



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CA Gléas ホワイトペーパー

～Juniper MAG/SecureAccess～

SAMLシングルサインオン設定（Google Apps）

Ver.1.0

2012年8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 CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

目次

1. はじめに	4
1.1. 本書について	4
1.2. 本書における環境	4
1.3. 本書における構成	5
1.4. 電子証明書の発行時における留意事項	6
2. SA での設定	6
2.1. 二因子認証用のレلم設定	6
2.2. サインインページの設定	8
2.3. SAML idP 設定	9
2.4. リソースポリシー設定	12
3. Google Apps の管理設定	14
4. Gléas の管理者設定（PC）	15
5. クライアント証明書を用いた SSO（PC）	16
5.1. Gléas の UA からのクライアント証明書インストール	16
5.2. Google Apps へのシングルサインオン	17
6. Gléas の管理者設定（iPad）	19
6.1. UA（ユーザ申込局）設定	19
7. クライアント証明書を用いた SSO（iPad）	20
7.1. 構成プロファイルのインストール	20
7.2. OTA エンロールメントを利用した証明書発行について	23
7.3. Google Apps へのシングルサインオン	23
8. シナリオ 2 における設定方法	25
8.1. SA の設定変更・追加	25
8.2. Google Apps の設定変更	26
8.3. Gléas の設定変更	26
8.4. iPad での利用	27
9. 問い合わせ	27

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CA Gléas」で発行したクライアント証明書とジュニパーネットワークス社製SSL-VPN装置「MAG」・「SecureAccess」シリーズを利用して、Google Inc.の提供するSaaSサービス「Google Apps」に対しSecurity Assertion Markup Language (SAML) を用いたシングルサインオン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。

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、9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アイデンティティプロバイダ (idP)】**
Juniper Networks SecureAccess IVEバージョン (バージョン7.2R1.1 (build 20761))
※以後、「SA」と記載します
※本書の内容はMAGシリーズにも適用できます
- **【認証局】JS3 プライベートCA Gléas (バージョン1.10)**
※以後、「Gléas」と記載します
- **【SAMLサービスプロバイダ (SP)】Google Apps for Business**
※以後、「Google Apps」と記載します
- **【クライアント (PC)】Microsoft Windows 7 Professional SP1**
【ブラウザ】Internet Explorer 9
※以後、「PC」と記載します
- **【クライアント (タブレット)】Apple iPad (第三世代、iOS 5.1.1)**
※以後、「iPad」と記載します
【VPNソフトウェア】Junos Pulse (バージョン4.0.0.22645)
※以後、「Pulse」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。

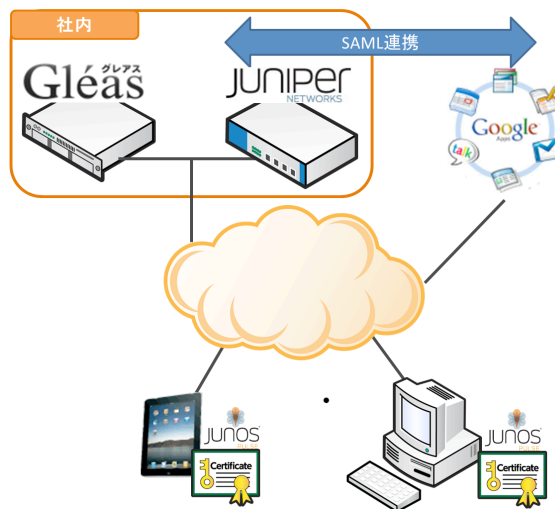
プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

- Google Appsの設定
- SAでのサーバ証明書設定やネットワーク設定、アクセス権限等の設定
- SAでのクライアント証明書認証を用いたトンネリングVPN設定
※弊社のWEBサイトでは、SAでクライアント証明書認証を用いたトンネリング環境を構築するためのホワイトペーパーを公開しておりますので、構築時の参考にしてください
参考URL：
<http://www.jcch-sss.com/service/support/2011/11/juniper-secureaccess-iphone-junos-pulse>
※本書では、上記ホワイトペーパーの2～3項での設定が既に済んでいることを前提としております
- Gléasでのユーザ登録やクライアント証明書発行等の基本設定
- PC・iOSでのネットワーク設定等の基本設定

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。



検証シナリオ1（2～7項）：SAにidPとしてアクセス

1. デバイス（PC・iPad）はGléasより資格情報（クライアント証明書）を含む構成プロファイルを取得する
2. ブラウザでGoogle Appsにアクセスすると、SAに転送される
3. SAでは有効なクライアント証明書を要求されるので、Gléasより取得した証明書による認証をおこなう
4. ユーザID・パスワードによる認証がおこなわれる。この時のユーザIDはクライアント証明書のサブジェクトのcn（一般名）が自動的に利用される

5. SAへのログインに成功すると、自動的にGoogle Apps（メール）に転送される
6. Google AppsをログアウトするとSAへのログイン状態を保持したままポータルページに遷移する（SAへの再ログインなしにVPN接続をおこなうことも可能）

以下のパターンにおける設定方法も別途記述します。

検証シナリオ2（設定変更・追加部分のみ8項）：SAにidPとしてアクセス（オンデマンドVPN併用。iPadのみ）

1. デバイス（iPad）はGléasより資格情報（クライアント証明書）及びVPN接続（オンデマンド）設定を含む構成プロファイルを取得する
2. ブラウザでGoogle Appsにアクセスすると、社内にあるSAに転送される
3. クライアント証明書認証によるVPNセッションが自動的に張られSAに接続する
4. 提示した証明書のサブジェクトのcnに対応したアカウントのGoogle Apps（メール）が表示される
5. Google AppsをログアウトするとVPNセッションを保持したままの状態が持続する

1.4. 電子証明書の発行時における留意事項

Gléasでクライアント証明書を発行する際には、以下の点に留意する必要があります。

- Gléasでのユーザアカウント（＝証明書サブジェクトのcn）と、SAでのユーザ名及びGoogle AppsのユーザIDは同一にする必要があります

2. SAでの設定

2.1. 二因子認証用のレルム設定

管理者画面左側メニューより[Users] > [User Realms] > [New User Realm...]と進み、右ペインで以下の設定をおこないます。

- [Name:]には、任意の名称を設定
- [Authentication]ドロップダウンは、[Auth. Servers]で設定した証明書サーバを選択
- [Additional Authentication Server]には、チェックを入れる
- [Authenticocation #2]には、[System Local]（或いは外部の認証サーバ）を選択

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

※ ログイン実行前に [Auth. Server] > [System Local] > [Users] タブにてログイン用ユーザーアカウントを作っておく必要があります。

- [Username is:]には、[predefined as:]を選択し、左のボックスに[<USER>]に設定されていることを確認

New Authentication Realm

* Name: sso_users
Description:

When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Gleas
Directory/Attribute: None
Accounting: None

Additional authentication server

You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specified by the user on credential.

Authentication #2: System Local
Username is:
 specified by user on sign-in page
 predefined as: <USER>
Password is:
 specified by user on sign-in page
 predefined as: <PASSWORD>
 End session if authentication against this server fails

Dynamic policy evaluation

Save changes?

以上を設定したら[Save Changes]ボタンをクリックします。

次に、[Role Mapping]タブをクリックし、[New Rule...]ボタンをクリックし以下の設定をおこないます。

- [Rule based on:]には、ドロップダウンメニューより[Username]を選択
※[Certificate]を選択した場合、証明書サブジェクトOU等による制御が可能
- [Name:]には、一意のルール名称を入力
- [Rule: If username...]項目にはこのルールを適用するユーザ名を入力
※ワイルドカードの利用（*）も可能
- [...then assign these roles]項目には、3.1項で作成したルールを選択
- 必要に応じその他の項目を設定

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

以下は、有効なクライアント証明書が提示された場合、証明書のサブジェクトCNが何であろうと「VPN Test」というロールにマッピングする例です。

※今回のテストの目的上、ロール「VPN Test」はVPNトンネリング設定を含んでいるものである必要があります

The screenshot shows the 'Role Mapping Rule' configuration page in the Juniper User Authentication Realms interface. The breadcrumb path is 'User Authentication Realms > sso_users >'. The rule is based on 'Username' and is named 'sso_mapping'. The rule condition is 'is *'. The 'then assign these roles' section shows 'Users' in the 'Available Roles' list and 'VPN Test' in the 'Selected Roles' list. The checkbox 'Stop processing rules when this rule matches' is checked. At the bottom, there are 'Save Changes' and 'Save + New' buttons.

以上を設定したら、[Save Changes]ボタンをクリックします。

2.2. サインインページの設定

管理者画面左側メニューより、[Authenticaiton] > [Signing In] > [Sign-In Policies]と進み、右ペインより[New URL...]をクリックし以下の設定をおこないます。

- [Sign-in URL:]には、SAML ログイン用に利用したいディレクトリ名を入力
- [Sign-in Page:]には、[Default Sign-In Page]を選択
- [Authentication Realm]には、[User picks from a list of authentication realms]を選択し、2.1 項で作成したレルムを[Selected realms:]に移す

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

The screenshot shows the 'New Sign-In Policy' configuration page. At the top left, there is a breadcrumb 'Signing In >' and the title 'New Sign-In Policy'. A 'Save Changes' button is located at the top left. The configuration fields include: 'User type' with radio buttons for 'Users' (selected), 'Administrators', and 'Authorization Only Access'; 'Sign-in URL' with a text input containing '*/sso/' and a format hint; 'Description' with a large text area; 'Sign-in page' with a dropdown menu set to 'Default Sign-In Page'; and 'Meeting URL' with a dropdown menu set to '*/meeting/'. Below these fields is the 'Authentication realm' section, which includes instructions and two radio button options: 'User types the realm name' and 'User picks from a list of authentication realms' (selected). The second option includes a list of 'Available realms' (containing 'Users') and 'Selected realms' (containing 'sso_users'), with 'Add ->', 'Remove', 'Move Up', and 'Move Down' buttons. The 'Configure Sign-in Notifications' section has two unchecked checkboxes: 'Pre-Auth Sign-in Notification' and 'Post-Auth Sign-in Notification'. At the bottom, there is a 'Save changes?' section with a 'Save Changes' button.

以上を設定したら、[Save Changes]ボタンをクリックします。

2.3. SAML idP 設定

管理者画面左側メニューより[System] > [Configuration] > [SAML]と進み、右ペインで[Setting]ボタンをクリックし、グローバル設定をおこないます。

- [Host FQDN for SAML]に、SAML サービスに利用するホスト名を入力

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

SAML >
Settings

Metadata Server Configuration

Timeout value for metadata fetch request: seconds 1 - 600. Specifies the time in seconds to wait for response metadata fetch request.

Validity of uploaded/downloaded metadata file: days 0 - 9999. Specifies the time in days after which downloaded metadata file expires. 0 means that SA does not enforce peer metadata file.

Host FQDN for SAML: The FQDN used for generating URLs for SAML services.

Alternate Host FQDN for SAML: The FQDN used for generating SA's Single Sign-On Service Pulse(NC) Session detection is enabled.

Save changes?

次に、左側メニューより[Authentication] > [Signing In] > [Sign-In SAML] > [Identity Provider]と進み、右ペインの[Identity Provider]をクリックします。

ここで idP 全体の設定をおこないます。

- [Protocol Binding to use for SAML Response]には、[POST]にチェックを入れる
- [Signing Certificate]には、サーバ証明書として利用している証明書を選択

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

Signing In

Sign-in Policies | Sign-in Pages | Sign-in Notifications | Sign-in SAML

Metadata Provider | Identity Provider

Basic Identity Provider (IdP) Configuration (Published in Metadata)

Protocol Binding to use for SAML Response

Post
 Artifact

* Signing Certificate: servercert.gleas.example Certificate to use for signing SAML n
Decryption Certificate: No Encryption Certificate to use for decrypting the

Other Configurations

Reuse Existing NC (Pulse) Session If enabled, the user's existing NC (P
 Accept unsigned AuthnRequest Individual SPs can choose to accept

Service-Provider-related IdP Configuration

The following settings apply to all Service Providers by default. Can be overridden in P

Relay State: 'RelayState' sent to SP in IdP-initiat

* Session Lifetime: None Suggested maximum duration of th
 Role Based
 Customize

* SignIn Policy: */ The SignIn Policy used by this IdP to

* Force Authentication Behavior: Reject AuthnRequest SA behavior if SP sends an authenti
 Re-Authenticate User

User Identity

* Subject Name Format: DN Format of 'NameIdentifier' field in g
* Subject Name: uid=<USERNAME> Template for generating user's iden

Save IdP configuration?

Save Changes Cancel

以上を設定したら、[Save Changes]ボタンをクリックします。

続けて Peer Service Provider Configuration にて[Add SP]ボタンをクリックし、以下の設定をおこないます。

- [Configuration Mode]が、[Manual]になっていることを確認
- [Entity Id:]には、SA 内での一意の識別子を設定
- [Assertion Consumer Service URL:]には、Google Apps の Assertion Consumer Service の URL を入力（"example.com"の部分は利用するドメイン名）
https://www.google.com/a/example.com/acs

* Configuration Mode: Manual Metadata If metadata is selected, uses metadata files uplo

Service Provider Configuration

* Entity Id: google.com/a/... Unique SAML Identifier of the SP.

* Assertion Consumer Service URL: /www.google.com/a/.../acs URL of the service on SP that recei

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

続いて、[Customize IdP Behavior]の設定をおこないます。

- [Override Default Configuration]に、チェックを入れる
- [Accept unsigned AuthnRequest]に、チェックを入れる
- [Sign-in Policy]には、2.2 項で設定したサインイン URL を選択
- [Subject Name Format:]には、[Email Address]を選択
- [Subject Name:]には、以下の通り入力（"example.com"の部分は利用するドメイン名）

<username>@example.com

Customize IdP Behavior

Override Default Configuration

Reuse Existing NC (Pulse) Session If enabled, the user's existing NC (Pulse) session if any

Accept unsigned AuthnRequest

Relay State: 'RelayState' sent to SP in IdP-initiated SSO scenario. If

* Session Lifetime: None Suggested maximum duration of the session at the SP
 Role Based
 Customize

* SignIn Policy: The SignIn Policy used by this IdP to authenticate the u

* Force Authentication Behavior: Reject AuthnRequest SA behavior if SP sends an authentication request with f
 Re-Authenticate User setting.

User Identity

* Subject Name Format: Format of 'NameIdentifier' field in generated Assertion.

* Subject Name: Template for generating user's identity as sent in 'Name

Save SP configuration?

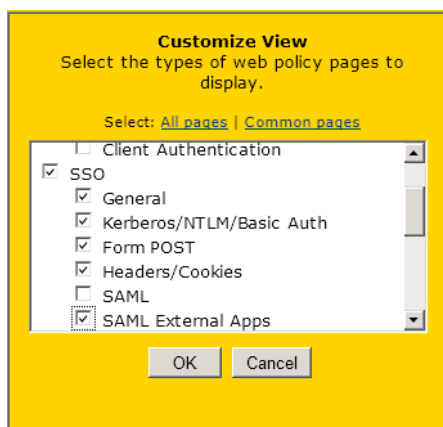
以上を設定したら、[Save Changes]ボタンをクリックします。

2.4. リソースポリシー設定

左側メニューより[Users] > [Resource Policies] > [WEB] > [SSO] > [SAML External Apps]を選択します。

※もし[SSO]を選んでも[SAML External Apps]が表示されない場合は、画面右側の[Customize]ボタンを押して[Customize View]ボックスを出現させ、[SAML External Apps]にチェックを入れると表示されるようになります。

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定 (Google Apps)



[New Policy]ボタンをクリックし、[General]タブにて以下の設定をおこないます。

- [Name]には、任意の名称を入力
- [Resource:]には、以下を入力 (“example.com”の部分は利用するドメイン名)
https://www.google.com/a/example.com/*
- [Rules:]には、このポリシーを適用する(或いは適用しない)ロールを選択する。
すべてのロールに適用する場合は、[Policy Applies to ALL roles]を選択
- [Service Provider Entity ID:]には、2.3 項で設定した ID を選択

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定 (Google Apps)

General Detailed Rules

* Name:
Description:

Resources

Specify the resources for which this policy applies, one per line. In order for your resource

* Resources:
 Examples:
*.domain.com/public
http://www.domain.com:8080/*
10.10.10.10/255.255.255.0:80
10.10.10.10/24:8000-9000

Roles

Policy applies to ALL roles
 Policy applies to SELECTED roles
 Policy applies to all roles OTHER THAN those selected below

Available roles:
Selected roles:

Action

Use the SAML SP defined below
 Do not use SAML SP
 Use Detailed Rules (see [Detailed Rules](#) page)

SAML SSO Details

Service Provider Entity ID:

Save changes?

設定終了後、[Save Change]をクリックして設定を保存してください。

3. Google Appsの管理設定

Google Appsの管理者画面にログインします。

[高度な設定] > [シングルサインオン (SSO) の設定]をクリックし、以下の設定をします。

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

- [認証の確認]に、2.3項で設定したサーバ証明書をアップロード
- [シングルサインオンを有効にする]にチェック
- [ログインページの URL]に以下を入力
https://2.3項[Host FQDN for SAML]で設定したFQDN/dana-na/auth/saml-ssso.cgi
- [ログアウトページの URL]に以下を入力
https://2.3項[Host FQDN for SAML]で設定したホスト名/
- [パスワード変更 URL]に以下を入力
https://2.3項[Host FQDN for SAML]で設定したホスト名/
- [ドメイン固有の発行元を使用]にチェック

シングル サインオン (SSO) の設定

SSO を設定するには次の情報を入力してください。 [SSOリファレンス](#)

シングル サインオンを有効にする

ログインページの URL *
 システムと Google Apps へのログイン用 URL

ログアウト ページ URL *
 ユーザーがログアウトするときリダイレクトする URL

パスワード変更 URL *
 ユーザーがシステムでパスワードを変更する際にアクセスする URL

認証の確認 *
認証ファイルのアップロードが完了しました。 [証明書を更新](#)

認証ファイルには、ログインリクエストを確認するための Google 公開キーが含まれている必要があります。 [詳細](#)

ドメイン固有の発行元を使用

ドメインで IDP アグリゲータを使用して SAML リクエストを処理する場合は、これを選択する必要があります。
有効になっていれば、SAML リクエストで送信した発行元は `google.com` ではなく `google.com/a/baxianpro.com`

ネットワーク マスク

ネットワーク マスクは、シングル サインオンで有効にできるアドレスを決定します。マスクが指定されない場合、ネットワーク マスクの区切りにはセミコロンを使用します。例: (64.233.187.99/8; 72.14.0.0/16)
範囲を指定する場合はダッシュを使用します。例: (64.233.167-204.99/32)
すべてのネットワーク マスクは CIDR で終わる必要があります。 [詳細](#)

以上を設定したら[変更を保存]をクリックします。

Google Apps の管理者設定は以上です。

4. Gléasの管理者設定（PC）

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、設定をおこなうUA（申込局）をクリックします。

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）



[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



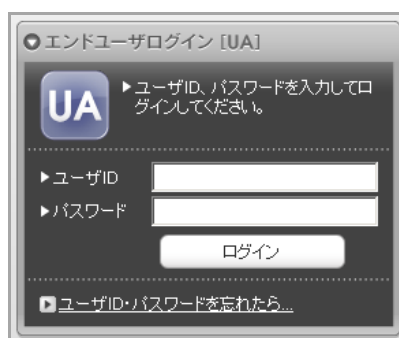
設定終了後、[保存]をクリックし設定を保存します。
各項目の入力が終わったら、[保存]をクリックします。

以上でGléasの設定は終了です。

5. クライアント証明書を用いた SSO（PC）

5.1. Gléas の UA からのクライアント証明書インストール

Internet Explorer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、ユーザIDとパスワードを入力しログインします。



ログインすると、ユーザ専用ページが表示されます。
初回ログインの際は、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てください。
その後、[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。

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

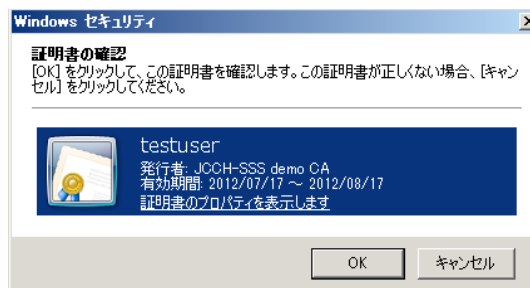


※「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません

5.2. Google Apps へのシングルサインオン

Internet ExplorerでGoogle Appsへアクセスします。URLは以下のとおりです。
<https://mail.google.com/a/<ドメイン名>>

提示可能なクライアント証明書が表示されるので、選択し[OK]をクリックします。



パスワード認証画面が表示されるので、パスワードを入力し[Sign In]ボタンをクリックします。

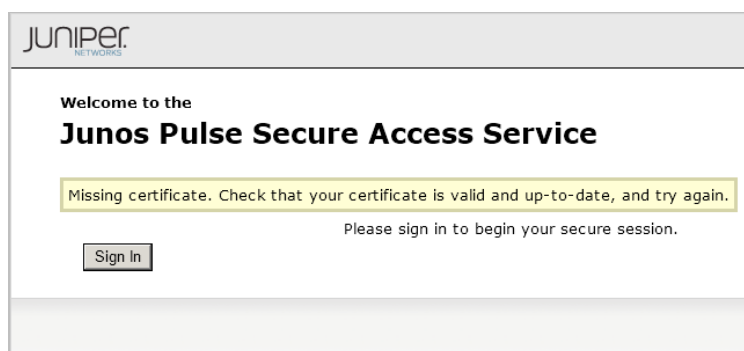
プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）



ログインに成功するとそのままGoogle Appsに遷移し、メール画面が表示されます。
なお Google Apps をログアウトすると、SA にはログインした状態のままでポータルページに戻りますので、継続して VPN を利用したりすることも可能です（SAでのロール設定によります）。

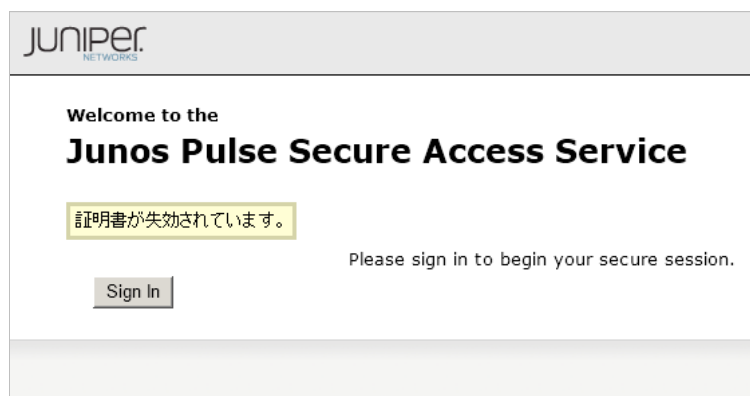


クライアント証明書のない状態でアクセスすると以下のとおりエラーとなります。



失効したクライアント証明書でアクセスすると以下の通りエラーとなります。
※失効情報がSAに伝搬されている必要があります

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）



6. Gléasの管理者設定（iPad）

※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

6.1. UA（ユーザ申込局）設定

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、iPad用となる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。

- [ダウンロードを許可]をチェック
- [インポートワンスを利用する]のチェック、[ダウンロード可能時間(分)]の設定
この設定を行うと、GléasのUAからダウンロードしてから、指定した時間（分）を経過した後に、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）。このインポートロックにより複数台のiPad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。

[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。

構成プロファイル生成に必要な情報を入力する画面が展開されるので、以下設

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

定を行います。

- [iPhone用レイアウトを利用する]にチェック
- [iPhone構成プロファイル基本設定]の各項目を入力
 - ※[名前]、[識別子]、[プロファイルの組織名]、[説明]は必須項目となります
 - ※[削除パスワード]を設定すると、iPadユーザが設定プロファイルを削除する際に管理者が定めたパスワードが必要となります（iPadユーザの故意や誤操作等による構成プロファイルの削除を防止できます）

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

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)

識別子(例: com.jcch-sss.profile)

プロファイルの組織名

説明

削除パスワード

設定終了後、[保存]をクリックして設定を保存します。

以上でGléasの設定は終了です。

構成プロファイルにWEBクリップ（ショートカットアイコン）設定を加えることも可能です。詳細は9項のお問合せ先までお問い合わせください。

7. クライアント証明書を用いた SSO（iPad）

GléasのUAに接続し、発行済みのクライアント証明書・構成プロファイルのインポートを行います。

7.1. 構成プロファイルのインストール

iPadのブラウザ（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、ユーザIDとパスワードを入力しログインします。

プライベート CA Gleás ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）



ログインすると、そのユーザ専用ページが表示されるので、[構成プロファイルのダウンロード]をタップし、ダウンロードを開始します。

※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



ダウンロードが終了すると、自動的にプロファイル画面に遷移するので、[インストール]をタップします。

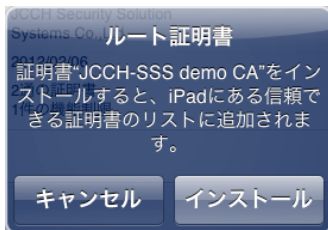
なお、[詳細]をタップすると、インストールされる証明書情報を見ることが可能ですので、必要に応じ確認してください。



インストール途中に、以下のようなルート証明書のインストール確認画面が現れますので、[インストール]をクリックして続行してください。

プライベート CA Gleás ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

※ここでインストールされるルート証明書は、通常Gleás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]をタップしてください。



元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトしてください。

以上で、iPadでの構成プロファイルのインストールは終了です。

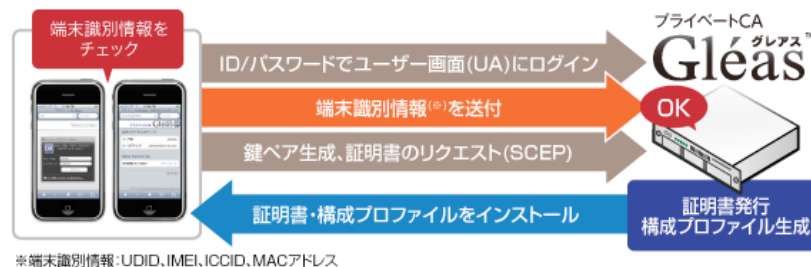
なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可能となります。



7.2. OTA エンロールメントを利用した証明書発行について

Gléasでは、iOSデバイスに対するOver The Air (OTA) エンロールメントを利用した証明書の発行・構成プロファイルの配布も可能です。

OTAを利用すると事前に指定した端末識別番号を持つ端末だけに証明書の発行を限定することも可能になります。



詳細は9項のお問い合わせ先までお問い合わせください。

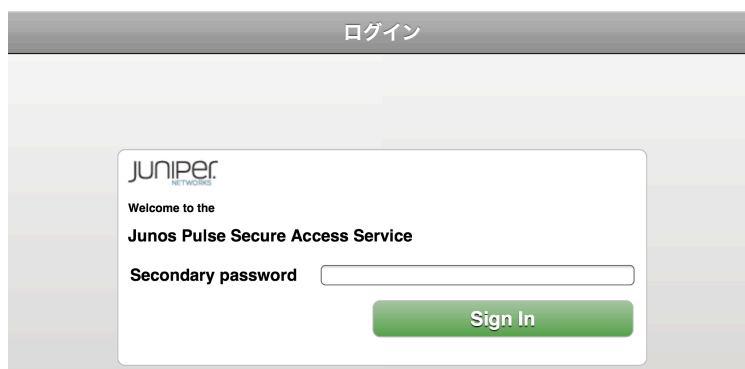
7.3. Google Apps へのシングルサインオン

SafariでGoogle Appsへアクセスします。URLは以下のとおりです。

<https://mail.google.com/a/<ドメイン名>>

提示可能なクライアント証明書が一枚の場合は、何も表示されずそのままSAのパスワード入力画面になります。

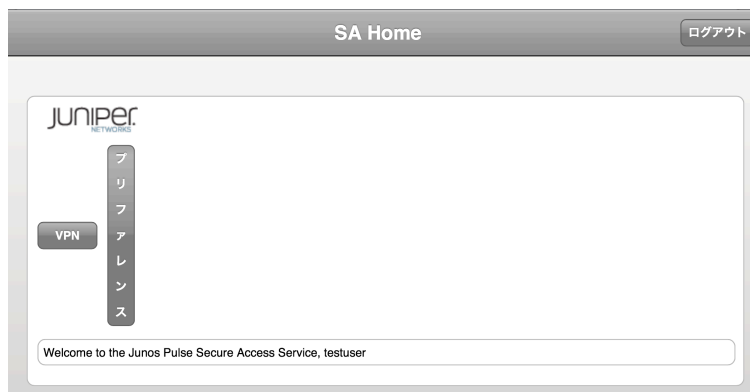
(提示可能な証明書が複数ある場合は選択ダイアログが出現しますので、適切な証明書を選択してください)



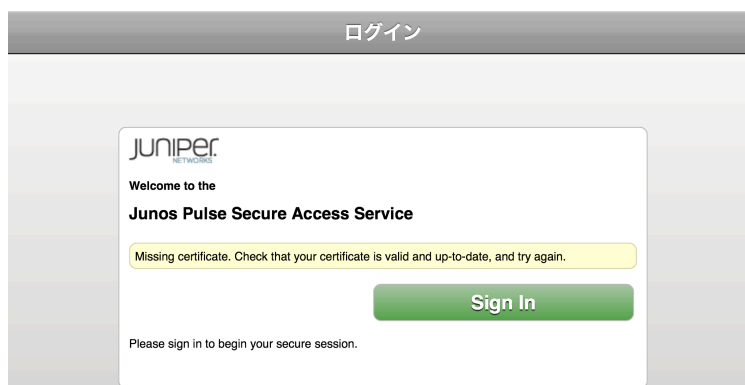
ログインに成功するとそのままGoogle Appsに遷移し、メール画面が表示されます。なおGoogle Appsをログアウトすると、SAにはログインした状態のままでポータルページに戻りますので、継続してVPNを利用したりすることも可能です(ポータル

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

タルページから何がおこなえるかは SA でのロール設定に依存します）。

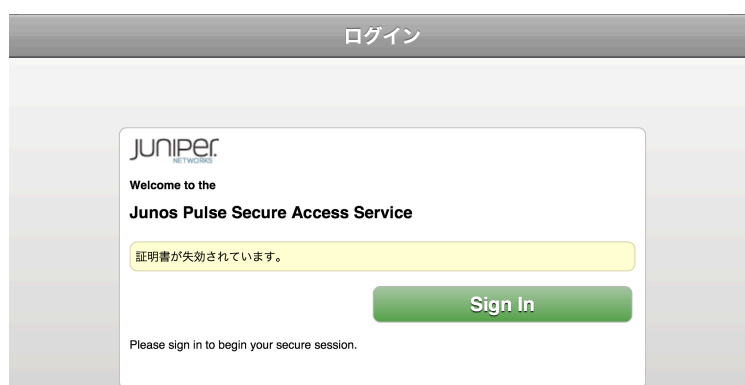


クライアント証明書のない状態でアクセスすると以下のとおりエラーとなります。



失効したクライアント証明書でアクセスするとSAのログイン画面まで進むことができません。

※失効情報がSAIに伝搬されている必要があります



8. シナリオ 2 における設定方法

8.1. SA の設定変更・追加

管理者画面左側メニューより[System] > [Configuration] > [SAML]と進み、右ペインで[Setting]ボタンをクリックし、グローバル設定をおこないます。

- [Alternate Host FQDN for SAML]に、SAML サービスに利用する内部ホスト名を追加

SAML >
Settings

Metadata Server Configuration

Timeout value for metadata fetch request: seconds 1 - 600. Specifies the time in seconds to wait for response metadata fetch request.

Validity of uploaded/downloaded metadata file: days 0 - 9999. Specifies the time in days after which downloaded metadata file expires. 0 means that SA does not enforce peer metadata file.

Host FQDN for SAML: The FQDN used for generating URLs for SAML services.

Alternate Host FQDN for SAML: The FQDN used for generating SA's Single Sign-On Service Pulse(NC) Session detection is enabled.

Save changes?

設定後、[Save Change]ボタンをクリックし保存し、その後に[Update Entity Ids]ボタンをクリックします。

※ここで設定した内部ホスト名はVPN 接続後に割り振られる DNS で名前解決できる状態になっている必要があるため、[User] > [Resource Policies] > [Connection Profiles] > [VPN Tunneling]で該当する接続プロファイルを確認しておきます。

DNS Settings

To override the standard DNS settings, specify custom settings for this profile here.

DNS Settings:

IVE DNS Settings

Manual DNS Settings

Primary DNS: IP address

Secondary DNS: IP address

DNS Domain(s): Example: "cc

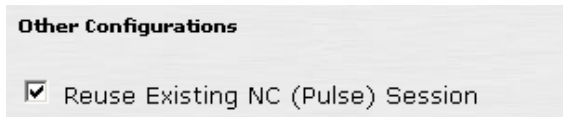
WINS: Name or IP address

DHCP DNS Settings (only applicable if DHCP Server is chosen)

次に、左側メニューより[Authentication] > [Signing In] > [Sign-In SAML] > [Identity Provider]と進み、右ペインの[Identity Provider]をクリックします。

ここで idP 全体の設定をおこないます。

- [Reuse Existing NC (Pulse) Session]に、チェックが入っていることを確認（入っていない場合はチェックし[Save Change]をクリック）



続けて Peer Service Provider Configuration にて、2.3 項で作成した SP をクリックし、以下の設定をおこないます。

- [Reuse Existing NC (Pulse) Session]に、チェックが入っていることを確認（入っていない場合はチェックし[Save Change]をクリック）

8.2. Google Apps の設定変更

Google Appsの管理者画面にログインします。

[高度な設定] > [シングルサインオン（SSO）の設定]をクリックし、以下の設定をします。

- [ログインページの URL]に、以下を入力
https://8.1項[Alternate Host FQDN for SAML]で設定したFQDN/dana-na/auth/saml-ss0.cgi
- [ログアウトページの URL]には、適当なページ（イントラネットサイト等）を入力
※SAのポータル等に設定するとログアウト時にVPNが切断されます
- [パスワード変更 URL]に以下を入力
https:// 8.1項[Alternate Host FQDN for SAML]で設定したFQDN/
※SAへの移行時にVPNが切断されますので、この方法ではパスワード変更はできません。
本ケースでは、SAへのログインにクライアント証明書のみを利用するので、この点は無視します

以上を設定したら[変更を保存]をクリックします。

8.3. Gléas の設定変更

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、iPad用となるUA（申込局）をクリックします。

[申込局詳細]画面が開くので、[認証デバイス情報]の[iPhone/iPadの設定] > [Juniper までスクSSL-VPNの設定]まで進み、以下の設定追加をおこないます。

- [SSL-VPN 接続名]には、適当な名前を入力

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定（Google Apps）

- [SecureAccess ホスト名]には、アクセス先となるSAの外部ホスト名（及びディレクトリ名）を入力
※8.1項の[Alternate Host FQDN for SAML]ではないので注意してください。iPadからみたトンネリングVPNの接続先となります。
※SAでの認証はクライアント証明書のみにしておく必要があります
- [オンデマンド接続先]には、8.1項の[Alternate Host FQDN for SAML]で設定したホスト名のドメイン名部分を指定（或いは、ホスト名そのものでも可）
※VPNオンデマンドとは：
事前に定義されているドメインにアクセスする際に、ユーザに意識させることなく自動的にVPN接続を確立する機能（証明書ベースでの認証が必須）

Juniper SSL-VPNの設定	
SSL-VPN 接続名	JS3 SSO
SecureAccess ホスト名	jcch-sss.com
オンデマンド接続先	jcch-sss.local

以上の設定が終わったら[保存]ボタンをクリックします。

8.4. iPad での利用

7.1項と同じ手順で構成プロファイルをインストールします。
構成プロファイルにより、VPNオンデマンドを含めたSAへの接続設定や、認証に利用するクライアント証明書は既にiPadにインストールされます。

その状態で7.2項同様にGoogle Appsへアクセスすると、自動的にJunos PulseによるVPN接続がおこなわれます（iPadの通知エリアに **VPN** アイコンが表示されます）。その後にはVPNでの認証情報を利用しGoogle Appsのメール画面に遷移します。

この方法ではGoogle Appsログアウト後もVPNセッションは持続するので、社内へのVPNアクセスは継続して可能です。

9. 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。

■MAG/SAに関するお問い合わせ先
ジュニパーネットワークス株式会社

プライベート CA Gléas ホワイトペーパー
～Juniper MAG/SecureAccess～
SAMLシングルサインオン設定 (Google Apps)

URL : otoiawase@juniper.net

■Gléasや検証用の証明書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