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

目次

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： 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

- 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

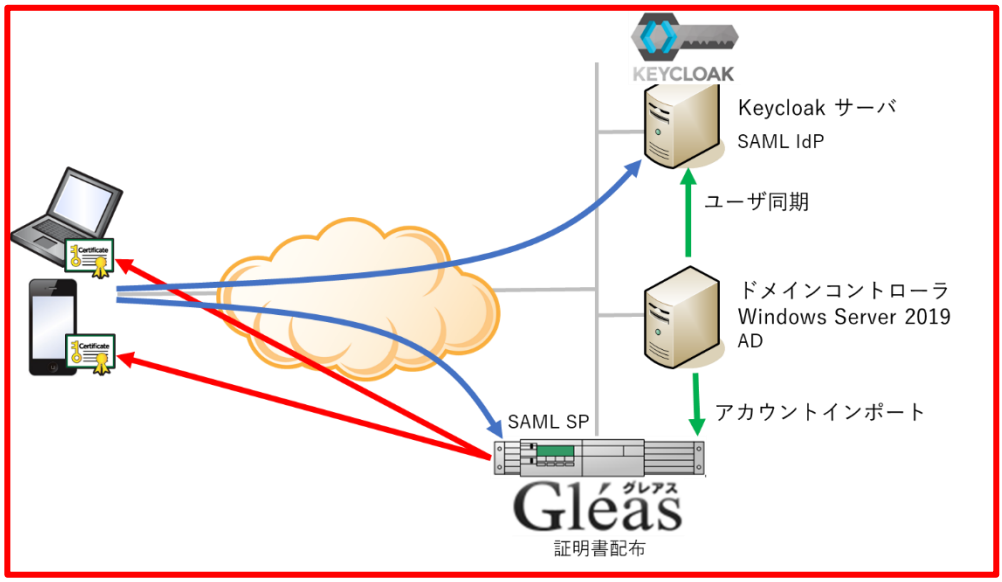
以下については、本書では説明を割愛します。

- 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。

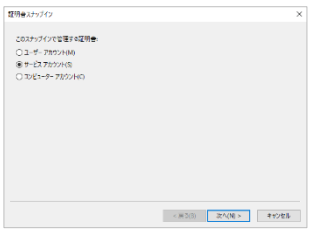
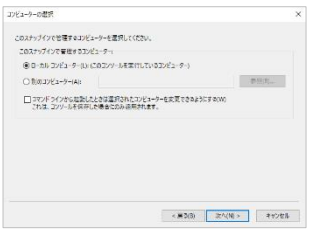
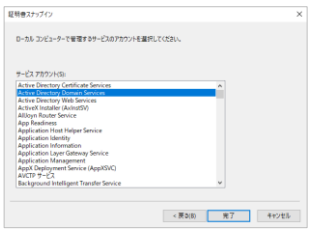
MMC を開き、メニューの[ファイル(F)] > [スナップインの追加と削除(N)]より[証明書]を追加します。

「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、

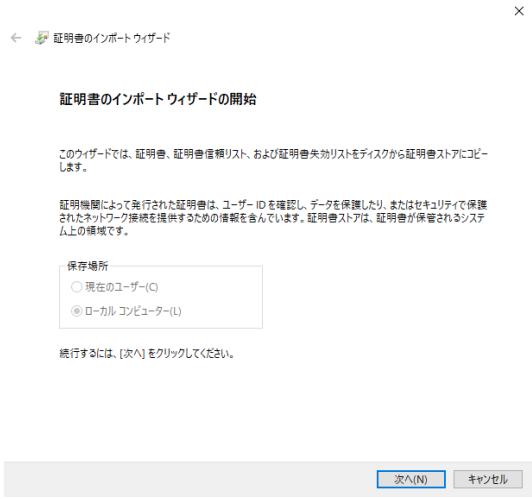
次の「証明書スナップイン」では、[Active Directory Domain Services)]を選択し、

[完了]をクリックします。

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

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。

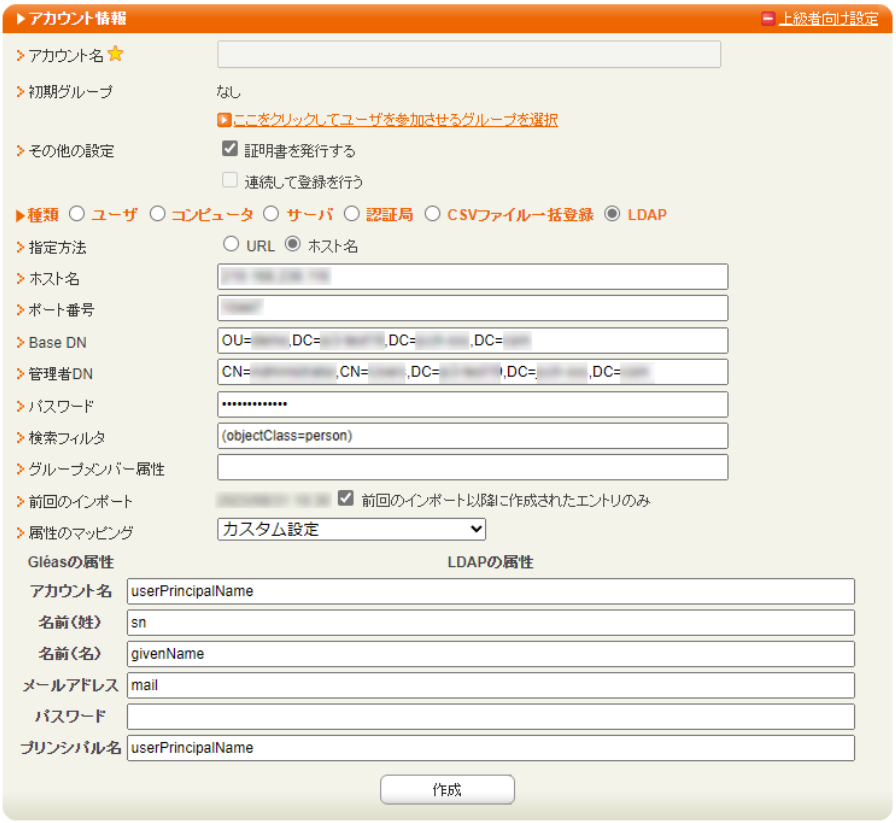
3. Gléas アカウントの登録

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。



- [▸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

- [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

[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

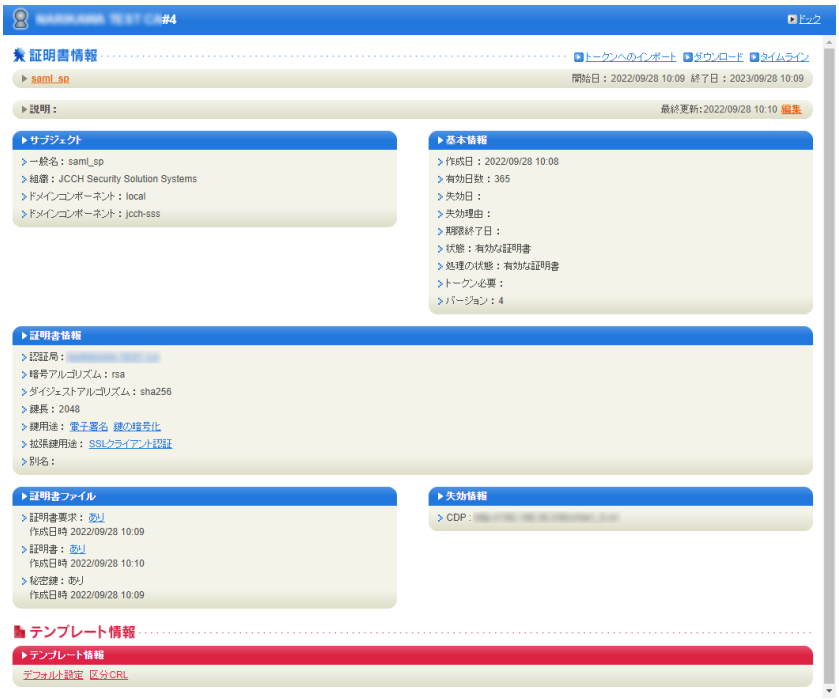
SAML SPとして使用する署名用証明書をGléasから発行します。

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。

[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。

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。

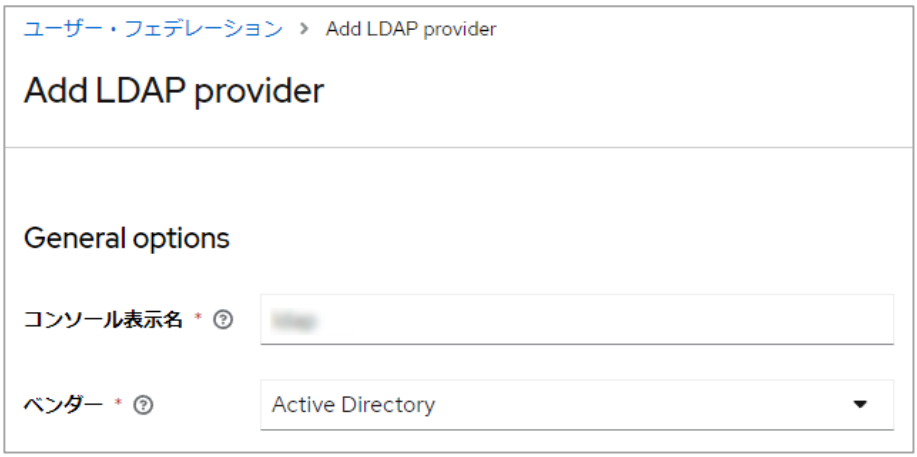
Keycloak 管理コンソール にログインします。

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



【Connection and authentication settings】

- [接続 URL] に AD の URL を入力

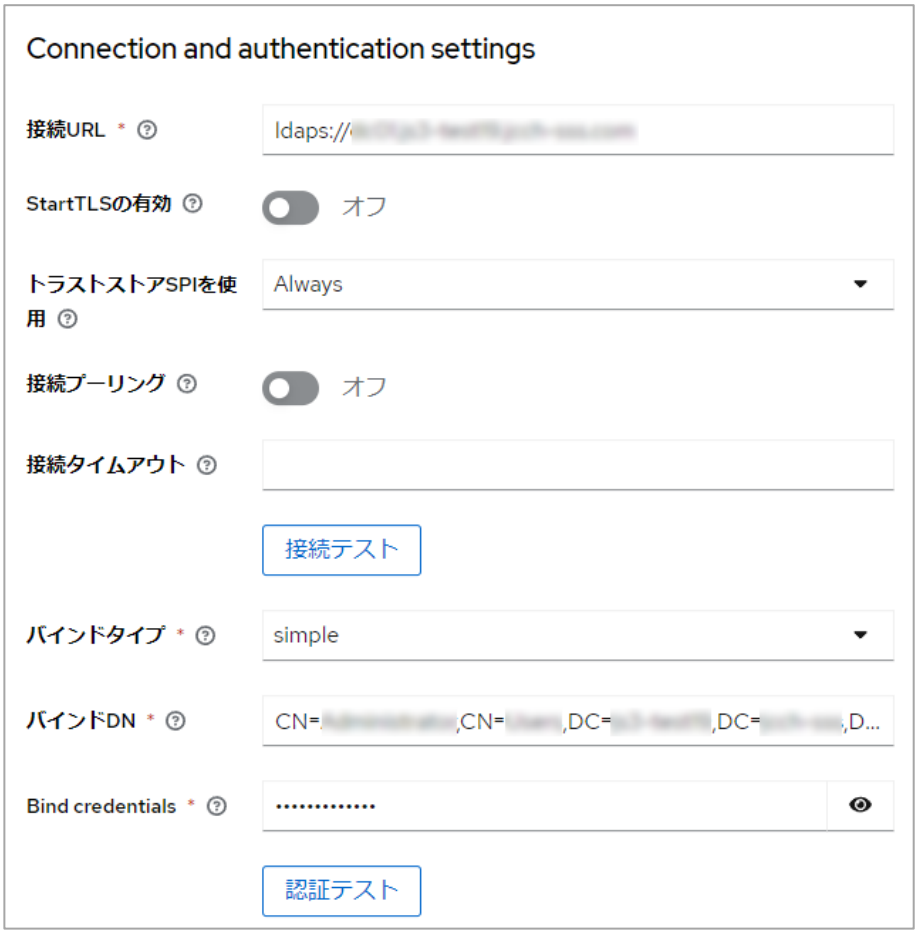
  ※ ldaps://[AD の FQDN]

- [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



【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

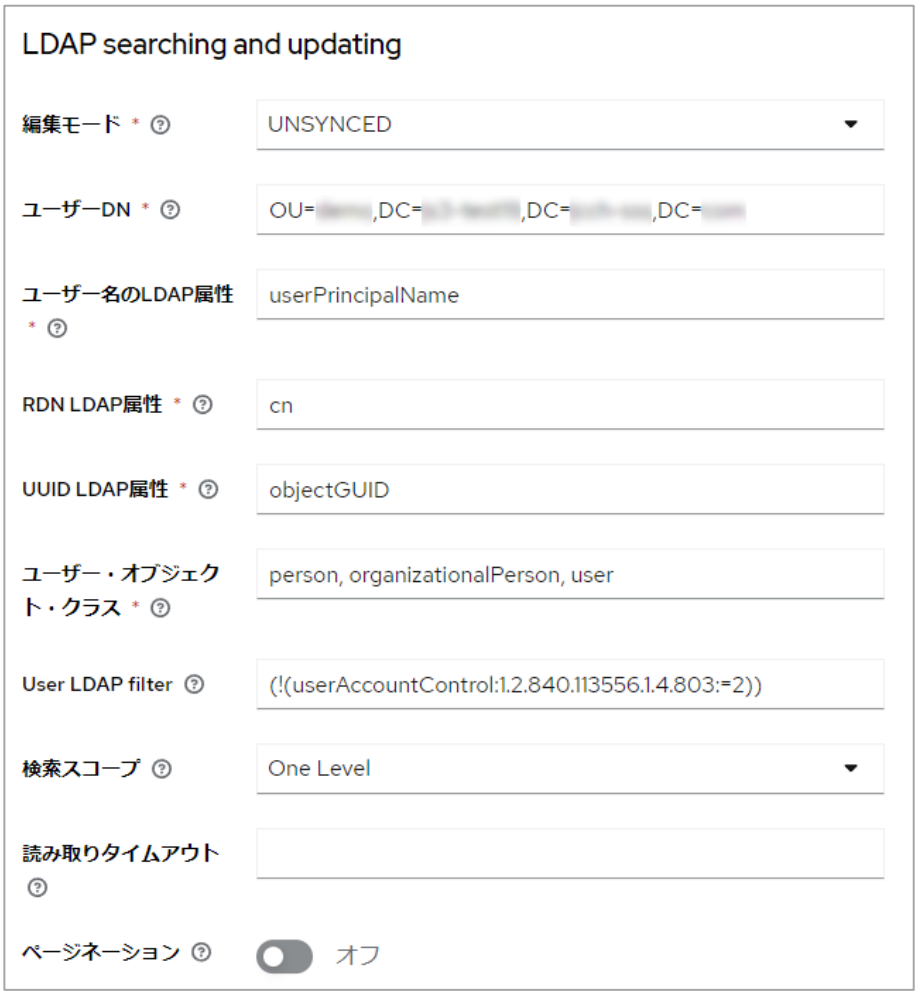
  ※例) userPrincipalName

- [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

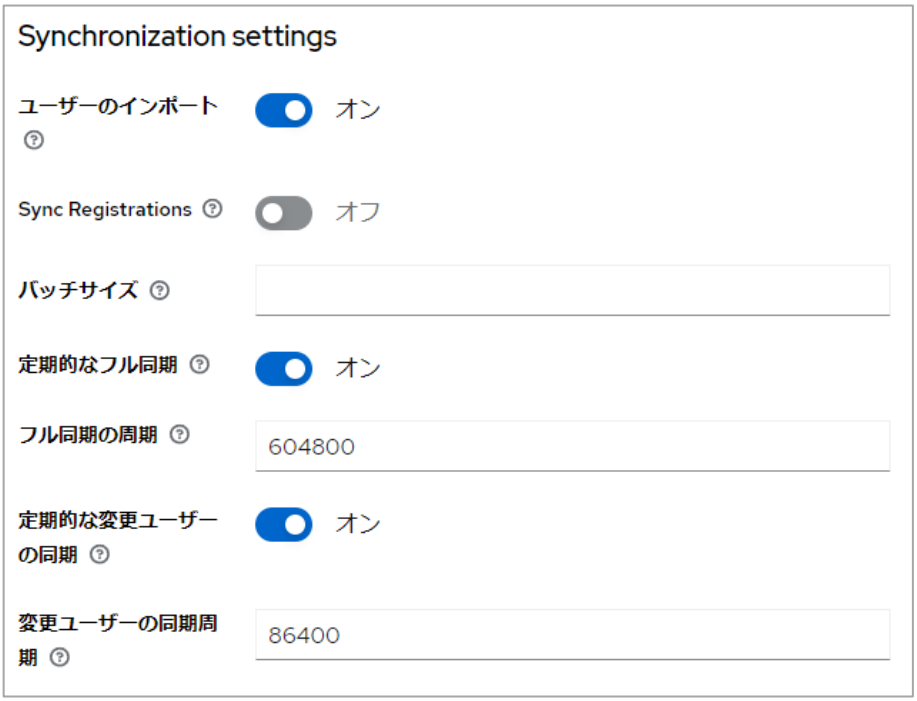
  ※例) “(!(userAccountControl:1.2.840.113556.1.4.803:=2))” とすると有効化したユーザのみ


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

【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



- [保存] をクリックして設定を保存

[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。

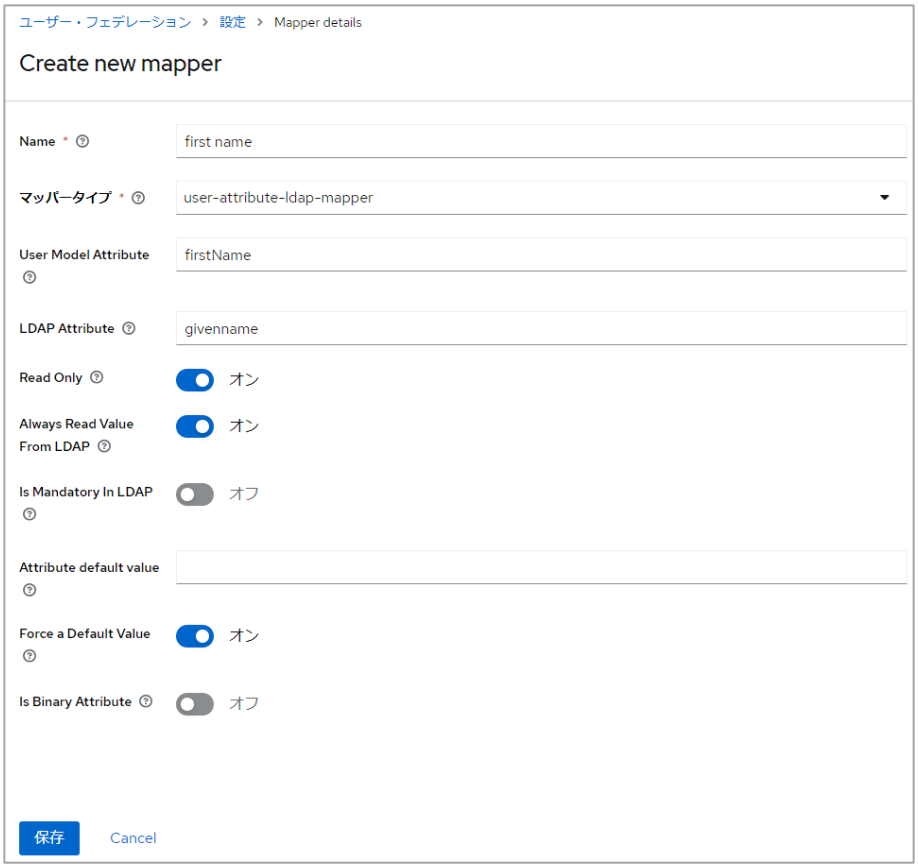
Keycloak のユーザ属性	LDAP の属性
ユーザ名	userPrincipalName
名前（姓）	sn
名前（名）	givenName
E メール	mail

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】

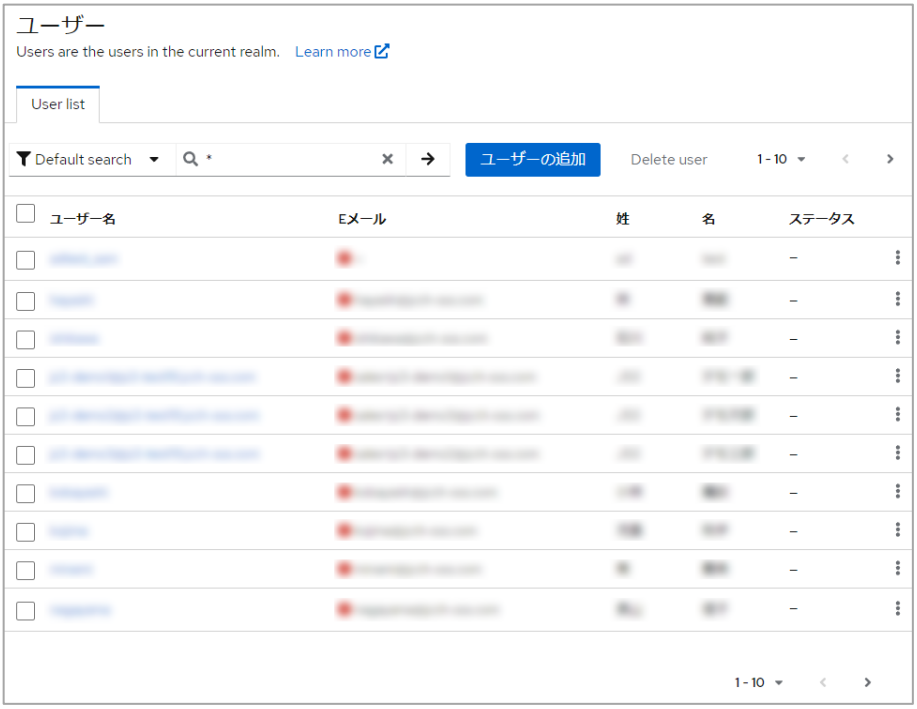
- [Name] に“first name”を入力
- [Mapper type] に [user-attribute-ldap-mapper] を選択
- [User Model Attribute] に "firstName" を入力
- [LDAP Attribute] に "givenname" を入力
- [Read Only] に [On] を選択
- [Always Read Value From LDAP] に [On] を選択
- [保存] をクリック


ユーザー・フェデレーション
設定
Mapper details
Create new mapper
Name *
first name
マッパータイプ *
user-attribute-ldap-mapper
User Model Attribute
firstName
LDAP Attribute
givenname
Read Only
オン
Always Read Value From LDAP
オン
Is Mandatory In LDAP
オフ
Attribute default value
Force a Default Value
オン
Is Binary Attribute
オフ
保存
Cancel

[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。



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。

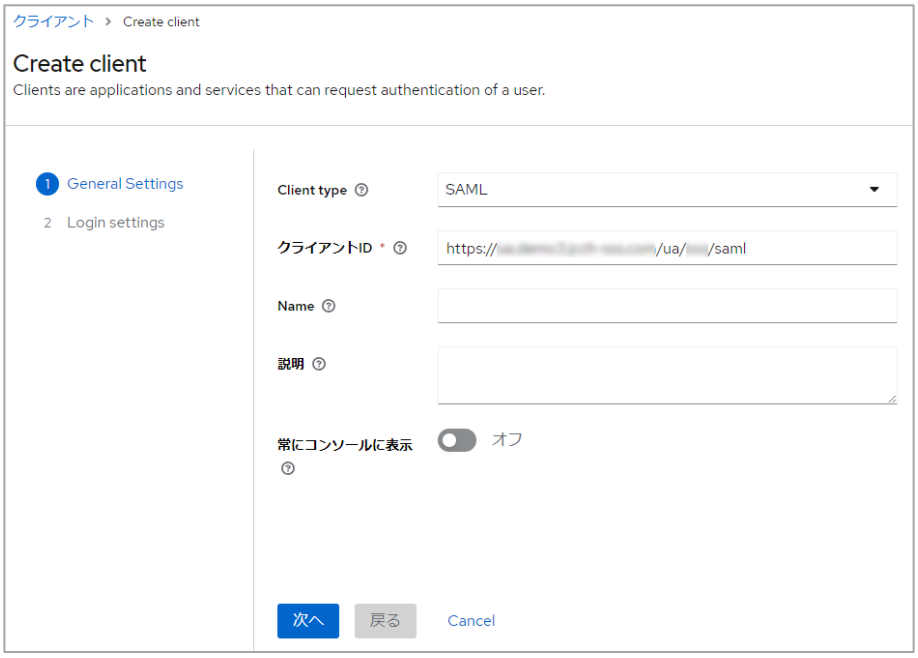
メニュー [クライアント] を選択します。

[Create client] をクリックします。

【① General Setteings】

- [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



【② Login settings】

- [Home URL] を入力

  ※ https://[UA の FQDN]/ua/[UA 名]/saml/sso

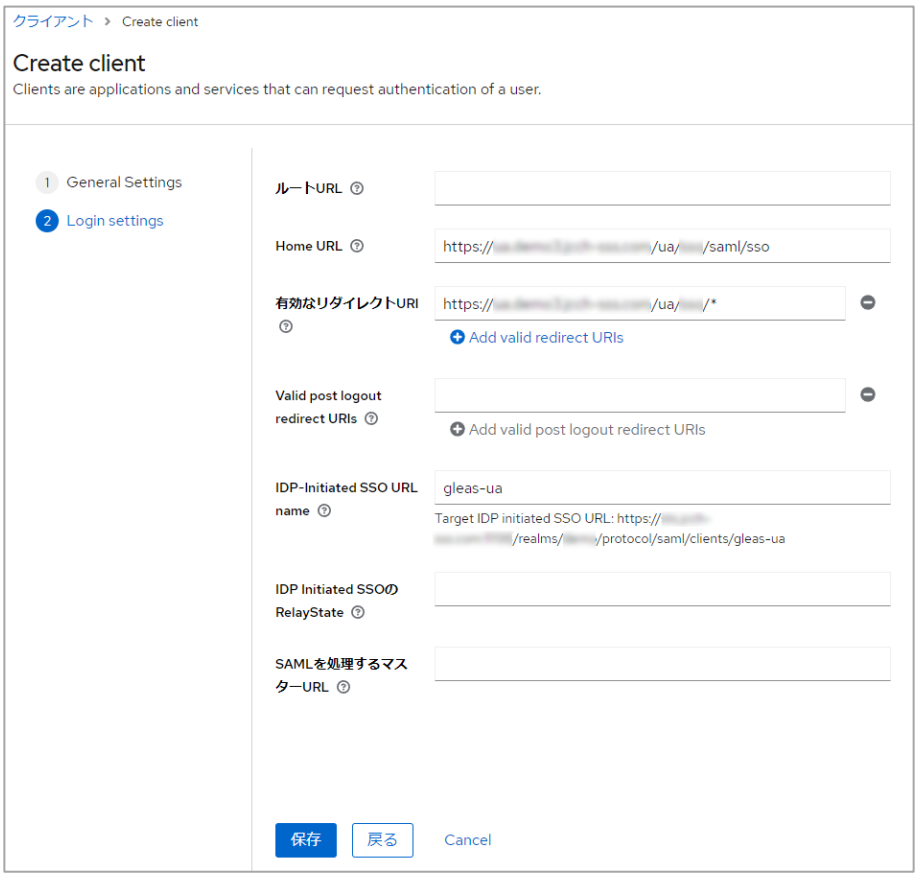
- [有効なリダイレクト URI] を入力

  ※ 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。

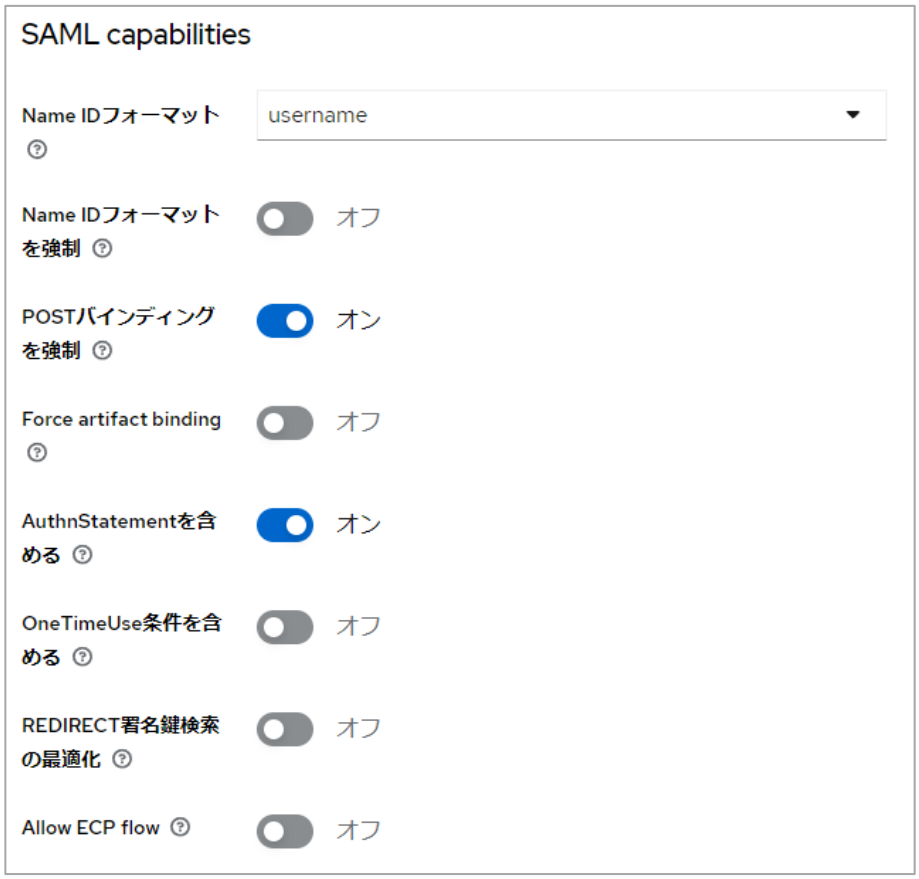
- [保存] をクリック



[設定] タブを選択

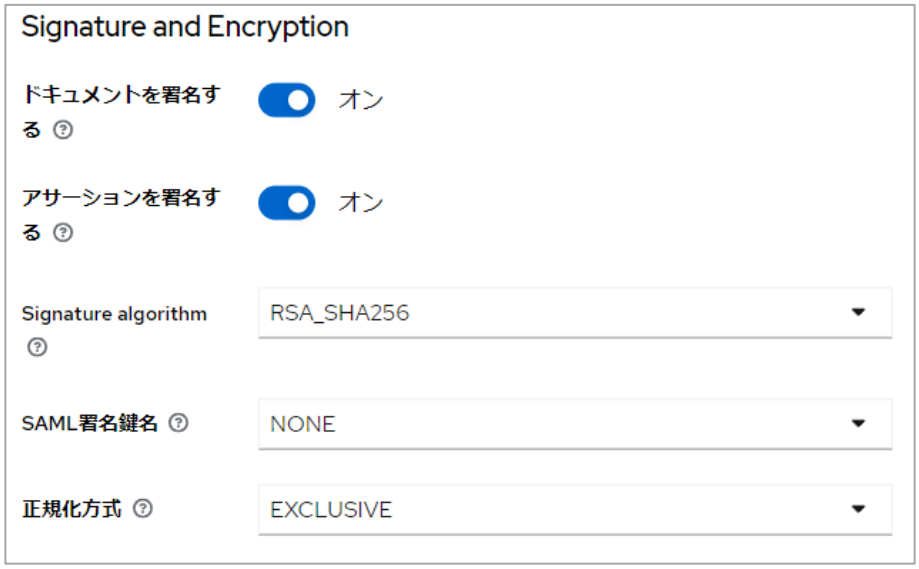
【SAML capabilities】

- [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



【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

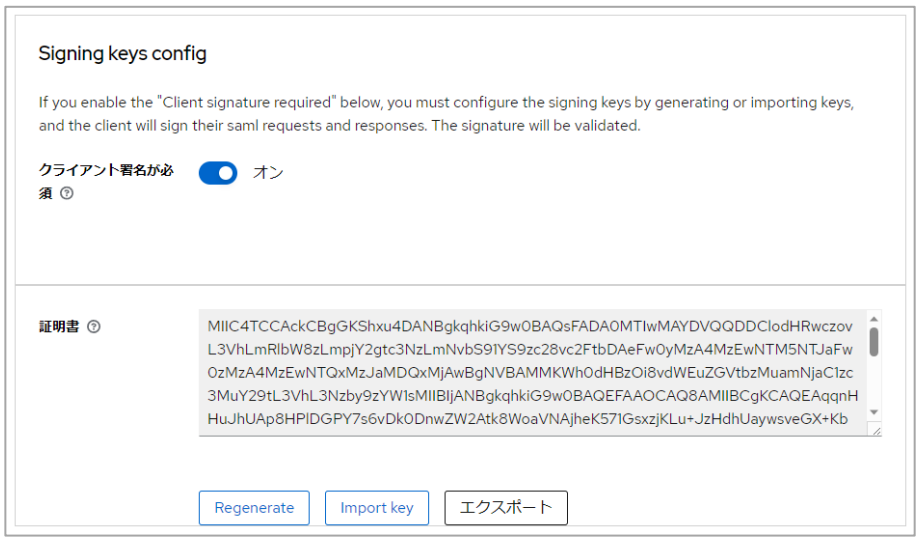


- [保存] をクリック

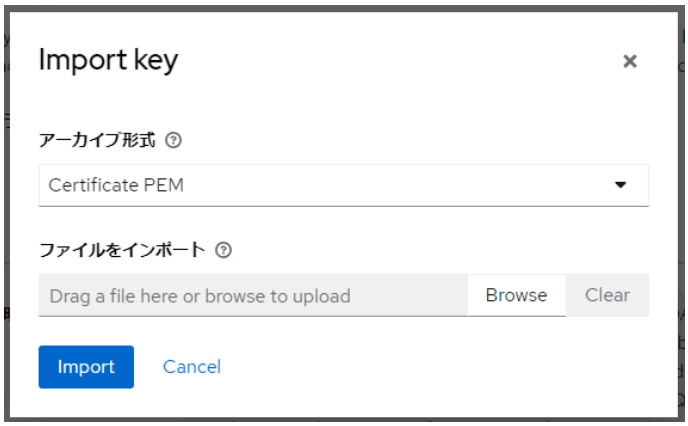
[鍵] タブを選択

【Signing keys config】

- [クライアント署名が必須] に [On] を選択



- [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

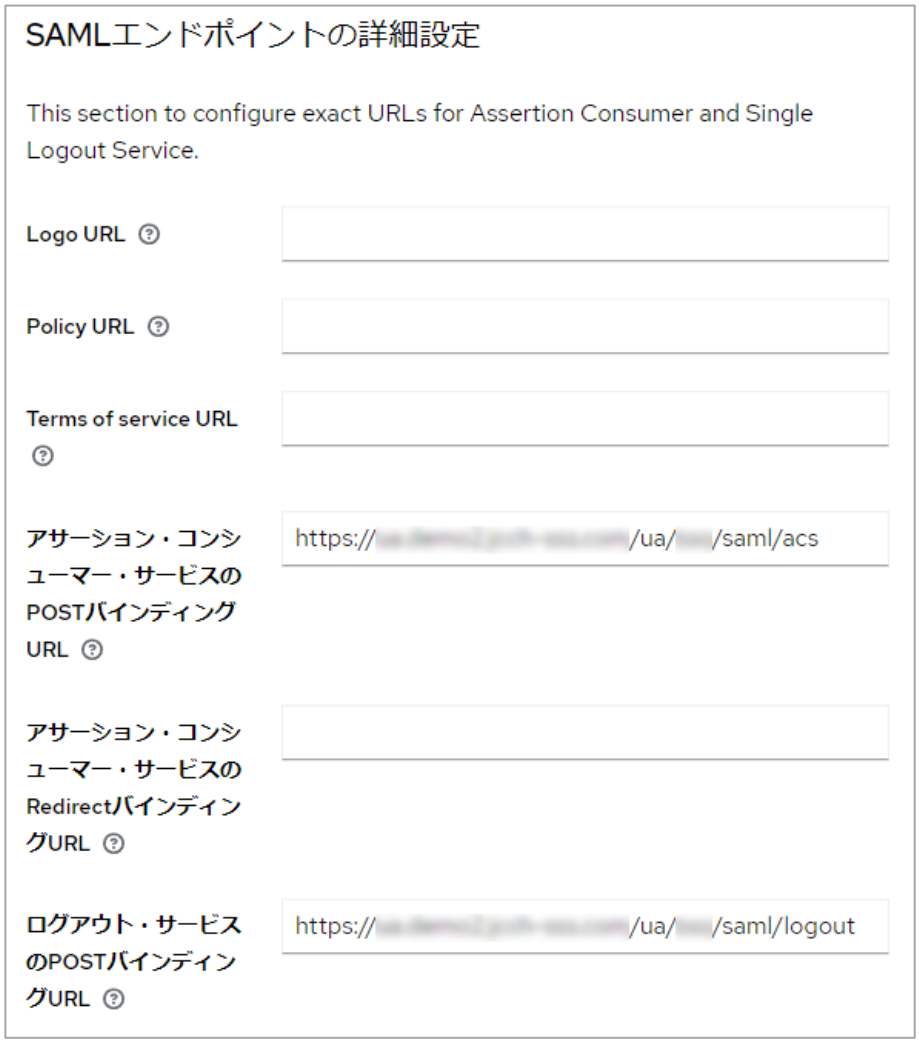


- [保存] をクリック

[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"



- [保存] をクリック

※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。

- [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

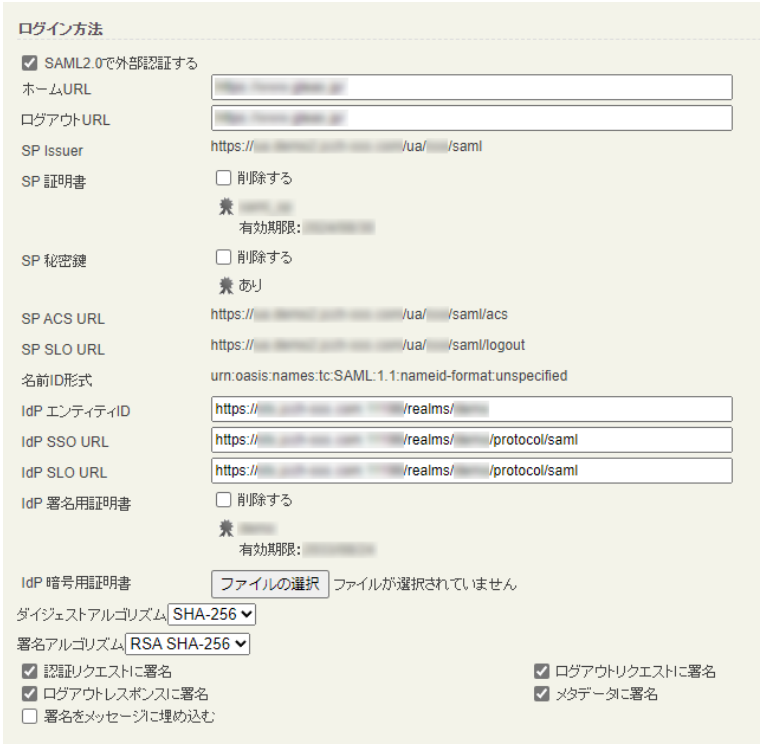
  ※ https://[Keycloak の FQDN]/realms/[レルム名]/protocol/saml
- [IdP SLO URL] を入力

  ※ 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
- [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



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。

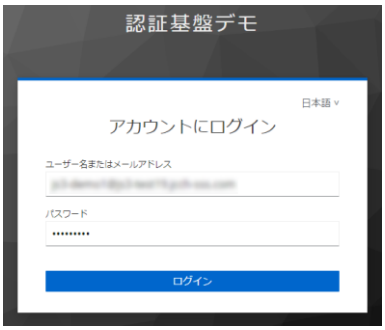
7. クライアントからのアクセス（Windows）

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。

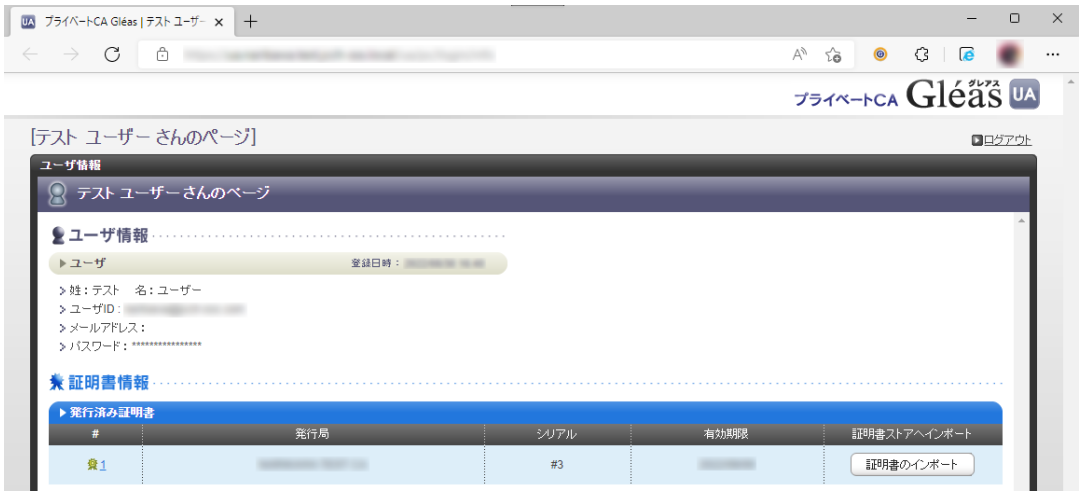


[ユーザー名]、[パスワード]を入力して[ログイン]をクリックします。

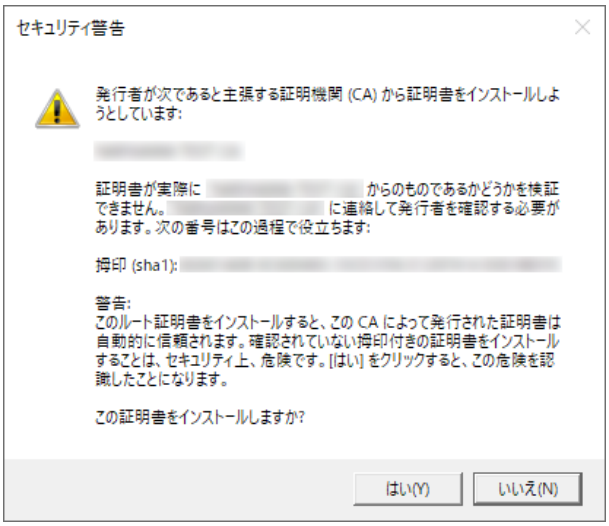
UAにログインし、ユーザ専用ページが表示されます。

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



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。

[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

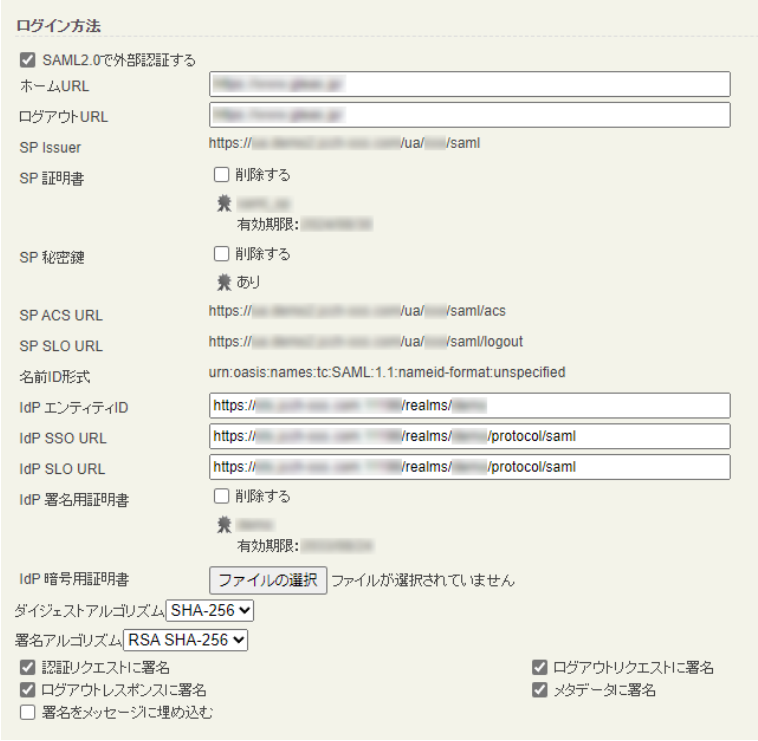
  ※ https://[Keycloak の FQDN]/realms/[レルム名]/protocol/saml
- [IdP SLO URL] を入力

  ※ 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

- [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



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。

構成プロファイルに必要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。

【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）

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。

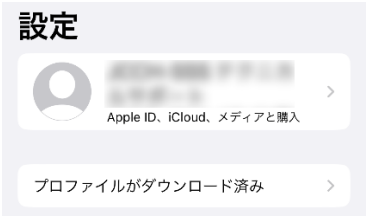
UAにログインし、ユーザ専用ページが表示されます。

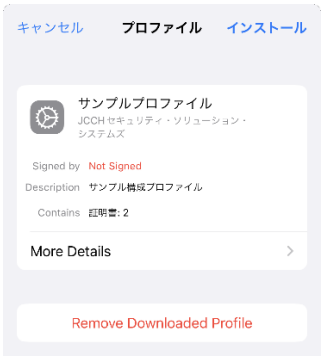
9.2. クライアント証明書のインポート

[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。



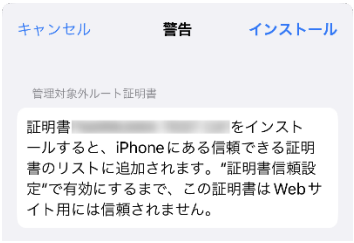


[インストール]をタップして続行してください。

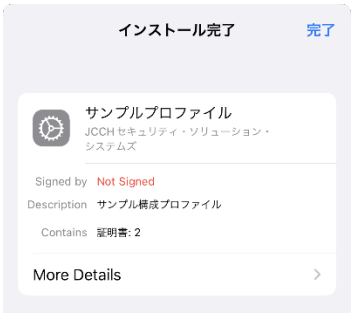
インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し

[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。

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。

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。

[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
- [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

設定完了後、[保存]をクリックし保存します。

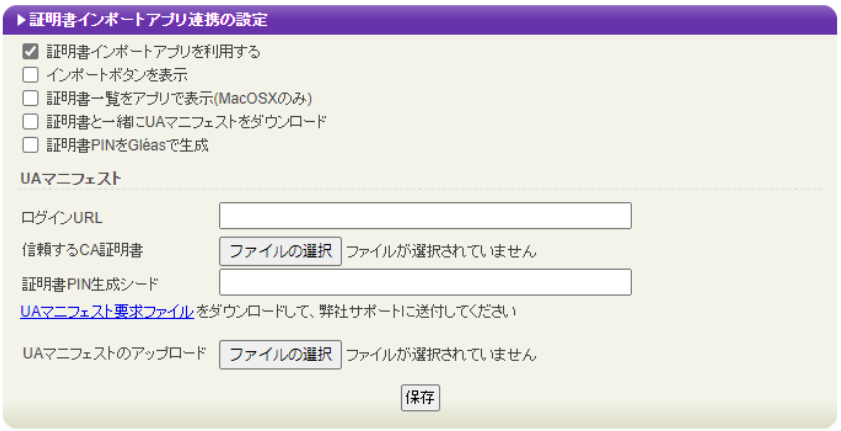
[認証デバイス情報]の[Androidの設定]までスクロールし、[Android用UAを利用する]をチェックします。

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。

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。



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。

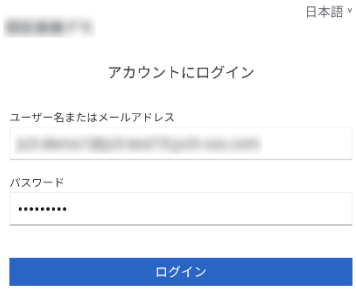
11. クライアントからのアクセス（Android）

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。

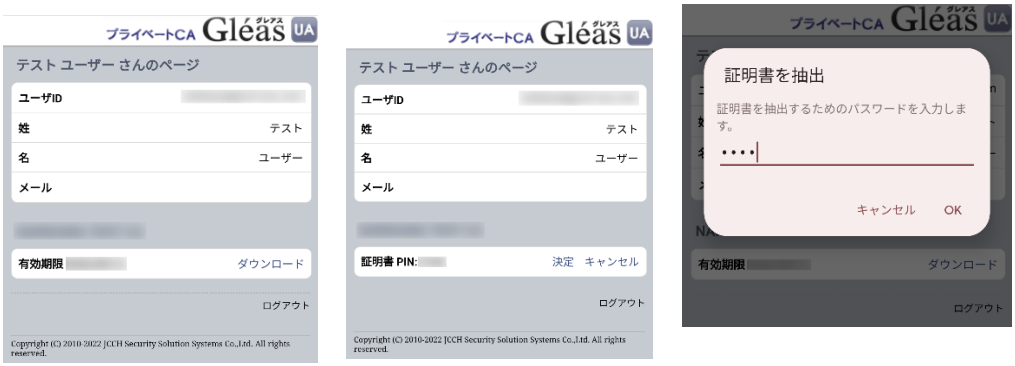


[ユーザー名]、[パスワード]を入力して[ログイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

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。

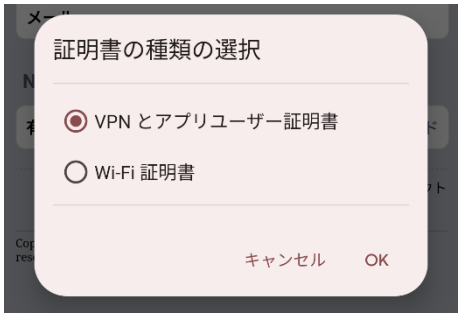


※　「証明書 PIN」の値を「証明書を抽出」のパスワードとして入力します。

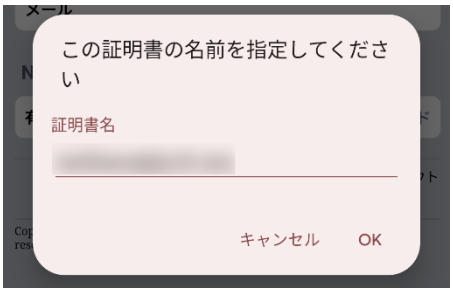
※　インポートロックを有効にしている場合は、この時点からカウントが開始されます

[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。

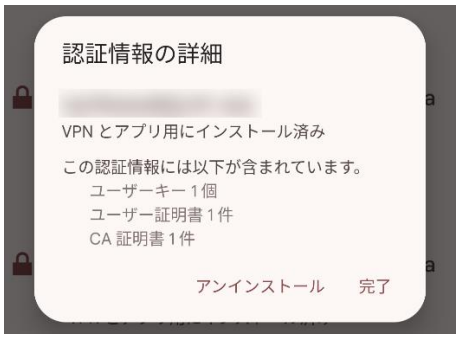


[OK]をタップします。

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。

[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