redirect URIs) with the value 'https://[redacted]/ua/[redacted]/*' and a plus icon to add more; 'Valid post logout redirect URIs' with an empty input field and a plus icon; 'IDP-Initiated SSO URL name' with the value 'gleas-ua' and a target URL 'https://[redacted]/realms/[redacted]/protocol/saml/clients/gleas-ua'; 'IDP Initiated SSOの RelayState' with an empty input field; and 'SAMLを処理するマスタURL' (SAML master URL) with an empty input field. At the bottom of the form, there are three buttons: '保存' (Save), '戻る' (Back), and 'Cancel'.

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 (Keycloak 連携)

[設定] タブを選択

【SAML capabilities】

- [Name ID フォーマット] に [username] を選択
- [Name ID フォーマットを強制] に [Off] を選択
- [POST バインディングを強制] に [On] を選択

SAML capabilities

Name IDフォーマット <small>?</small>	<input type="text" value="username"/>
Name IDフォーマットを強制 <small>?</small>	<input type="checkbox"/> オフ
POSTバインディングを強制 <small>?</small>	<input checked="" type="checkbox"/> オン
Force artifact binding <small>?</small>	<input type="checkbox"/> オフ
AuthnStatementを含める <small>?</small>	<input checked="" type="checkbox"/> オン
OneTimeUse条件を含める <small>?</small>	<input type="checkbox"/> オフ
REDIRECT署名鍵検索の最適化 <small>?</small>	<input type="checkbox"/> オフ
Allow ECP flow <small>?</small>	<input type="checkbox"/> オフ

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 (Keycloak 連携)

【Signature and Encryption】

- [ドキュメントを署名する] に [On] を選択
- [アサーションを署名する] に [On] を選択
- [Signature algorithm] に [RSA_SHA256] を選択
- [SAML 署名鍵名] に [NONE] を選択
- [正規化方式] に [EXCLUSIVE] を選択

Signature and Encryption

ドキュメントを署名する オン

アサーションを署名する オン

Signature algorithm RSA_SHA256

SAML 署名鍵名 NONE

正規化方式 EXCLUSIVE

- [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 (Keycloak 連携)

[鍵] タブを選択

【Signing keys config】

- [クライアント署名が必須] に [On] を選択

Signing keys config

If you enable the "Client signature required" below, you must configure the signing keys by generating or importing keys, and the client will sign their saml requests and responses. The signature will be validated.

クライアント署名が必須 オン

証明書

```
MIIC4TCCAckCBgGKShxu4DANBgkqhkiG9w0BAQsFADAOMTIwMAYDVQQDDClodHRwczovL3VhLmRlbW8zLmpjY2gtc3NzLmNvbS9lYS99c28vc2FtbDAeFw0yMzA4MzEwNTM5NTJhFw0zMzA4MzEwNTQxMzJaMDQxMjAwBgNVBAMMKWh0dHBzOi8vdWEuZGVtbzMuamNjaC1zc3MuY29tL3VhL3Nzby9zYW1sMIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAcqH-HuJhUAp8HPIDGPY7s6vDk0DnwZW2Atk8WoaVNAjheK57lGsxzjKLu+JzHdhUaywsveGX+Kb
```

Regenerate Import key エクスポート

- [証明書] の [Import key] をクリックしてダイアログを開く
- [アーカイブ形式] に [Certificate PEM] を選択
- [ファイルをインポート] の [Browse] をクリックして SAML SP 証明書を選択
- [Import] をクリック

Import key

アーカイブ形式

Certificate PEM

ファイルをインポート

Drag a file here or browse to upload Browse Clear

Import Cancel

- [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 (Keycloak 連携)

[Advanced] タブを選択

【SAML エンドポイントの詳細設定】

- [アサーション・コンシューマー・サービスの POST バインディング URL] を入力
- "https://[UA の FQDN]/ua/[UA 名]/ua/sso/saml/acs"
- [ログアウト・サービスの POST バインディング URL] を入力
- "https://[UA の FQDN]/ua/[UA 名]/saml/logout"

SAMLエンドポイントの詳細設定

This section to configure exact URLs for Assertion Consumer and Single Logout Service.

Logo URL ?

Policy URL ?

Terms of service URL ?

アサーション・コンシューマー・サービスの POST バインディング URL ?

アサーション・コンシューマー・サービスの Redirect バインディング URL ?

ログアウト・サービスの POST バインディング URL ?

- [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 (Keycloak 連携)

※Keycloak のクライアント登録は、UA 毎に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、それぞれクライアント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Keycloakのクライアント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 (Keycloak 連携)

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]に任意に URL を入力
 - ※ UA の「ログイン画面に戻る」リンクで遷移する URL となります
- [ログアウト URL]に任意の URL を入力
 - ※ UA の「ログアウト」リンクで遷移する URL となります/
- [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://\[KeycloakのFQDN\]/realms/\[レルム名\]](https://[KeycloakのFQDN]/realms/[レルム名])
- [IdP SSO URL] を入力
 - ※ [https://\[KeycloakのFQDN\]/realms/\[レルム名\]/protocol/saml](https://[KeycloakのFQDN]/realms/[レルム名]/protocol/saml)
- [IdP SLO URL] を入力
 - ※ [https://\[KeycloakのFQDN\]/realms/\[レルム名\]/protocol/saml](https://[KeycloakのFQDN]/realms/[レルム名]/protocol/saml)
- [IdP 署名用証明書]に IdP 署名用証明書ファイルを指定
 - ※署名用証明書はメタデータ(XML)から取得する
 - ※ [https://\[KeycloakのFQDN\]/realms/\[レルム名\]/protocol/saml/descriptor](https://[KeycloakのFQDN]/realms/[レルム名]/protocol/saml/descriptor)
- [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 (Keycloak 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

The screenshot shows the 'ログイン方法' (Login Method) configuration page for SAML2.0 external authentication. The page is in Japanese and contains the following fields and options:

- SAML2.0で外部認証する
- ホームURL: [text input]
- ログアウトURL: [text input]
- SP Issuer: https://[text input]/ua/ /saml
- SP 証明書: 削除する
業 [text input]
有効期限: [text input]
- SP 秘密鍵: 削除する
業 あり
- SP ACS URL: https://[text input]/ua/ /saml/acs
- SP SLO URL: https://[text input]/ua/ /saml/logout
- 名前ID形式: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
- IdP エンティティID: https://[text input]/realms/[text input]
- IdP SSO URL: https://[text input]/realms/[text input]/protocol/saml
- IdP SLO URL: https://[text input]/realms/[text input]/protocol/saml
- IdP 署名用証明書: 削除する
業 [text input]
有効期限: [text input]
- IdP 暗号用証明書: [ファイルの選択] 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: SHA-256
- 署名アルゴリズム: RSA SHA-256
- 認証リクエストに署名
- ログアウトレスポンスに署名
- 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。

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)

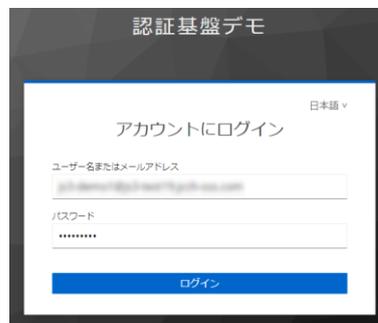
7.1. シングルサインオンで UA にログイン

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`

※URL `https://[KeycloakのFQDN]/realms/[レルム名]/protocol/saml/clients/gleas-ua/`

Keycloakのログインページに遷移します。



[ユーザー名]、[パスワード]を入力して[ログイン]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。

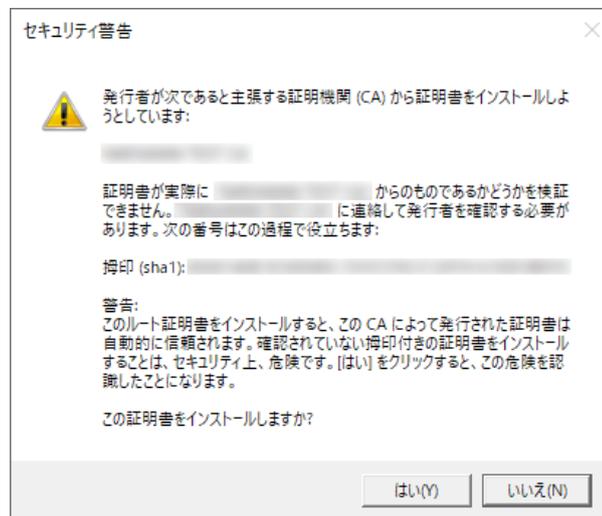
プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Keycloak 連携)

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 (Keycloak 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Keycloakのクライアント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 (Keycloak 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)

CA証明書を含めない

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

[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]に任意に URL を入力
 - ※ UA の「ログイン画面に戻る」リンクで遷移する URL となります
- [ログアウト URL]に任意の URL を入力
 - ※ UA の「ログアウト」リンクで遷移する URL となります/
- [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://[Keycloak の FQDN]/realms/[レルム名]`
- [IdP SSO URL] を入力
 - ※ `https://[Keycloak の FQDN]/realms/[レルム名]/protocol/saml`
- [IdP SLO URL] を入力
 - ※ `https://[Keycloak の FQDN]/realms/[レルム名]/protocol/saml`
- [IdP 署名用証明書]に IdP 署名用証明書ファイルを指定
 - ※署名用証明書はメタデータ(XML)から取得する
 - ※ `https://[Keycloak の FQDN]/realms/[レルム名]/protocol/saml/descriptor`
- [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

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 (Keycloak 連携)

- [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
- [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
✖
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
✖
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
 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。

[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。

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 (Keycloak 連携)

認証デバイス情報

▶ iPhone / iPadの設定

iPhone/iPad 用 UA を利用する

保存

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`

※URL `https://[KeycloakのFQDN]/realms/[レルム名]/protocol/saml/clients/gleas-ua/`

Keycloakのログインページに遷移します。



[ユーザー名]、[パスワード]を入力して[ログイン]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 (Keycloak 連携)

9.2. クライアント証明書のインポート

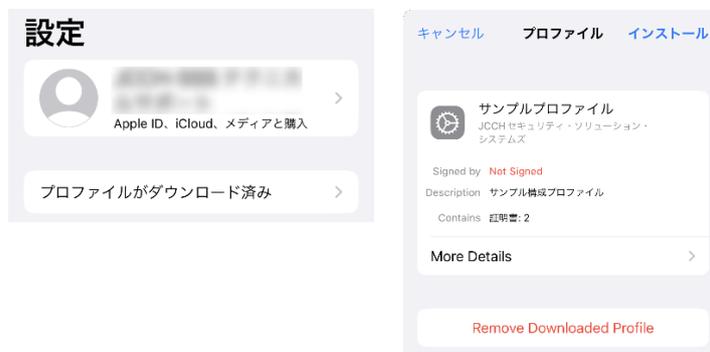
[ダウンロード]をタップし、構成プロファイルのダウンロードをおこないます。



※ 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。



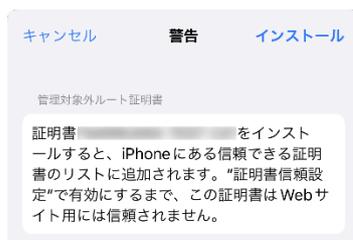
[インストール]をタップして続行してください。

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 (Keycloak 連携)

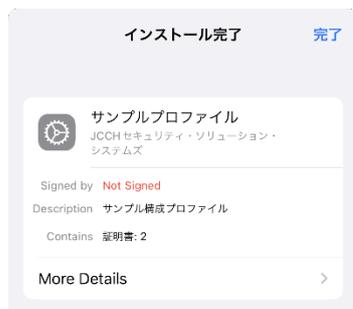
インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し

[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 (Keycloak 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 shows a user profile page for 'テストユーザー' (Test User) in the Gléas UA system. The page includes a header with the Gléas UA logo and a 'ログアウト' (Logout) button. The user information is displayed in a table-like format:

テストユーザーさんのページ	
ユーザーID	[Redacted]
姓	テスト
名	ユーザー
メール	[Redacted]
有効期限	ダウンロード済み
有効期限	ダウンロード済み

At the bottom of the page, there is a 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Keycloakのクライアント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 (Keycloak 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)

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

[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]に任意に URL を入力
 - ※ UA の「ログイン画面に戻る」リンクで遷移する URL となります
- [ログアウト URL]に任意の URL を入力
 - ※ UA の「ログアウト」リンクで遷移する URL となります/
- [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://\[KeycloakのFQDN\]/realms/\[レルム名\]](https://[KeycloakのFQDN]/realms/[レルム名])
- [IdP SSO URL] を入力
 - ※ [https://\[KeycloakのFQDN\]/realms/\[レルム名\]/protocol/saml](https://[KeycloakのFQDN]/realms/[レルム名]/protocol/saml)
- [IdP SLO URL] を入力
 - ※ [https://\[KeycloakのFQDN\]/realms/\[レルム名\]/protocol/saml](https://[KeycloakのFQDN]/realms/[レルム名]/protocol/saml)
- [IdP 署名用証明書]に IdP 署名用証明書ファイルを指定
 - ※署名用証明書はメタデータ(XML)から取得する
 - ※ [https://\[KeycloakのFQDN\]/realms/\[レルム名\]/protocol/saml/descriptor](https://[KeycloakのFQDN]/realms/[レルム名]/protocol/saml/descriptor)
- [IdP 暗号用証明書]は指定しない

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 (Keycloak 連携)

- [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
- [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
✖
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
✖
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
 ログアウトレスポンスに署名
 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 (Keycloak 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。



▶ Android の設定

Android 用 UA を利用する

ダウンロードの動作

ログインパスワードで証明書を保護 数字のみの PIN を表示

証明書ダウンロードの種類 PKCS#12ダウンロード

保存

証明書のダウンロード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。

- [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 (Keycloak 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`

※URL `https://[KeycloakのFQDN]/realms/[レルム名]/protocol/saml/clients/gleas-ua/`

Keycloakのログインページに遷移します。



[ユーザー名]、[パスワード]を入力して[ログイン]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 Gleás ホワイトペーパー
シングルサインオンによる Gleás UA ログイン (Keycloak 連携)

11.2. クライアント証明書のインポート

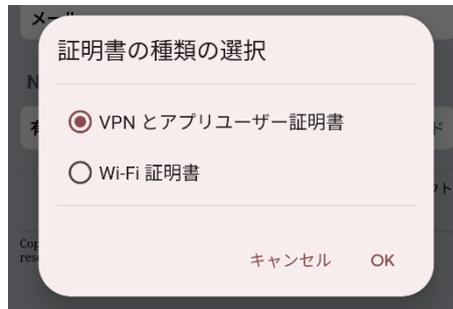
[ダウンロード]をタップし、証明書ファイルのダウンロードをおこないます。



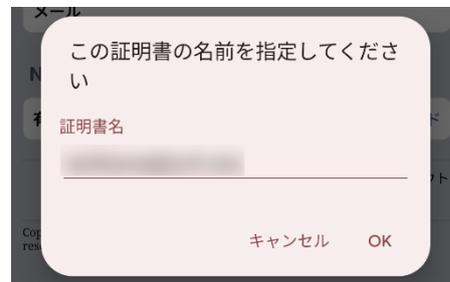
- ※ 「証明書 PIN」の値を「証明書を抽出」のパスワードとして入力します。
- ※ インポートロックを有効にしている場合は、この時点からカウントが開始されます

[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。

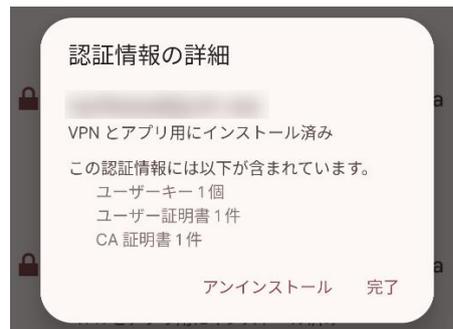
プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (Keycloak 連携)

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 Gleás ホワイトペーパー
シングルサインオンによる Gleás UA ログイン (Keycloak 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