



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 (AD FS 連携)

Ver.1.1

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 (AD FS 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. AD FS の設定	16
5.1. SAML SP 署名用証明書の信頼	16
5.2. 証明書利用者信頼を追加	18
5.3. 証明書利用者信頼の設定	27
5.4. SAML IdP 暗号用証明書の取得	32
5.5. SAML IdP 署名用証明書の取得	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 (AD FS 連携)

6. Gléas の管理者設定 (Windows 向け)	36
7. クライアントからのアクセス (Windows)	39
7.1. シングルサインオンで UA にログイン	39
7.2. クライアント証明書のインポート	41
8. Gléas の管理者設定 (iPhone 向け)	43
9. クライアントからのアクセス (iPhone)	47
9.1. シングルサインオンで UA にログイン	47
9.2. クライアント証明書のインポート	49
10. Gléas の管理者設定 (Android 向け)	52
11. クライアントからのアクセス (Android)	57
11.1. シングルサインオンで UA にログイン	57
11.2. クライアント証明書のインポート	59
12. 問い合わせ	62

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、Active Directory フェデレーション サービス (AD FS) の証明書利用者として登録し、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 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
- Active Directory フェデレーション サービス： Microsoft Windows Server 2019
 - ※以後「ADFS」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 (AD FS 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。
- Web アプリケーション プロキシ : Microsoft Windows Server 2019
※以後「WAP」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。

- AD、ADFS、WAP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 での UA へのログイン方法

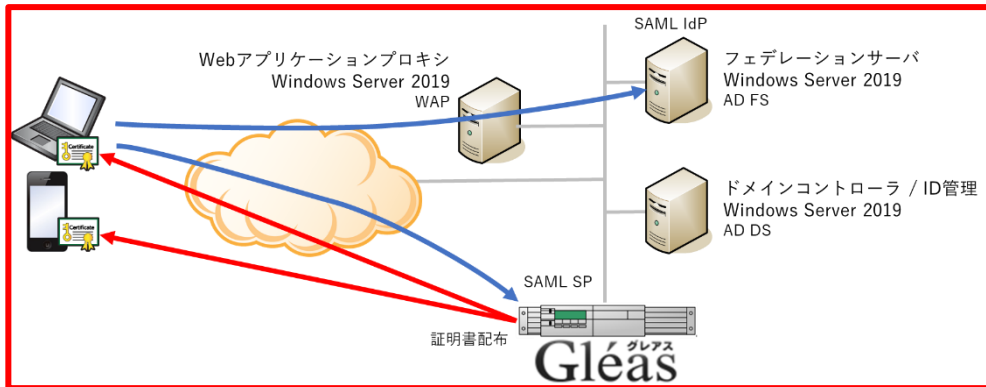
これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている

販売店にお問い合わせください。

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 (AD FS 連携)

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ADFSのサインイン画面に画面遷移。ADFS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ADFSのログイン画面に画面遷移。ADFS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ADFSのログイン画面に画面遷移。ADFS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。

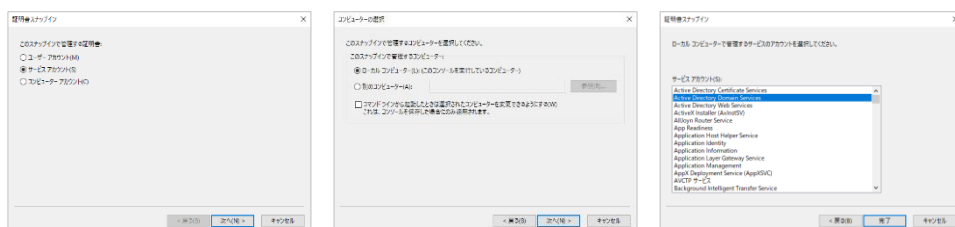
MMC を開き、メニューの[ファイル(F)] > [スナップインの追加と削除(N)]より[証明書]を追加します。

「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、

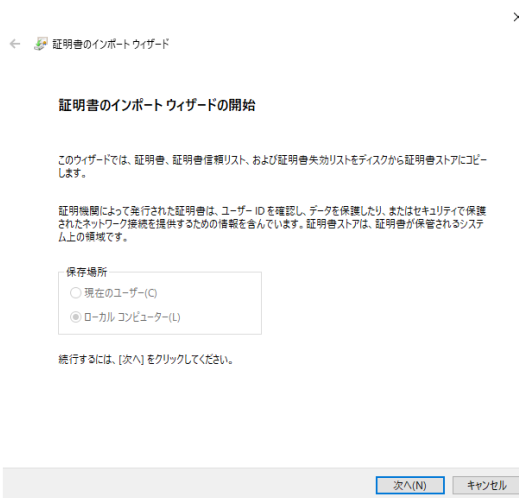
[完了]をクリックします。



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 (AD FS 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 (AD FS 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 interface. 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 '属性のマッピング' (Attribute Mapping) section is expanded, showing the mapping of Gléas attributes to LDAP attributes. The '作成' (Create) button is visible 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 (AD FS 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	sn
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。

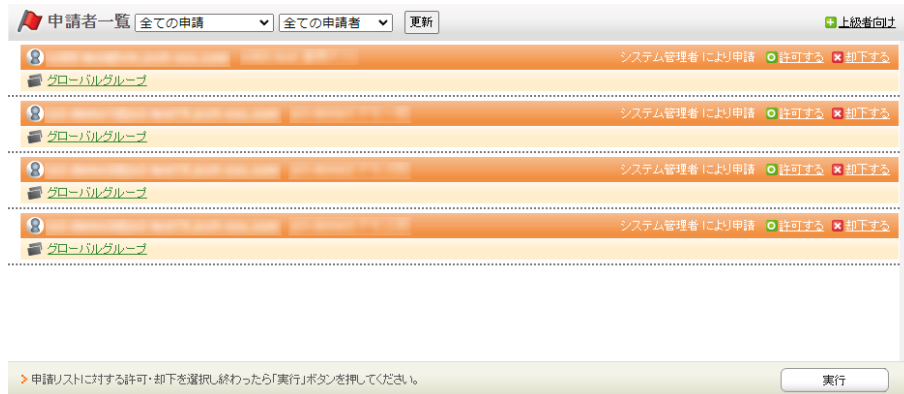


- 内容を確認し[実行]をクリック

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 (AD FS 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。

※ADFSとの連携に使用するSAML SP署名用証明書には、CRL配布ポイントの記載が必要となりますのでご注意ください。詳しくはお問い合わせください。

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。

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

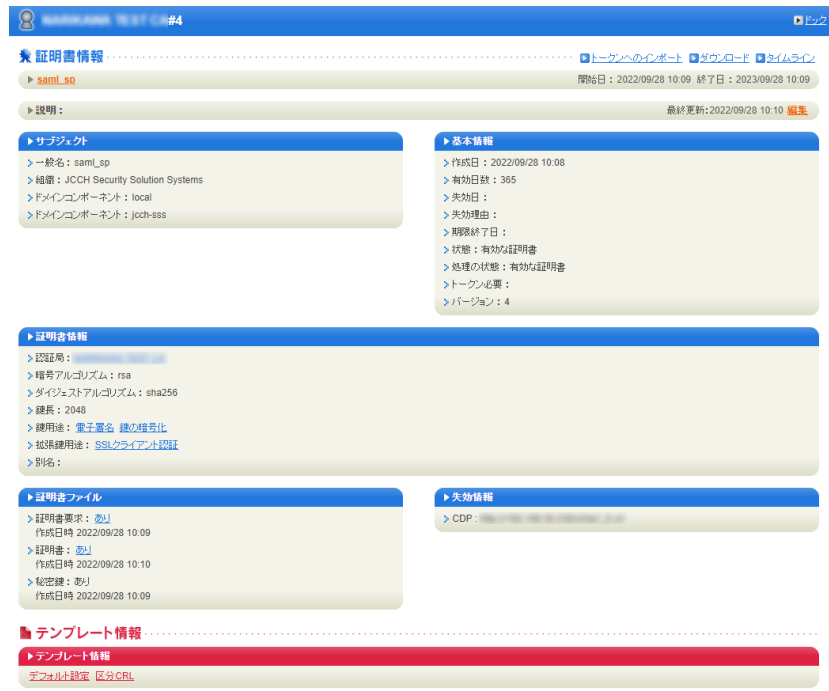
- 必須 デフォルト設定
- 必須 区分CRL

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 (AD FS 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. AD FS の設定

5.1. SAML SP 署名用証明書の信頼

SAML SP 署名用証明書を ADFS が信頼できるようにします。

Gléas からルート証明書をダウンロードします。

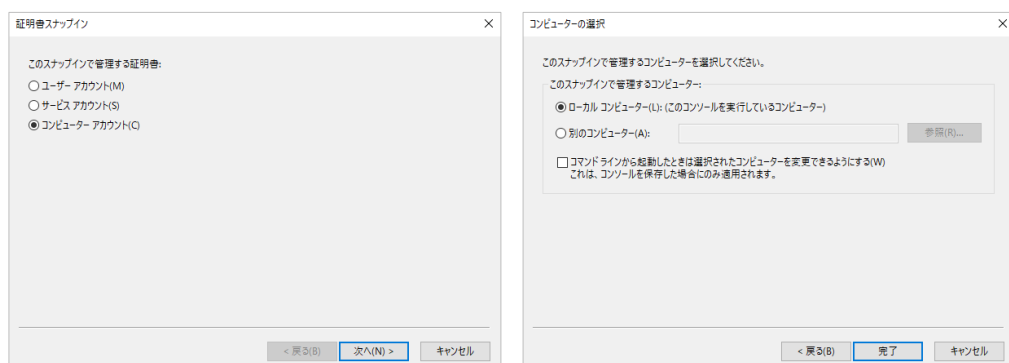
※ダウンロードURLは、 `https://[RAのFQDN]/crl/ia1.pem`

※PowerShellで行なう例

```
Invoke-WebRequest "http://[RA の FQDN]/crl/ia1.pem" -OutFile "ia1.cer"
```

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。

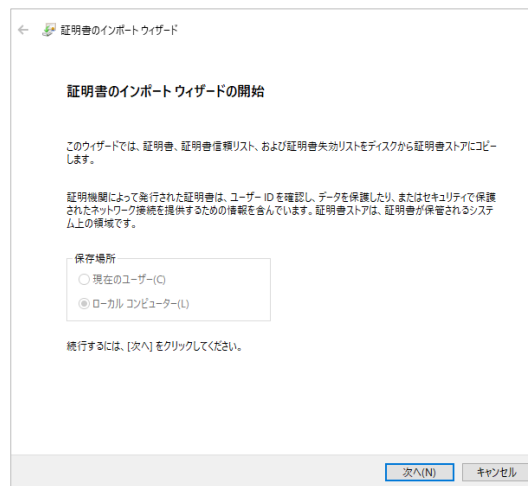
「証明書のスナップイン」では、[コンピューター アカウント(C)]を選択し、次の「コンピューターの選択」では、[ローカルコンピューター(L)]を選択し、[完了]をクリックします。



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 (AD FS 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)] > [信頼されたルート証明機関]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、ルート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	ルート証明書ファイル (拡張子: pem/der/crt) を指定して、[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[信頼されたルート証明機関]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 (AD FS 連携)

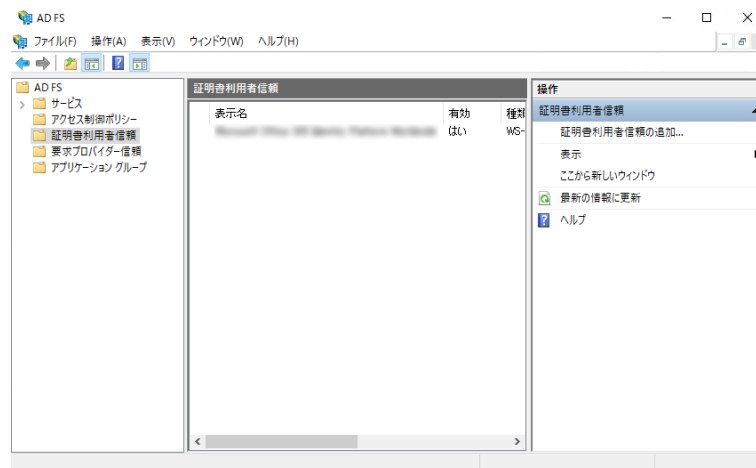
5.2. 証明書利用者信頼を追加

証明書利用者信頼として UA を登録します。

スタートメニューから [ADFS の管理] を起動します。

左ペインの [証明書利用者信頼] を選択します。

右ペインの [証明書利用者信頼の追加...] をクリックします。



証明書利用者信頼の追加ウィザードが起動します。

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 (AD FS 連携)

[ようこそ] ページ

- [要求に対応する(C)] を選択



[開始(S)] をクリックします。

[データ ソースの選択] ページ

- [証明書利用者についてのデータを手動で入力する(T)] を選択

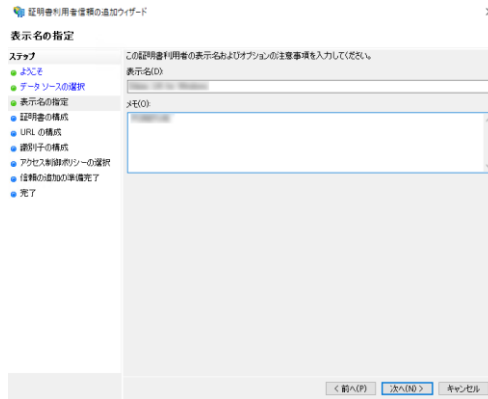


[次へ(N)>] をクリックします。

[表示名の指定] ページ

- [表示名(I)] に任意の名前を入力
- [メモ(C)] に証明書利用者の説明を入力

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 (AD FS 連携)



[次へ(N)>] をクリックします。

証明書の構成] ページ

※オプション



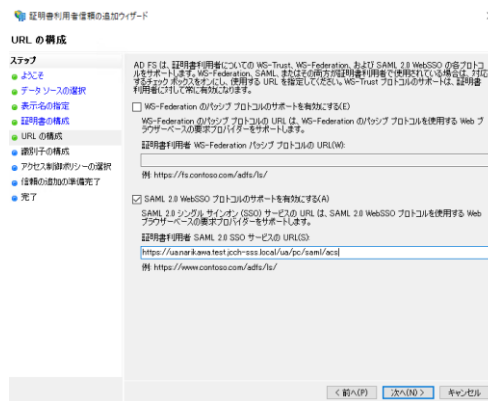
[次へ(N)>] をクリックします。

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 (AD FS 連携)

[URL の構成] ページ

- [SAML 2.0 WebSSO プロトコルのサポートを有効にする(A)] をチェック
- [証明書利用者 SAML 2.0 SSO サービスの URL(S)] 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)



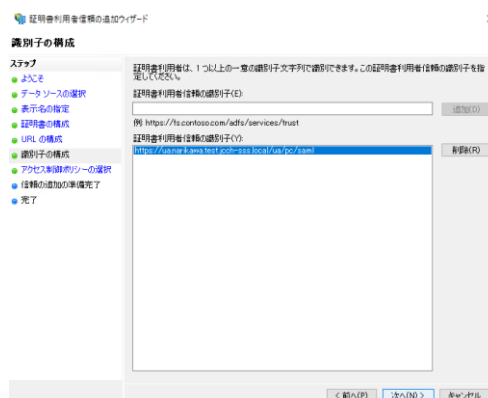
[次へ(N)>] をクリックします。

[識別子の構成] ページ

- [証明書利用者信頼の識別子(E)] を入力

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

- [追加(D)] をクリック

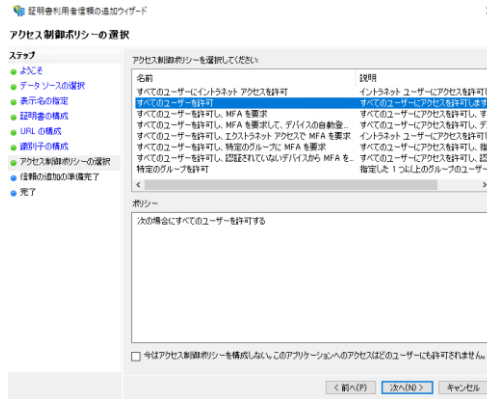


[次へ(N)>] をクリックします。

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 (AD FS 連携)

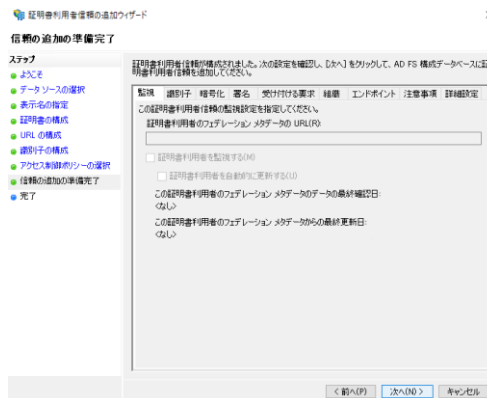
[アクセス制御ポリシーの選択] ページ

- [アクセスポリシーを選択してください] で [すべてのユーザーを許可] を選択



[次へ(N)>] をクリックします。

[信頼の追加の準備完了] ページ



[次へ(N)>] 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 (AD FS 連携)

[完了] ページ

- [このアプリケーションの要求発行ポリシーを構成する(C)] をチェック



[閉じる(C)] をクリックします。

自動的に [要求発行ポリシーの編集] ダイアログボックスが表示されます。



[規則の追加(A)...] をクリックします。

変換要求規則の追加ウィザードが表示されます。

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 (AD FS 連携)

[規則テンプレートの選択] ページ

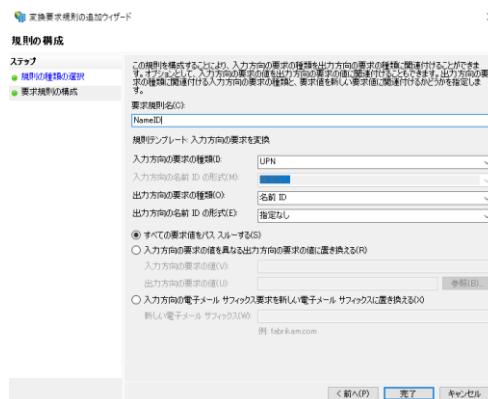
- [要求規則テンプレート(C)] に [入力方向の要求を変換] を選択



[次へ(N)>] をクリックします。

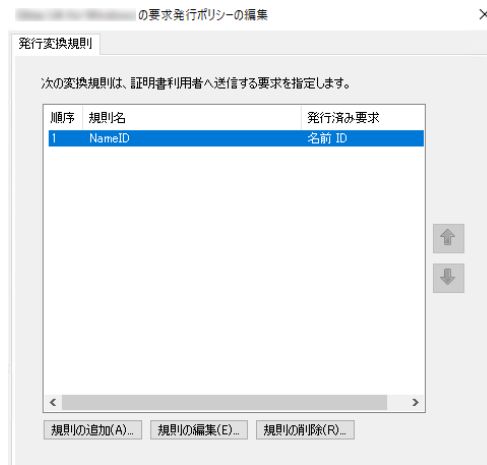
[規則の構成] ページ

- [要求規則名(C)] に "NameID" と入力
- [入力方向の要求の種類]に[UPN]を選択
- [出力方向の要求の種類]に[名前 ID]を選択
- [出力方向の名前 ID の形式]に[指定なし]を選択
- [すべての要求値をパススルーする]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 (AD FS 連携)

[完了] をクリックします。



[規則の追加(A)] をクリックします。

変換要求規則の追加ウィザードが表示されます。

[規則テンプレートの選択] ページ

- [要求規則テンプレート(C)] に [LDAP 属性を要求として送信] を選択



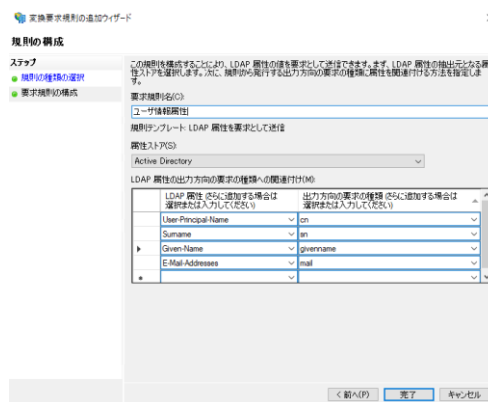
[次へ(N)>] をクリックします。

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 (AD FS 連携)

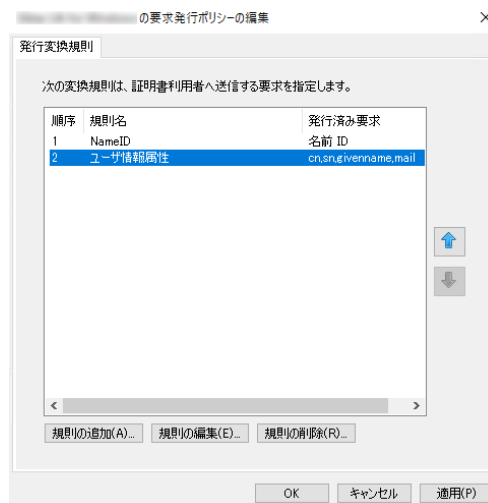
[規則の構成] ページ

- [要求規則名(C)] に "ユーザ情報属性" と入力
- [属性ストア(S)] に [Active Directory] を選択
- [LDAP 属性の出力方向の要求の種類への関連付け(M)] を以下のように入力

[LDAP 属性]	[出力方向の要求の種類]
[User-Principal-Name]	"cn"
[Surname]	"sn"
[Given-Name]	"givenname"
[E-Mail-Addresses]	"mail"



[完了] をクリックします。



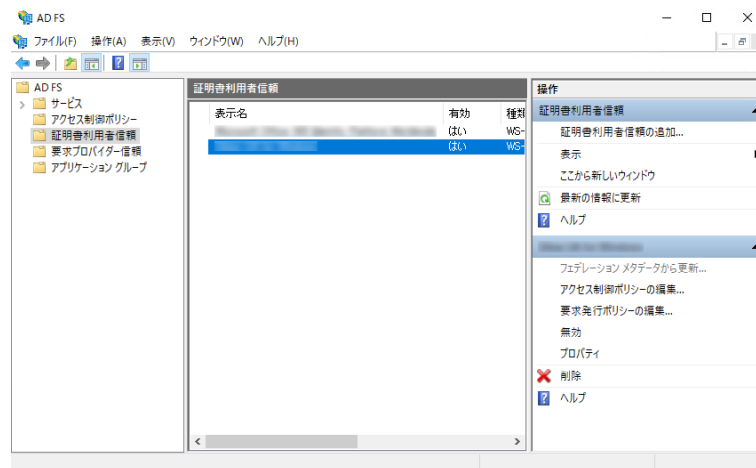
[OK] をクリックします。

5.3. 証明書利用者信頼の設定

証明書利用者信頼のその他設定を行います。

SAML SP 署名用証明書ファイルを ADFS サーバにコピーします。

スタートメニューから [ADFS の管理] を起動します。



左ペインの[証明書利用者信頼] を選択します。

中央ペインの [表示名] から 追加した証明書利用者信頼 を選択します。

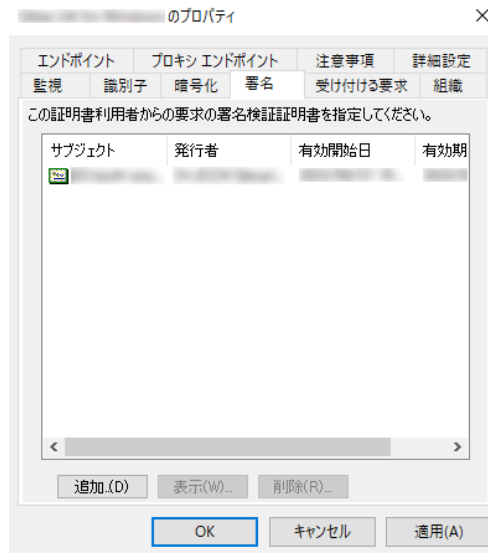
右ペインの[プロパティ]をクリックします。

[プロパティ]ダイアログが表示されます。

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 (AD FS 連携)

[署名]タブを選択します。

- [追加 (D)]をクリック
- SP の署名用証明書ファイルを選択

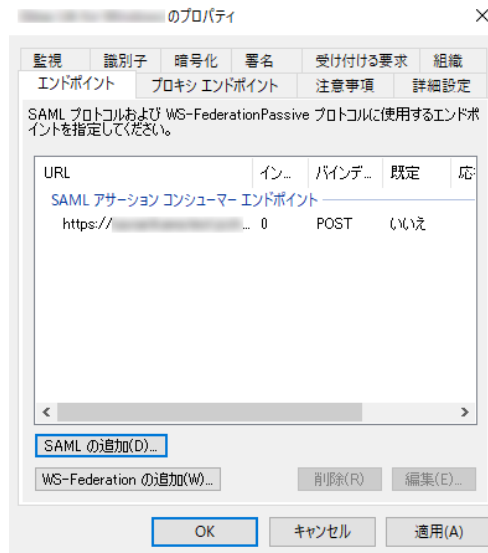


プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (AD FS 連携)

[エンドポイント]タブを選択します。

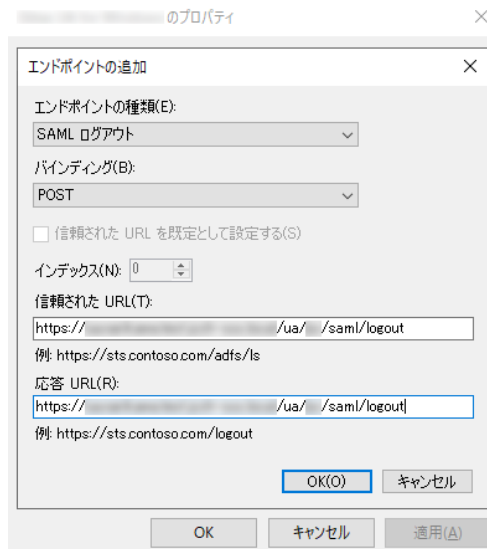
[SAML の追加(D)...]をクリックします。

[エンドポイントの追加] ダイアログボックスが表示されます。



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 (AD FS 連携)

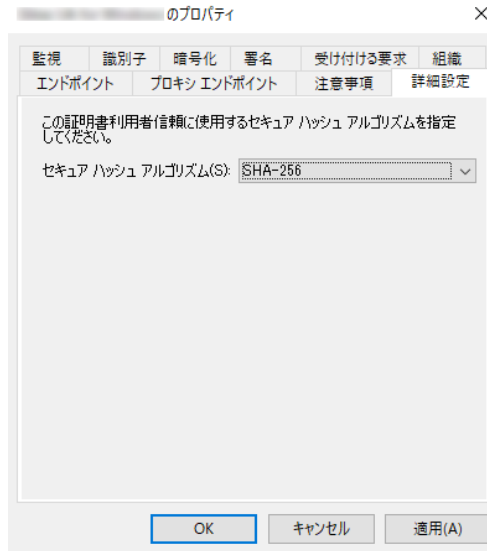
- [エンドポイントの種類(E)] に [SAML ログアウト]を選択
- [バインディング]に[POST]を選択
- [信頼された URL]に UA のログアウト URL を入力
※https://[UA の FQDN]/ua/[UA の名前]/saml/logout
- [応答 URL]に UA のログアウト URL を入力
※https://[UA の FQDN]/ua/[UA の名前]/saml/logout
- [OK(O)] をクリック



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 (AD FS 連携)

[詳細設定] タブを選択します。

- [セキュアハッシュアルゴリズム(S)] に [SHA-256] を選択



[OK] をクリックします。

※証明書利用者信頼の追加、設定は、UA 毎に登録する必要があります。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、それぞれ証明書利用者信頼の追加を行う必要があります。

5.4. SAML IdP 暗号用証明書の取得

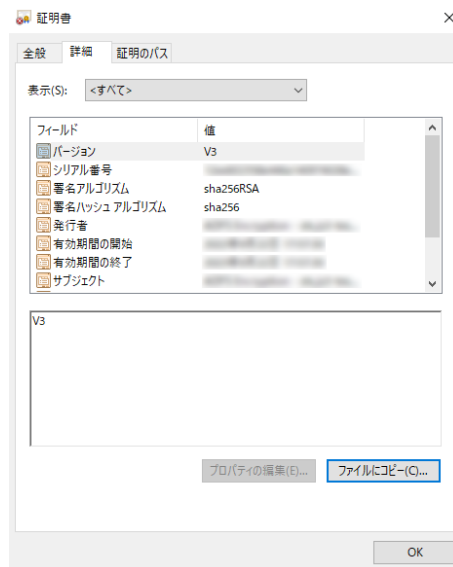
Gléas に設定する SAML IdP の暗号用証明書を ADFS から取得します。

スタートメニューから [ADFS の管理] を起動します。

左ペインの [サービス] > [証明書] を選択します。

中央ペインの [トークン暗号化解除] の証明書を右クリックしてメニューを表示します。

[証明書の表示(V)] をクリックすると[証明書]ダイアログボックスが表示されます。



[詳細]タブで[ファイルにコピー(C)...] をクリックします。

[証明書のエクスポートウィザード]が起動します。

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 (AD FS 連携)



- [次へ(N)] をクリック
- [Base 64 Encoded X.509 (.CERT)(s)] を選択
- [次へ(N)] をクリック
- [参照(R)...] をクリックして出力先を選択
- [次へ(N)] をクリック
- [完了] をクリック

エクスポートしたSAML IdP暗号用証明書をローカルPCに保存します。

5.5. SAML IdP 署名用証明書の取得

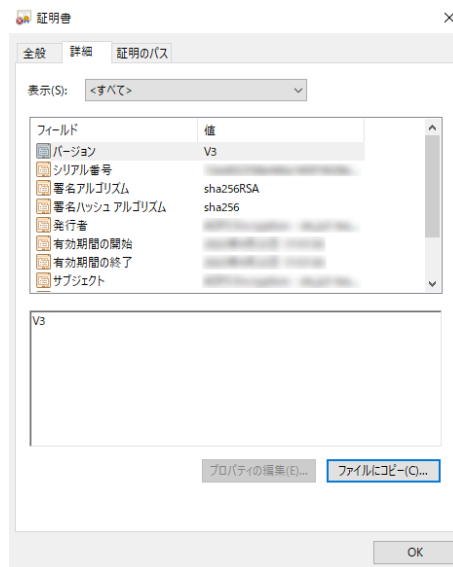
Gléas に設定する SAML IdP の署名用証明書を ADFS から取得します。

スタートメニューから [ADFS の管理] を起動します。

左ペインの [サービス] > [証明書] を選択します。

中央ペインの [トークン暗号化解除] の証明書を右クリックしてメニューを表示します。

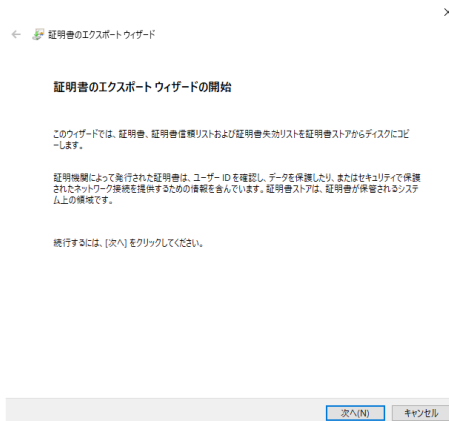
[証明書の表示(V)] をクリックすると[証明書]ダイアログボックスが表示されます。



[詳細]タブで[ファイルにコピー(C)...] をクリックします。

[証明書のエクスポートウィザード]が起動します。

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 (AD FS 連携)



- [次へ(N)] をクリック
- [Base 64 Encoded X.509 (.CERT)(s)] を選択
- [次へ(N)] をクリック
- [参照(R)...] をクリックして出力先を選択
- [次へ(N)] をクリック
- [完了] をクリック

エクスポートしたSAML IdP署名用証明書をローカルPCに保存します。

6. Gléas の管理者設定 (Windows 向け)

GléasのWindows向けUA (申込局) をSAML SPとして動作するように設定します。

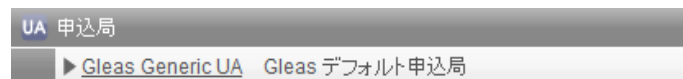
※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

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。

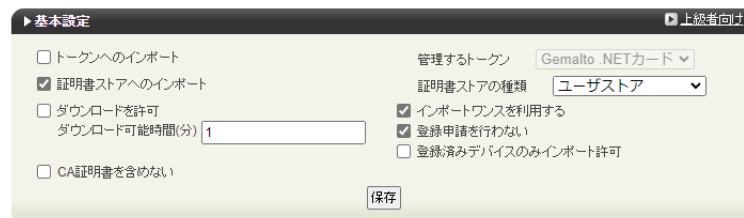
※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します



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 (AD FS 連携)

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力
 - ※ [https://\[フェデレーションサービス名\]/adfs/ls/IdpInitiatedSignOn.aspx](https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx)
- [ログアウト URL]を入力
 - ※ [https://\[フェデレーションサービス名\]/adfs/ls/IdpInitiatedSignOn.aspx](https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx)
- [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
 - ※ [http://\[フェデレーションサービス名\]/adfs/services/trust](http://[フェデレーションサービス名]/adfs/services/trust)
 - ※https ではなく、http であることに注意
- [IdP SSO URL] を入力
 - ※ [https://\[フェデレーションサービス名\]/adfs/ls](https://[フェデレーションサービス名]/adfs/ls)
- [IdP SLO URL] を入力
 - ※ [https://\[フェデレーションサービス名\]/adfs/ls](https://[フェデレーションサービス名]/adfs/ls)
- [IdP 署名用証明書]に IdP 署名用証明書ファイルを指定
- [IdP 暗号用証明書]に IdP 暗号用証明書ファイルを指定
- [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 (AD FS 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
 ADFS Signing - ...
有効期限: ...

IdP 暗号用証明書 削除する
 ADFS Encryption - ...
有効期限: ...

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。

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。

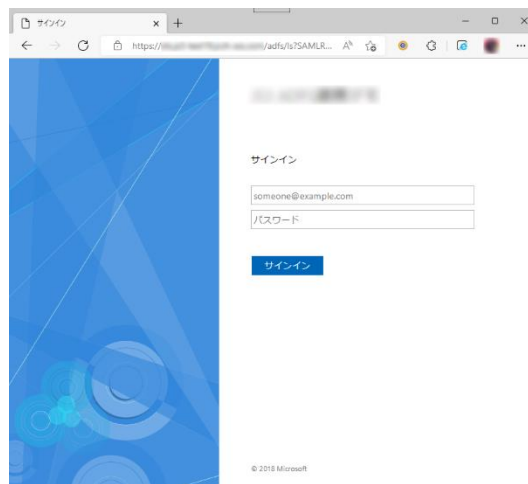
7. クライアントからのアクセス (Windows)

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、ADFSのサインインページにアクセスします。

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

アクセスするとADFSのサインインページに遷移します。



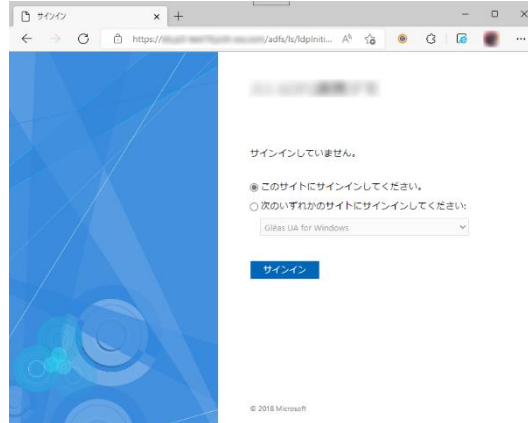
[サインイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

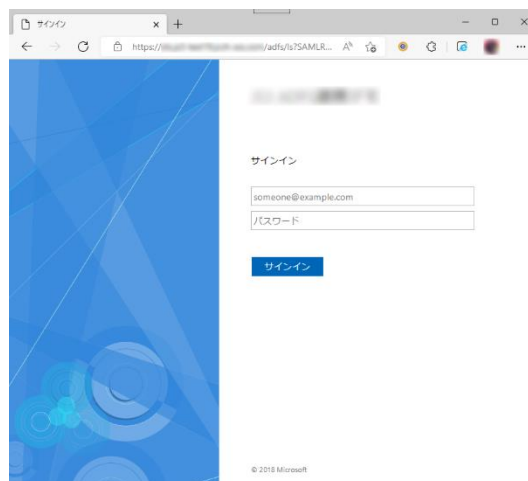
プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (AD FS 連携)

ADFSのサインインページからUAにログインすることもできます。

※URL `https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx`



サイトを選択してサインインします。



[サインイン]をクリックします。

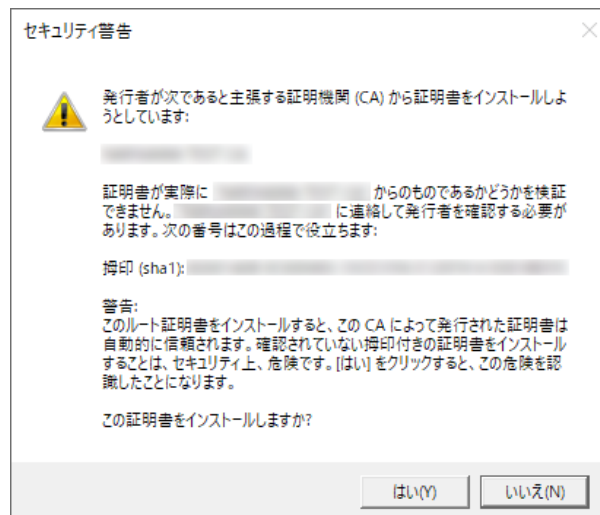
UAにログインし、ユーザ専用ページが表示されます。

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。

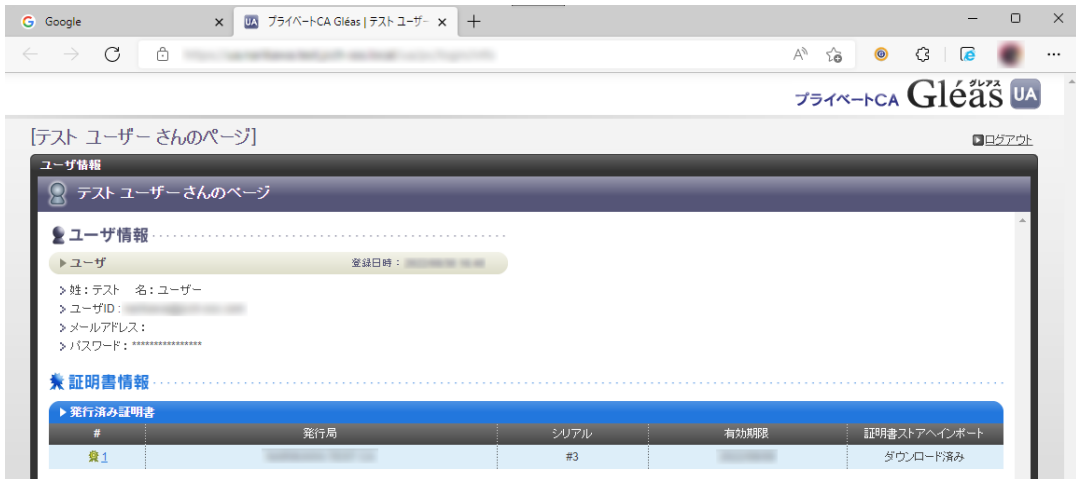


※ 証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印を確認するなど正当性を確認してから[はい]をクリックします



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 (AD FS 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SAML SPとして動作するように設定します。

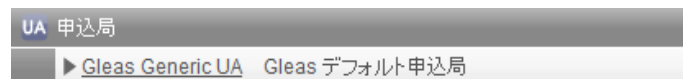
※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

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。

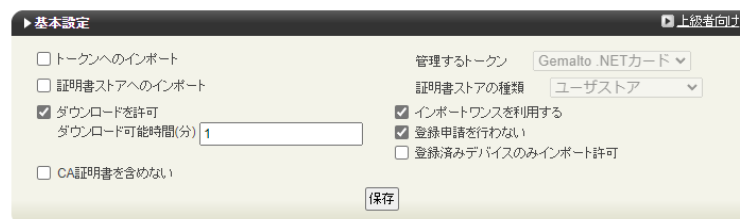
- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック

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。

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 (AD FS 連携)

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力
 - ※ [https://\[フェデレーションサービス名\]/adfs/ls/IdpInitiatedSignOn.aspx](https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx)
- [ログアウト URL]を入力
 - ※ [https://\[フェデレーションサービス名\]/adfs/ls/IdpInitiatedSignOn.aspx](https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx)
- [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
 - ※ [http://\[フェデレーションサービス名\]/adfs/services/trust](http://[フェデレーションサービス名]/adfs/services/trust)
 - ※https ではなく、http であることに注意
- [IdP SSO URL] を入力
 - ※ [https://\[フェデレーションサービス名\]/adfs/ls](https://[フェデレーションサービス名]/adfs/ls)
- [IdP SLO URL] を入力
 - ※ [https://\[フェデレーションサービス名\]/adfs/ls](https://[フェデレーションサービス名]/adfs/ls)
- [IdP 署名用証明書]に IdP 署名用証明書ファイルを指定
- [IdP 暗号用証明書]に IdP 暗号用証明書ファイルを指定
- [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 (AD FS 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

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。

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 (AD FS 連携)

【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

iPhone 構成プロファイル基本設定

名前(デバイス上に表示)	<input type="text" value="サンプルプロファイル"/>
識別子(例: com.jcch-sss.profile)	<input type="text" value="local.jcch-sss.profile"/>
プロファイルの組織名	<input type="text" value="JCCHセキュリティ・ソリューション・システムズ"/>
説明	<input type="text" value="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。

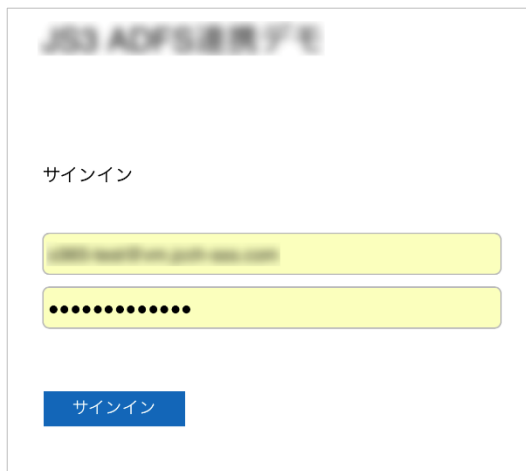
9. クライアントからのアクセス (iPhone)

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、ADFSのサインインページにアクセスします。

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

アクセスするとADFSのサインインページに遷移します。



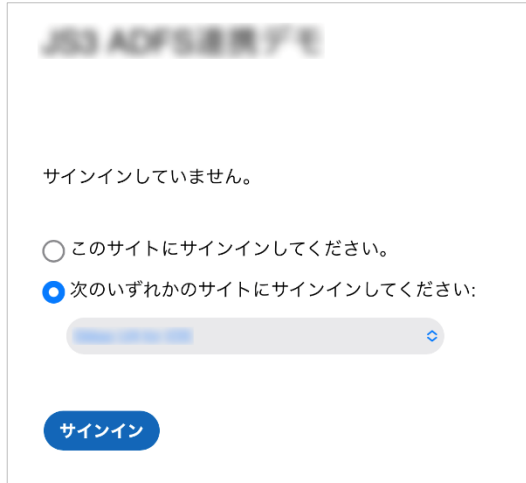
[サインイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

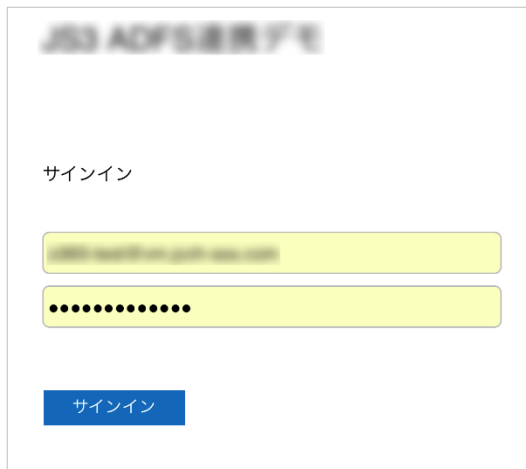
プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (AD FS 連携)

ADFSのサインインページからUAにログインすることもできます。

※URL [https://\[フェデレーションサービス名\]/adfs/ls/IdpInitiatedSignOn.aspx](https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx)



サイトを選択してサインインします。



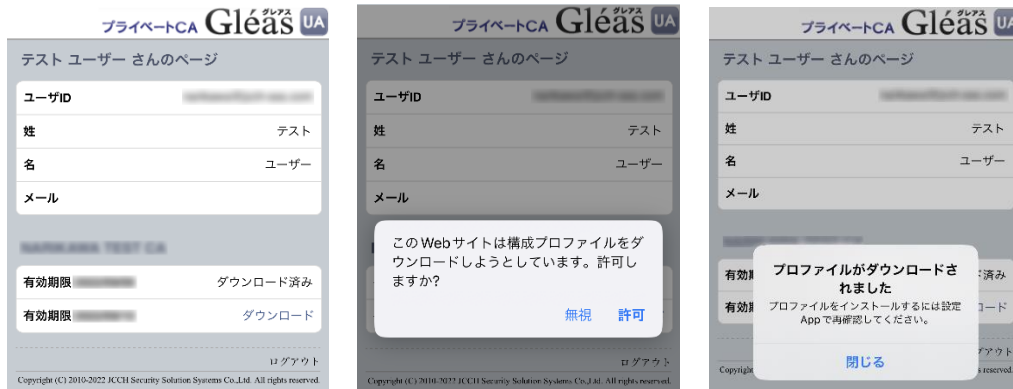
[サインイン]をクリックします。

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 (AD FS 連携)

9.2. クライアント証明書のインポート

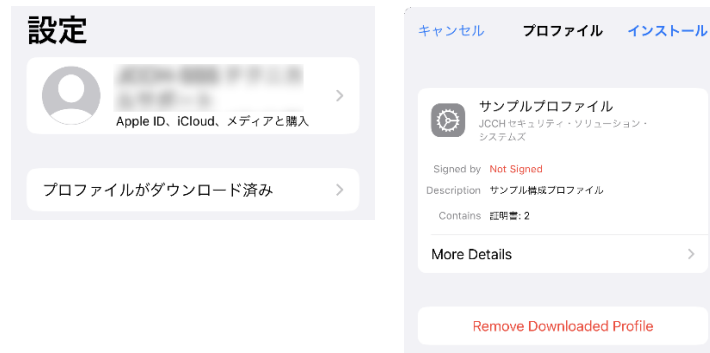
[ダウンロード]をタップし、構成プロファイルのダウンロードをおこないます。



※ 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。



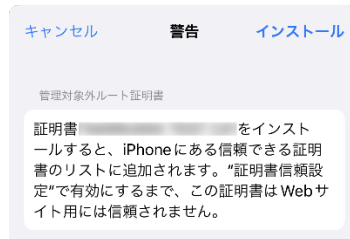
[インストール]をタップして続行してください。

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 (AD FS 連携)

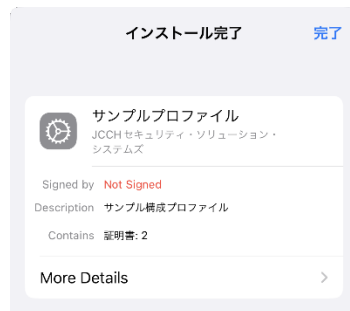
インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し

[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 (AD FS 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. At the top, it says 'プライベートCA Gléas UA'. Below that, it identifies the user as 'テストユーザーさんのページ'. The user information is as follows:

ユーザーID	[Redacted]
姓	テスト
名	ユーザー
メール	[Redacted]

Below the user information, there are two rows showing download status:

有効期限 [Redacted]	ダウンロード済み
有効期限 [Redacted]	ダウンロード済み

At the bottom right, there is a 'ログアウト' 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SAML SPとして動作するように設定します。

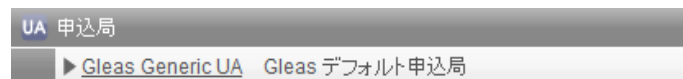
※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

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。

す。



[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 (AD FS 連携)

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力
 - ※ [https:// \[フェデレーションサービス名\]/adfs/ls/IdpInitiatedSignOn.aspx](https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx)
- [ログアウト URL]を入力
 - ※ [https:// \[フェデレーションサービス名\]/adfs/ls/IdpInitiatedSignOn.aspx](https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx)
- [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
 - ※ [http://\[フェデレーションサービス名\]/adfs/services/trust](http://[フェデレーションサービス名]/adfs/services/trust)
 - ※https ではなく、http であることに注意
- [IdP SSO URL] を入力
 - ※ [https://\[フェデレーションサービス名\]/adfs/ls](https://[フェデレーションサービス名]/adfs/ls)
- [IdP SLO URL] を入力
 - ※ [https://\[フェデレーションサービス名\]/adfs/ls](https://[フェデレーションサービス名]/adfs/ls)
- [IdP 署名用証明書]に IdP 署名用証明書ファイルを指定
- [IdP 暗号用証明書]に IdP 暗号用証明書ファイルを指定
- [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 (AD FS 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: [redacted]

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
 ADFS Signing - [redacted]
有効期限: [redacted]

IdP 暗号用証明書 削除する
 ADFS Encryption - [redacted]
有効期限: [redacted]

ダイジェストアルゴリズム

署名アルゴリズム

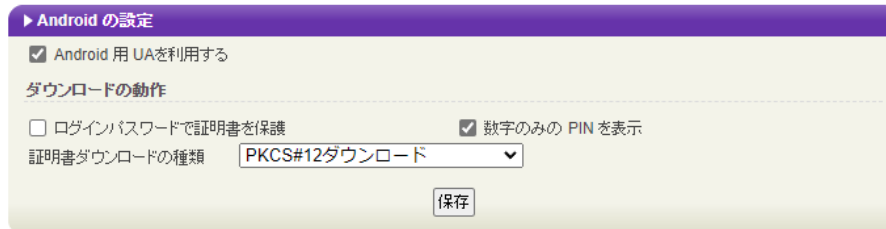
認証リクエストに署名
 ログアウトレスポンスに署名
 署名をメッセージに埋め込む

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 (AD FS 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 (AD FS 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UAMニフェストをダウンロード
- 証明書PINをGléasで生成

UAM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

[UAM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

UAM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。

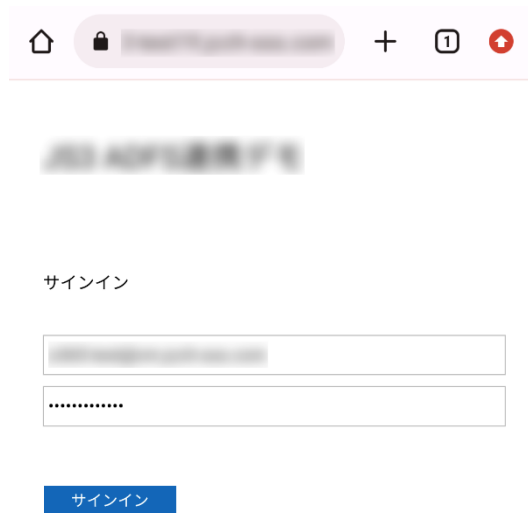
11. クライアントからのアクセス (Android)

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`

アクセスするとADFSのサインインページに遷移します。



[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 (AD FS 連携)

ADFSのサインインページからUAにログインすることもできます。

※URL [https://\[フェデレーションサービス名\]/adfs/ls/IdpInitiatedSignOn.aspx](https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx)

この ADFS 連携サービス

サインインしていません。

このサイトにサインインしてください。

次のいずれかのサイトにサインインしてください:

このサイトにサインイン

サインイン

サイトを選択してサインインします。

この ADFS 連携サービス

サインイン

.....

サインイン

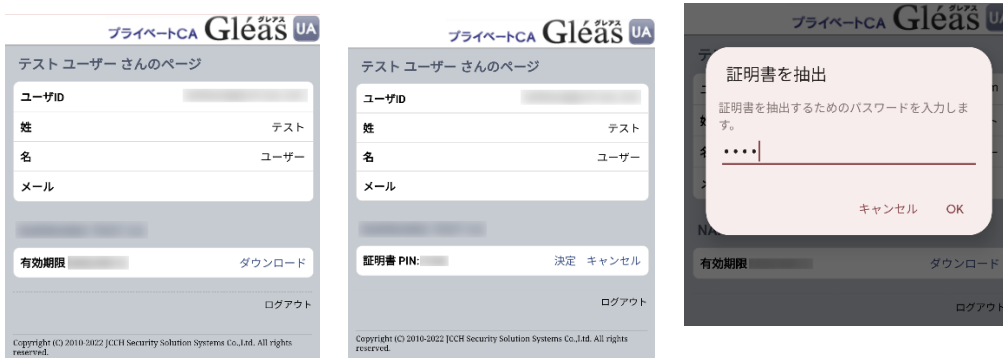
[サインイン]をクリックします。

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 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 (AD FS 連携)

11.2. クライアント証明書のインポート

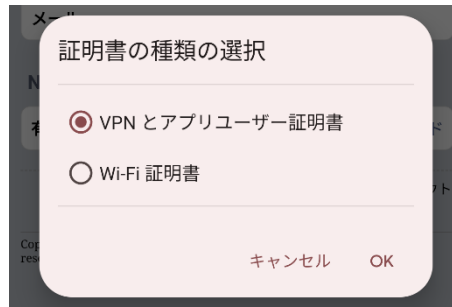
[ダウンロード]をタップし、証明書ファイルのダウンロードをおこないます。



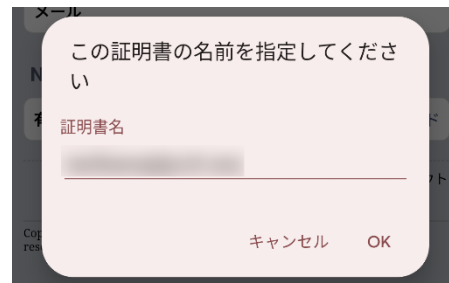
- ※ 「証明書 PIN」の値を「証明書を抽出」のパスワードとして入力します。
- ※ インポートロックを有効にしている場合は、この時点からカウントが開始されます

[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。

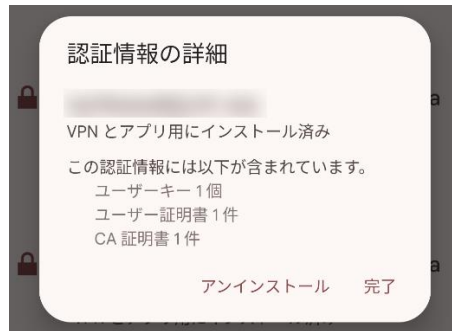
プライベート認証局 Gléas ホワイトペーパー
シングルサインオンによる Gléas UA ログイン (AD FS 連携)

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 (AD FS 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