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

Akamai Enterprise Application Access (EAA) でのクライアント証明書認証

Ver. 1.0
2020 年 8 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」で発行されたクライアント証明書を利用して、アカマイ・テクノロジーズのリモートアクセスサービス「Enterprise Application Access」にてクライアント証明書認証をおこなう環境を構築するため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。

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。

- リモートアクセスサービス：Enterprise Application Access
  URL：https://www.akamai.com/jp/ja/products/security/enterprise-application-access.jsp
  ※以後、「EAA」と記載します
- JS3 プライベート認証局 Gléas （バージョン2.2.2）
  ※以後、「Gléas」と記載します
- クライアント：Windows 10 Pro（バージョン1909） / EAA Client (バージョン 2.0.3.1b7852fe)
  ※以後、「Windows」と記載します
- クライアント：macOS Catalina（バージョン10.15.6） / Gléas CertImporter (バージョン 1.3) / EAA Client (バージョン 2.0.3.1b7852fe)
  ※以後、「macOS」と記載します

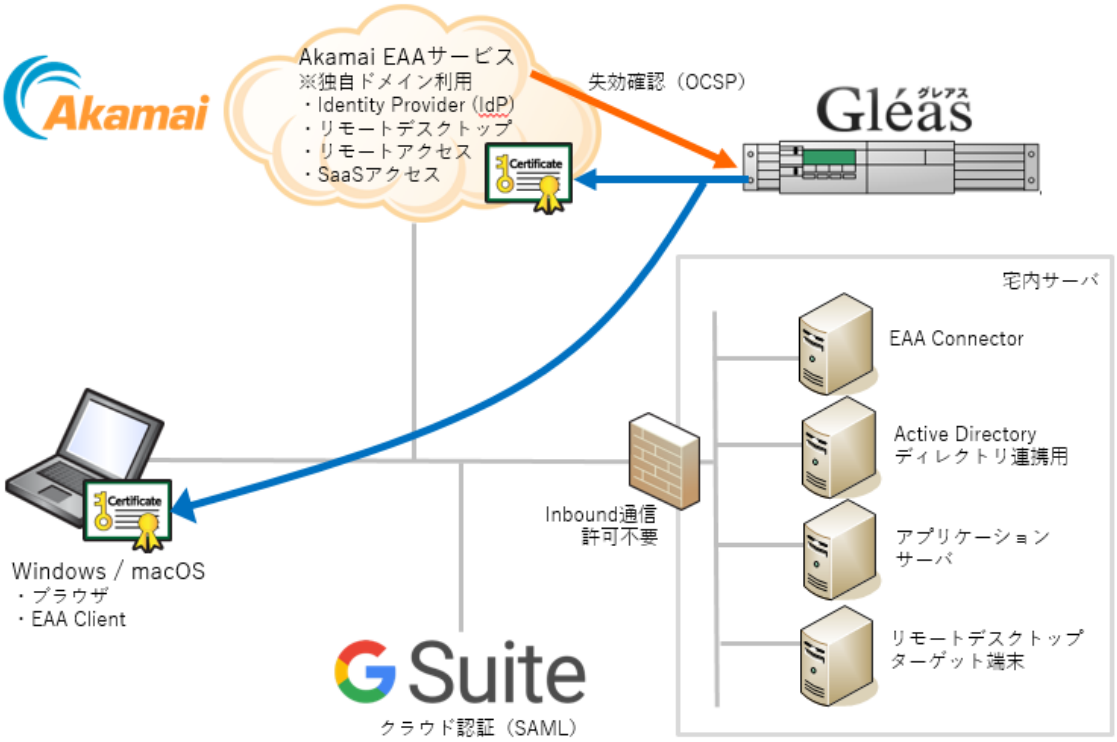
以下については、本書では説明を割愛します。

- EAAの一般的な設定（IdP、EAA Client接続など）
  ※パスワード認証環境を構築可能な前提で本書は記載されています
- Active Directoryとのディレクトリ連携
  ※本書の内容においてAD連携は必須ではありません
- Gléasでのサーバ・クライアント証明書の発行などの基本操作

これらについては、各製品・サービスのマニュアル・ヘルプをご参照いただくか、各製品を取り扱う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. EAAでアイデンティティ・プロバイダ(IdP)、クライアントアクセスアプリ(EAA Client アプリ接続）、リモートデスクトップWebアプリを構成する。
   それぞれ独自ドメインによるホスト名で構成をおこなう。
2. Gléasはサーバ証明書を発行し、EAAに適用する。
   上記1での各ホスト名をサーバ証明書の「サブジェクトの代替名」に入れることにより1枚のサーバ証明書で複数ホストをカバーできるようにする。
3. Gléasはクライアント証明書を発行し、デバイスに配布する。
4. 各デバイス（Windows / macOS） はGléasよりクライアント証明書を取得し、 EAAでのクライアント証明書（失効確認を含む)とActive Directoryのパスワード認証を経て、宅内アプリケーションやSaaSにアクセスをおこなう。

1.4. Gléas における留意事項

Gléasで電子証明書を発行する際に以下の点に留意する必要があります。

- Gléasで発行するサーバ証明書の有効期間は825日未満である必要があります。
  （macOS 10.15以降、およびiOS 13以降における制約）

- サーバ証明書には、サブジェクトの別名に複数のホスト名を含めることができます。Gléasではサーバアカウントの[ホスト名]欄に";"(セミコロン)で区切ることによりこの対応をおこなえます。

- OCSPレスポンダのリッスンするポートが80であることが必須になります。(Gléasのデフォルトは2560)
- EAA Clientアプリ利用時の対応事項として、Gléasのルート証明書を以下にインポート(信頼設定)をする必要があります。
  ※本書記載の設定では、GléasのUAからはWindowsの場合はカレントユーザの証明書ストアに、macOSの場合はログイン・キーチェーンにルート証明書がインポートされます

  【Windowsの場合】
  ローカルコンピュータの証明書ストア（certlm.msc）の[信頼されたルート証明機関]配下

  【macOSの場合】
  キーチェーンアクセス.appのシステム・キーチェーン配下。加えて信頼設定で、SSLについて[常に信頼]を設定する。

2. EAAの設定

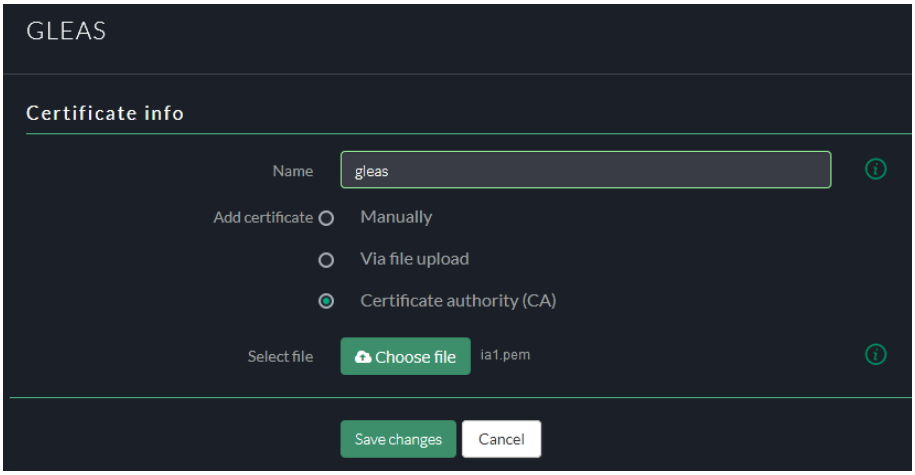
2.1. ルート証明書のインポート

事前に Gléas よりルート証明書ファイルをダウンロードしておきます。
デフォルトのルート証明書ダウンロード URL は以下の通りです。
http://gleas.example.com/crl/ia1.pem

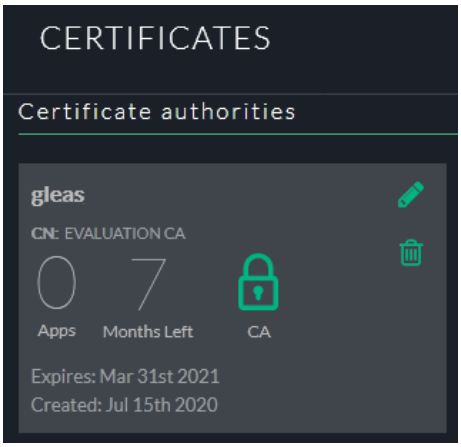
EAA の管理 Web サイトから[System] > [Certificates]と進み、[Add Certificates]からルー

ト証明書をアップロードします。

- [Name]には、識別名称を入力
- [Add Certificate]には、”Certificate Authority (CA)”を選択
- [Select File]で、ダウンロードしたファイルを指定



成功すると、以下のように表示されます。

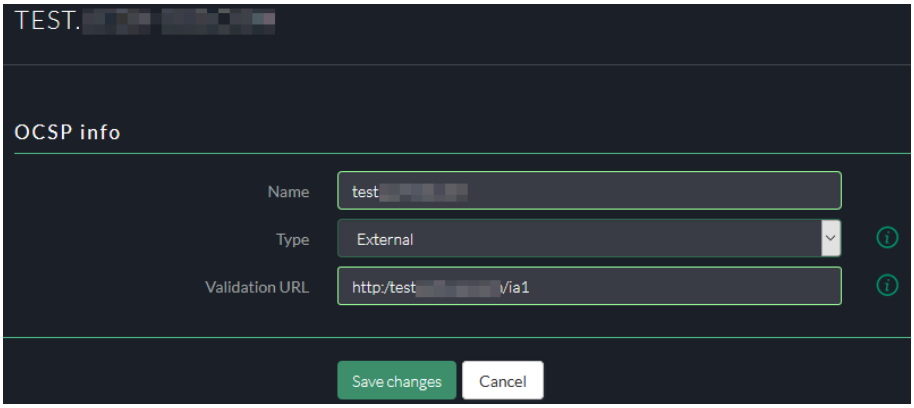


2.2. 失効確認（OCSP レスポンダ）の設定

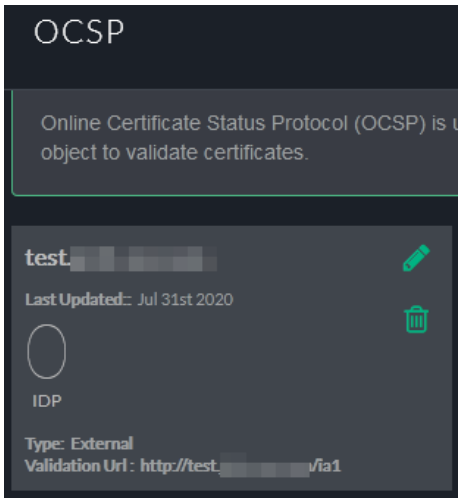
EAA の管理 Web サイトから[System] > [OCSP]と進み、[Add Certificates]からルート証明書をアップロードします。

- [Name]には、識別名称を入力
- [Type]には、”External”を選択
  OCSP レスポンダが社内などにあり、EAA Connector 経由で接続する場合は”Internal”を選択（弊社未検証）
- [Validation URL]には、OCSP レスポンダの URL を入力
  Gléas のデフォルト CA のレスポンダ URL は以下の通りです（リッスンポートが 80 に

なっている前提）
http://gleas.example.com/ia1



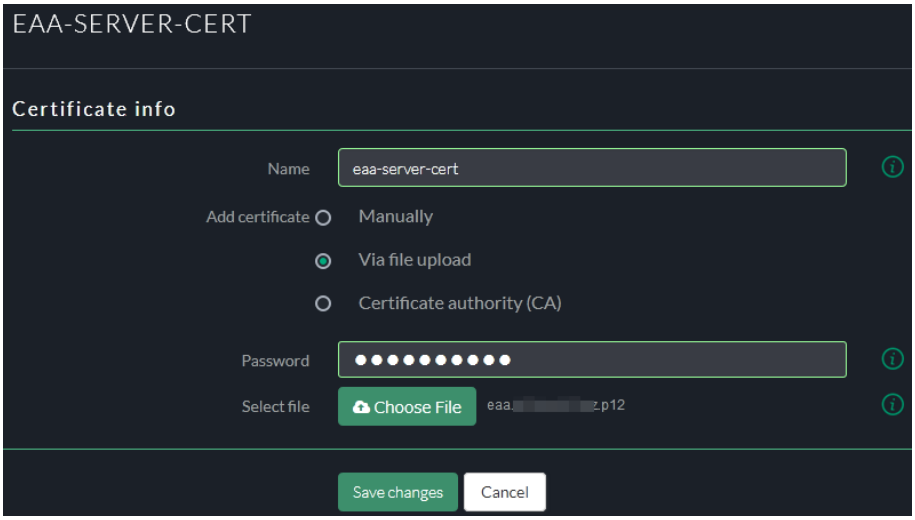
成功すると以下のように表示されます。



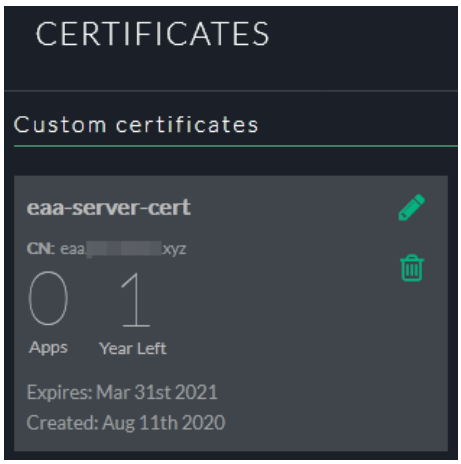
2.3. サーバ証明書のインポートと設定

事前に Gléas でサーバ証明書を発行しておき、PKCS#12 形式（*.p12）の証明書ファイルをダウンロードしておきます。
EAA の管理 Web サイトから[System] > [Certificates]と進み、[Add Certificates]からその証明書をアップロードします。

- [Name]には、識別名称を入力
- [Add Certificate]には、”Via file upload”を選択
- [Password]には、Gléas で証明書ファイルをダウンロードする際に設定したパスワードを入力
- [Select File]で、ダウンロードした証明書ファイルを指定

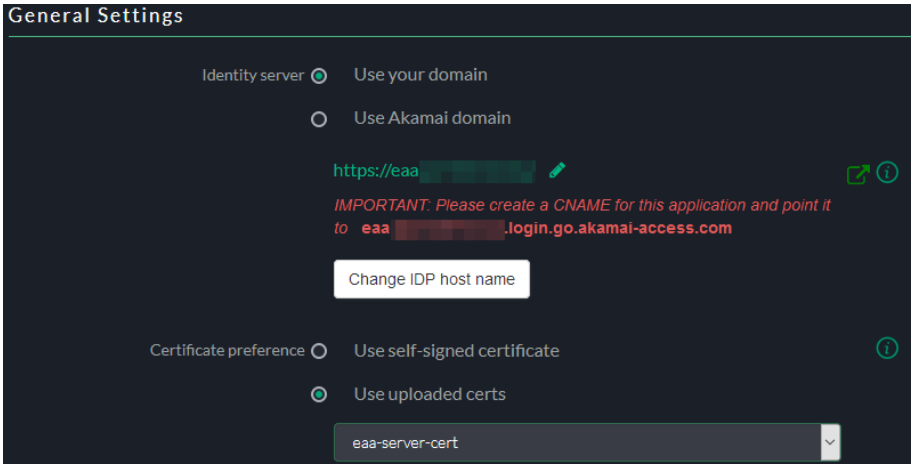


成功すると以下のように表示されます。



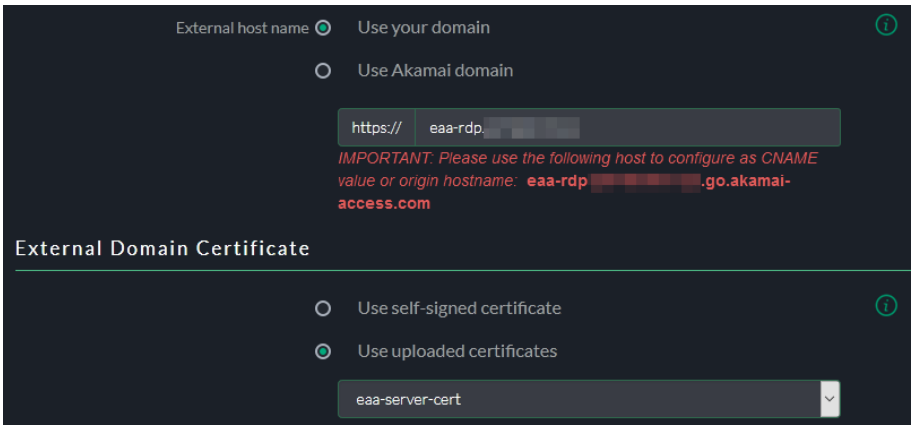
このサーバ証明書を IdP とアプリケーションに適用します。
EAA の管理 Web サイトから[Identity] > [Identity Providers]と進み、[Add Identity Provider]から新規に IdP を作成するか、既存の IdP を編集します。
[General Settings]でサーバ証明書の設定をおこないます。

- [Certificate preference]に、”Use uploaded certs”を選択
  ドロップボックスが表示されるので、上でインポートしたサーバ証明書を選択



他の設定も終了したら、Deploy をして設定を反映させます。

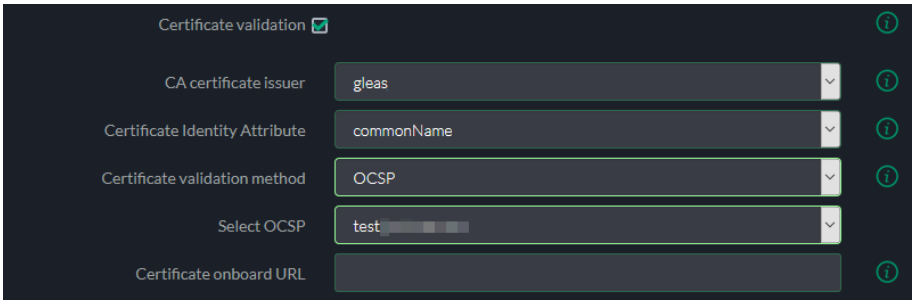
各アプリケーションについても同様に、サーバ証明書を設定して Deploy をします。



2.4. クライアント証明書認証の設定

上記の IdP の設定画面で以下を設定します。

- [Certificate validation]をチェック
- [CA certificate issuer]には、2.1 項でインポートしたルート証明書を選択
- [Certificate Identity Attribute]は、”commonName”を選択
- [Certificate validation method]は、”OCSP”を選択
- [Select OCSP]には、2.2 項で作成した OCSP レスポンダを選択
- [Certificate onboard URL]は、空欄のまま
  証明書認証ができない場合のリダイレクト先を指定できるので、Gléas の UA（エンドユーザ画面）の URL を指定するといった使い方が考えられます。



また、以下を設定することで証明書のみのログインが可能となります。

- [Certificate Identity is username]をチェック
  ※この場合、[Certificate Identity Attribute]で指定された証明書のサブジェクト属性がユーザ ID となるようです

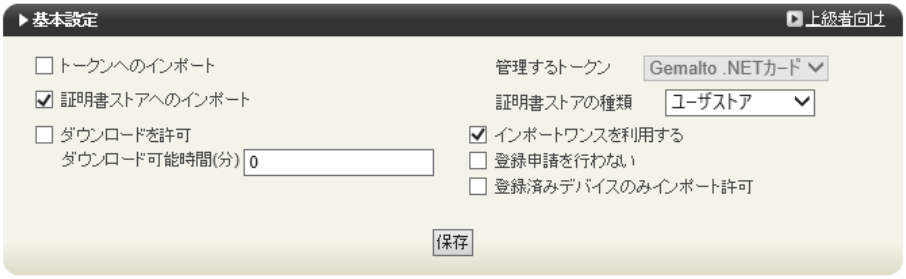
3. Gléasの管理者設定（Windows用）

GléasのUA（申込局）より発行済み証明書をWindowsクライアントにインポートできるよう設定します。
※下記設定は、Gléas納品時等に弊社で設定を既に行っている場合があります

GléasのRA（登録局）にログインし、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。

- [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



設定終了後、[保存]をクリックし設定を保存します。
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/Windows Phone の設定の、[Android / Windows Phone 用 UA を利用する]
- 証明書インポートアプリ連携の設定の、[証明書インポートアプリを利用する]

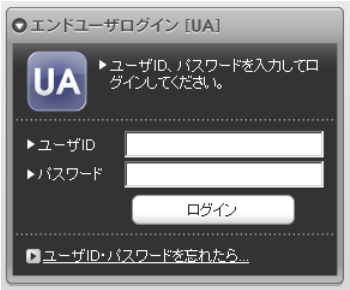
4. クライアントからのアクセス（Windows）

4.1. クライアント証明書のインポート

Internet Explorer（IE）でGléasのUAサイトにアクセスします。
ログイン画面が表示されるので、Gléasでのユーザ IDとパスワードを入力しログインします。

※ UAのログイン認証をActive Directoryで行うことも可能です。詳細は最終項のお問い合わせ先までご連絡ください

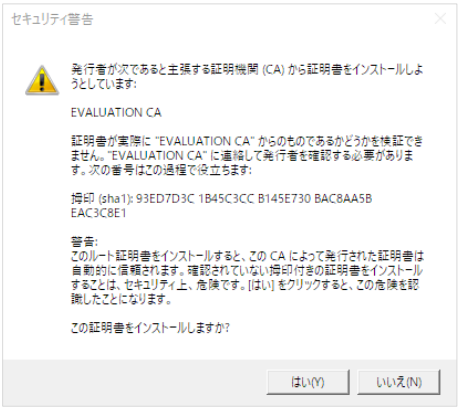
※ インポートにはIEを利用しますが、インポートされた証明書はchromeやEdgeなど他ブラウザで利用することが可能です



ログインすると、ユーザ専用ページが表示されます。
[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。

※ 初回ログイン時にはActiveXコントロールのインストールを求められるので、画面の指示に従いインストールを完了します

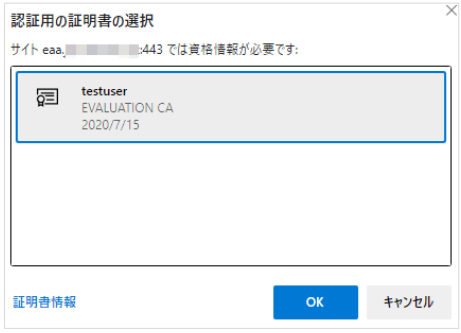
※ 証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印を確認するなど正当性を確認してから[はい]をクリックします



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おこなうことはできません。

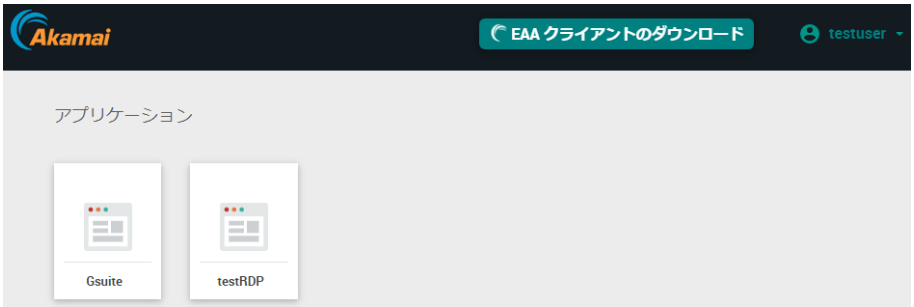
4.2. EAA へのアクセス（ブラウザ）

ブラウザでIdPへアクセスすると、クライアント証明書を求められます。

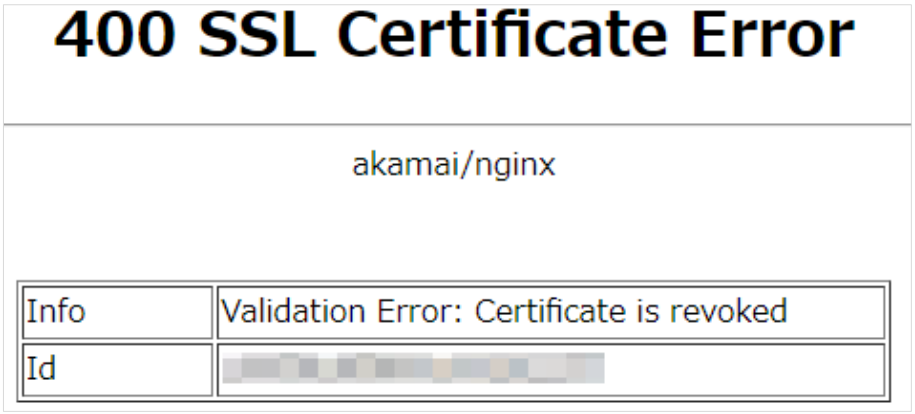


証明書認証が成功すると、IDとパスワードを入力するよう求められます。Active Directoryのユーザ IDとパスワードでログインします。
（EAAのログインユーザIDに利用するADの属性は、ディレクトリの設定項目”Login Preference”に依存します）

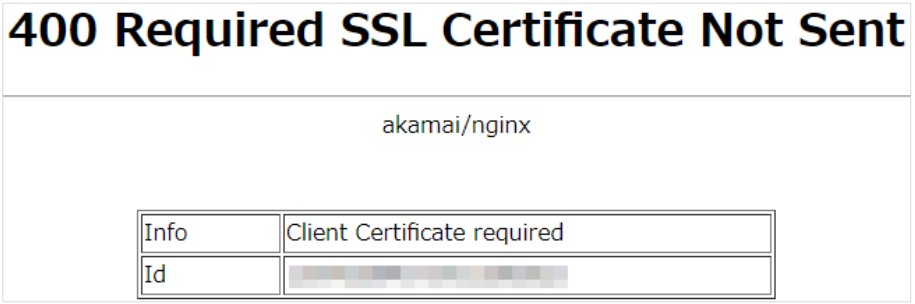
パスワード認証に成功すると、ポータル画面が表示され割り当てられたアプリを利用できます。



なお、失効した証明書でアクセスをすると、エラー表示となります。



またクライアント証明書がない場合は、以下のメッセージが表示されます。

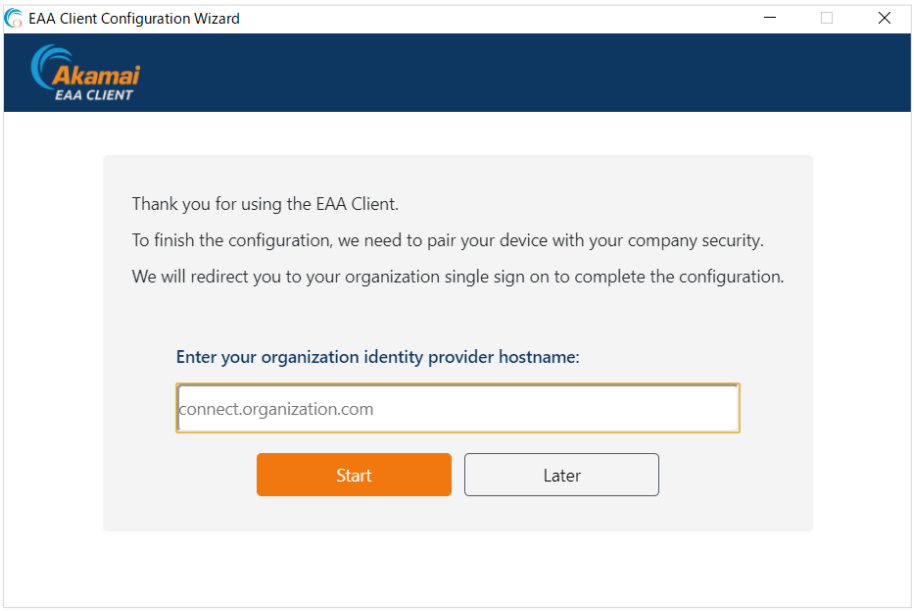


4.3. EAA へのアクセス（EAA Client）

※既定のブラウザをFirefox以外にしておこなう必要があります（OSの証明書ストア内の証明書を参照しないため）

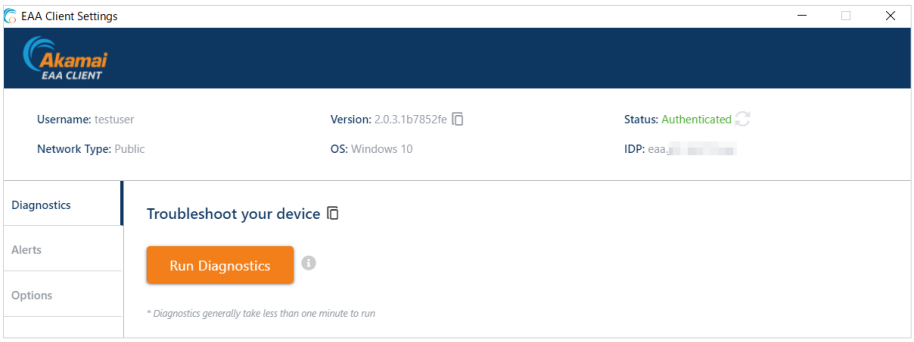
EAA Clientをインストールしたのちに、タスクトレイからEAAのアイコンを右クリックし、[Configure]をクリックします。

[Enter your organization identity provider hostname:]に、2項で設定したIdPのホスト名を入力します。



ブラウザが呼び出され前項と同じ認証フローがおこなわれます。認証成功すると以下が表示され、EAA Clientに設定が反映されます。

EAA Clientを開いてStatusを見ると、認証された状態であることが分かります。



この状態で宅内へのリモートアクセスが可能となります。

5. Gléasの管理者設定（macOS用）

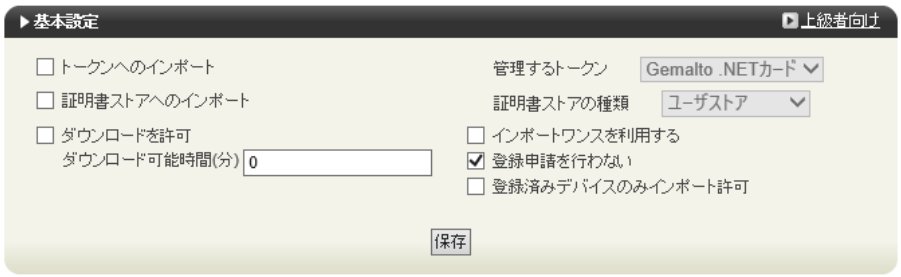
GléasのUA（申込局）より発行済み証明書をmacOSクライアント端末にインポートできるよう設定します。

※下記設定は、Gléas納品時等に弊社で設定を既に行っている場合があります

GléasのRA（登録局）にログインし、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。

[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。

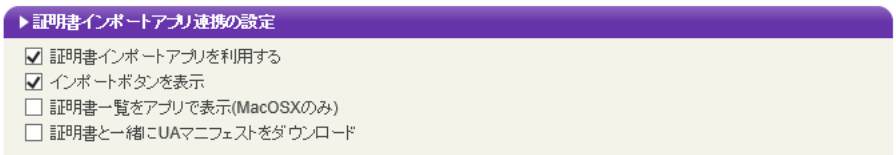
- [登録申請を行わない]以外のチェックをすべて外す
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック



設定終了後、[保存]をクリックし設定を保存します。

同じ画面下部の[証明書インポートアプリ連携の設定]で以下を設定します。

- [証明書インポートアプリを利用する]にチェック
- [インポートボタンを表示]にチェック



設定終了後、下部の[保存]をクリックし設定を保存します。

6. クライアントからのアクセス（macOS）

6.1. クライアント証明書のインポート

事前にGléas CertImporterをインストールして、SafariでGléasのUAサイトにアクセスします。

ログイン画面が表示されるので、GléasでのユーザIDとパスワードを入力しログインすると、ユーザ専用ページが表示されます。

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

インポートワンスついてもWindowsとほぼ同様になり、一度インポートした証明書を再度ログインしてインポートすることはできません。

6.2. EAA へのアクセス（ブラウザ）

SafariなどのブラウザでIdPへアクセスすると、クライアント証明書を求められます。

※以下、Windowsと同じ画面遷移のためスクリーンショットは省きます

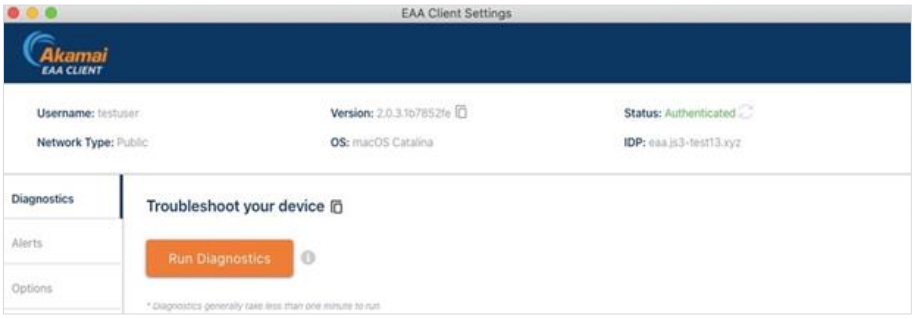
証明書認証が成功すると、IDとパスワードを入力するよう求められ、パスワード認証に成功

すると、ポータル画面が表示され割り当てられたアプリを利用できます。
失効した証明書でのアクセス、あるいは証明書をもっていない場合の動作についても、Windowsと同じです。

6.3. EAA へのアクセス（EAA Client）

※既定のブラウザをFirefox以外にしておこなう必要があります（OSのキーチェーンを参照しないため）
EAA Clientをインストールしたのちに、メニューバーからEAAのアイコンを右クリックし、[Configure]をクリックします。
[Enter your organization identity provider hostname:]に、2項で設定したIdPのホスト名を入力します。

ブラウザが呼び出され前項と同じ認証フローがおこなわれます。認証成功するとEAA Clientに設定が反映されます。
EAA Clientを開いてStatusを見ると、認証された状態であることが分かります。



この状態で宅内へのリモートアクセスが可能となります。

7. 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
営業本部
Tel:　050-3821-2195
Mail:　sales@jcch-sss.com