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

(VMware Workspace ONE Access 連携)

Ver.1.1

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、VMware Workspace ONE Access (旧称 VMware Identity Manager) のWeb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： VMware Workspace ONE Access (旧称 VMware Identity Manager)
  ※以後「WS1 Access」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。
  ※WS1 AccessとのID同期には、Workspace ONE Access Connectorを使用しています。

- 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

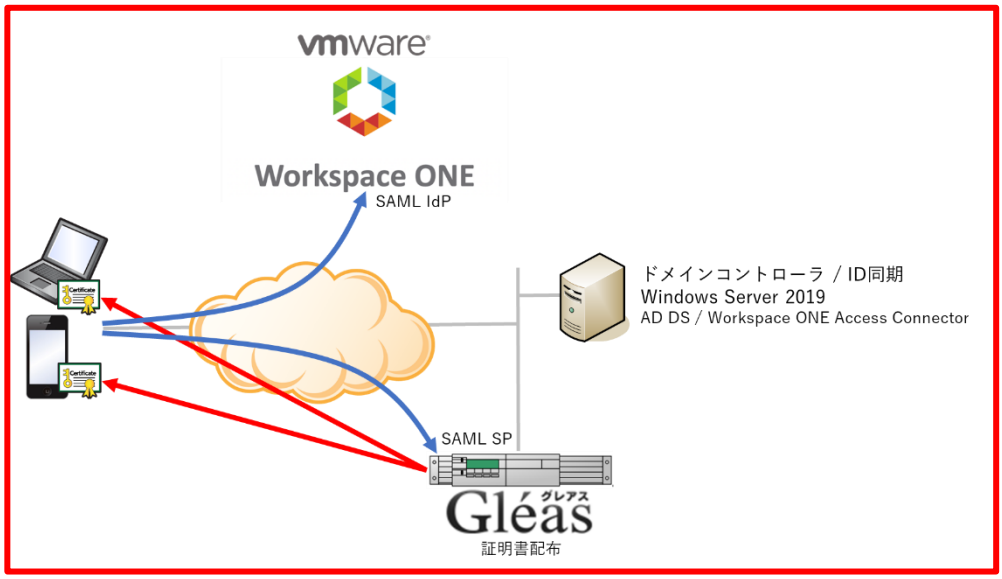
以下については、本書では説明を割愛します。

- WS1 Accessの基本設定、およびADとのID同期方法
- 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WS1 Accessのログイン画面に画面遷移。WS1 Access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WS1 Accessのログイン画面に画面遷移。WS1 Access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WS1 Accessのログイン画面に画面遷移。WS1 Access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。

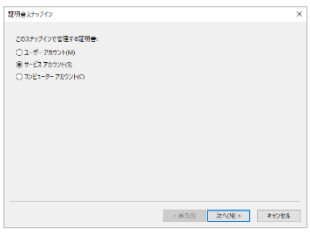
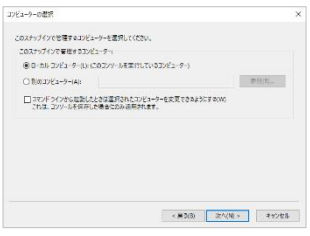
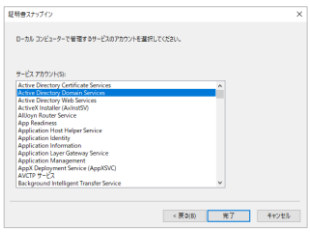
MMC を開き、メニューの[ファイル(F)] > [スナップインの追加と削除(N)]より[証明書]を追加します。

「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、

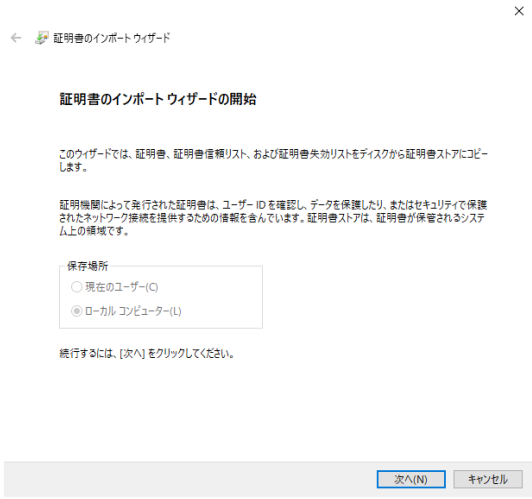
次の「証明書スナップイン」では、[Active Directory Domain Services)]を選択し、

[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。

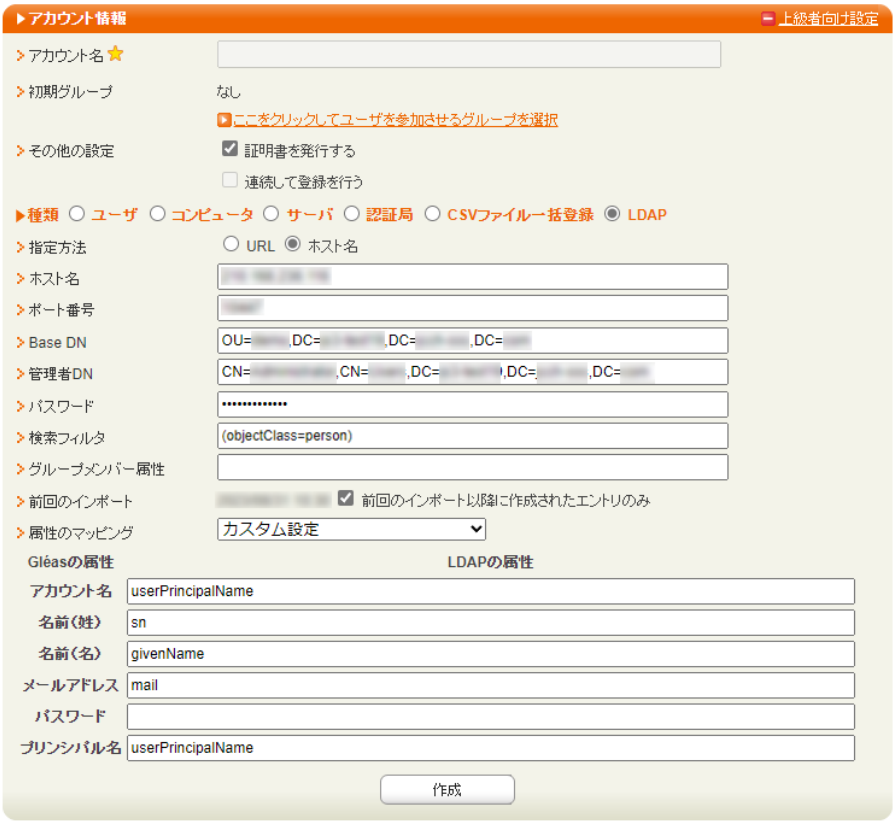
3. Gléas アカウントの登録

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。

- [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。

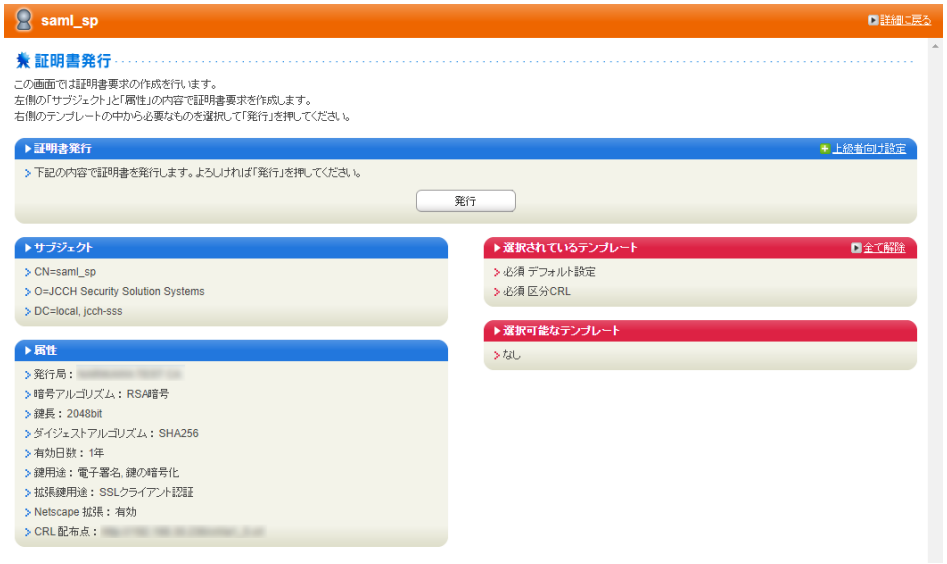
4. SAML SP 署名用証明書の発行

SAML SPとして使用する署名用証明書をGléasから発行します。

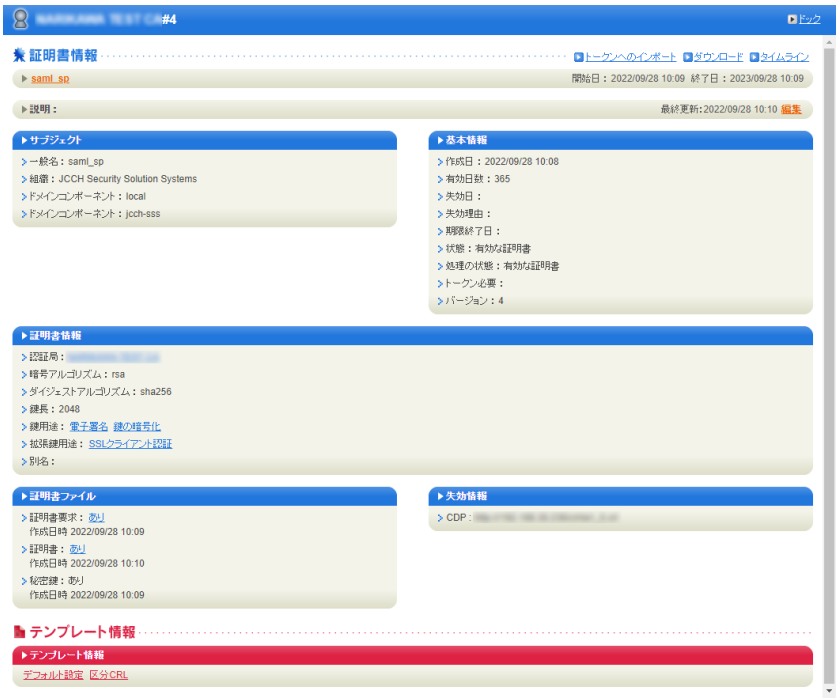
GléasのRA（登録局）にログインします。

[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。

[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。

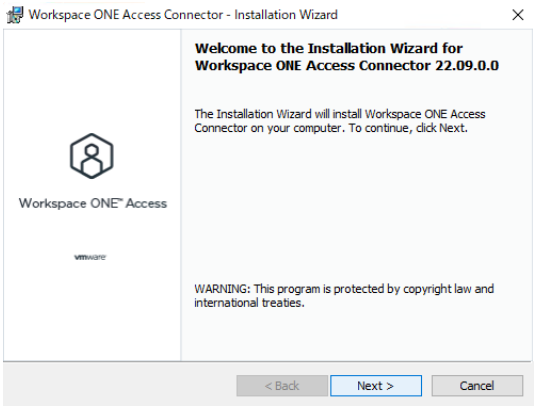
5. WS1 Access の設定

5.1. AD ユーザ情報を同期

AD のユーザ情報を WS1 Access に同期します。

【Workspace ONE Access Connector をセットアップ】

ドメイン参加している Windows サーバに Workspace ONE Access Connector をインストールし、WS1 Access と接続します。



【ディレクトリを追加】

Workspace ONE Access コンソール にログインします。

メニュー [統合] > [コネクタ] > [ディレクトリ] を選択します。

[ディレクトリを追加] > [Active Directory] をクリックします。

- [ディレクトリ名] に任意のディレクトリ名を入力
- [LDAP 経由の Active Directory] を選択
- [ディレクトリ同期ホスト] に同期対象 AD ホストをチェック
- [認証] に [はい] を選択
- [ユーザー認証ホスト] に同期対象 AD ホストをチェック
- [ユーザー名] に [userPrincipalName] を選択

  ※AD の userPrincipalName が Workspace ONE Access のユーザ名となります
- [外部 ID] に "objectGUID" を入力

  ※Workspace ONE Access ディレクトリ内ユーザの一意の ID として使用する属性
- [このディレクトリ は DNS サービス ロケーションをサポートします] のチェックを外す
- [サーバ ホスト名] に 同期対象 AD の FQDN を入力
- [サーバ ポート] に "636" を入力
- [すべての接続に必要な LDAPS] をチェック

- [SSL 証明書] に PEM 形式で LDAPS の証明書チェインを貼り付け

  ※サーバ証明書 > 中間証明書 > ルート証明書の順

- [ベース DN] に 同期対象となる DN を入力

- [バインド ユーザー DN] にベース DN にアクセスできる管理者 DN を入力

- [バインド ユーザー パスワード] にベース DN にアクセスできる管理者パスワードを入力

[保存と設定] をクリックします。

【ディレクトリ同期設定】

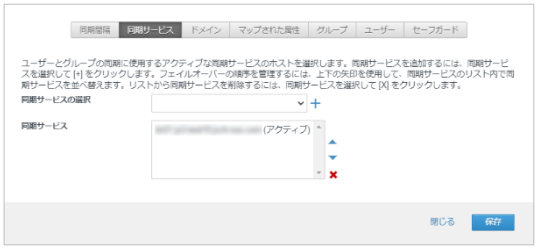
メニュー［統合］> ［コネクタ］> ［ディレクトリ］を選択します。

作成したディレクトリ名のリンクをクリックします。

［同期設定］をクリックします。

［同期サービス］タブを選択します。

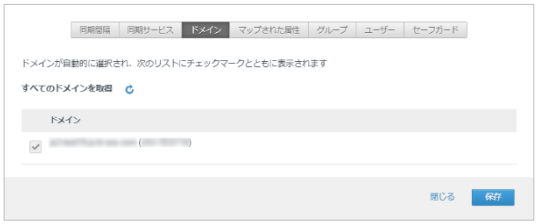
- ［同期サービス］に同期対象ディレクトリが指定されていることを確認



［ドメイン］タブを選択します。

- ［すべてのドメインを取得］の右の アイコンをクリック

- ［ドメイン］に 同期対象のドメイン名が表示されることを確認

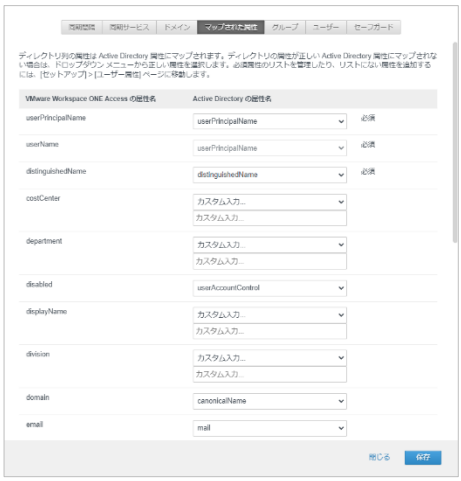


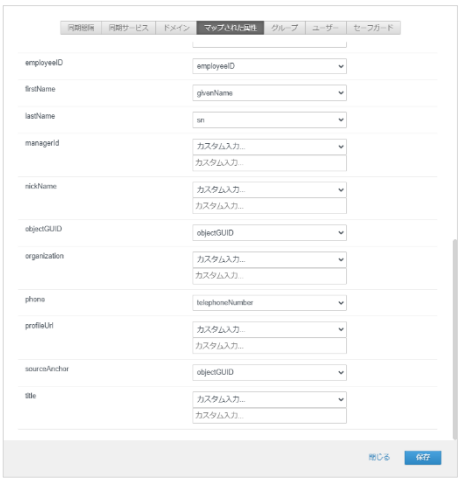
[マップされた属性] タブを選択します。

- WS1 Access と AD の LDAP 属性のマッピングを確認、修正

※以下は検証時に指定した値

VMware Workspace ONE Access の属性名	Active Directory の属性名
userPrincipalName	userPrincipalName
username	userPrincipalName
distinguishedName	distinguishedName
Disabled	userAccountControll
domain	canoricalName
email	mail
employeeID	employeeID
firstName	givenName
lastName	sn
objectGUID	objectGUID
Phone	telephoneNumber
sourceAnchor	objectGUID





[グループ] タブを選択します。

- [ネストされたグループ メンバーを同期] をチェック

[ユーザー] タブを選択します。

- [ユーザー DN を指定] に同期対象の AD ユーザを選択する DN を入力

※[テスト] をクリックして同期対象ADユーザの存在確認ができます。

- [ユーザーを除外するフィルタ...] に同期対象から除外する AD ユーザを指定します。

[保存] をクリックします。

[閉じる] をクリックします。

[同期] > [セーフガードを使用した同期] をクリックすると同期が開始されます。

同期が完了すると、WS1 Access のユーザが登録されます。

5.2. ID プロバイダの作成

WS1 Access に IdP（ID プロバイダ）を追加します。

Workspace ONE Access コンソール にログインします。

メニュー [統合] > [ID プロバイダ] を選択します。

[ID プロバイダを追加] > [組み込み ID プロバイダを作成] をクリックします。

【組み込み ID プロバイダを追加】

- [ID プロバイダ名] に任意の名前を入力
- [ユーザー] に AD 同期しているディレクトリをチェック
- [コネクタ認証方法] に [パスワード(クラウドデプロイ)] をチェック
- [認証方法] は指定しない。
- [ネットワーク] に [すべての範囲] をチェック


IDプロバイダ名
ユーザー
コネクタ認証方法
認証方法
認証方法を関連付ける
パスワード (クラウド デプロイ)
認証方法
IDプロバイダがユーザー認証に使用する認証方式を選択します。
認証方法
認証方法を関連付ける
VMware Verify
モバイル SSO (iOS 版)
パスワード (ローカル ディレクトリ)
モバイル SSO (Android 版)
Workspace ONE UEM の外部アクセス トークン
Workspace ONE UEM でのパスワード
Workspace ONE UEM とのデバイス順守
証明書 (クラウド デプロイ)
ネットワーク
このIDプロバイダにアクセスできるネットワークを選択します。次の利用可能なネットワーク範囲から選択します。
すべての範囲
KDC 証明書のエクスポート
証明書をダウンロード
モバイル デバイス管理プロファイルで使用するための KDC サーバのルート証明書をエクスポートします。
追加
キャンセル

[追加] をクリックします。

5.3. ユーザーグループの作成

Web アプリケーション（Gléas UA）にアクセスするユーザをグループ化します。

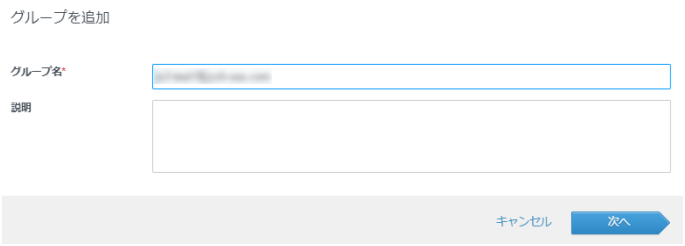
Workspace ONE Access コンソール にログインします。

メニュー [アカウント] > [ユーザーグループ] を選択します。

[グループを追加] をクリックします。

【グループを追加】

- [グループ名] に 任意のグループ名を入力

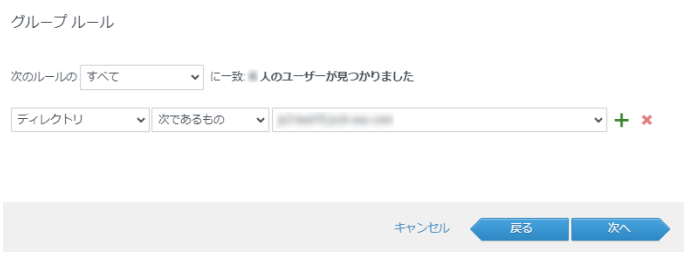


[次へ] をクリックします。

- [グループにユーザーを追加] は指定しない

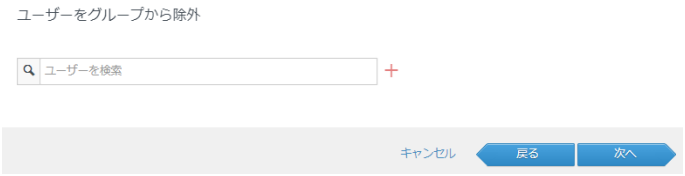
[次へ] をクリックします。

- 次のルール [すべて] に一致 を選択
- [ディレクトリ] [次であるもの] [AD と同期したディレクトリ] を指定

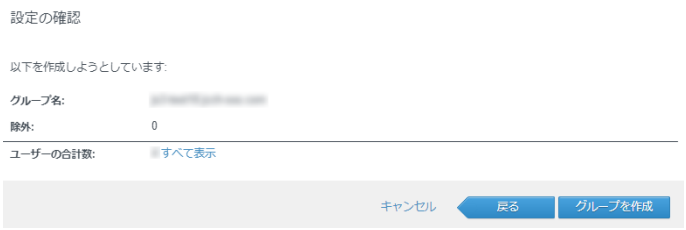


[次へ] をクリックします。

- [ユーザーをグループから除外] は指定しない



[次へ] をクリックします。



[グループを作成]をクリックします。

5.4. Web アプリケーションの登録

Web アプリケーション（Gléas UA）を SAML SP として登録します。

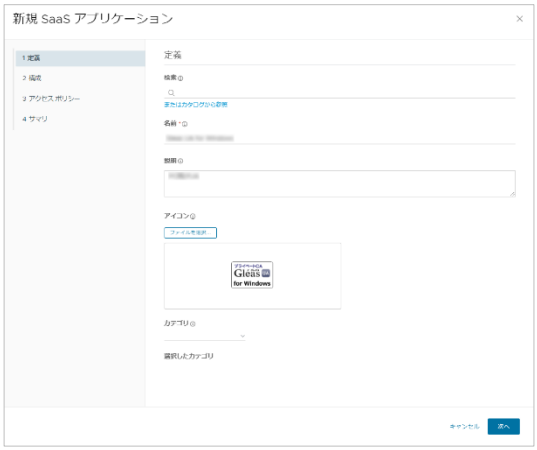
Workspace ONE Access コンソール にログインします。

メニュー [リソース] > [Web アプリケーション] を選択します。

[新規] をクリックします。

【定義】

- [名前] に任意のアプリ名を入力
- [説明] に任意のアプリ説明を入力
- [アイコン] に任意のアイコン画像ファイルを選択



[次へ] をクリックします。

【シングルサインオン】

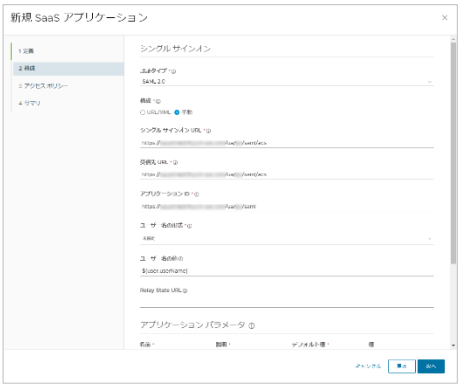
- **[認証タイプ] に [SAML 2.0] を選択**
- **[構成] に [手動] を選択**
- **[シングル サインオン URL] を入力**

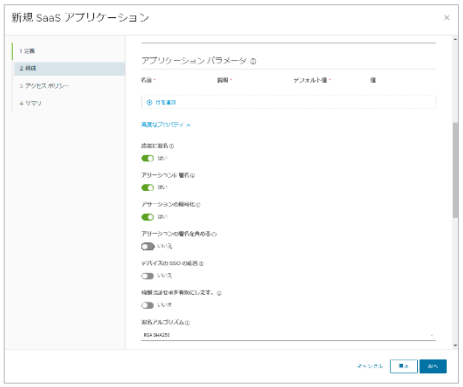
  ※https://[UA の FQDN]/ua/[UA の名前]/saml/acs
- **[受信先 URL] を入力**

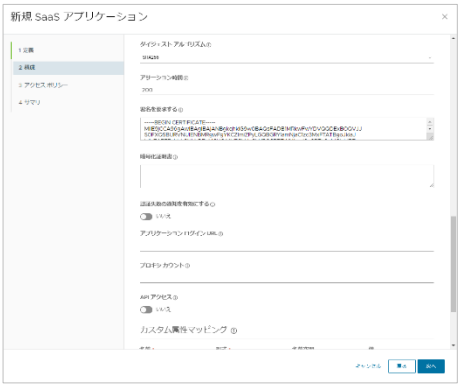
  ※https://[UA の FQDN]/ua/[UA の名前]/saml/acs
- **[アプリケーション ID] を入力**

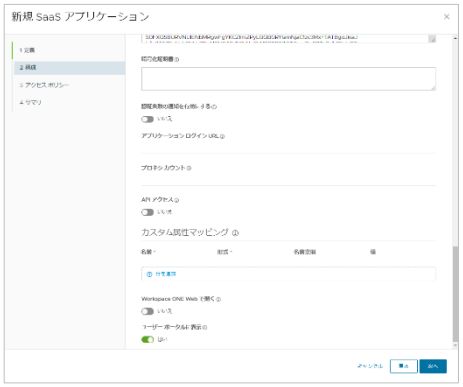
  ※https://[UA の FQDN]/ua/[UA の名前]/saml
- **[ユーザー名の形式] に [未指定] を選択**
- **[ユーザー名の値] に "${user.userName}" を入力**
- **[Relay State URL] は指定しない**
- **[アプリケーション パラメータ] は指定しない**
- **[高度なプロパティ] リンクをクリック**
- **[応答に署名] に [はい] を指定**
- **[アサーションに署名] に [はい] を指定**
- **[アサーションの暗号化] に [はい] を指定**
- **[アサーションの署名を含める] に [いいえ] を指定**
- **[デバイスの SSO の応答] に [いいえ] を指定**
- **[強制認証要求を有効にします] に [いいえ] を指定**

- [署名アルゴリズム] に [RSA SHA256] を選択
- [ダイジェスト アルゴリズム] に [SHA256] を選択
- [アサーション時間]に "200" を入力
- [署名を要求する] に PEM 形式の SAML SP 署名用証明書を貼付け
- [暗号化証明書] は指定しない
- [認証失敗の通知を有効にする] に [いいえ] を指定
- [アプリケーション ログイン URL] は指定しない
- [プロキシ カウント] は指定しない
- [API アクセス] に [いいえ] を指定
- [カスタム属性マッピング] は 指定しない
- [Workspace ONE Web で開く] に [いいえ] を指定
- [ユーザー ポータルに表示] に [はい] を指定





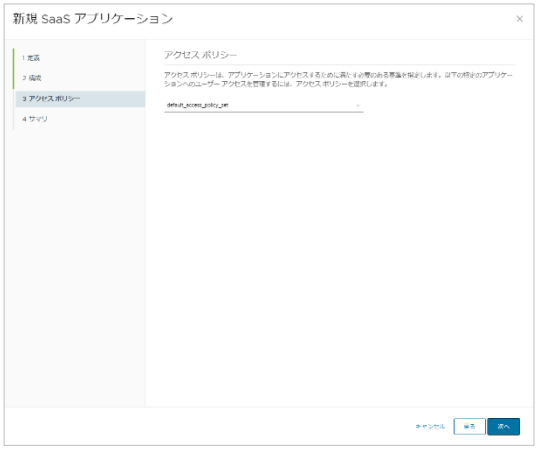




[次へ] をクリックします。

【アクセスポリシー】

- [default_access_policy_set] を選択



[次へ] をクリックします。

【サマリ】

[保存] をクリックします。

5.5. Web アプリケーションの割り当て

作成した Web アプリケーションをユーザーグループに割り当てることで、ユーザが利用できるようにします。

Workspace ONE Access コンソール にログインします。

メニュー [リソース] > [Web アプリケーション] を選択します。

作成した Web アプリケーションをチェックします。

[割り当て] をクリックします。

【割り当て】

- [選択されたユーザー/ユーザー グループ] に作成したユーザーグループを選択
- [展開の種類]に[ユーザーによるアクティベーション] を選択
- [資格タイプ] に [含める] を選択

[保存] をクリックします。

※Web 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 Web 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WS1 AccessのWeb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。

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力

  ※ https://[WS1 Access の FQDN]/
- [ログアウト URL]を入力

  ※ https://[WS1 Access の FQDN]/
- [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://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml
- [IdP SSO URL] を入力

  ※ https://[WS1 Access の FQDN]/SAAS/auth/federation/sso
- [IdP SLO URL] を入力

  ※ https://[WS1 Access の FQDN]/SAAS/auth/auth/logout
- [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://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml
- [IdP 暗号用証明書]に IdP 暗号用証明書ファイルを指定

  ※暗号用証明書はメタデータ(XML)から取得する

  ※ https://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml
- [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

WS1 Accessのログインページに遷移します。

ドメインを選択して[次へ]をクリックします。

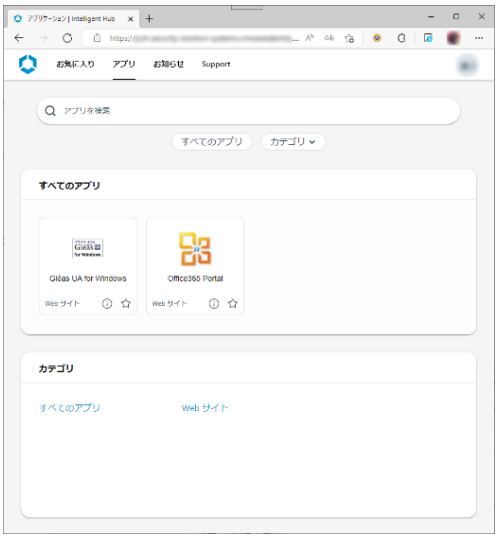
[ユーザー名]、[パスワード]を入力して[ログイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

Workspace ONE ポータルからログインすることもできます。

ドメインを選択して[次へ]をクリックします。

[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。

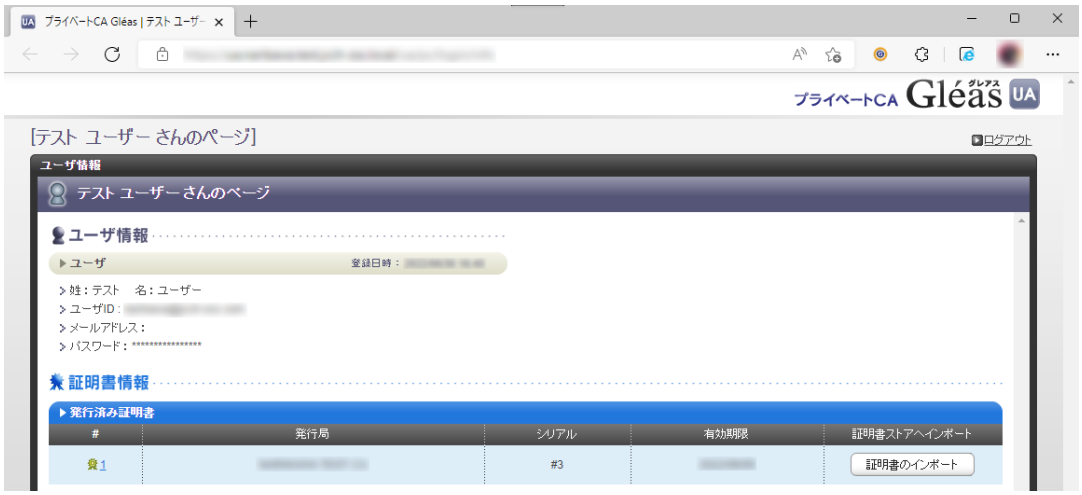


[アプリ]タブから登録した「Webアプリケーション」を選択します。

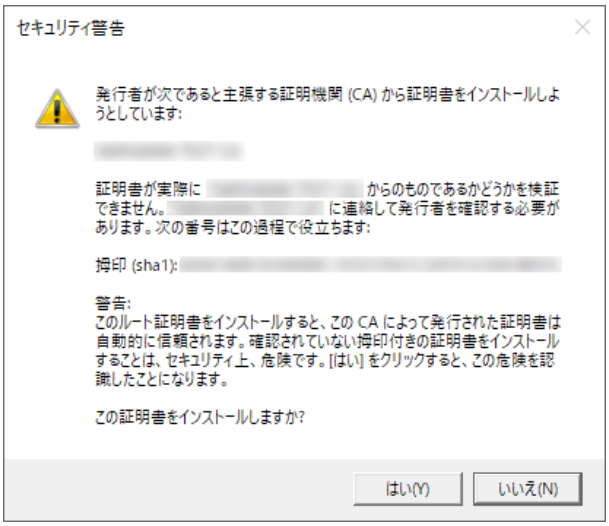
UAにログインし、ユーザ専用ページが表示されます。

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WS1 AccessのWeb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。

[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://[WS1 Access の FQDN]/
- [ログアウト URL]を入力

  ※ https://[WS1 Access の FQDN]/
- [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://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml
- [IdP SSO URL] を入力

  ※ https://[WS1 Access の FQDN] /SAAS/auth/federation/sso
- [IdP SLO URL] を入力

  ※ https://[WS1 Access の FQDN]/SAAS/auth/auth/logout
- [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://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml
- [IdP 暗号用証明書]に IdP 暗号用証明書ファイルを指定

  ※暗号用証明書はメタデータ(XML)から取得する

  ※ https://[テナント名].vmwareidentity.asia/SAAS/API/1.0/GET/metadata/idp.xml

- [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

WS1 Accessのログインページに遷移します。

ドメインを選択して[次へ]をクリックします。

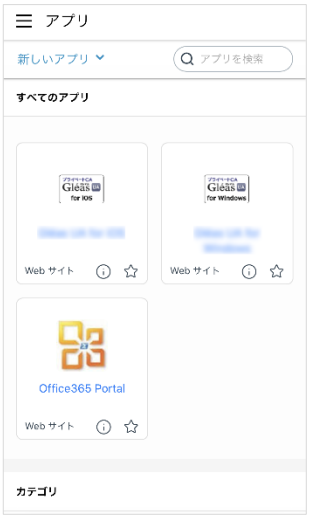
[ユーザー名]、[パスワード]を入力して[ログイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

Workspace ONE ポータルからログインすることもできます。

ドメインを選択して[次へ]をクリックします。

[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。



メニュー[アプリ]から登録した「Webアプリケーション」を選択します。

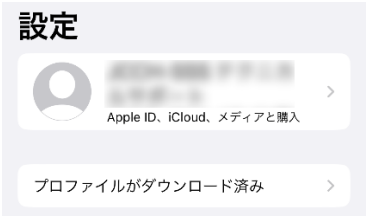
UAにログインし、ユーザ専用ページが表示されます。

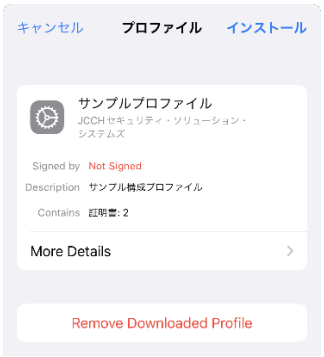
9.2. クライアント証明書のインポート

[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。



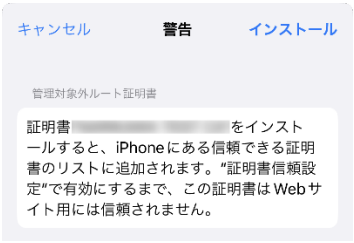


[インストール]をタップして続行してください。

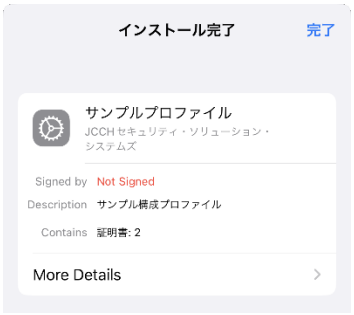
インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し

[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WS1 AccessのWeb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。

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力

  ※ https://[WS1 Access の FQDN]/
- [ログアウト URL]を入力

  ※ https://[WS1 Access の FQDN]/
- [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://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml
- [IdP SSO URL] を入力

  ※ https://[WS1 Access の FQDN]/SAAS/auth/federation/sso
- [IdP SLO URL] を入力

  ※ https://[WS1 Access の FQDN]/SAAS/auth/auth/logout
- [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://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml
- [IdP 暗号用証明書]に IdP 暗号用証明書ファイルを指定

  ※暗号用証明書はメタデータ(XML)から取得する

  ※ https://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml

- [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。

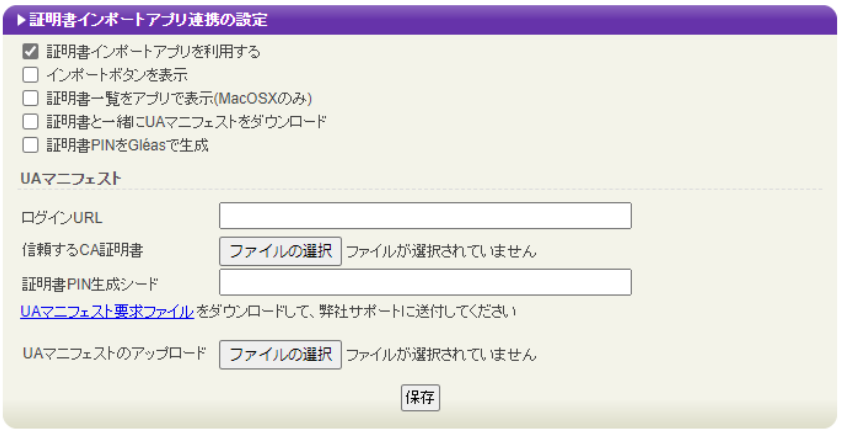
[認証デバイス情報]の[Androidの設定]までスクロールし、[Android用UAを利用する]をチェックします。

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。

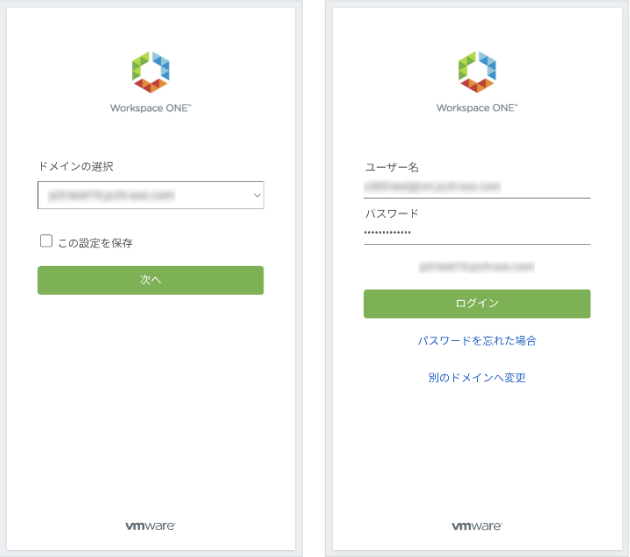
11. クライアントからのアクセス（Android）

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

WS1 Accessのログインページに遷移します。

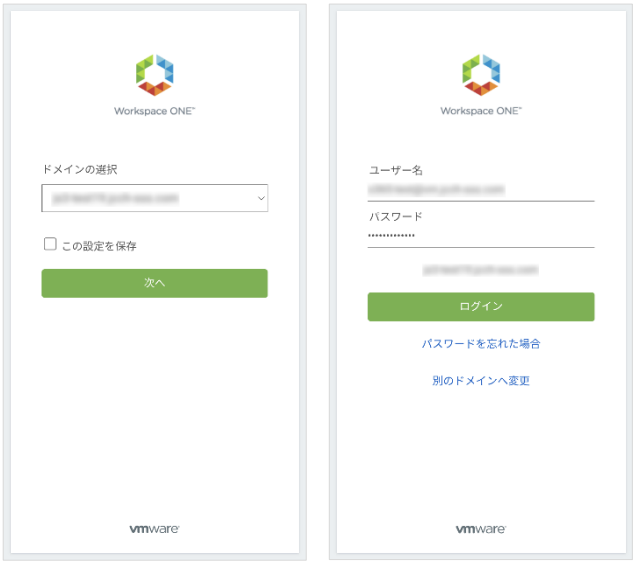


ドメインを選択して[次へ]をクリックします。

[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。

Workspace ONE ポータルからログインすることもできます。



ドメインを選択して[次へ]をクリックします。

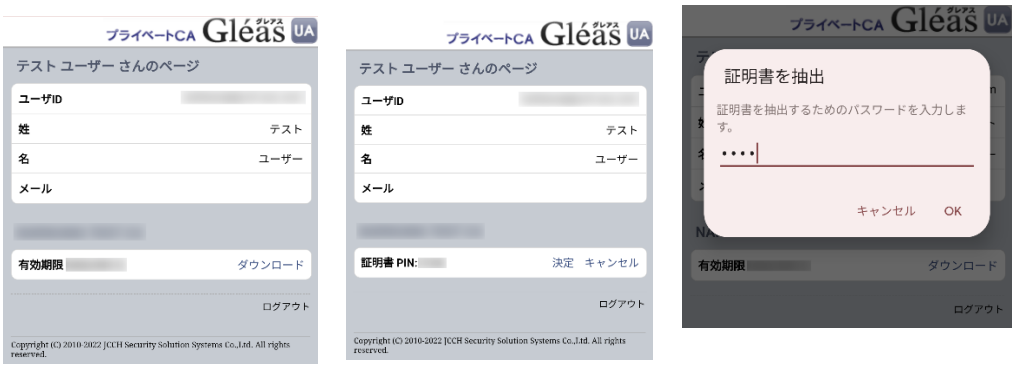
[ユーザー名]、[パスワード]を入力して[ログイン]をクリックします。

メニュー [アプリ]から登録した「Webアプリケーション」を選択します。

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。

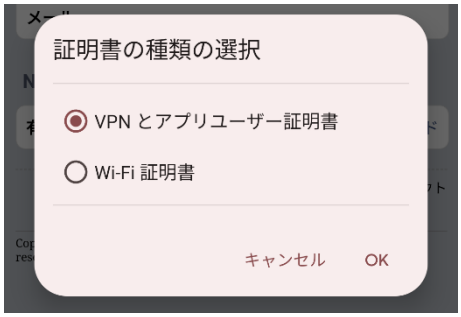


※　「証明書 PIN」の値を「証明書を抽出」のパスワードとして入力します。

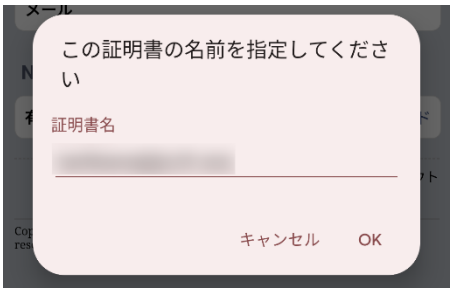
※　インポートロックを有効にしている場合は、この時点からカウントが開始されます

[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。

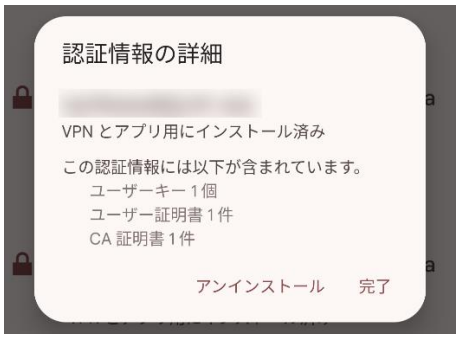


[OK]をタップします。

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