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～

iOSデバイスでのクライアント証明書による認証設定

（Microsoft Exchange ActiveSync編）

Ver.2.0

2011 年 11 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CA Gléas」で発行したクライアント証明書・iOS構成プロファイルを利用して、ジュニパーネットワークス社製SSL-VPN装置「MAG」「SecureAccess」シリーズを経由してMicrosoft Exchange ActiveSyncを行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。

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、5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。

- Juniper Networks SecureAccess DTE （バージョン7.1R3 （build 18671））
  ※以後、「SA」と記載します
  ※本書の内容はMAGシリーズでも適用できます
- JS3 プライベートCA Gléas （バージョン1.9）
  ※以後、「Gléas」と記載します
- iPhone 4 （iOS 5.0）
  ※以後、「iPhone」と記載します。本書の内容はiPad、iPad2でも適用できます
  ※以後、Exchange ActiveSyncは「ActiveSync」と記載します
- Microsoft Windows Server 2008 R2 Standard / Exchange Server 2010

以下については、本書では説明を割愛します。

- 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
- 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
- iPhoneでのネットワーク設定等の基本設定
- Microsoft Windows Server 2008 R2、Active Directoryのセットアップ
- Exchange Server 2010のセットアップ（ActiveSync設定を含む）

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。

2. SAの設定

2.1. 信頼するルート認証局の設定

今回利用するクライアント証明書のトラストアンカとなるルート認証局を設定します。
管理者画面左側のメニューより[Configuration] > [Certificates] > [Trusted Client CAs]と進み、右側画面に出現する[Import CA Certificate…]ボタンをクリックします。

[Import From:]のところで[参照]ボタンを押し、ローカルに保存してあるルート証明書を選択し、[Import Certificate]ボタンをクリックします。
成功すると以下のような画面が現れます。

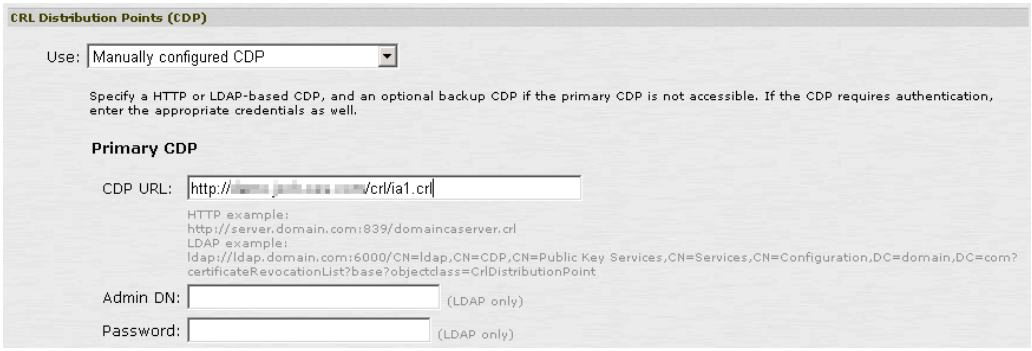
失効リスト（CRL）を利用したクライアント証明書の失効確認を行う場合は、Client certificate status checking 項目で、[Use CRLs (Certificate Revocation Lists)]を選択してください。

ここで一度[Save Setting]をクリックして、設定を保存してください。

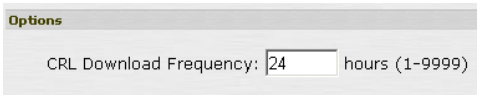
その後、同じ設定画面の最下部にある CRL Setting の項目で、[CRL Checking Options…]をクリックします。
CRL Checking Option の設定画面に移動しますので、以下の設定を行います。

- [Use:]のドロップボックスより[Manually Configured CDP]を選択
- Primary CDP の[CDP URL]に CRL 配布ポイントとなる URL を入力
  ※CRL 配布点が複数ある場合は、Backup CDP を設定することも可能

以下は Gléas が http で公開している CRL を取得しに行く場合の設定例となります。



また CRL の取得間隔を指定したい場合は、Options 項目で[CRL Download Frequency]を指定することにより可能です。
以下は CRL の有効期限に関係なく、24 時間毎に CRL を取得しに行く場合の設定例となります。



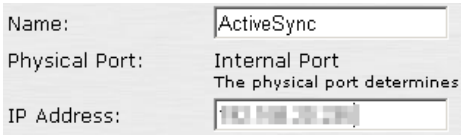
設定終了後、[Save Setting]をクリックして設定を保存してください。

2.2. バーチャルポートの設定

SAのInternalインターフェースにバーチャルポートを設定し、ActiveSyncに関する通信はバーチャルポートで行うよう設定します。

左側のメニューから[Network] > [Internal Port] > [Virtual Ports]をクリックします。
右側画面で以下を設定します。

- [Name:]には、一意の名称を入力
- [IP Address:]にはこのバーチャルポートに割り当てるIPアドレスを入力

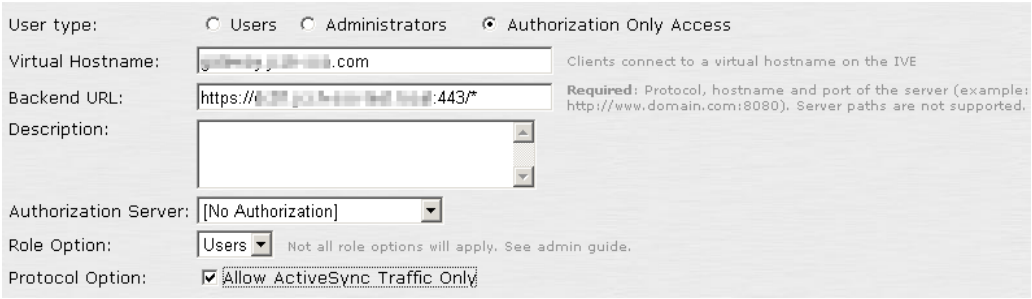


設定終了後、[Save Setting]をクリックして設定を保存してください。

2.3. サインイン URL の設定

左側のメニューから[Signing-in] > [Sign-in Policies]をクリックし、右側の画面の[New URL…]ボタンをクリックします。
移動した画面で以下を設定します。

- [User type:]では、[Authorization Only Access]を選択
- [Virtual Hostname:]には、2.2項で設定したバーチャルポートに紐付くホスト名を入力
- [Backend URL]には、Exchangeサーバのホスト名を入力
- [Authorization Server]には、No Authorizationを選択
- [Role Option]には、適当なロールを選択
  ※ここでは選択したロールの一部の設定（接続タイムアウト時間やIPアドレス制限等）のみが適用されます。詳細はSAのヘルプ項目「Enabling ActiveSync」を参照してください
- [Protocol Option]では、[Allow ActiveSync Traffic Only]をチェック



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。
以下の通り、バーチャルホスト名が作成されていること確認してください。

2.4. バーチャルポート用のサーバ証明書の設定

左側のメニューから[Configuration] > [Certificates] > [Device Certificates]をクリック

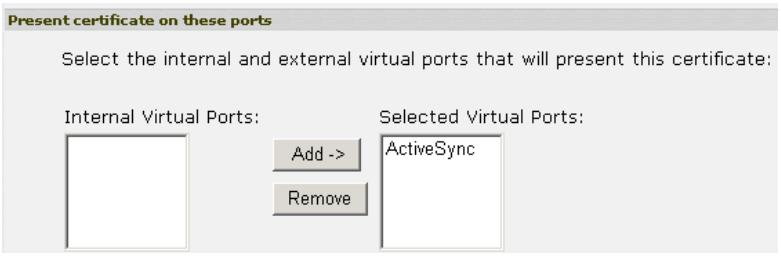
し、右側の画面の[Import Certificate & Key…]ボタンをクリックします。
移動した画面のIf certificate file includes private key:の項目で以下を設定します。

- [Certification File:]には、サーバ証明書のPKCS#12ファイルを選択
  ※Gléasで発行したサーバ証明書を利用する場合は、事前にサーバ証明書・秘密鍵をPKCS#12ファイルとしてダウンロードし、そのファイルを指定してください
  ※証明書と秘密鍵とが異なるファイルの場合は、その下のIf certificate and private key are separate files:項目よりインポートすることが可能です（弊社未検証）
- [Password Key:]には、上記PKCS#12ファイルの保護パスワードを入力

上記入力後、[Import]ボタンをクリックします。

インポートに成功すると元の画面に戻りますので、サーバ証明書が追加されていることを確認し、そのサーバ証明書名をクリックしCertificate Detailの設定画面に移動します。
その画面のPresent certificate on these portsの項目で以下の設定を行います。

- [Internal Virtual Ports:]の中にある2.2項で作成したバーチャルポートを、 [Add ->]ボタンをクリックし [Selected Virtual Ports:]に移動する



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

2.5. 証明書認証を利用するバーチャルポートの指定

左側のメニューより[Configuration] > [Security] > [SSL Options]をクリックします。
移動した画面の下部 Require client certificate on these ports 項目で以下の設定を行います。

- [Internal Virtual Ports:]の中にある2.2項で作成したバーチャルポートを、[Add ->]ボタンをクリックし[Selected Virtual Ports:]へ移動する

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. Gléasの管理者設定（ActiveSync）

Gléas で、発行済みのクライアント証明書を含む ActiveSync 接続設定（構成プロファイル）を iPhone にインポートするための設定を本章では記載します。

※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

3.1. UA（ユーザ申込局）設定

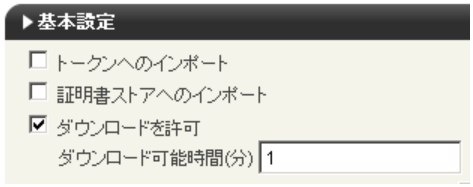
GléasのRA（登録局）にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、iPhone用となるUA（申込局）をクリックします。

上記の場合は、iPhone用UAと記載のあるものをクリックします。

[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
- [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iPhone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となる情報を入力する画面が展開されるので、以下設定を行います。

- [iPhone用レイアウトを利用する]をチェック
- iPhone OS 3を利用しているユーザがいる場合は[ログインパスワードで証明書を保護]をチェック
  iPhone OS 3では構成プロファイルのインストール時に証明書のインポート用パスワードを求められますが、ここをチェックすることにより、UAへのログインパスワードを利用できます。
- [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]は必須項目となります
  ※[削除パスワード]を設定すると、iPhone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（iPhoneユーザの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）
- [Exchangeホスト名]にアクセス先となるSAのホスト名（FQDN）を入力
- [パスワードの入力方法]には、Exchange用パスワードの入力方法を以下より選択
  [ログインパスワードを利用]： UAへのログインパスワードを利用
  [UAでパスワードを入力]： UA画面内でパスワードを入力
  [パスワードを保存しない]： 構成プロファイルのインストール時にパスワードを要求されるので入力

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。

4. iPhone での構成プロファイル・証明書のインストール

4.1. Gléas の UA からのインストール

iPhone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。

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、[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や設定情報を見ることが可能ですので、必要に応じ確認します。

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ます。

※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。

※iPhone OS 3の場合は、この前にクライアント証明書の保護パスワードを要求される画面が出現するので、UAログインに利用したパスワードを入力します

[パスワードの入力方法]に、[パスワードを保存しない]を設定した場合は、以下の画面になりますので、Exchangeパスワードを入力します。

[インストール完了画面になりますので、[完了]をタップします。

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能となります。

4.2. Exchange ActiveSync の利用

インストールした構成プロファイルにより、アクセス先SAの設定や、認証に利用するクライアント証明書やユーザIDは既にiPhoneにインストールされていますので、メールアプリケーションよりExchange ActiveSyncによるアクセスが可能となって

います。
クライアント証明書によるセキュアな接続をお試しください。

5. 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。

■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
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