モバイル VPN
簡単設定ガイド

ウォッチガード・テクノロジー・ジャパン株式会社

2014 年 8 月 Rev-04

目次

改訂履歴:

第 1 版	2010 年 3 月 17 日	初版発行
第 2 版	2011 年 2 月 17 日	
第 3 版	2012 年 7 月 10 日	
第 4 版	2014 年 8 月 19 日	

はじめに

XTM は、モバイル VPN の接続に以下の3つのプロトコルをサポートしています。

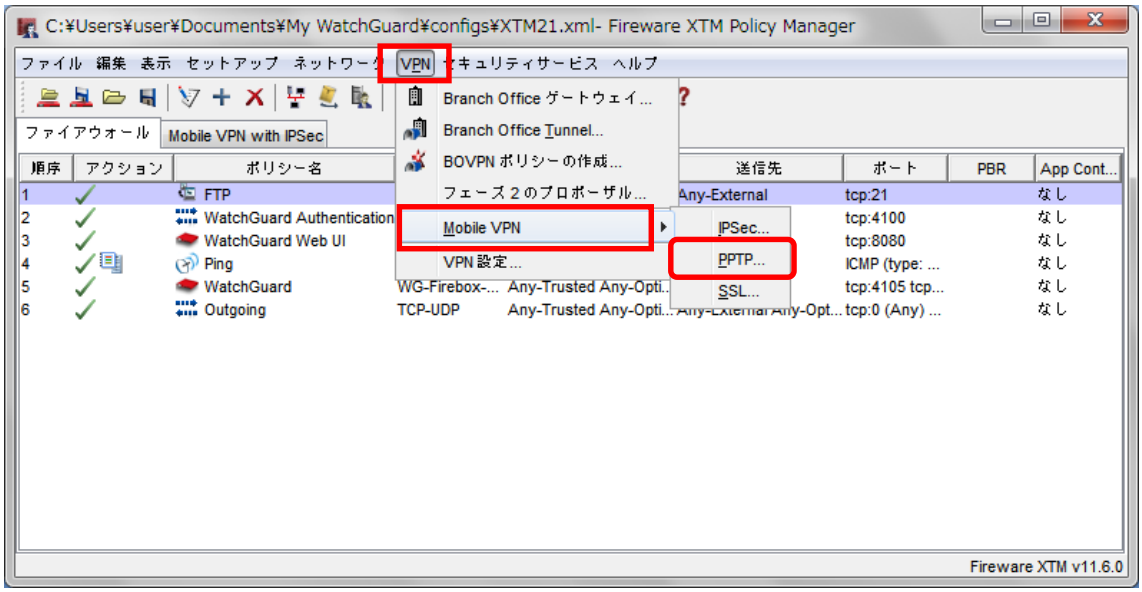
- PPTP(Point-to-Point Tunneling Protocol)
- IPsec(Security Architecture for Internet Protocol)
- SSL(Secure Socket Layer)

このガイドでは、プロトコル毎の設定方法を説明します。

モバイル VPN PPTP の設定方法

Firebox 側の PPTP 有効化と設定

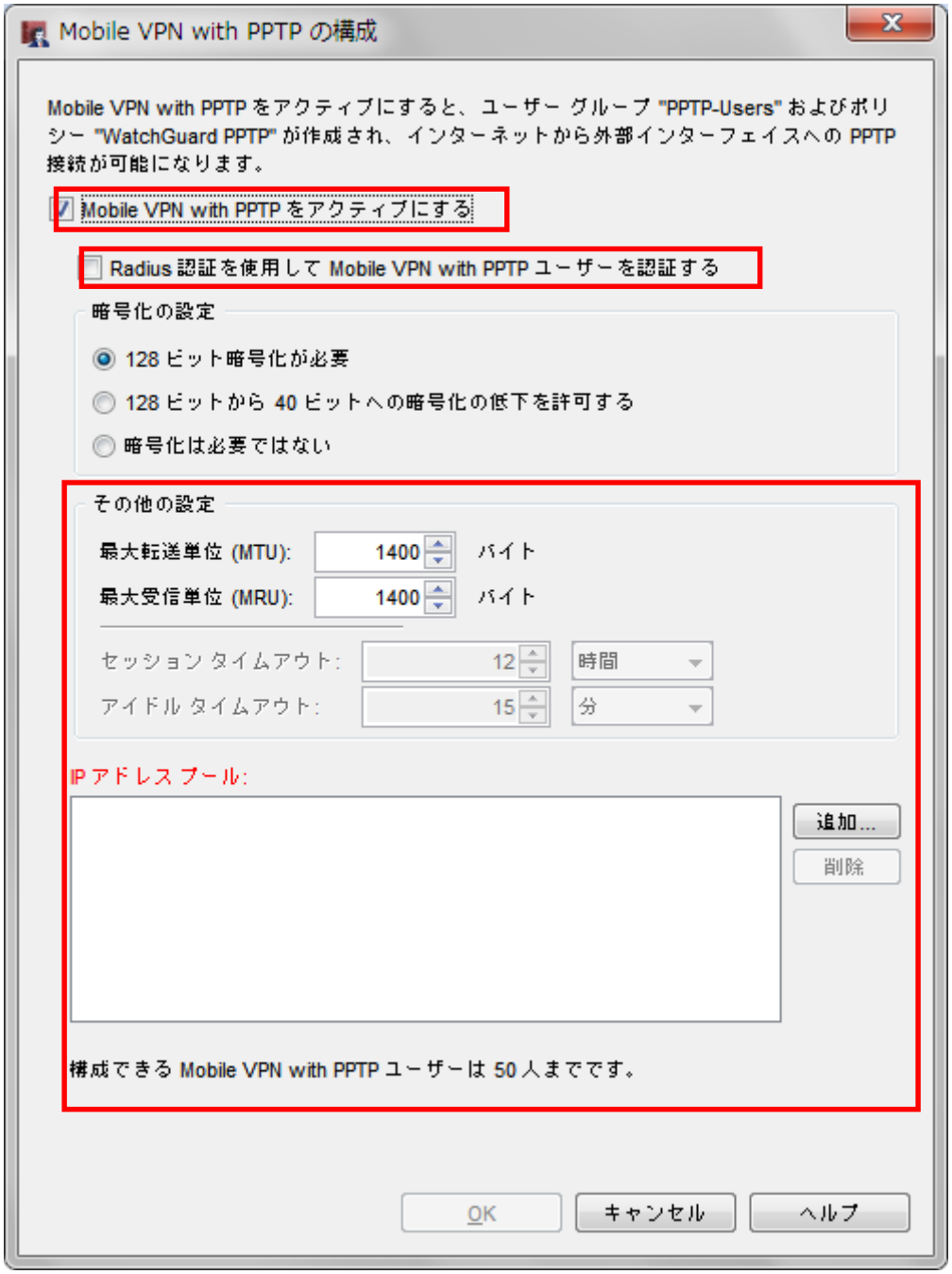
① ポリシーマネージャーから VPN > Mobile VPN > PPTP を選択します。



② 次にモバイル VPN（PPTP）を利用するために、「Mobile VPN with PPTP をアクティブにする」にチェックをいれます。この項目にチェックをいれると、WatchGuard PPTP ポリシーと、PPTP ユーザーが自動的に追加されます。

また、PPTP 接続では、Radius サーバーによる認証を利用することができます。

Radius サーバーを利用する場合、「Radius 認証を使用して Mobile VPN with PPTP ユーザーを認証する」にチェックを入れてください。

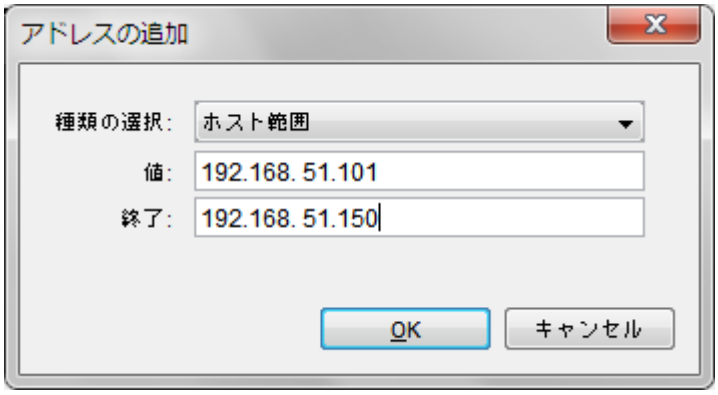


次にその他の設定を行います。

設定できる項目は以下となります。

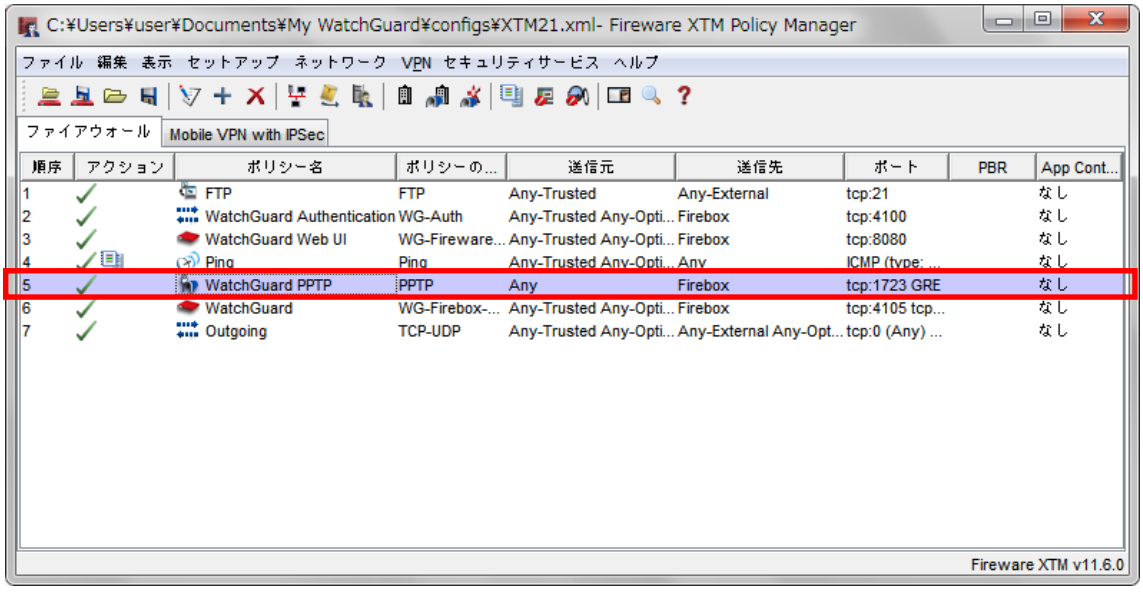
- 最大転送単位(MTU):1 回の転送で送信できるデータの最大値を変更
- 最大受信単位(MRU):1 回の転送で受信できるデータの最大値を変更
- セッションタイムアウト:デフォルトでは 12 時間に設定
- アイドルタイムアウト:デフォルトでは 15 分に設定
- IP アドレスプール:XTM では、同時セッション数が 50 に制限されており IP アドレスにより、接続ユーザーを制限することができます。

IP Address Pool 横の Add ボタンをクリックすると、Add Address ダイアログが表示されます。プールする IP アドレスは、ホスト IP もしくは、ホスト範囲で指定することができます。



③　設定完了後、「OK」ボタンをクリックします。

ポリシーマネージャーに「WatchGuard PPTP」ポリシーが追加されていることを確認してください。

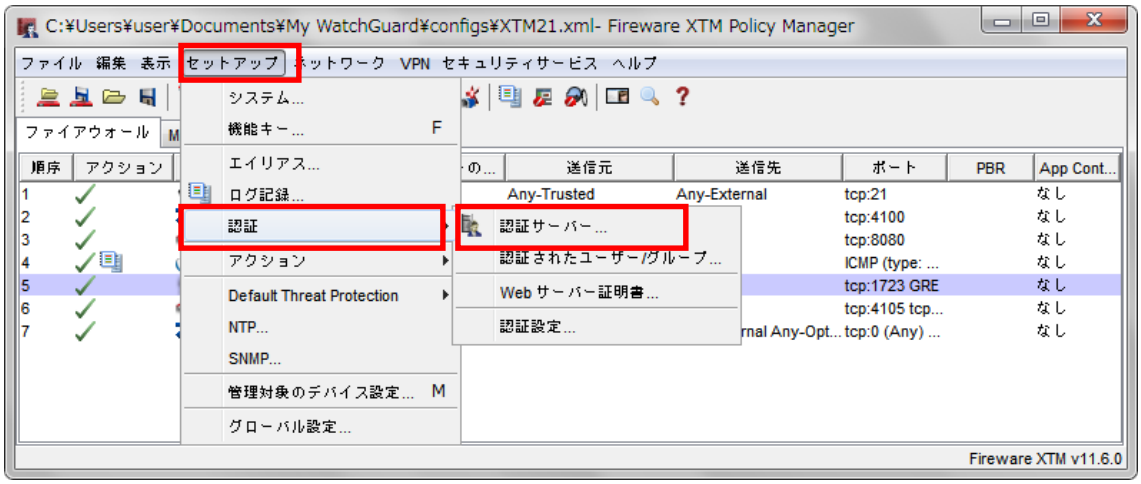


以上で、XTM 側のモバイル VPN(PPTP)の設定は終了となります。

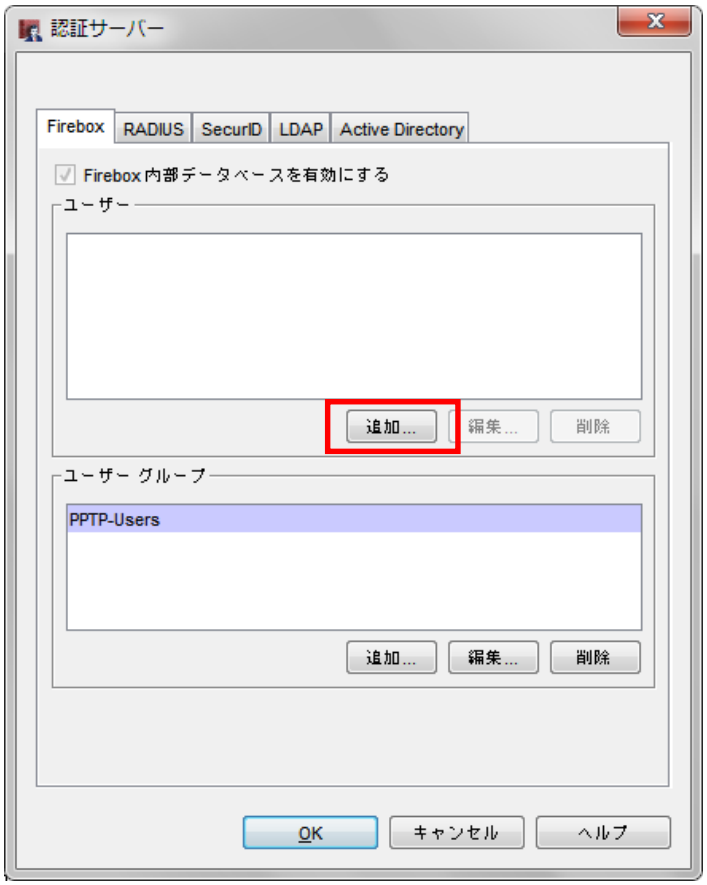
モバイル PPTP ユーザーの作成

次にモバイル PPTP で接続するためのユーザーを作成します。

ポリシーマネージャーのセットアップ＞ 認証＞ 認証サーバーをクリックします。



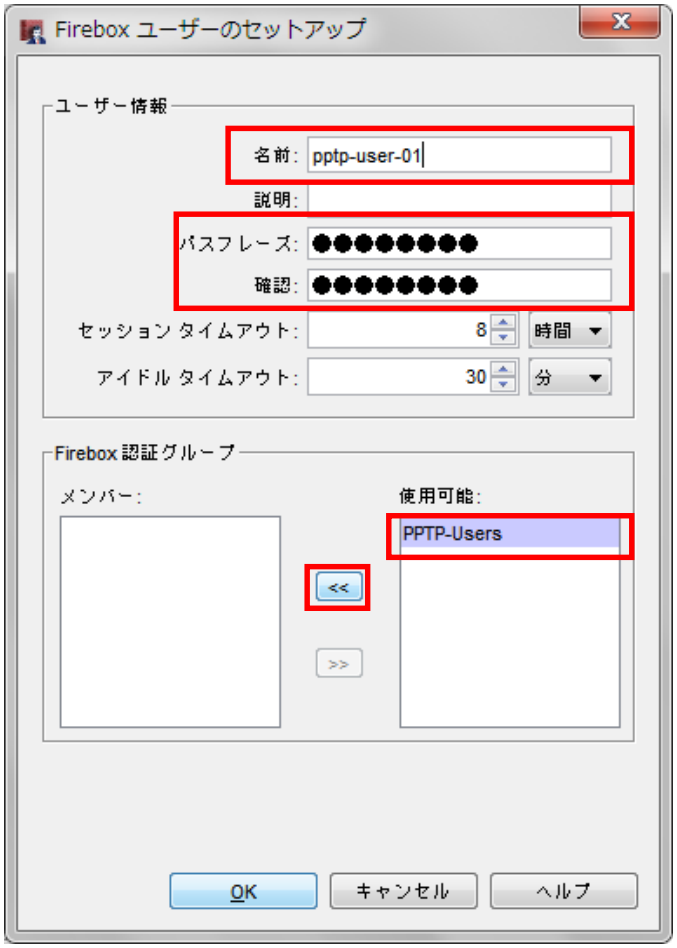
認証サーバーのダイアログで「追加」をクリックします。



ユーザー情報に任意の名前を入力します。

パスフレーズは 8 文字以上の英数字を入力します。

Firebox 認証グループには、PPTP を有効にしたときに自動的に作成された PPTP-Users を選択し、<< をクリックし、新しいユーザーを PPTP-Users グループに含めます。



以下の状態になります。

ユーザー追加と認証サーバーのダイアログの OK をクリックして閉じたら、ポリシーマネージャーで設定を保存します。

次にクライアント機の設定を行います。ここでは例として Windows7 の設定方法を記載します。その他の Windows バージョンにつきましては、ヘルプの「PPTP 用クライアント コンピュータを準備する」を参照ください。

PPTP クライアントの設定

① Windows のスタートメニュー＞コントロールパネル>ネットワークと共有センターを選択します

② ネットワーク設定の「新しい接続またはネットワークのセットアップ」をクリックします。

③ 新しい接続ウィザードの開始画面が表示されたら、「次へ」をクリックします

④ 「職場に接続します」を選択し、「次へ」をクリックします

⑤ 「既存の接続を利用しますか？」には、「いいえ、新しい接続を作成します」を選択し「次へ」をクリックします

⑥ 「インターネット接続(VPN)を使用します」をクリックします

⑦ インターネットアドレスには、XTM の External のアドレス、もしくは名前解決できるのであればホスト名を入力します。接続先の名前は任意（例：モバイル PPTP VPN 接続）です。入力したら「次へ」をクリックします

⑧ ユーザー名、パスワードを入力し、「このパスワードを記憶する」にチェックを入れ、最後に「接続」をクリックします。

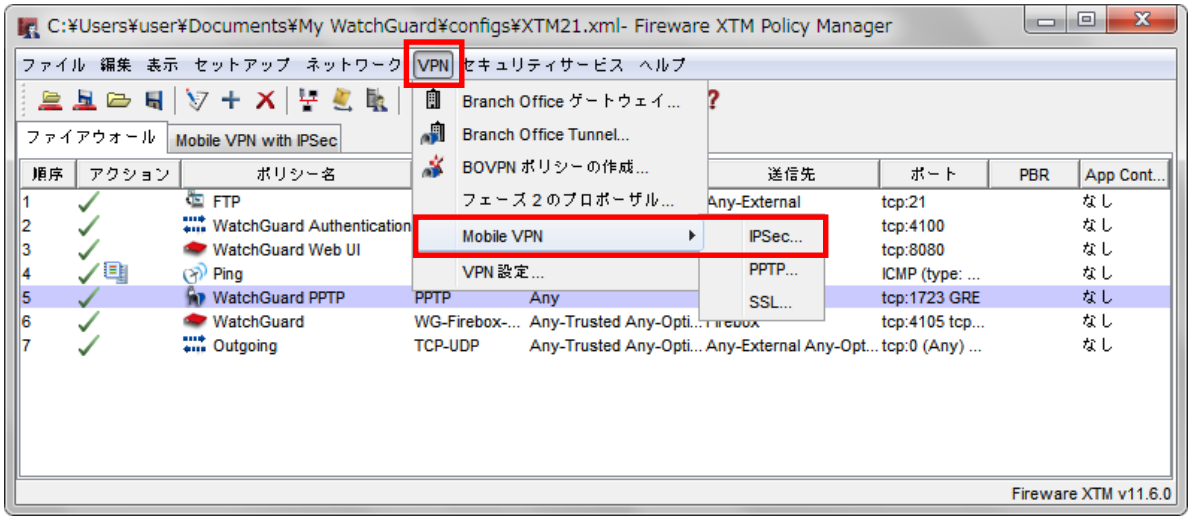
⑨ 以上の設定内容で接続が始まります。「接続されています」と表示されれば設定完了です。

以上で、モバイル VPN(PPTP)の設定は終了です。

モバイル VPN IPSEC の設定方法

Firebox 側の IPSec VPN 有効化と設定

① ポリシーマネージャーから VPN > Mobile VPN > IPsec を選択します。



② 次に新しいモバイル VPN（IPsec）接続を作成します。追加ボタンをクリックします。

「Add mobile VPN with IPsec Wizard」が起動するので「次へ」をクリックします。

③ 次に IPsec 接続に使用する認証サーバーを設定します。認証サーバーは、以下の 5 つから選択することができます。

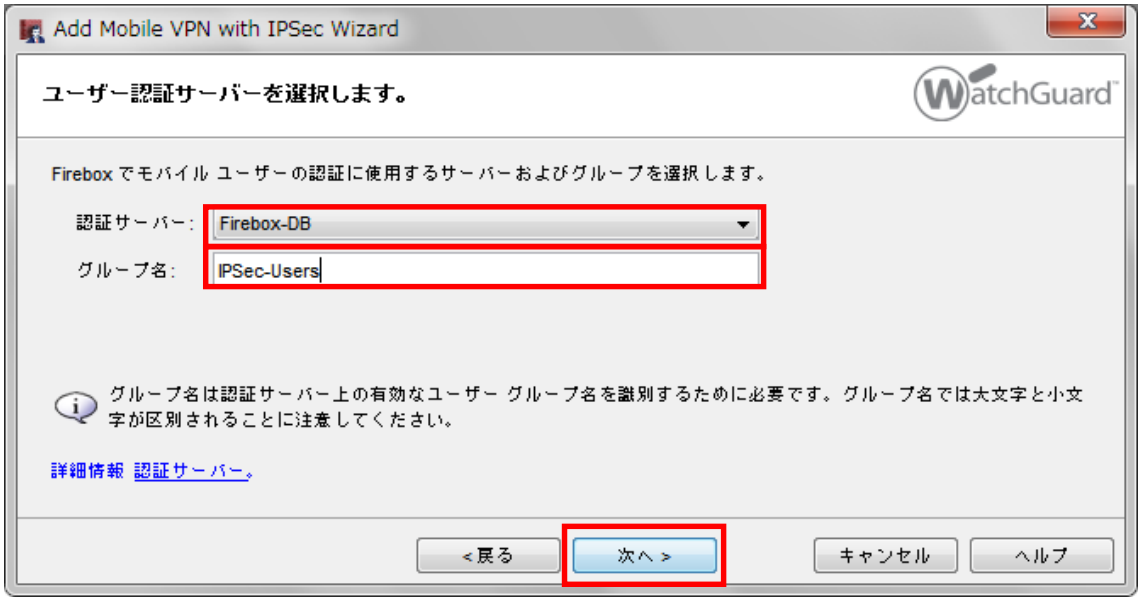
- Firebox-DB
- RADIUS
- SecureID
- LDAP

ここでは、例として認証サーバーに Firebox-DB を選択します。

Group Name は、認証はサーバーとして Firebox-DB を選択した場合、新たに作成したいグループ名を入力してください。ウィザード終了時に自動的にユーザグループが作成されます。

その他の認証サーバーを選択した場合は、実際に認証サーバー上に存在するグループ名を入力してください。

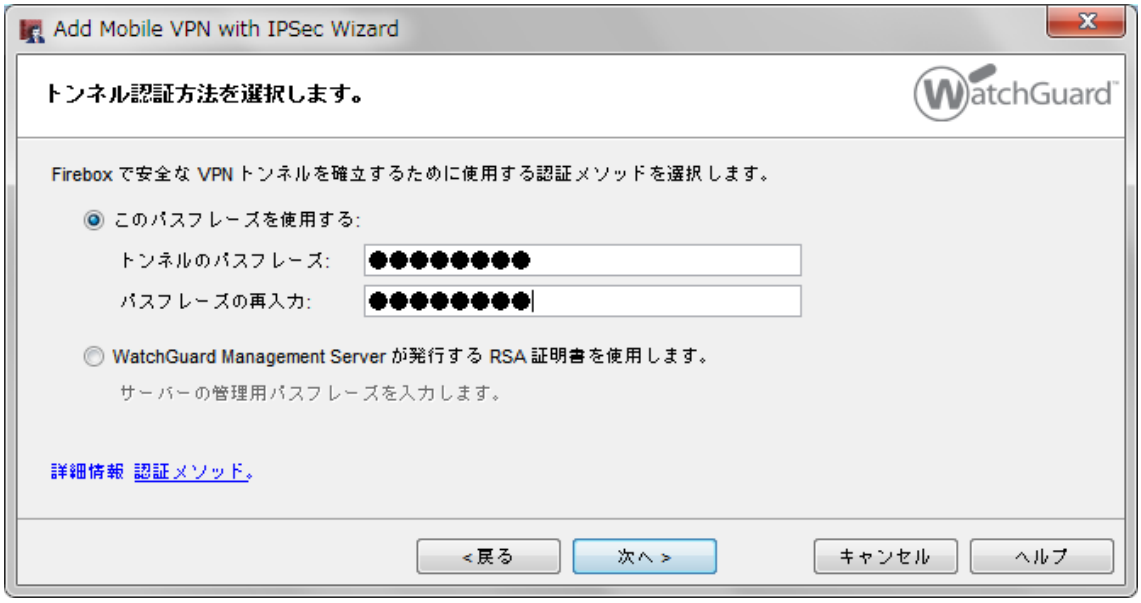
入力後、「次へ」ボタンをクリックし次に進んでください。



④　次に認証方法を設定します。

VPN 接続でパスワード認証を行う場合は、「このパスフレーズを使用する」にチェックを入れてください。

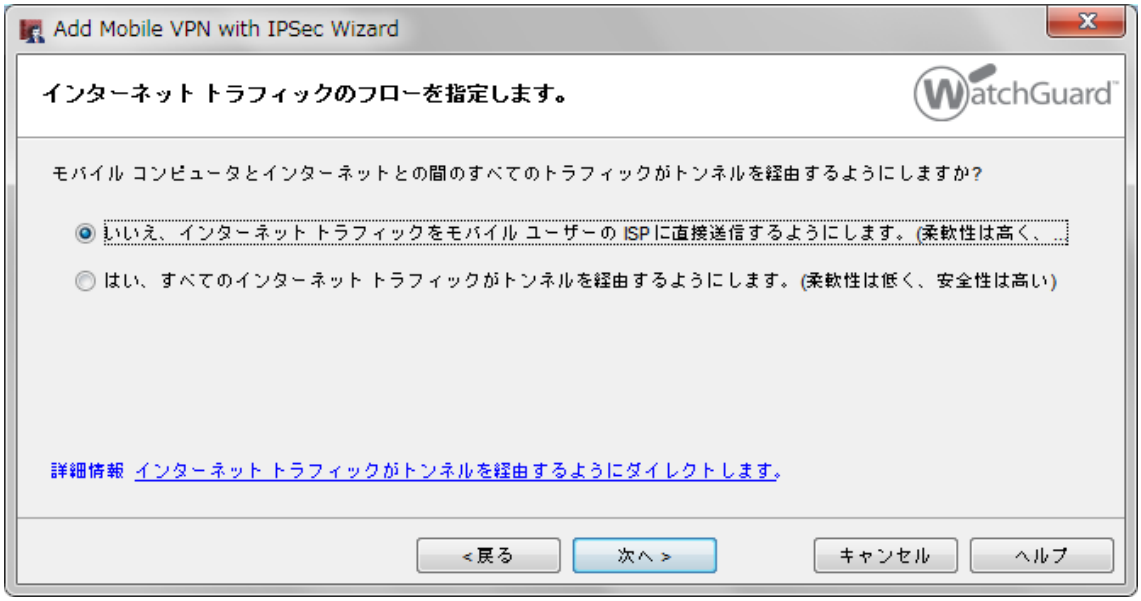
8 文字以上の英数字を使い、パスフレーズを入力します。



WatchGuard Management Server による RSA 認証を利用する場合は、「WatchGuard Management Server が発行する RSA 証明書を使用します」にチェックを入れます。

IP Address 及び Administration Passphrase には、Management Server の情報を入力します。

⑤　次にインターネットトラフィックのフローを指定します。



インターネットトラフィックは直接 ISP へ接続する場合

→「いいえ、インターネットトラフィックをモバイルユーザーの ISP に直接送信するようにします。」を選択し、⑥-1 に進む

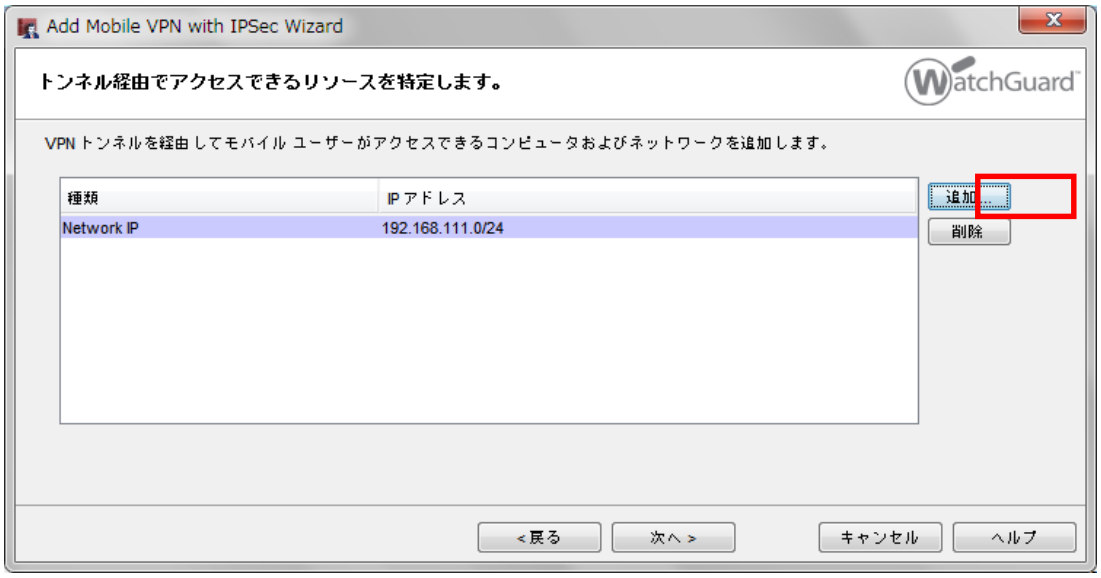
インターネットトラフィックを VPN トンネル経由で接続する場合

→「はい、すべてのインターネットトラフィックがトンネルを経由するようにします。」を選択し、⑥-2 に進む

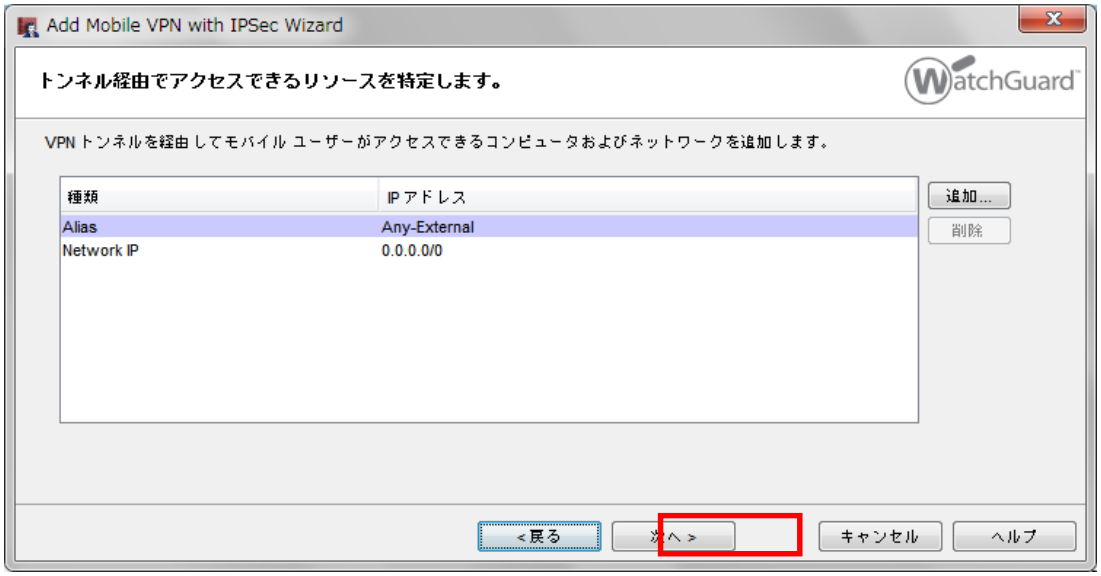
⑥-1

VPN トンネルを経由させる IP アドレスを設定する画面が表示されます。

IP アドレスは、ホスト IP またはネットワーク IP 単位で登録することができます。「追加」をクリックし、登録後、「次へ」をクリックします。



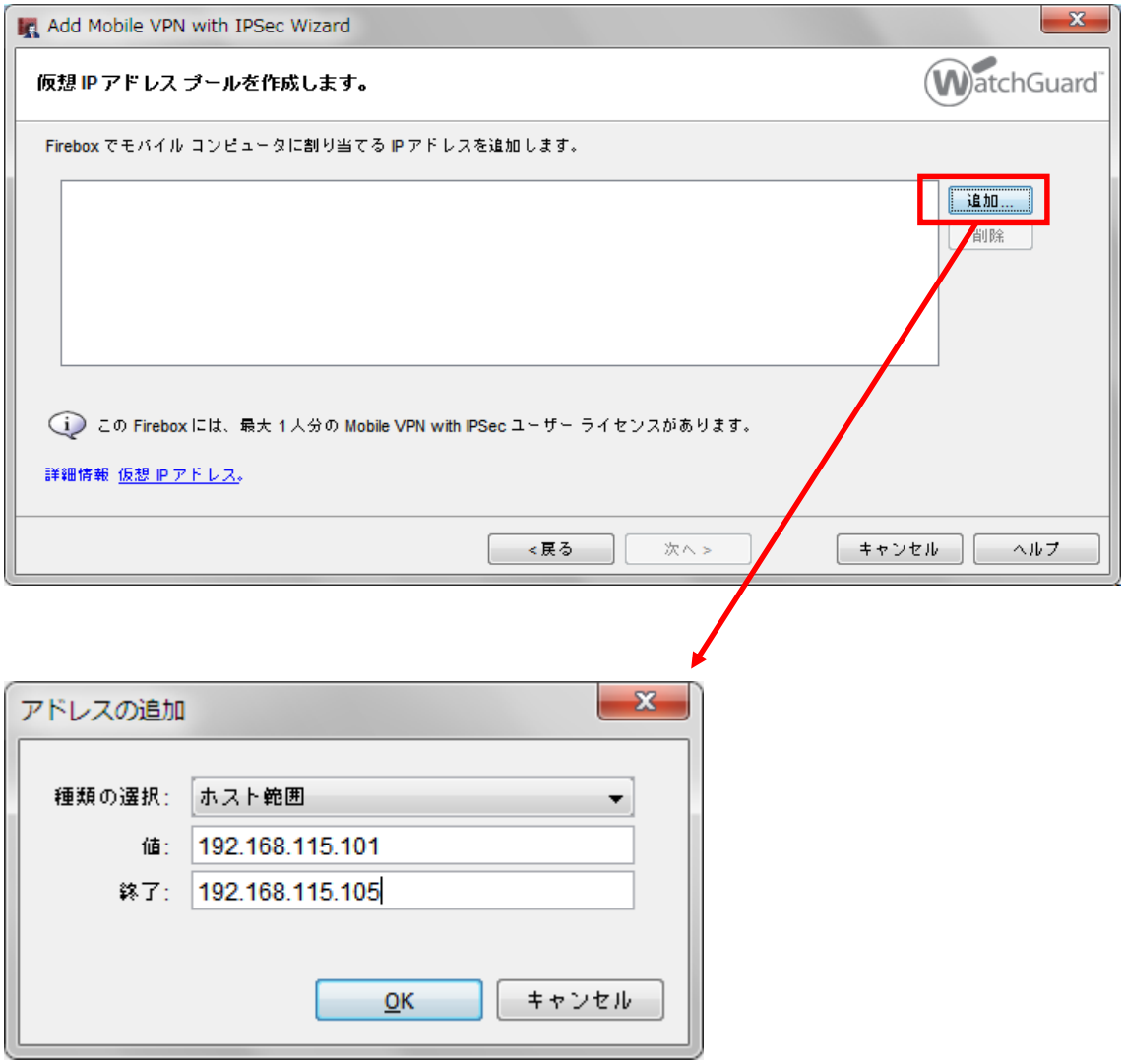
⑥-2VPN トンネルを経由するネットワークが表示されます。デフォルトでは Any-External と 0.0.0.0/0 が表示されるので、「次へ」をクリックしてください。



⑦　次に VPN トンネルで使用する IP アドレスを設定します。

ここで登録した IP アドレスは、モバイル VPN ユーザーに割り当てられます。

「追加」をクリックし、ホスト IP またはホストレンジを登録し、「次へ」をクリックし、任意のローカル IP アドレス（例：192.168.0.10-192.168.0.15）を設定してください。



⑧　以下の画面が表示されたら、モバイル VPN（IPsec）の設定は終了となります。

注意：ウィザードが成功すると、VPN 設定ファイルの保存場所が表示されるので、ご確認ください。このファイルには、shared key、ユーザー情報、IP アドレス、VPN の設定情報が含まれており、クライアント機の設定に使用します。

また、このファイルはパスフレーズにより暗号化されており、このファイル自体を編集することはできません。

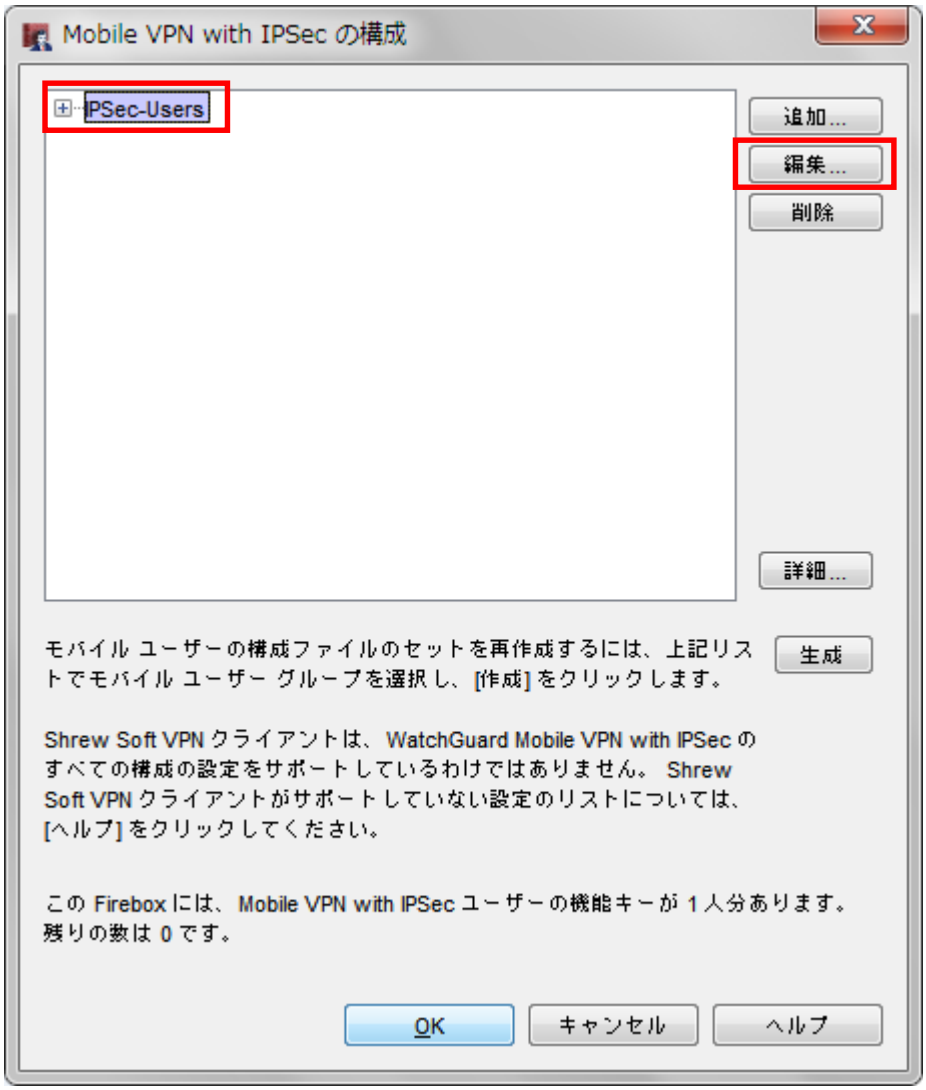
また、「IPSec-Users にユーザーを追加する」(グループ名は作成時の任意のもの)にチェックを入れると、自動的にモバイル VPN ユーザグループにユーザーが追加されます。

必ずチェックを入れてから「完了」ボタンをクリックしてください。

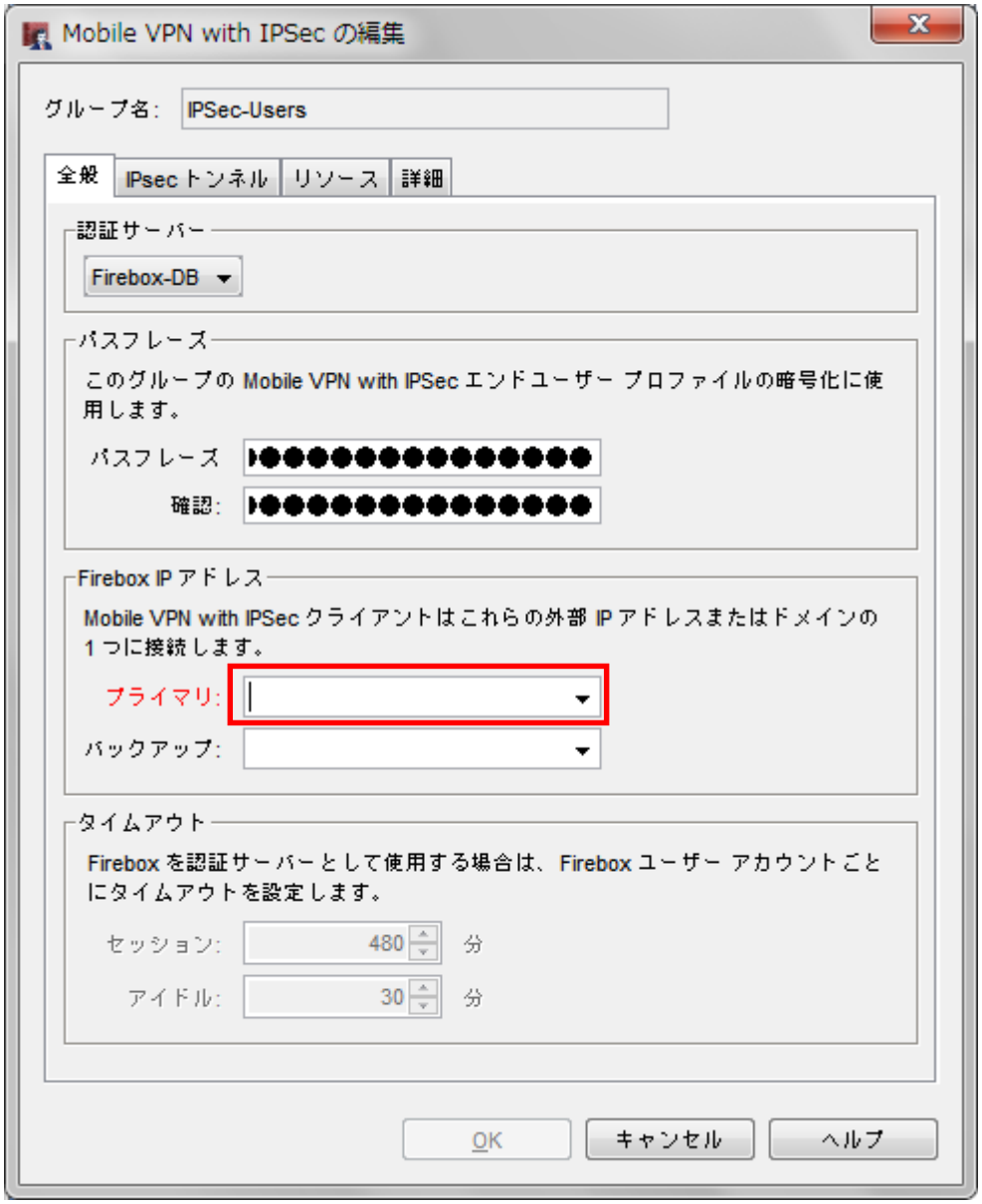
ウィザードの完了後、次のようなアラートが表示されたら、追加で設定が必要になります。

以下の手順で追加設定を完了させてください。

① 接続プロファイルを選択し、編集ボタンをクリックします

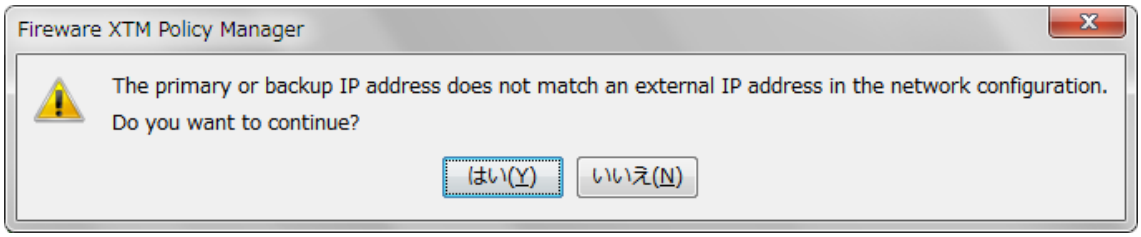


② Firebox IP アドレスの欄に VPN 接続用の External IP アドレスもしくはホスト名を指定します。



入力すると OK ボタンがアクティブになりますので、OK をクリックして設定を反映させます。

External の IP アドレスが固定でなく、DDNS のホスト名を指定した場合には以下のアラートが表示されますが、「はい」をクリックしてください。

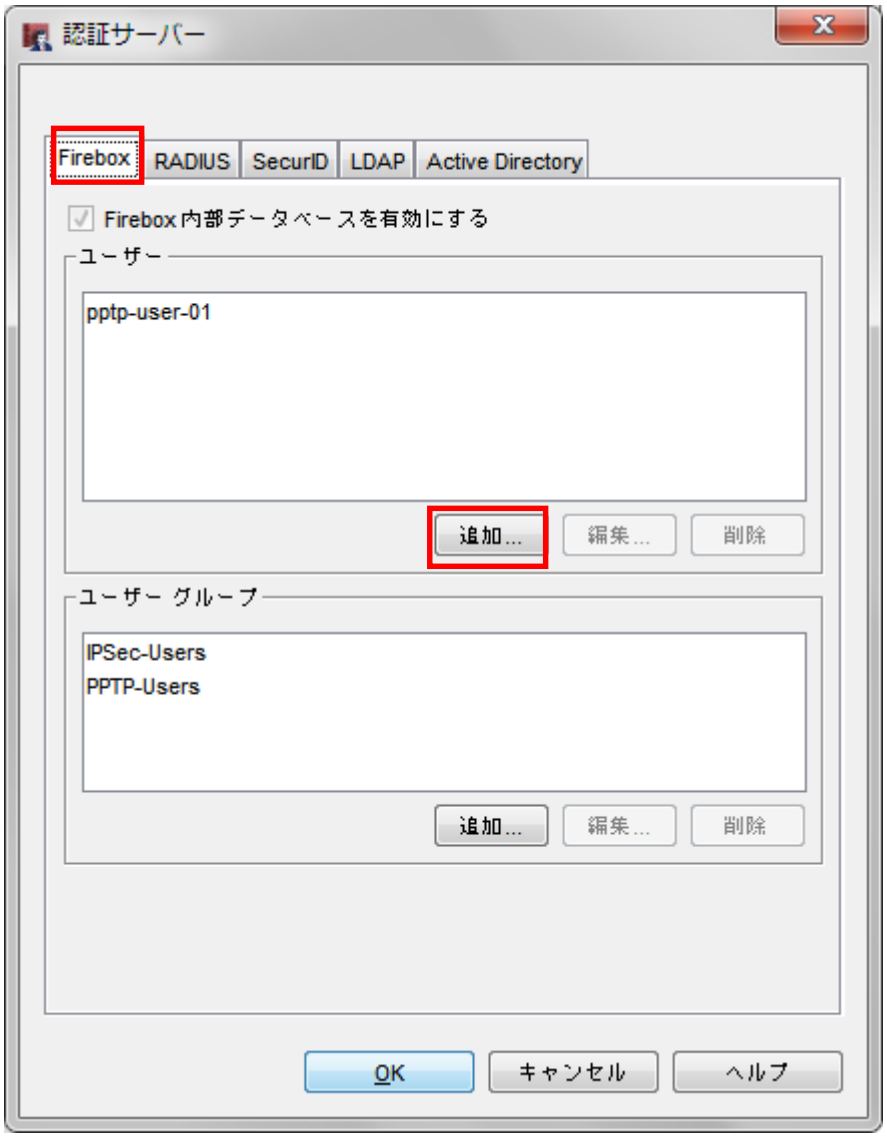


モバイル IPsec ユーザーの作成

次に IPsec 接続を行うユーザーを作成します。

① ポリシーマネージャーからセットアップ> 認証> 認証サーバーを選択します。

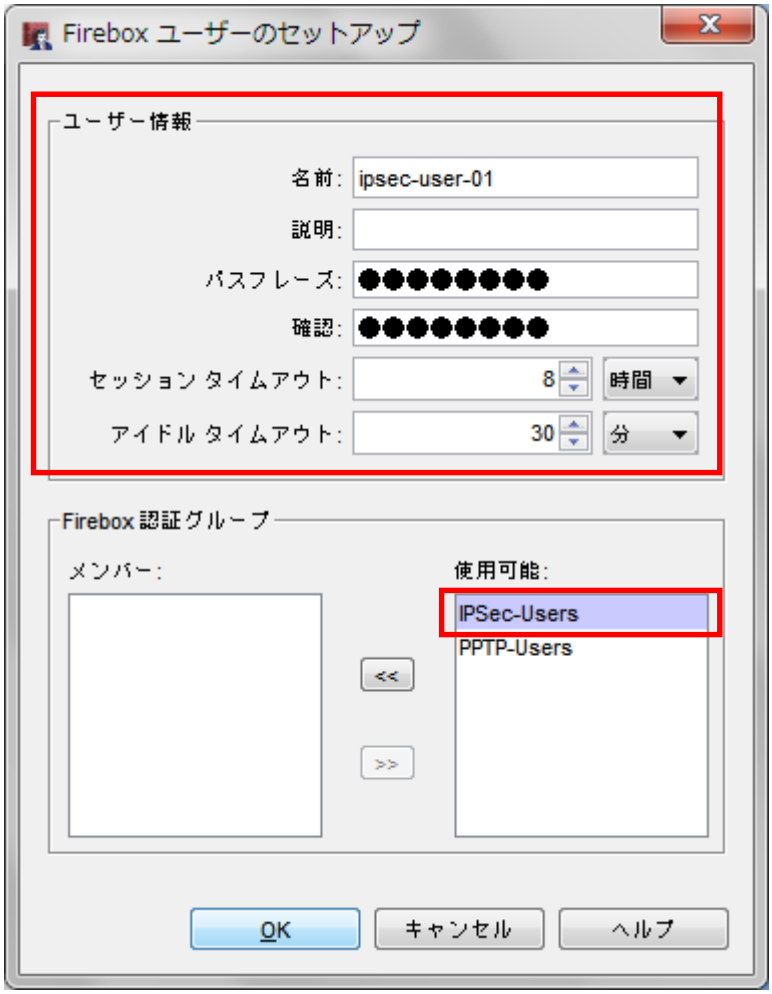
Firebox タブからユーザー欄下の追加ボタンをクリックします。



② IPsec ユーザーを作成します。

- 名前:ユーザー名
- 説明:ユーザーの説明(備考)
- パスフレーズ:ユーザーのパスフレーズ
- 確認:パスフレーズの確認
- セッションタイムアウト:セッション開始後の時間の閾値(デフォルトは 8 時間)
- アイドルタイムアウト:アイドル状態の時間の閾値(デフォルトは 30 分)

「Firebox 認証グループ」には、先程のウィザードで作成したユーザグループを選択し、Member 欄に追加後、OK ボタンをクリックします。



以上で、IPsec ユーザーの作成は終了です。

IPsec クライアントの設定

IPsec クライアントを設定するには、クライアントソフトウェア Shrew VPN Client のインストールが必要です。

クライアントソフトウェアは、WatchGuard Customer Support サイトからダウンロード可能です。

https://www.watchguard.com/support/index.asp

ご利用の Firebox バージョンにあわせた IPsec クライアントソフトウェアをダウンロードしてください。

vpn-client-*.*.*-release.zip(*印はバージョン)を展開すると、インストーラーの vpn-client-*.*.*-release.exe が抽出できます。

クライアントの必要条件:

- モバイル VPN IPsec クライアントソフトウェアをインストールするには、以下のバージョンの Windows が必要です。
  - Windows 2000
  - Windows XP (32-bit and 64-bit)
  - Windows Vista (32-bit and 64-bit)
  - Windows 7 (32-bit and 64-bit)
  - また、クライアント PC にインストールされている Firewall（Windows Firewall）を無効にする必要があります。
- モバイル VPN　IPsec クライアントソフトウェアをインストールする前に、すべてのサービスパックが利用できるか確認することをお勧めいたします。
  - モバイル VPN　IPsec クライアントソフトウェアをインストールすると、VPN 接続に使用する WINS サーバーと DNS サーバーの情報がクライアント PC にインポートされます。

クライアントソフトウェアのインストール:

クライアントソフトウェアのインストールは、2つのパートに分かれています。

- クライアントソフトウェアのインストール
- エンドユーザープロフィールのインポート

また、インストールを始める前に、以下のインストールコンポーネントがあることを確認してください。

- Mobile VPN クライアントソフトウェア（vpn-client-*.*.*-release.exe）
- エンドユーザ プロファイル（ファイルの拡張子が.vpn のファイル）

→ウィザードが成功すると表示される VPN 設定ファイルです。デフォルトでは、

C:¥Users¥Public¥Shared WatchGuard¥muvpn 配下にあります。

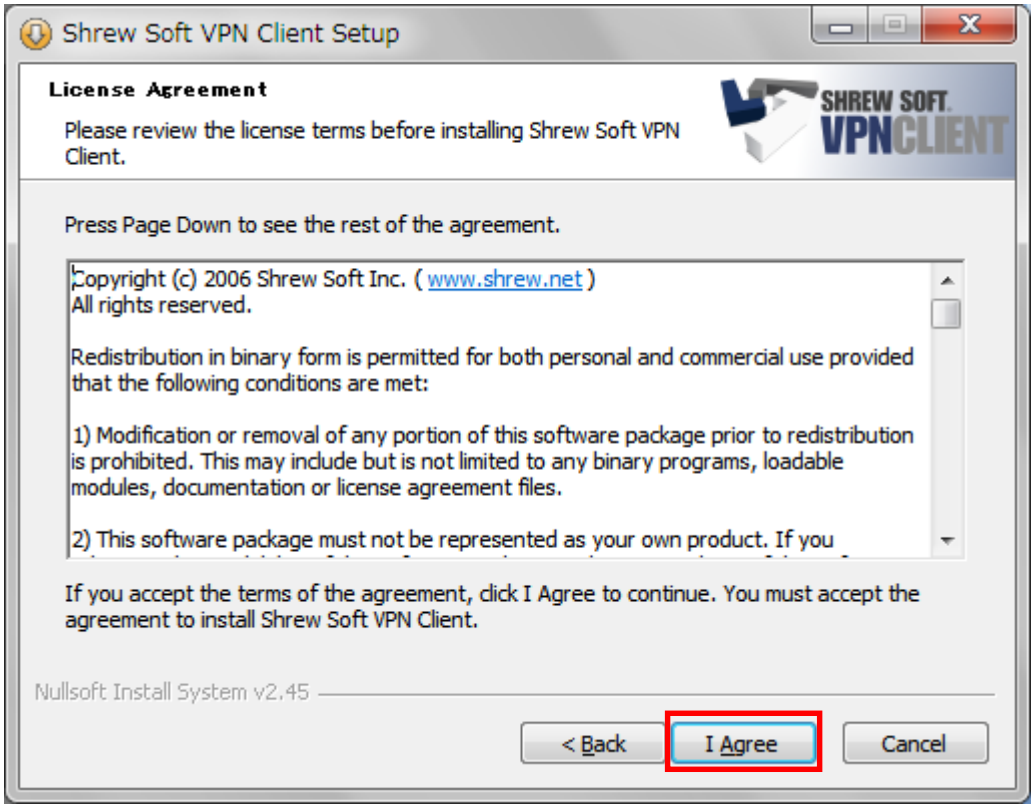
- パスフレーズ（Add mobile VPN with IPsec Wizard の④で設定したパスフレーズ）
- 認証に証明書を利用する場合、cacert.pem ファイルと.p12 ファイル
- ユーザー名とパスワード

インストール方法

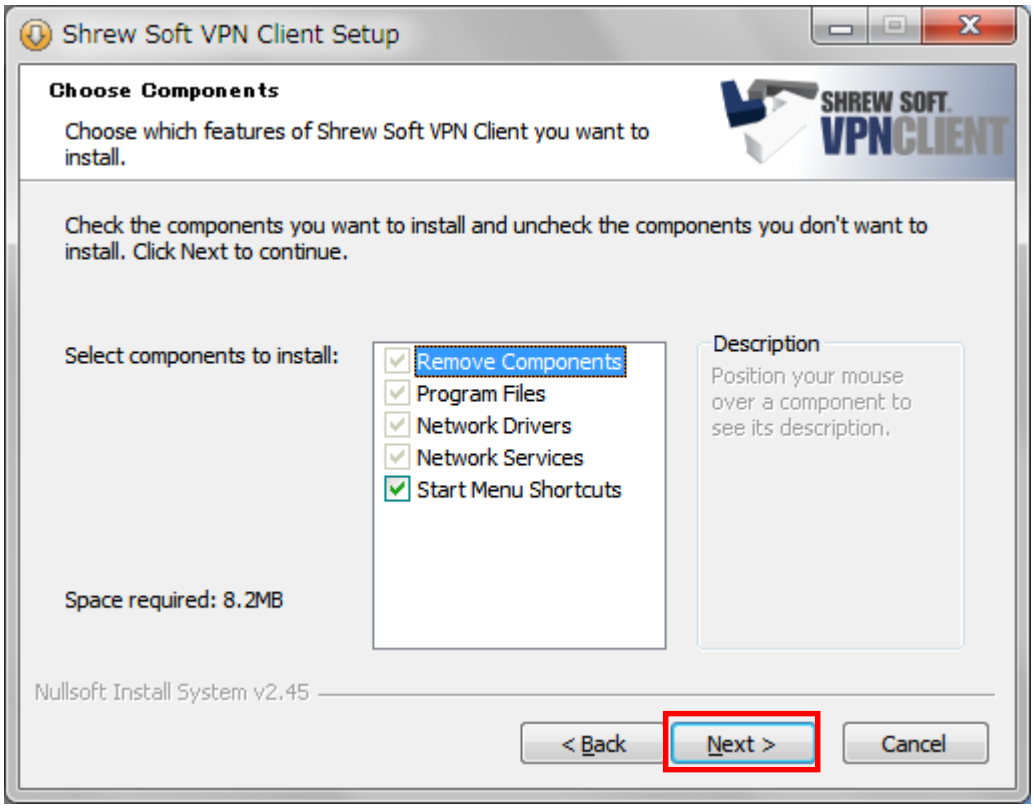
① ステップ 1 でダウンロードしたソフトウェアをダブルクリックすると、WatchGuard モバイル VPN インストールウィザードが始まります。

② Welcome の画面では「Next」をクリックしてください

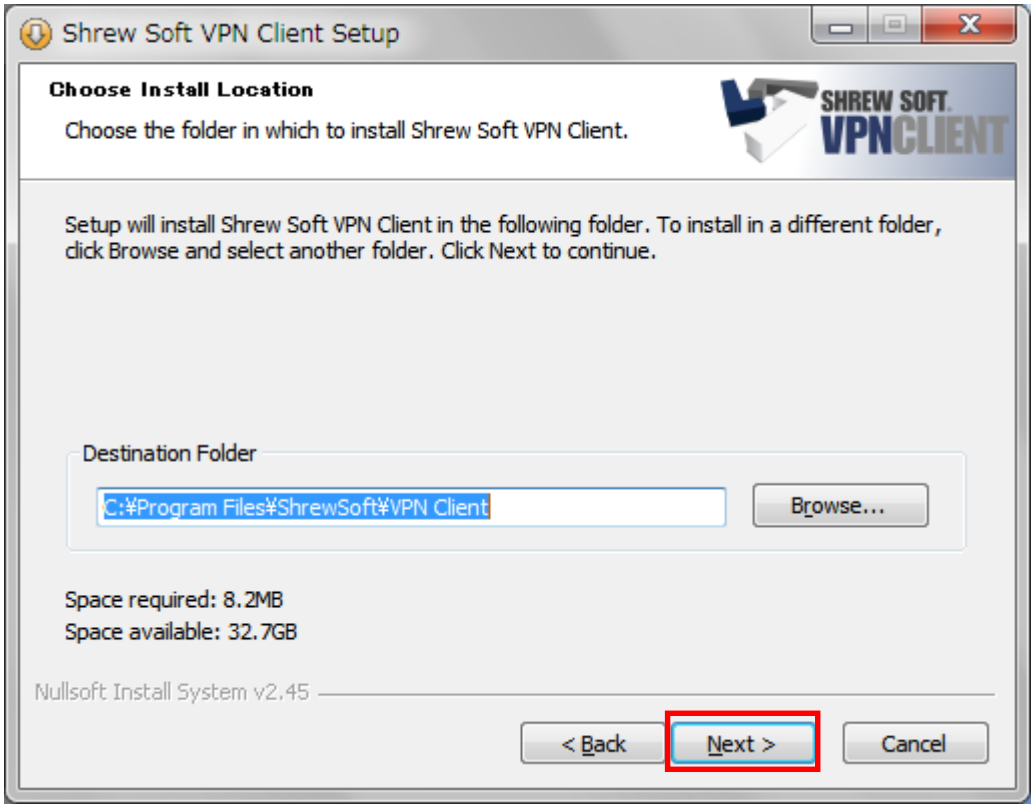
③　License Agreement（ライセンスの同意）では「I Agree」をクリックします



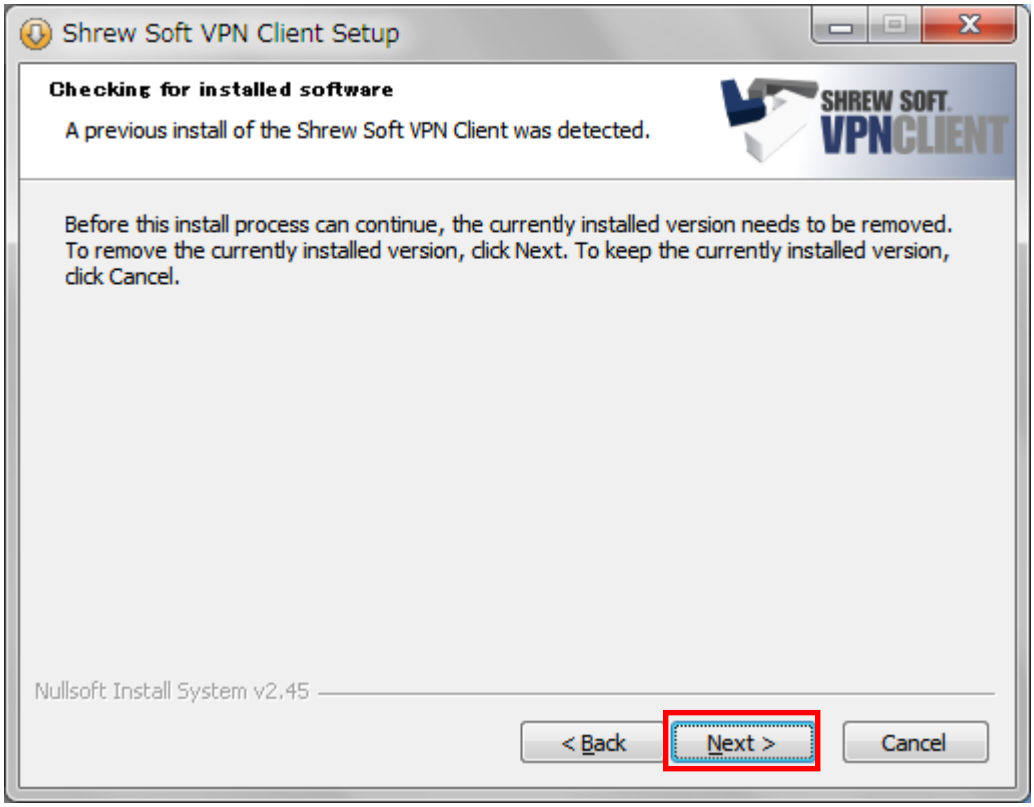
④　Choose Component（コンポーネントの選択）ではそのままの状態で「Next」をクリック

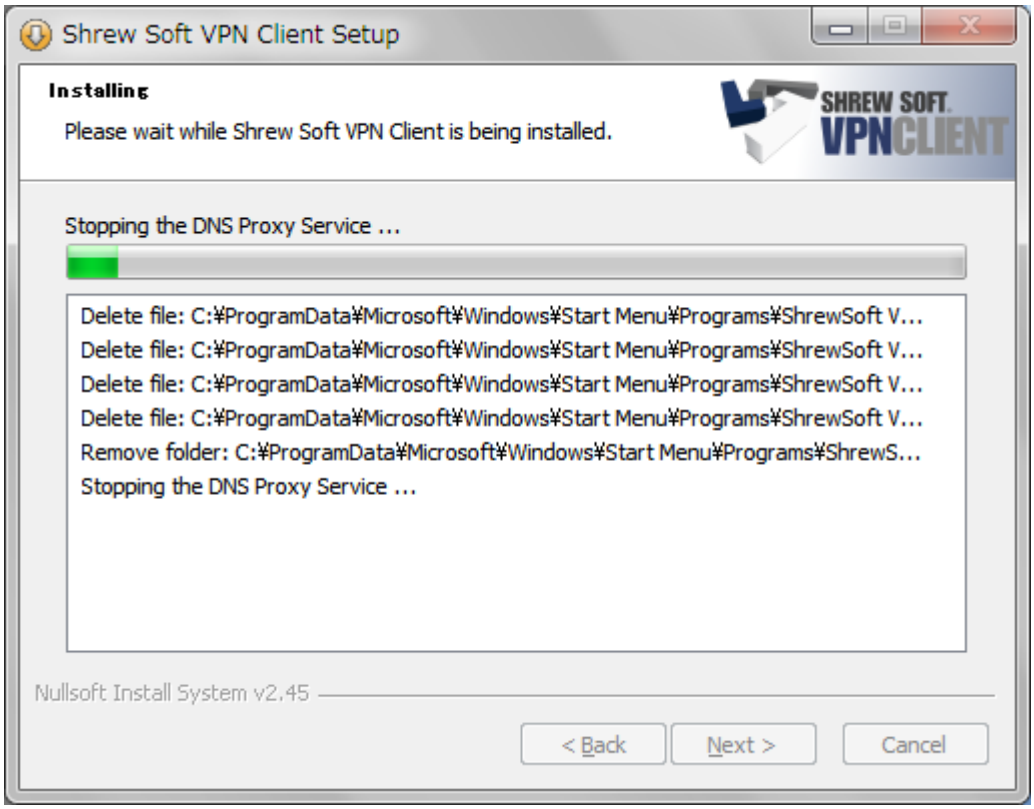


⑤　Choose Install Location（インストール先）はそのままで「Next」をクリックします



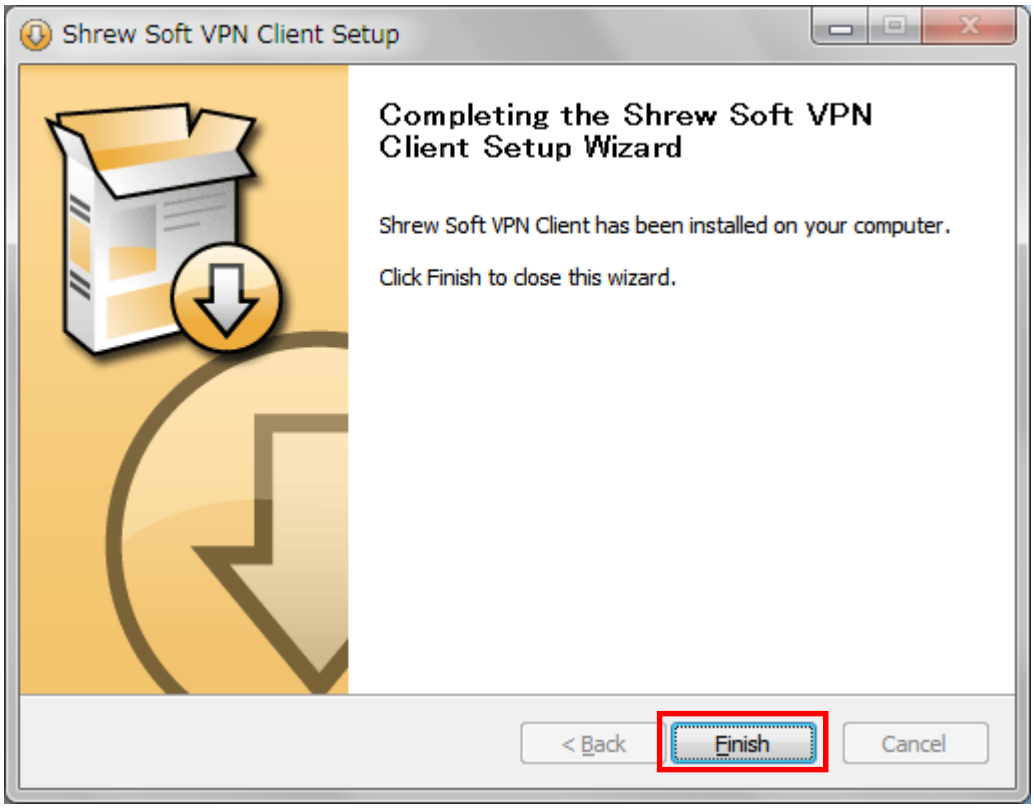
⑥　次の画面が表示されたら、「Next」をクリックしてインストールを開始します





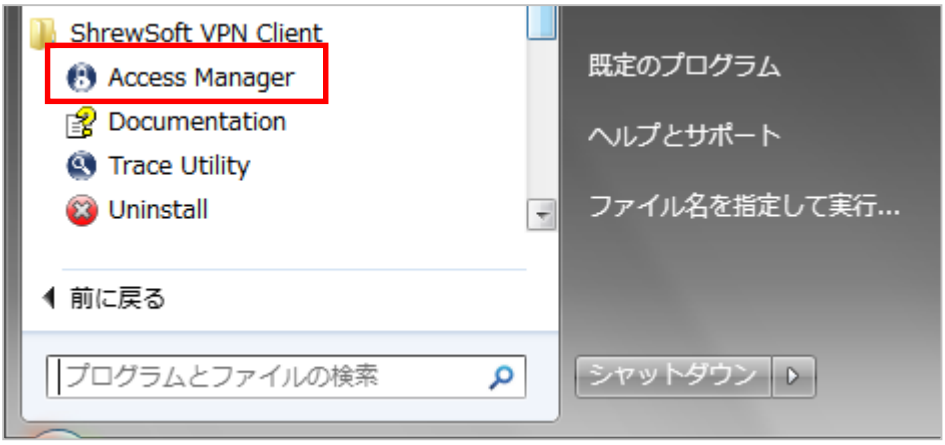
⑦ 以下の画面が表示されたら、インストールウィザードは完了です。

Finish をクリックしてください。

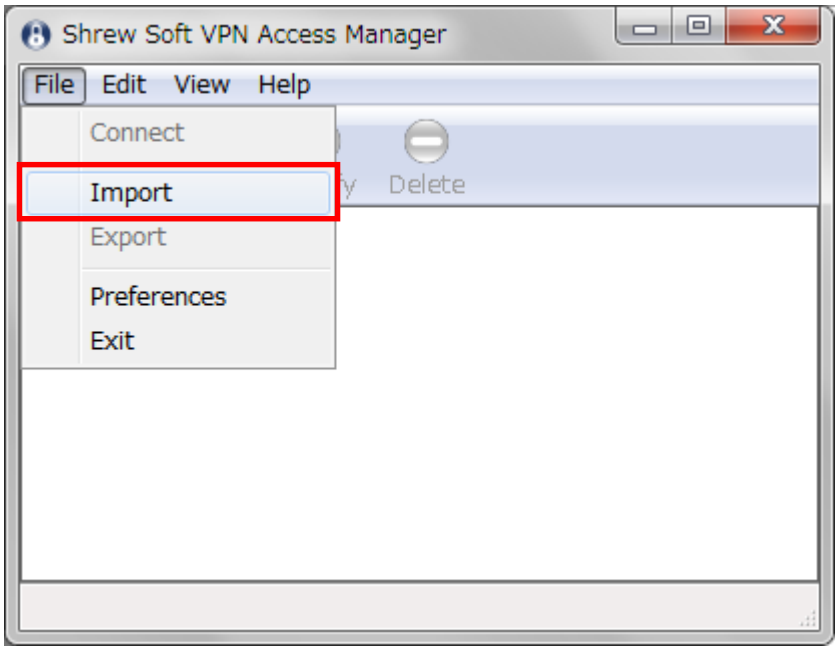


エンドユーザプロファイルのインポート方法

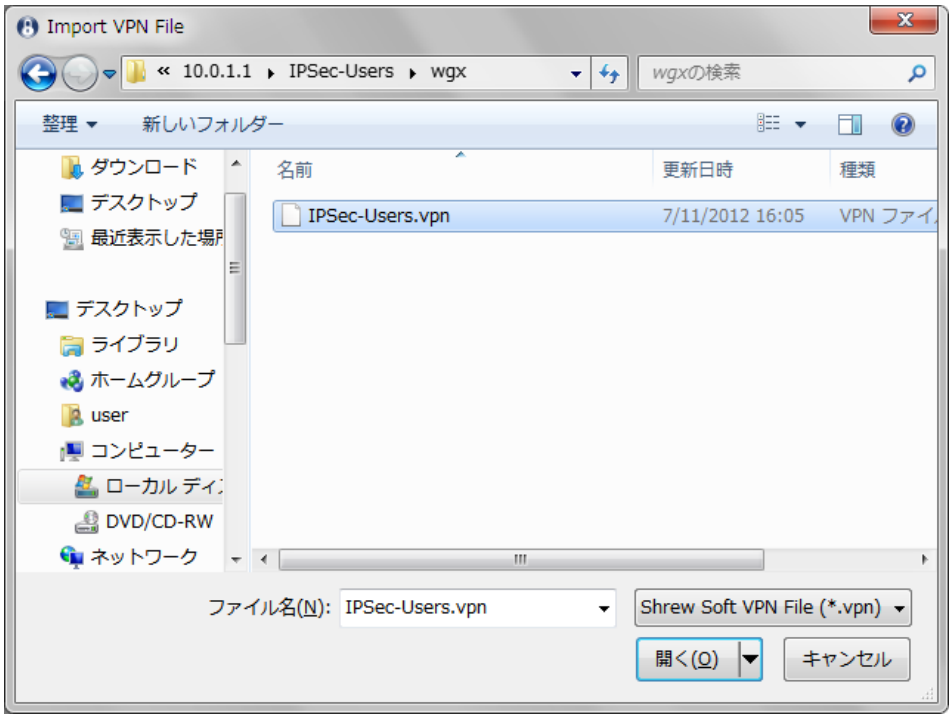
① Windows のスタートメニューからプログラム > ShrewSoft VPN Client > Access Manager をクリックします



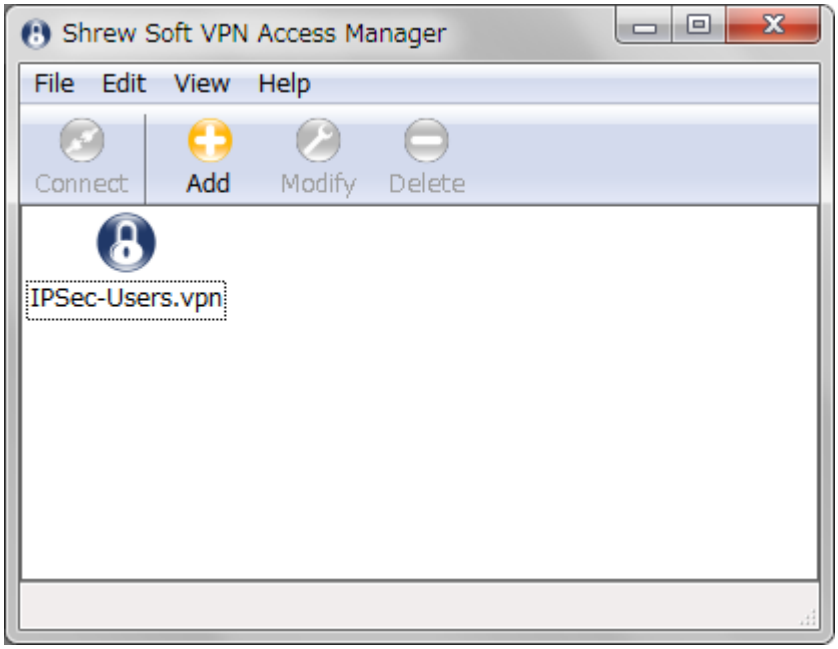
② File> Import をクリックします



③　IPsec ウィザードで作成されたエンドユーザプロファイル（.vpn ファイル）を選択します



④　.vpn ファイルを選択すると Access Manager に接続設定のエントリーが表示されます

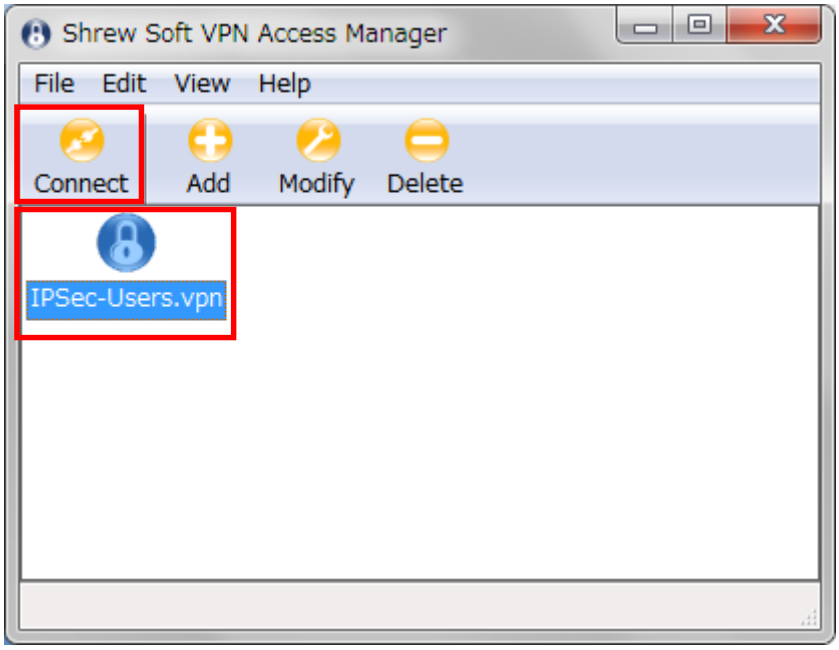


以上でプロファイルのインポートは完了です。

モバイル VPN（IPsec）クライアントの接続方法

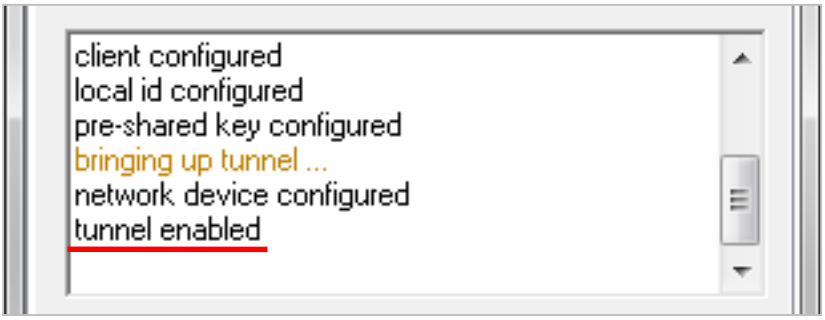
① Windows のスタートメニューからプログラム ＞ ShrewSoft VPN Client > Access Manager をクリックします

② 接続するプロファイルを選択し、Connect ボタンをクリックします



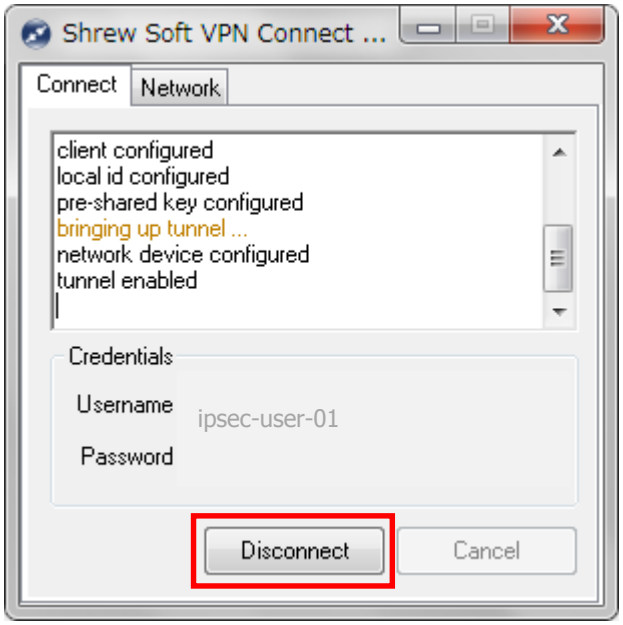
③ 接続のダイアログが表示されますので、Username と Password を入入力し、Connect ボタンをクリックします

以下のように tunnel enabled と表示されれば接続成功です。



モバイル VPN（IPsec）クライアントの切断方法

Mobile VPN Monitor ダイアログボックスから Disconnect をクリックします。

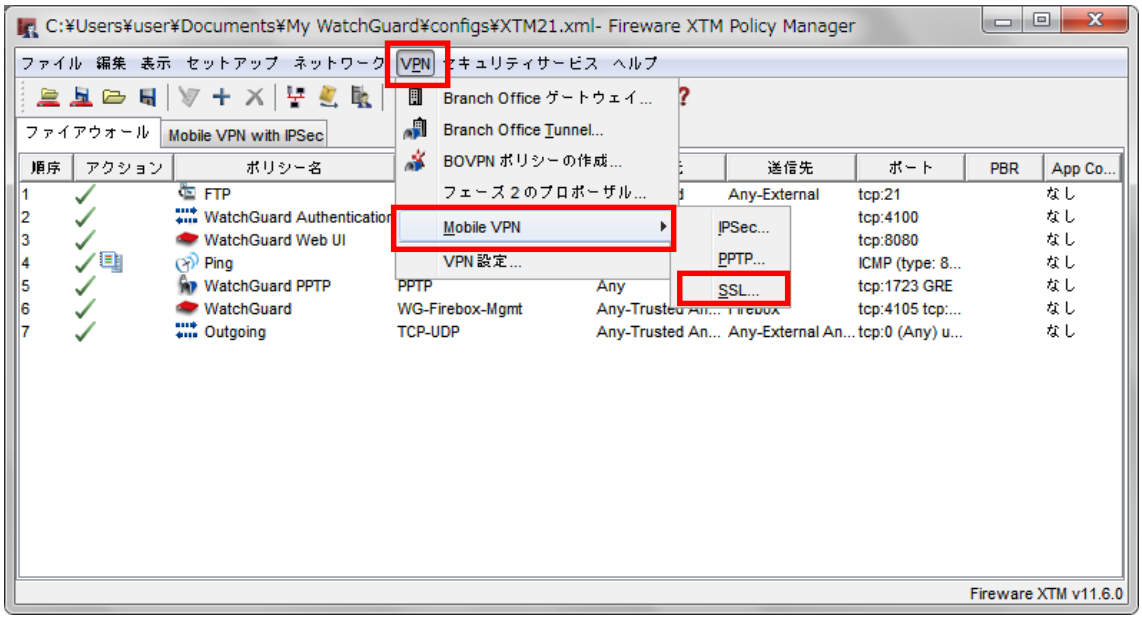


モバイル VPN SSL の設定方法

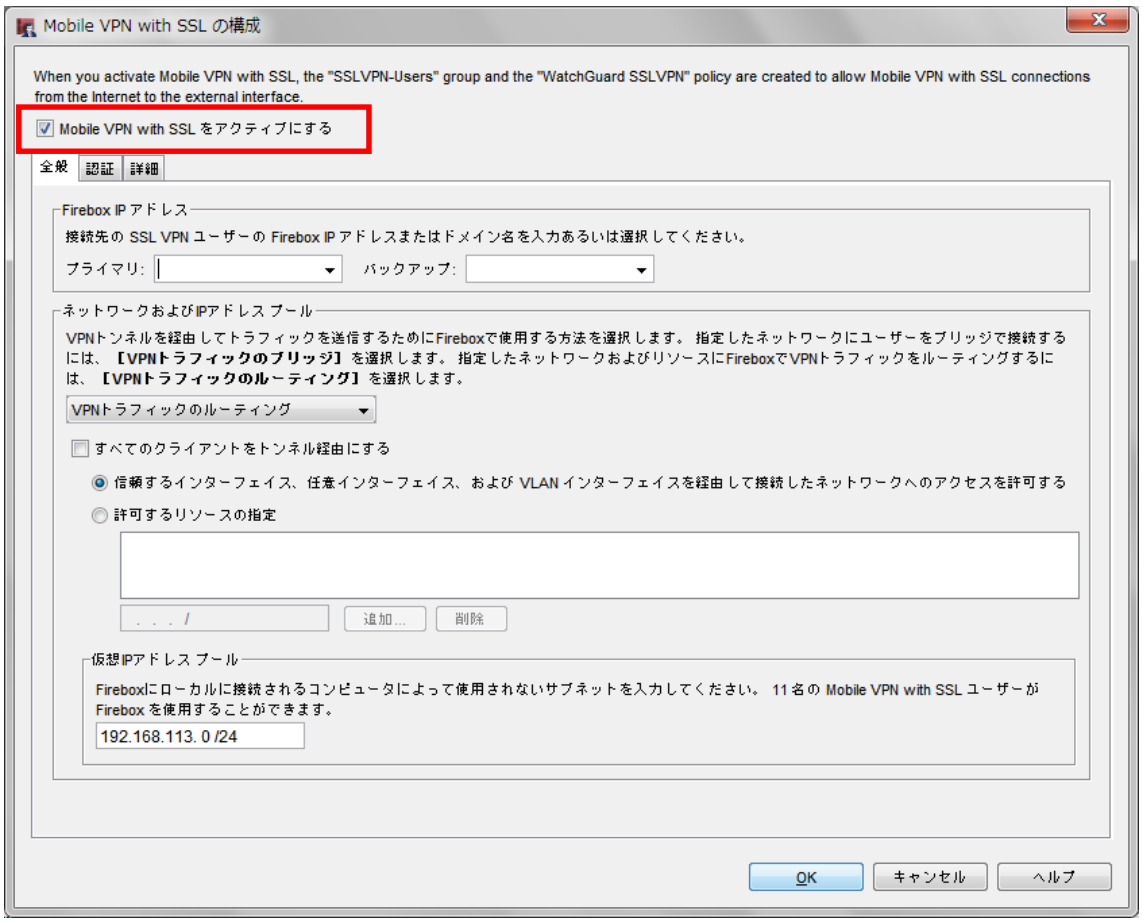
モバイル VPN (SSL) クライアントは、ソフトウェアアプリケーションのインストールが必要です。モバイル VPN クライアントは SSL（Secure Sockets Layer）を使用します。

Firebox 側の設定

① ポリシーマネージャーから VPN > Mobile VPN > SSL を選択すると Mobile VPN with SSL Configuration ダイアログが表示されます。



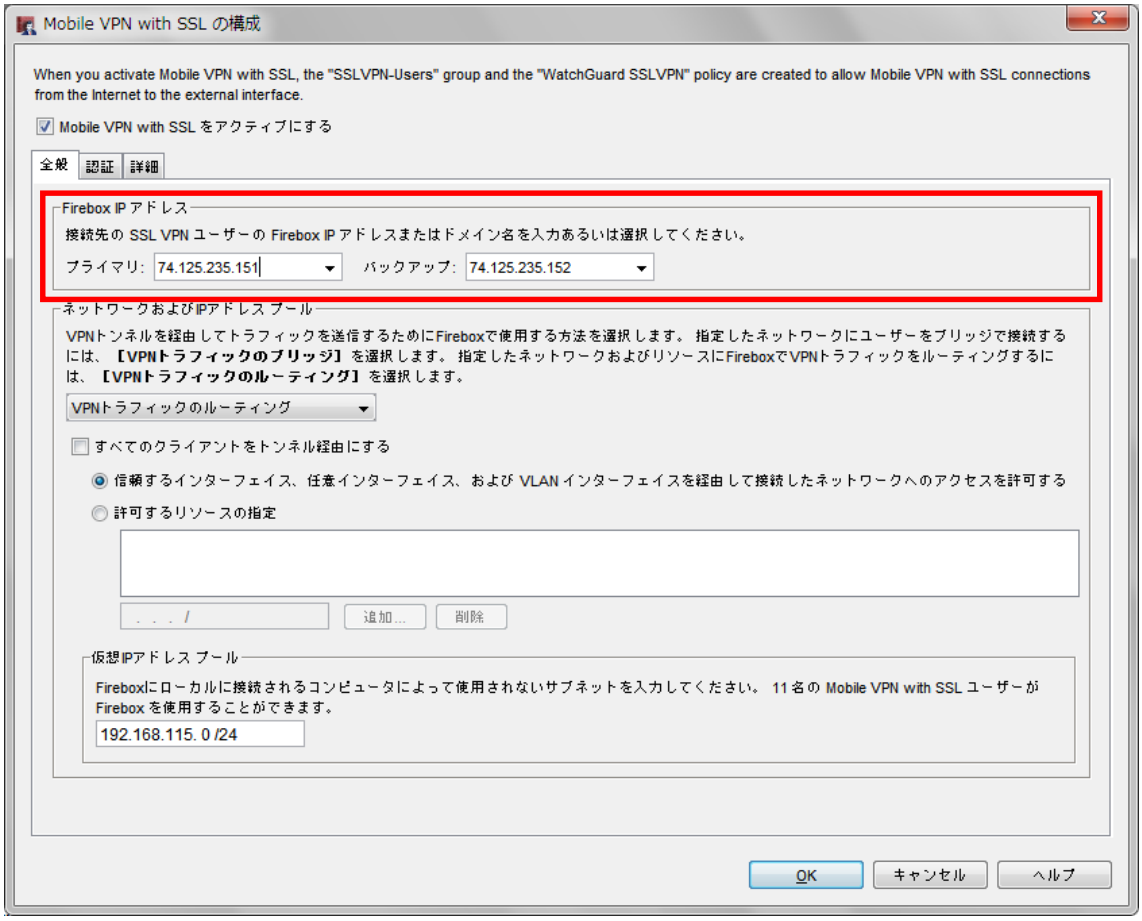
② Activate Mobile VPN with SSL にチェックを入れ、モバイル VPN（SSL）を有効にします。この欄にチェックをいれると SSL VPN Users Group と WatchGuard SSL VPN ポリシーが自動的に作成されます。



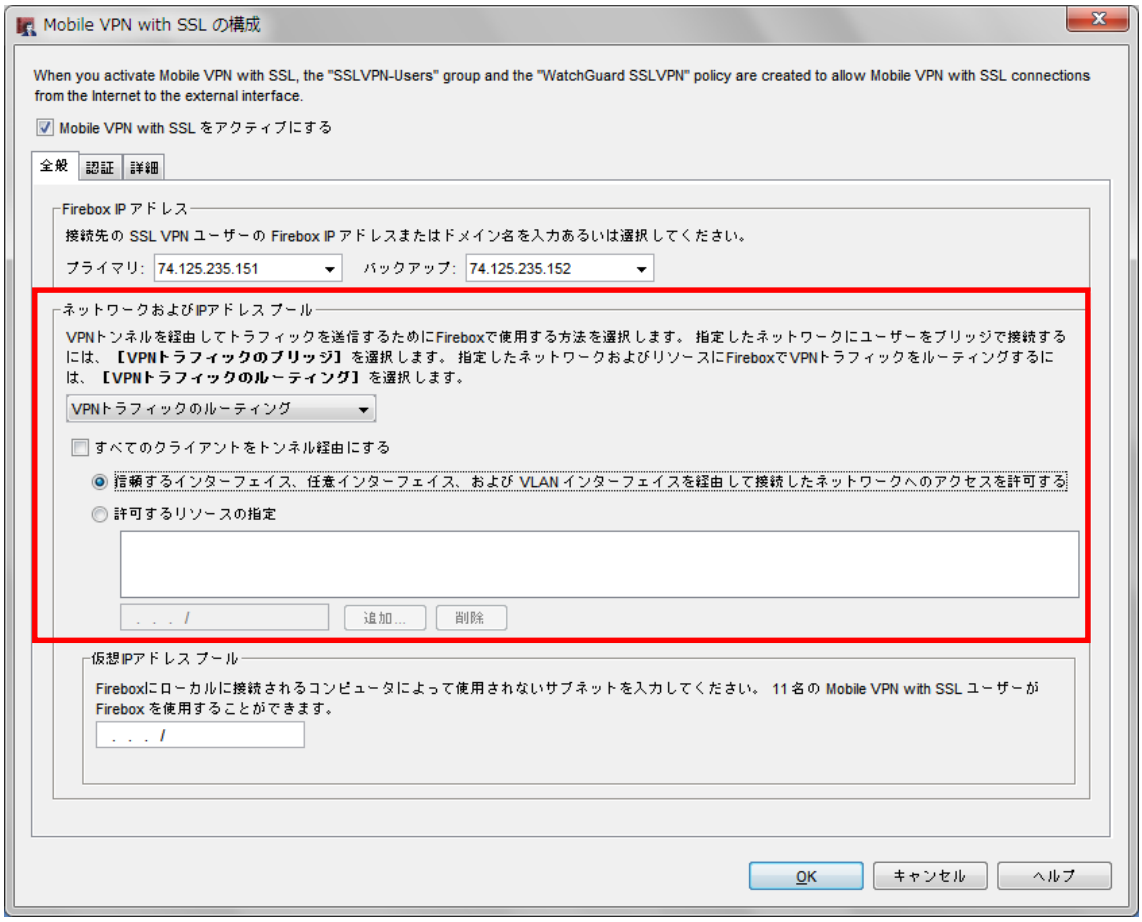
③　次に SSL VPN ユーザーが接続に使用する IP アドレスかドメイン情報を設定します。

Firebox が複数の WAN 接続を持っている場合、Backup のドロップダウンリストから、違うグローバルな IP アドレスを選択してください。

SSL クライアントを持つモバイル VPN は、Primary に設定した IP アドレスとの通信が確立できない際に Backup の IP アドレスを使用します。



④　次にモバイル VPN SSL クライアントが使用するネットワークと IP アドレスプールを設定します。



⑤　Firebox がトラフィックを送信するために使用するメソッドを選択します。

・　VPN トラフィックのルーティング

・　VPN トラフィックのブリッジ

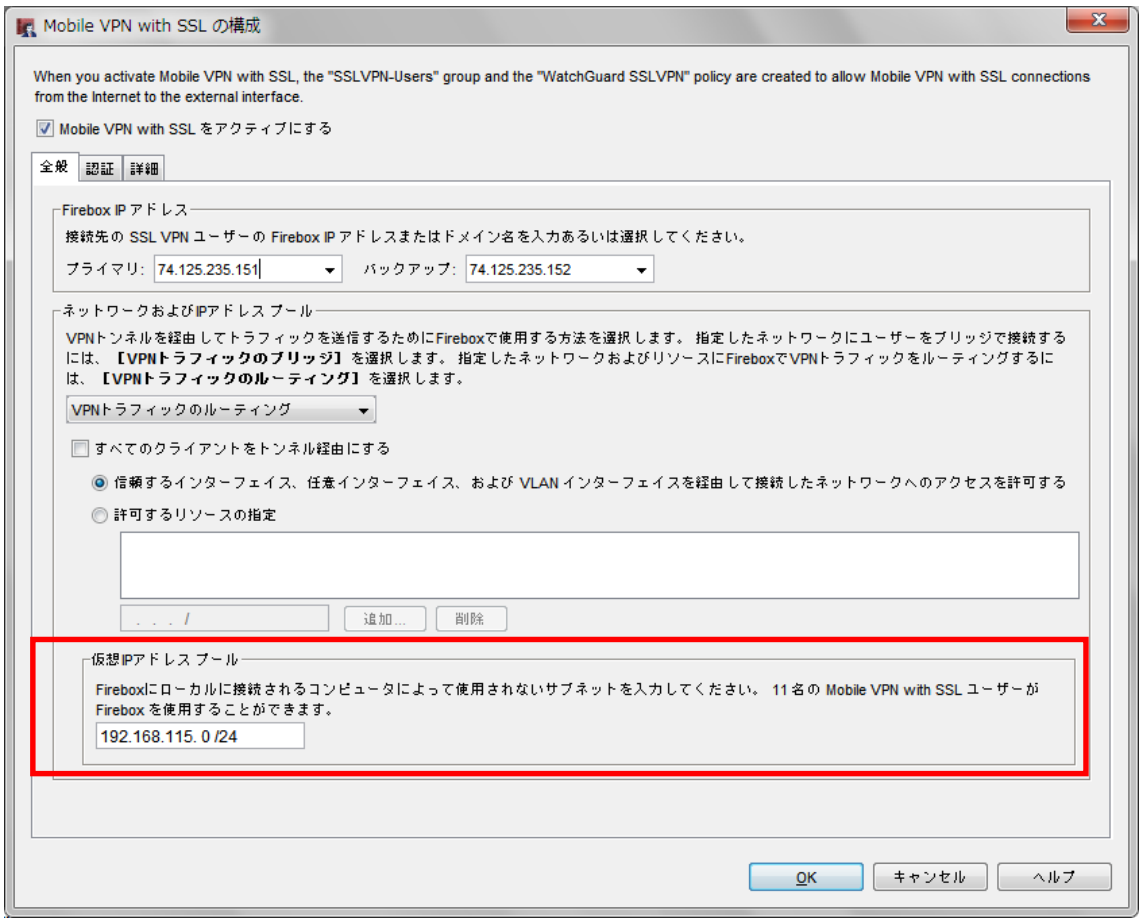
・

⑥　次に「すべてのクライアントをトンネル経由にする」を設定します。

この欄にチェックを入れた場合、すべてのプライベートネットワーク・トラフィックとインターネットトラフィックが全て VPN トンネルを経由します。

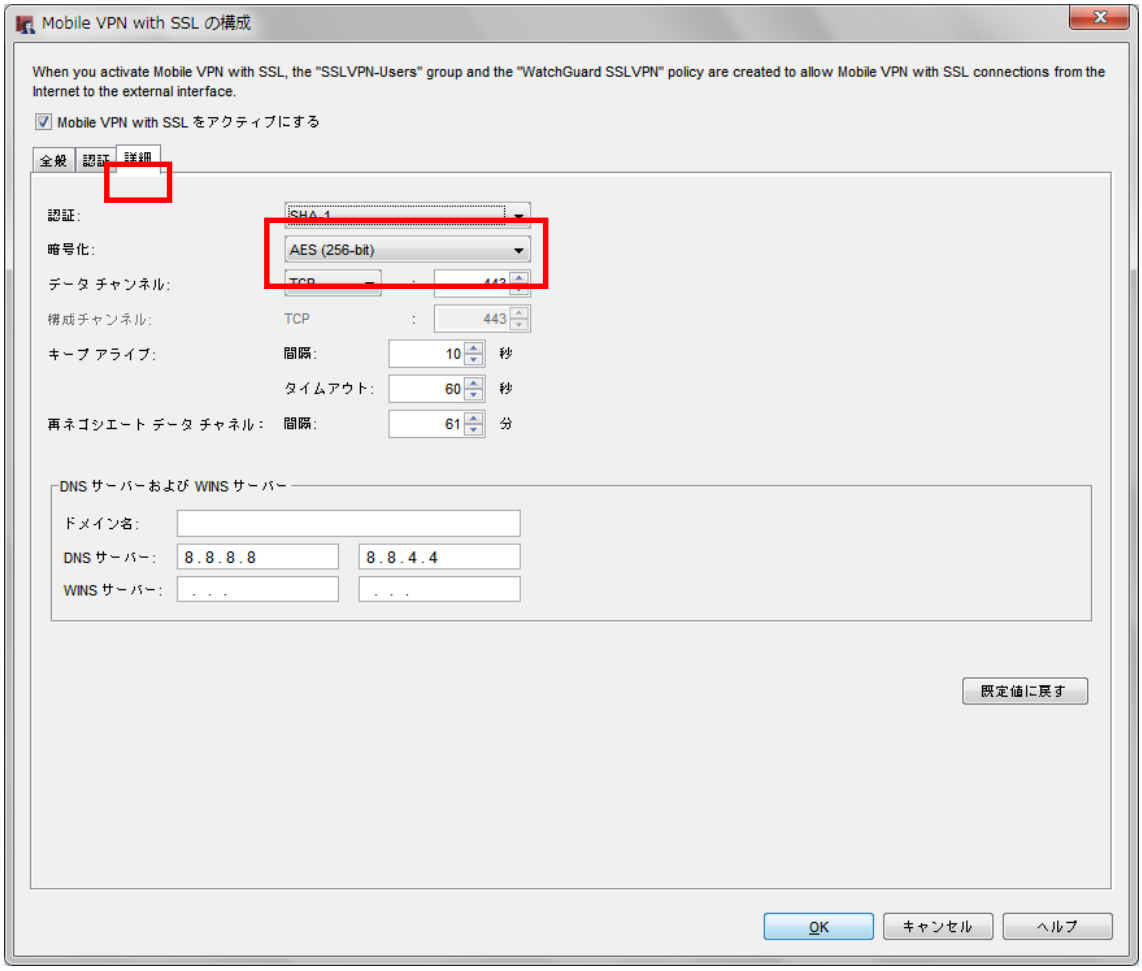
⑦　次に「仮想 IP アドレスプール」を設定します。

モバイル VPN（SSL）クライアントが使用する IP アドレスを入力します。このアドレスプールの中の仮想 IP アドレスが SSL VPN で接続したクライアントデバイスに割当てられます。



IP アドレスを入力後、「OK」をクリックしてください。

⑧　次に詳細タブをクリックします。



詳細タブでは以下の項目を設定します。

・　認証：認証で使用するアルゴリズムを選択します。選択肢は以下です。

MD5, SHA, SHA-1, SHA-256, SHA-512

・　暗号化：暗号化で使用するアルゴリズムを選択します。選択肢は以下です。

Blowfish, DES, 3DES, AES (128 bit,192 bit,256 bit)

暗号化の強度とパフォーマンスの高さから、MD5 と Blowfish の組み合わせをお勧めします。

・　データ チャンネル：SSL 接続に使用するプロトコル（TCP or UDP）とポート番号を設定します。デフォルトは、TCP の 443 番ポートです。

・　キープ アライブ：SSL 接続のキープアライブを設定します。

・　再ネゴシエートデータチャネル：SSL の再接続を要求する時間間隔です。デフォルトは 61 分です。

・　DNS and WINS Servers：内部ネットワークの DNS/WINS サーバーを登録します。

リモート環境から内部ネットワーク資源の名前解決を行う場合に必要です。

⑨　以上で、Firebox モバイル VPN（SSL）の設定は終了です。

ポリシーマネージャーに「Allow SSLVPN-Users」ポリシーが追加されていることを確認してください。

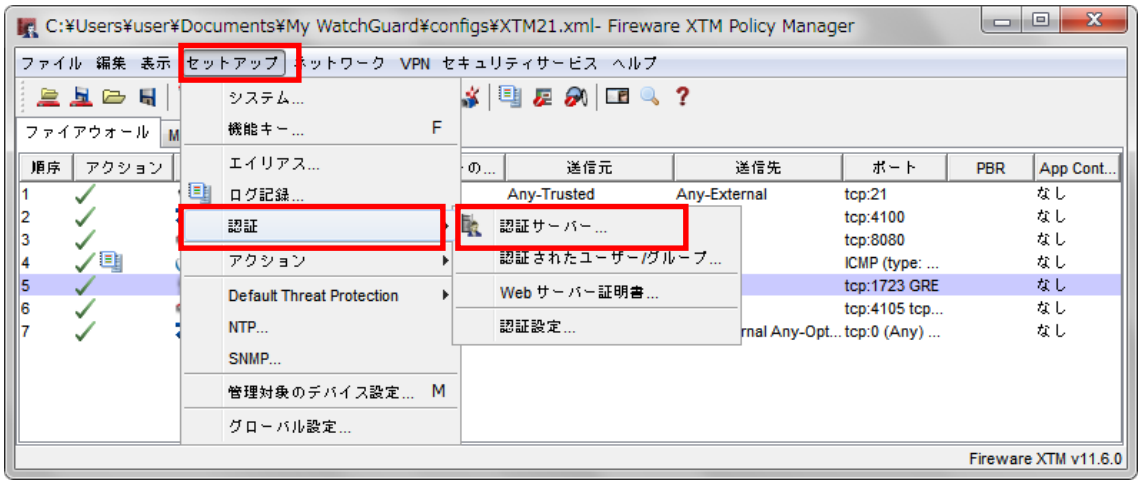
また、ポリシーマネージャーよりセットアップ> 認証> 認証サーバーを選択し、ユーザグループに「SSL VPN-Users group」が追加されていることを確認してください

注意:「Allow SSLVPN-Users」ポリシーでは、Trusted Network へのアクセスを許可していません。Trusted Network のアクセスを許可するには、ヘルプの「信頼済みネットワークへアクセスするように Mobile VPN with SSL ユーザーを許可する」を参照ください。

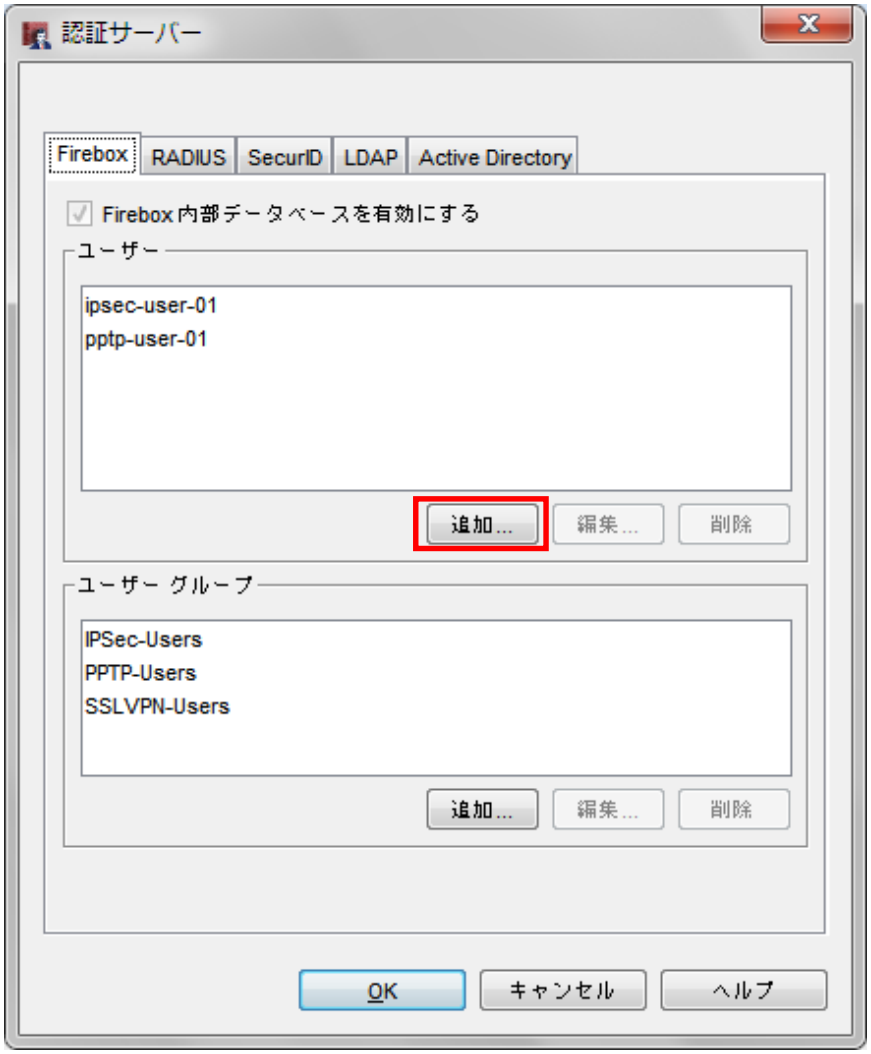
モバイル SSL VPN のユーザー作成

次にモバイル PPTP で接続するためのユーザーを作成します。

ポリシーマネージャーのセットアップ＞ 認証＞ 認証サーバーをクリックします。



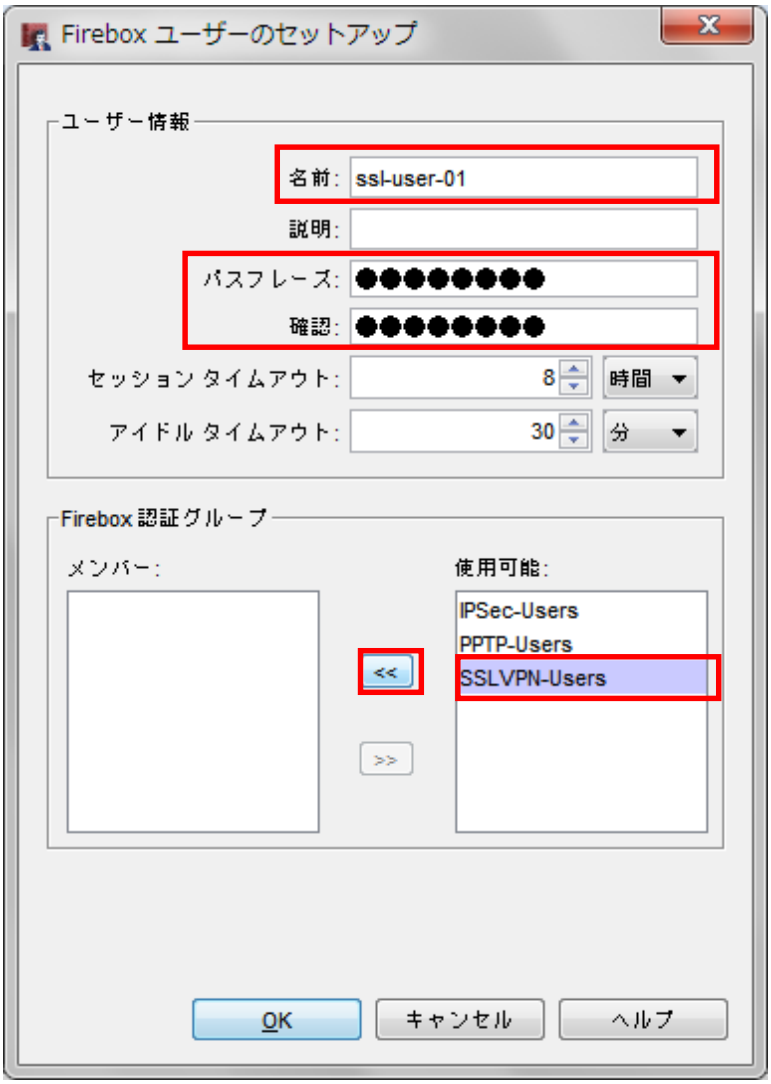
認証サーバーのダイアログで「追加」をクリックします。



ユーザー情報に任意の名前を入力します。

パスフレーズは 8 文字以上の英数字を入力します。

Firebox 認証グループには、PPTP を有効にしたときに自動的に作成された PPTP-Users を選択し、<< をクリックし、新しいユーザーを PPTP-Users グループに含めます。



以下の状態になります。

ユーザー追加と認証サーバーのダイアログで OK をクリックして閉じたら、ポリシーマネージャーで設定を保存します。

Windows/MacOS の SSL クライアントの設定

クライアントの条件

モバイル VPN（SSL）クライアントソフトウェアをインストールできる OS は以下となります。

- Microsoft Windows Vista (32-bit および 64-bit)
- Microsoft Windows 7 および 8 (32-bit および 64-bit)
- Microsoft Windows Server 2003 (32 ビット)
- Mac OS X 10.5 (Leopard)以降

- クライアント PC が Windows Vista または 7 および 8 の場合、モバイル VPN SSL クライアントソフトウェアのインストールは管理者権限で行う必要があります。
- クライアント PC が MacOS X の場合、SSL クライアントのインストールおよび利用に管理者権限は必要ありません。
- クライアント PC に Firewall ソフトウェアがインストールされている場合、次のポートを許可してください。

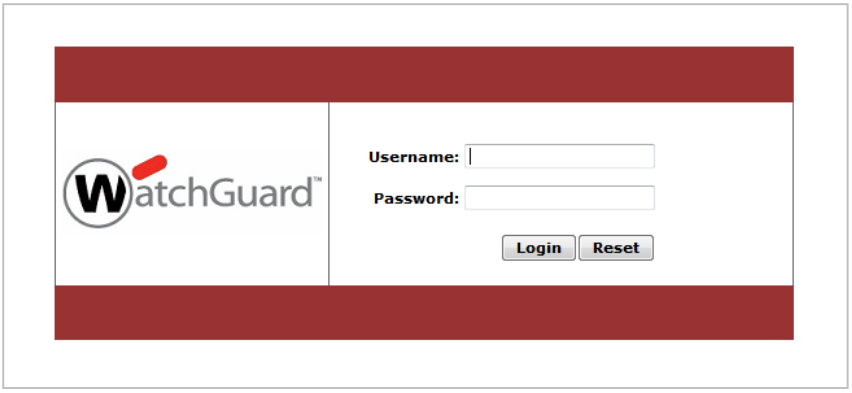
  TCP 4100 ポート

クライアントソフトウェアのダウンロード

① 次のサイトにアクセスします

https:// XTM の IP アドレス:4100/sslvpn.html

② あらかじめ作成しておいた SSLVPN ユーザーのユーザー名とパスワードを入力します



ログインするとダウンロードサイトが表示されます。

③ クライアント PC の OS に応じたインストーラーをダウンロードしてください

④ ダウンロードしたインストーラーをデスクトップ等の任意の場所に保存します

クライアントソフトウェアのインストール

Windows の場合

① WG-MVPN-SSL.exe.をダブルクリックすると、The Mobile VPN with SSL client Setup ウィザードが起動します

② デフォルトの設定が表示されるため「Accept」ボタンをクリックしてください

③ 「Finish」ボタンをクリックし、ウィザードを閉じてください

Mac OS の場合

① WG-MVPN-SSL.dmg をダブルクリックすると、デスクトップに WatchGuard Mobile VPN Volume が作成されます

② WatchGuard Mobile VPN Volume をダブルクリックすると WatchGuard Mobile VPN with SSL Installer V15.mpkg が起動します

③ デフォルトの設定が表示されるため「Accept」ボタンをクリックしてください

④ 「Finish」ボタンをクリックし、ウィザードを閉じてください

クライアントソフトウェアのインストール後、自動的に XTM に接続します。XTM に接続する度に、クライアントソフトウェアのアップデータがないか確認します。

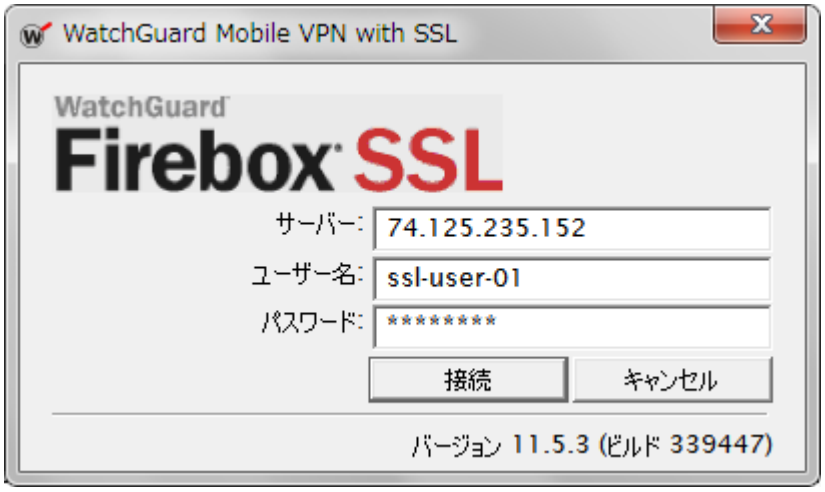
SSL VPN の接続方法

（Windows の場合）

① クライアントソフトウェアを起動します

- スタートメニュー＞プログラム＞WatchGuard Mobile VPN with SSL client＞Mobile VPN with SSL client を選択

② サーバー、ユーザー名、パスワードを入力します



※サーバーは、通常 External インターフェースに設定されている IP アドレスです

③ 「接続」ボタンをクリックします

(Mac OS の場合)

① Finder ウィンドウを開き、Applications > WatchGuard から WatchGuard　Mobile VPN with SSL アプリケーションをダブルクリックします

② メニューバーに WatchGuard Mobile VPN with SSL　アイコンが表示されます

③ 表示されたアイコンをクリックし、「Connect」を選択します

④ 接続したい XTM の IP アドレスとユーザー名、パスワードを入力します

※XTM の IP アドレスは、通常 External インターフェースに設定されている IP アドレスです

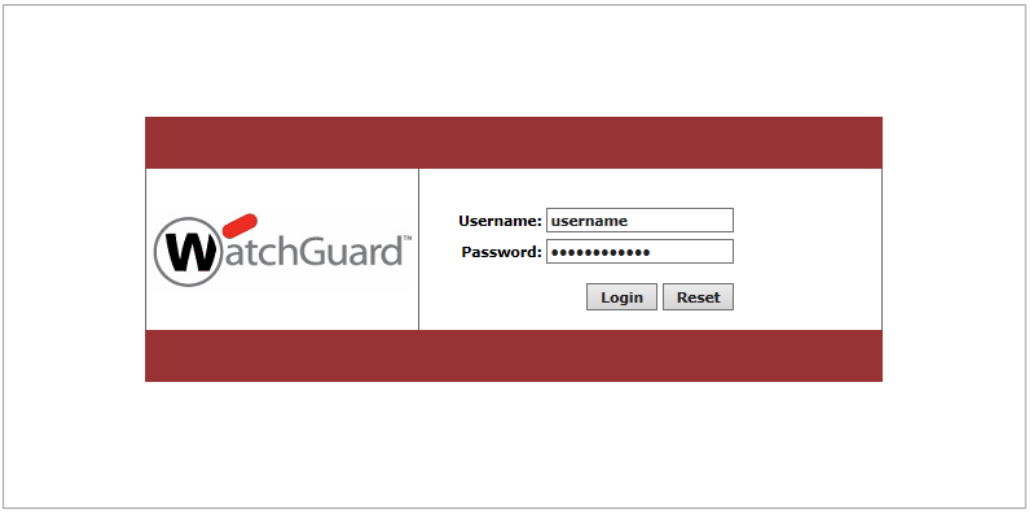
⑤ 「Connect」ボタンをクリックします

Android OS の SSL クライアントの設定

プロファイルのダウンロード

モバイルデバイスの SSL クライアントアプリケーションから読み込むプロファイルは

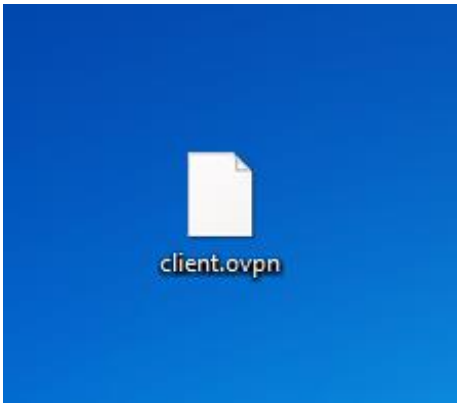
https://XTM の IP:4443/sslvpn.html にアクセスし、作成済みのアカウントでログインします。



Mobile VPN with SSL client profile の download ボタンをクリックします。

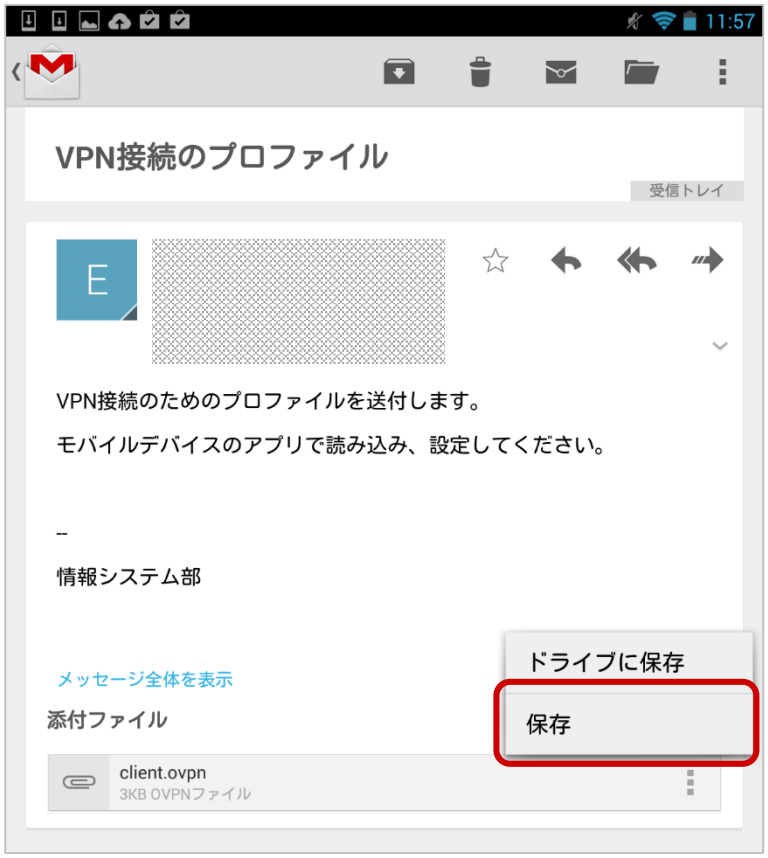
保存します。

client.ovpn というファイルが保存されます。



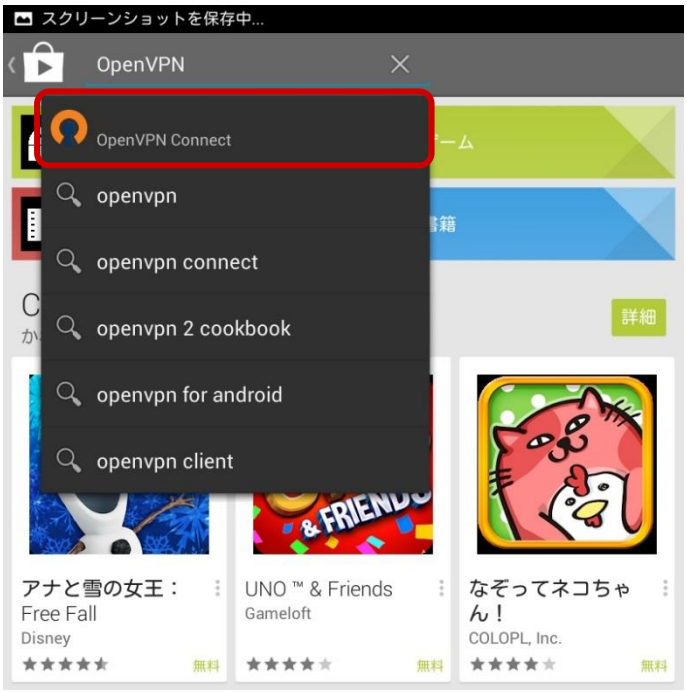
このファイルを SD カードに保存し、Android デバイスに転送します。

もしくはメールの添付ファイルで送信し、Android デバイスで受信したものを保存しておきます。



クライアントソフトウェアのインストール

Google Play ストアで OpenVPN を検索します。検索結果の OpenVPN Connect をタップします。

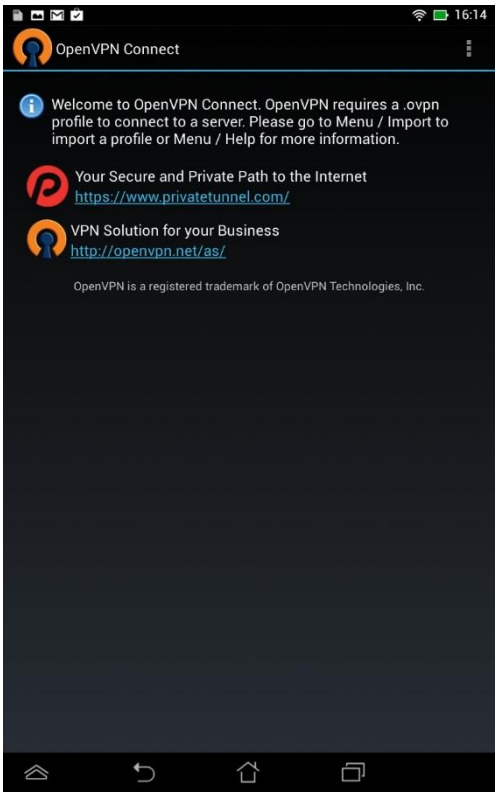


OpenVPN Connect インストールします。

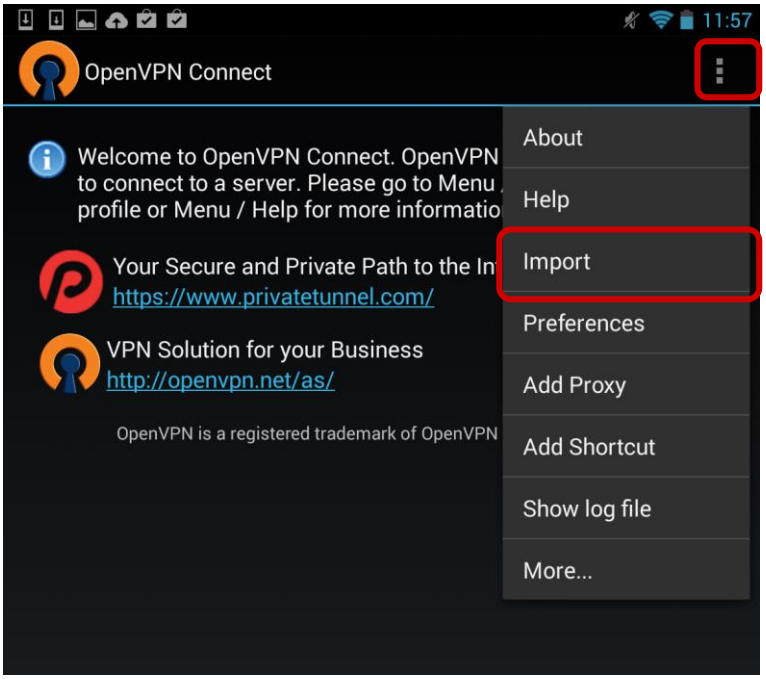
画像/メディア/ファイル へのアクセスに同意します。

インストールが完了したら、アプリを開いてみます。

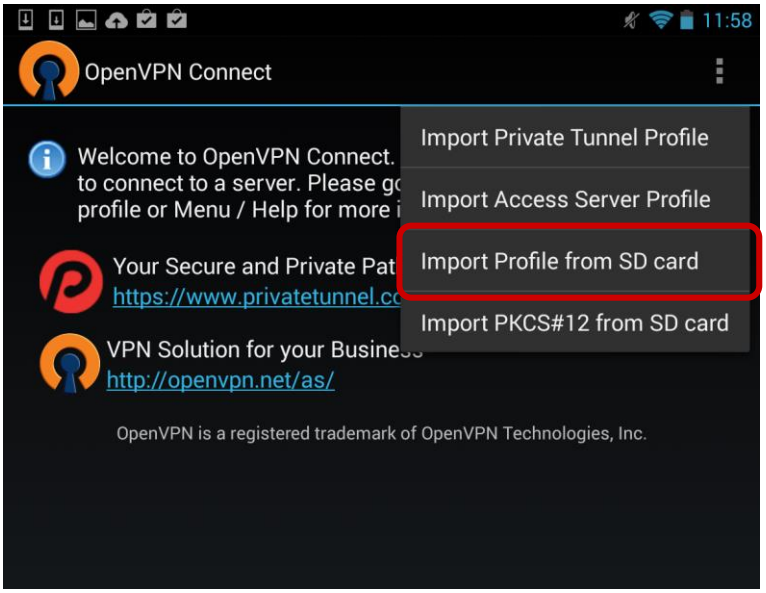
起動すればインストールは完了です。



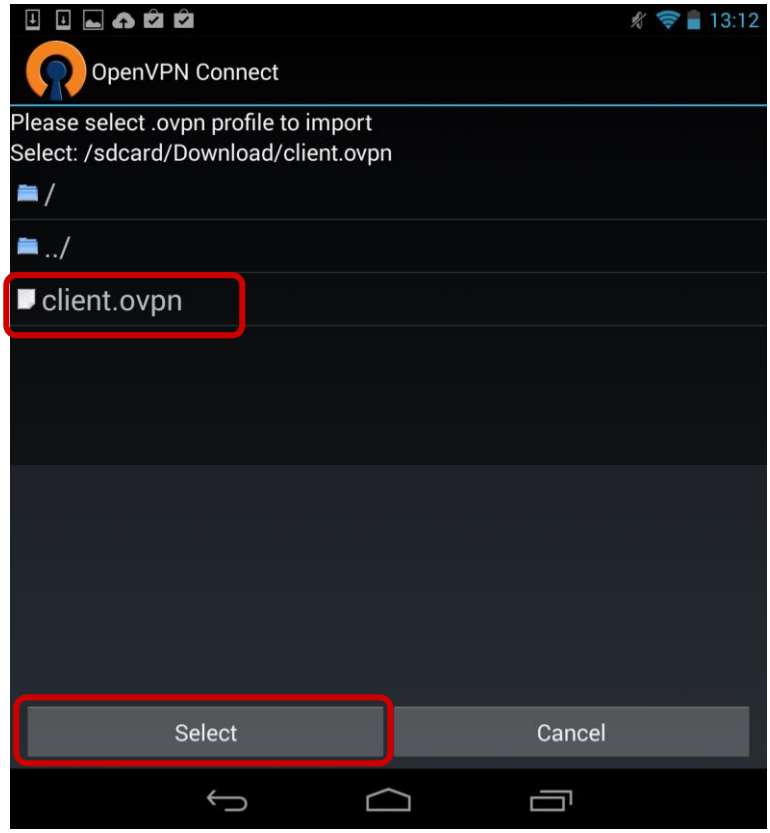
右上の ドロップダウンメニュー — Import をタップします。



Import Profile from SD card をタップします。

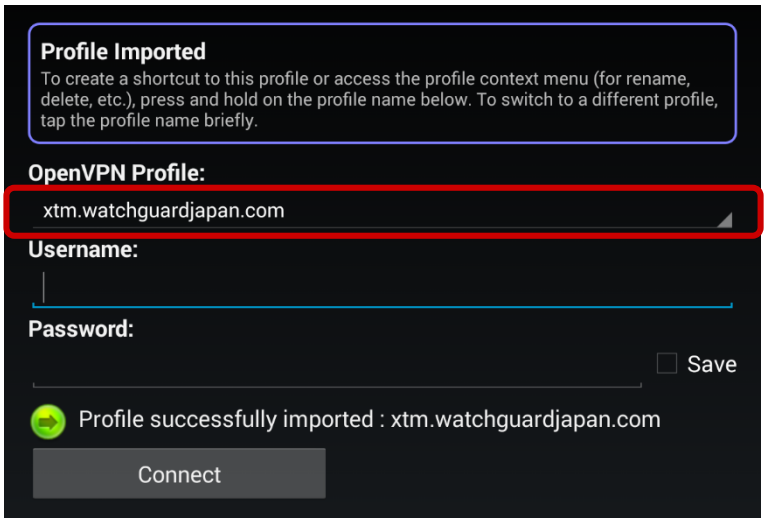


保存しておいたプロファイルを選択し、Select ボタンをタップします。

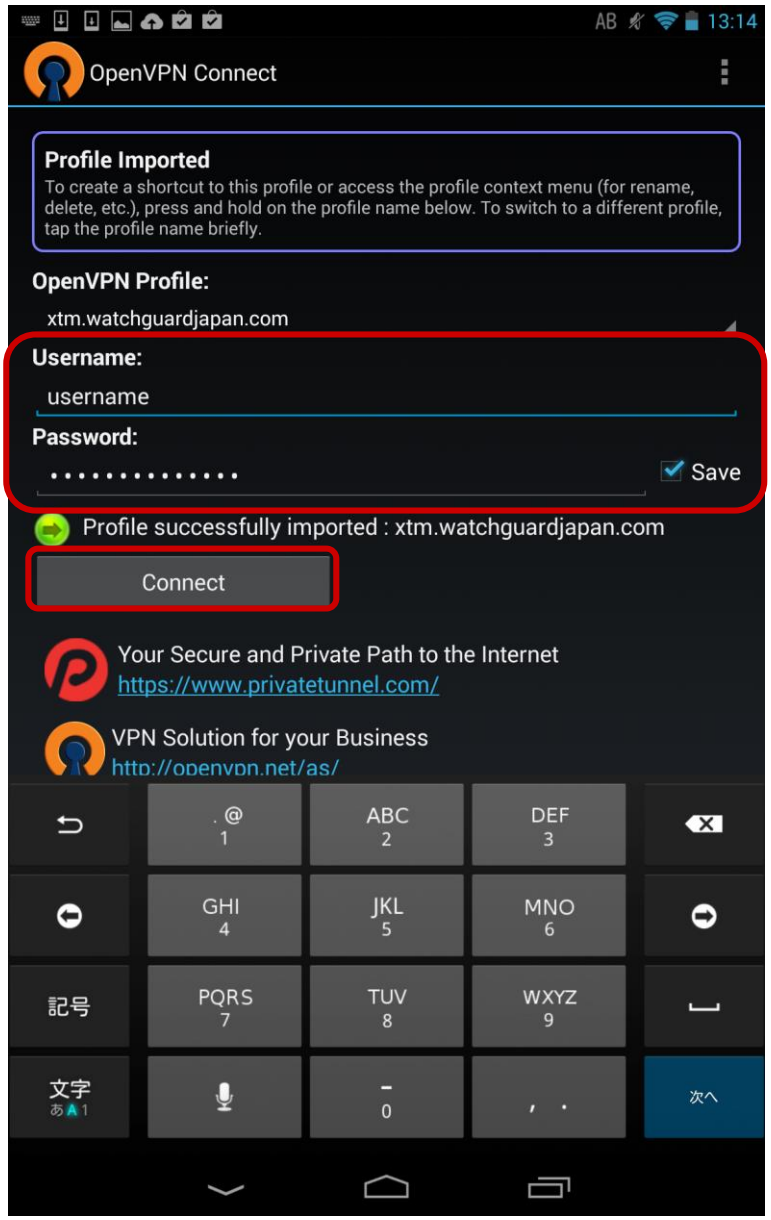


プロファイル　インポートの画面になります。

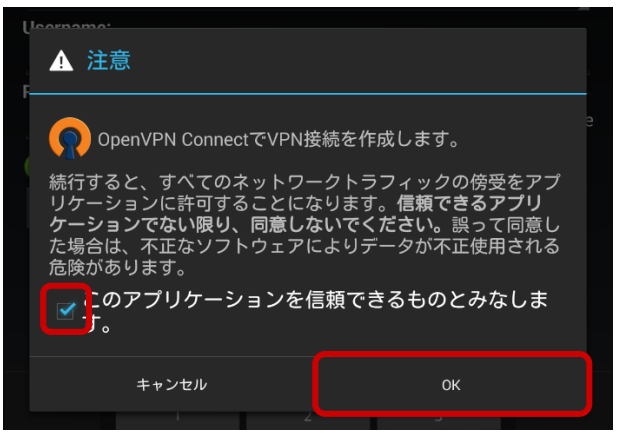
接続先の XTM のホスト名または IP アドレスになっているか確認してください。



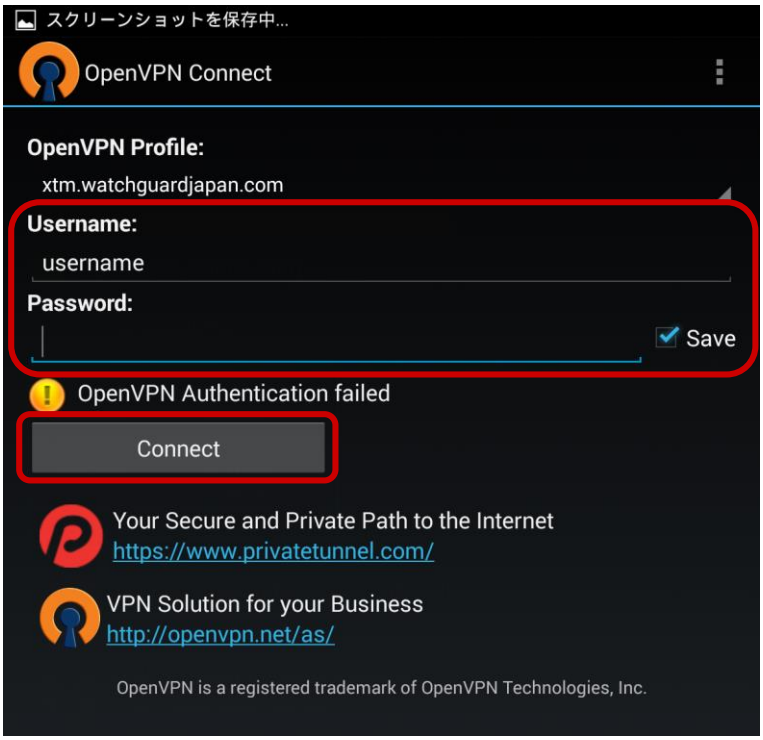
Username と Password を入力して Connect ボタンをタップします。



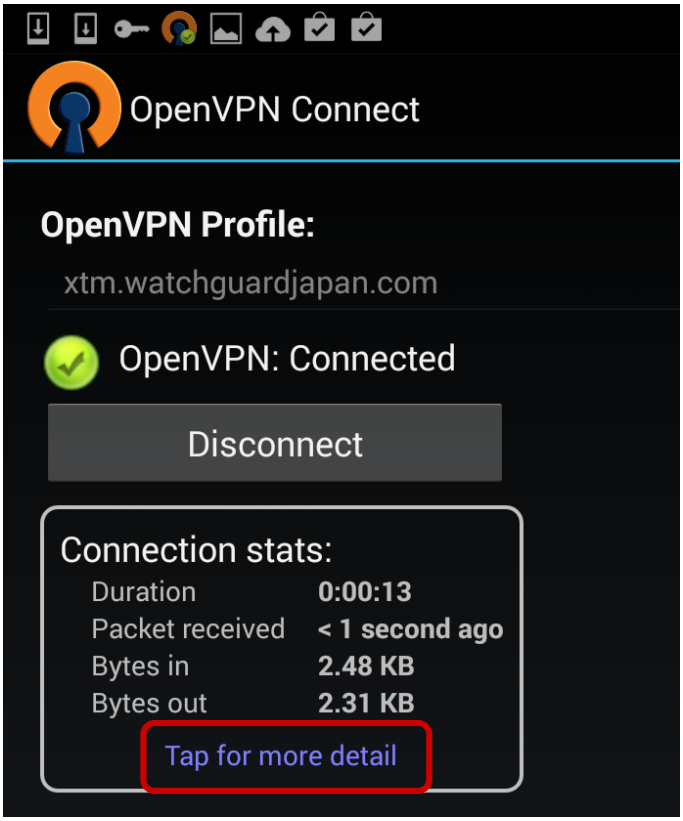
VPN 接続が作成される際にアラートが表示されますので、チェックして OK をタップします。



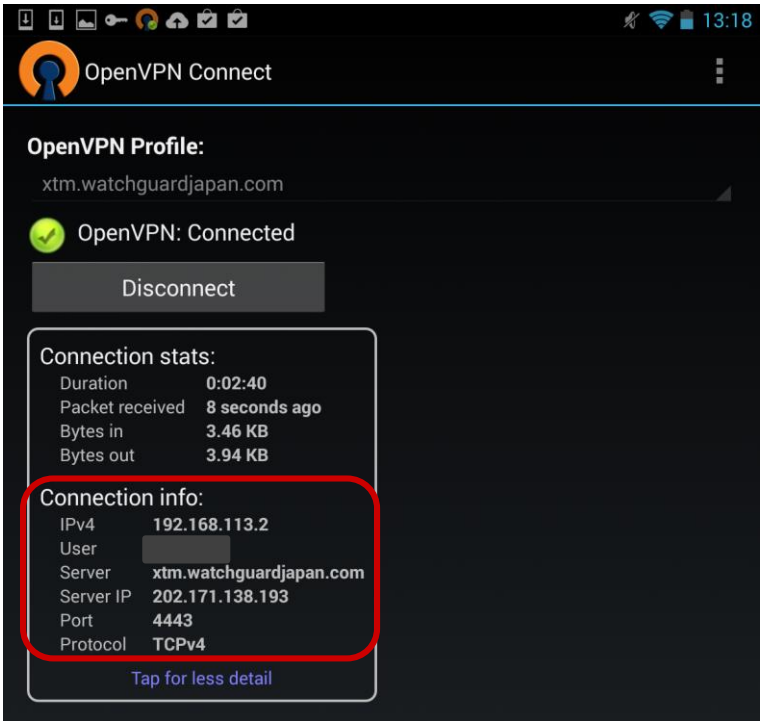
Username と Password を入力し、Connect ボタンをクリックします。



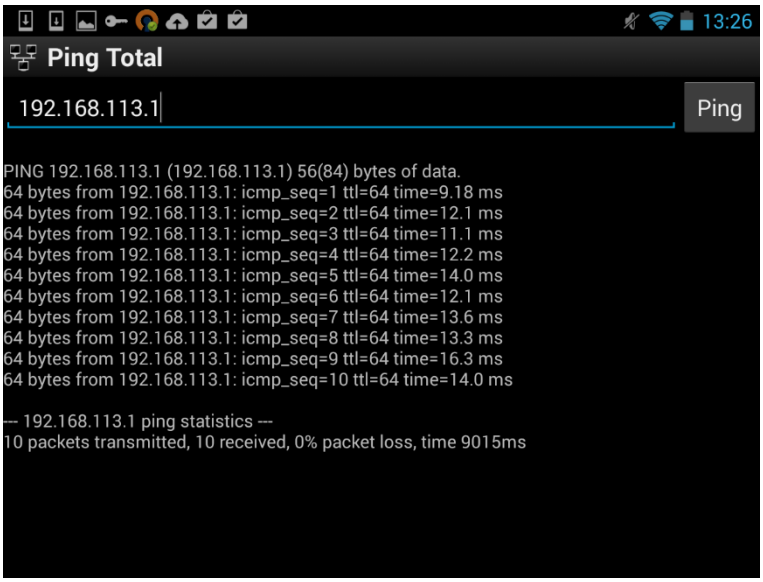
接続が成功すると、OpenVPN: Connected と表示されます。Tap for more detail リンクをタップすると、VPN の接続状況の詳細が確認できます。



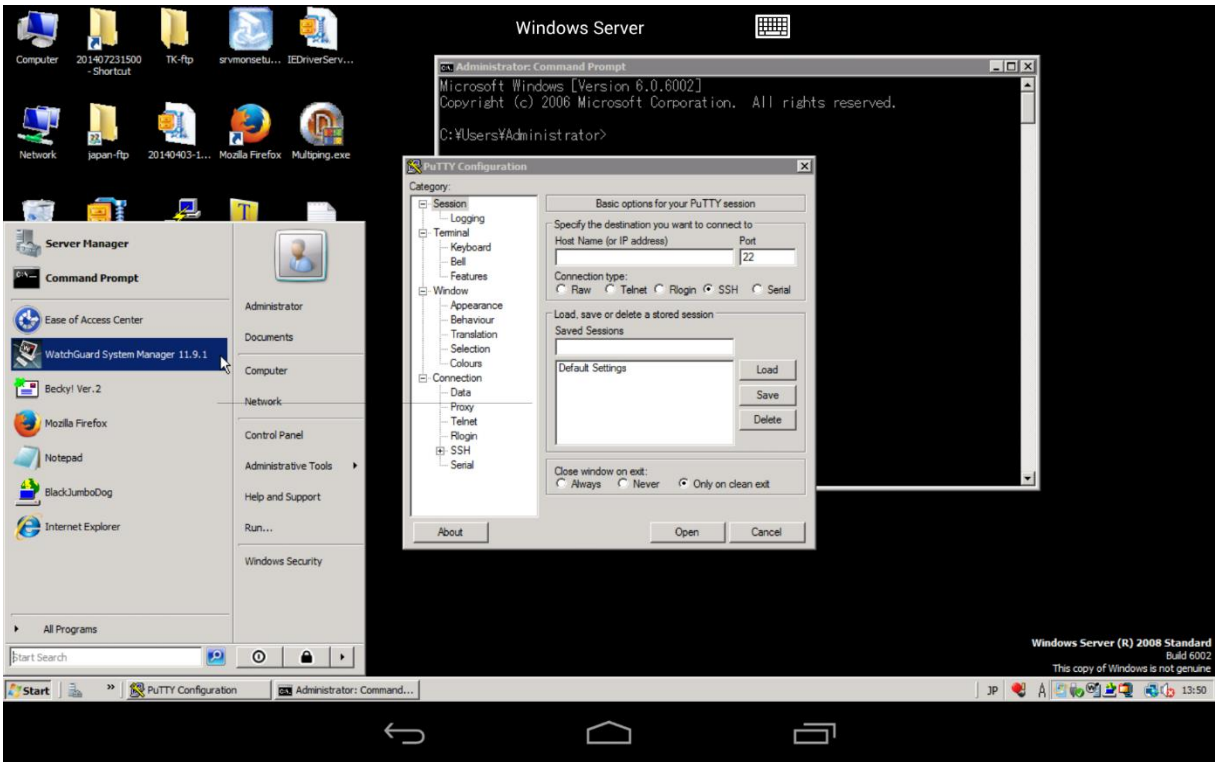
VPN 接続でデバイスが付与された IP アドレスなどが確認できます。



Ping コマンドを実行するアプリで、応答を確認できます。



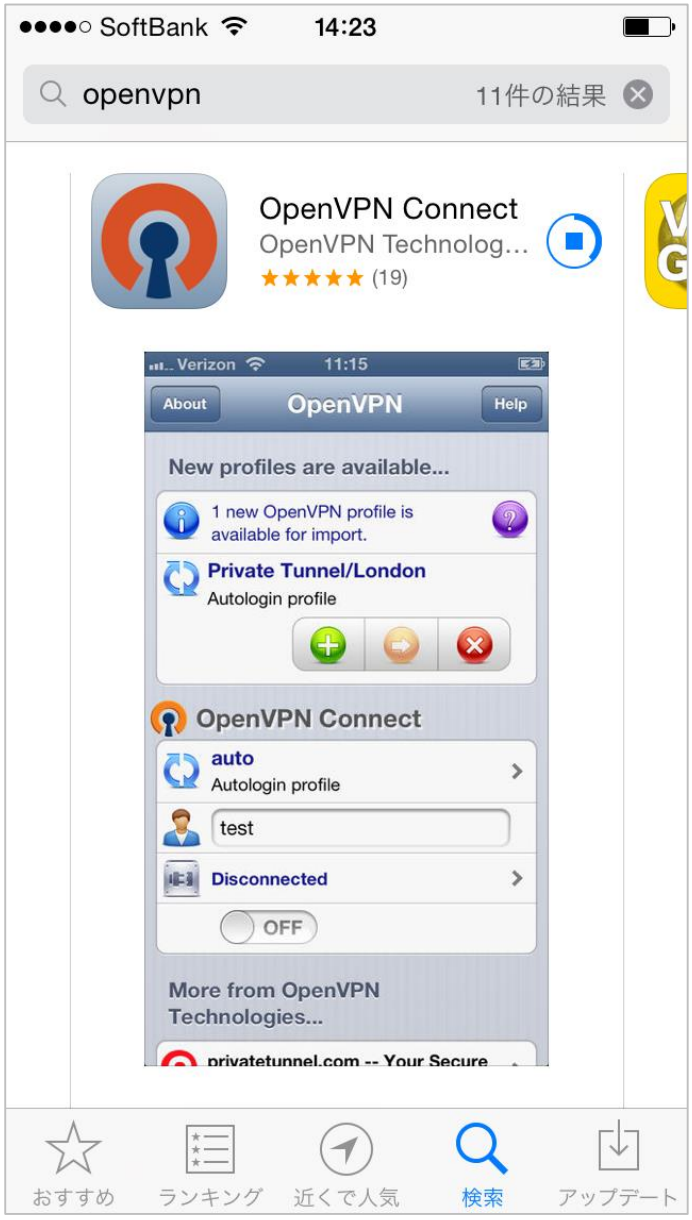
RDP アプリで Windows マシンにアクセスできます。



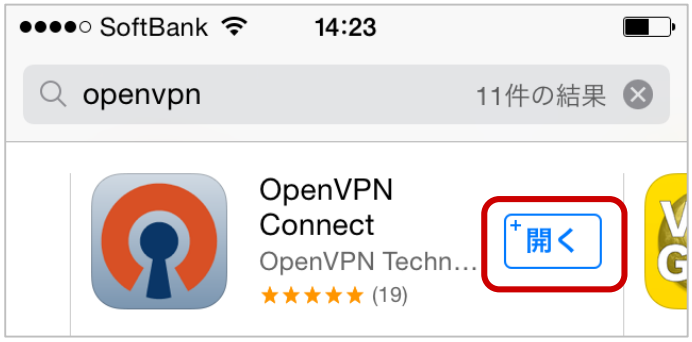
iOS の SSL クライアントの設定

クライアントソフトウェアのインストール

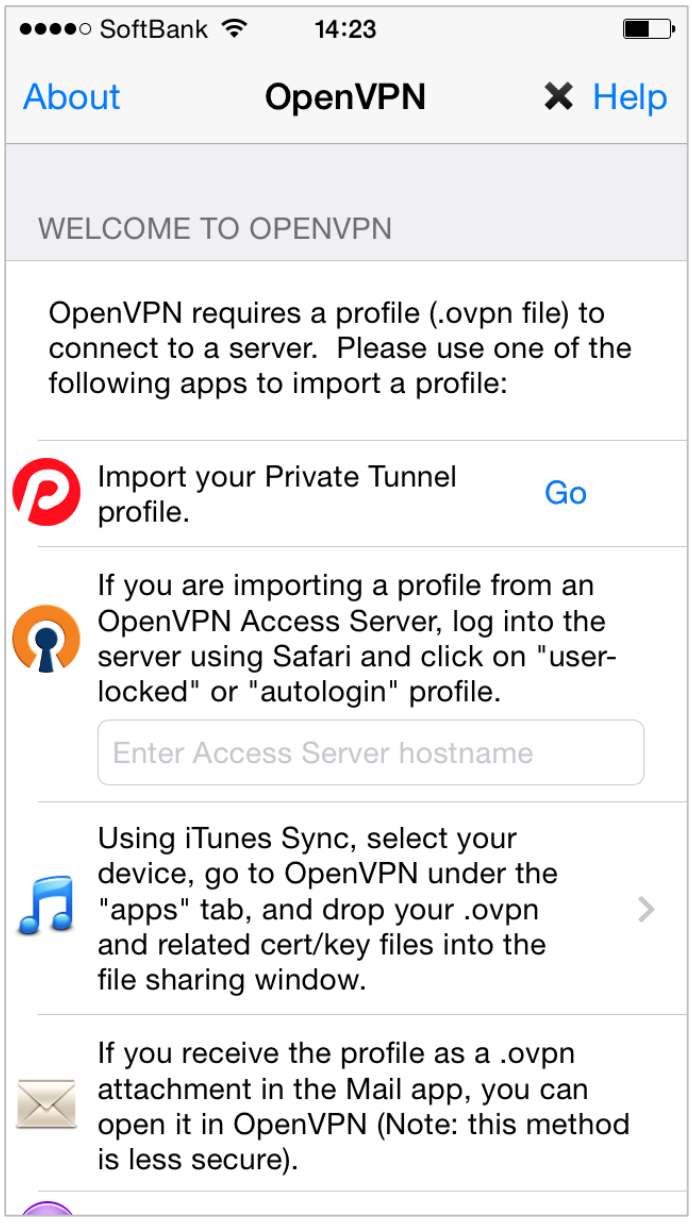
App Store で OpenVPN を検索し、OpenVPN Connect をインストールします。



アプリを開きます。



正常に起動すればインストールは完了です。



SSL VPN の接続方法

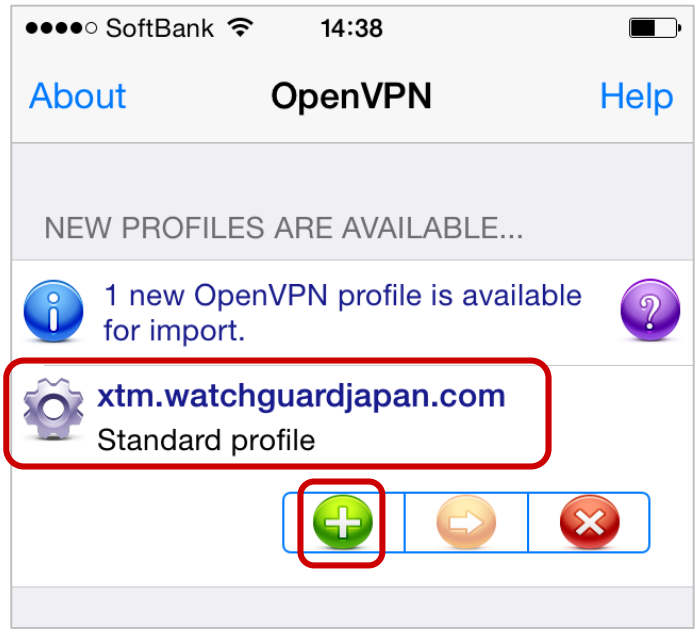
プロファイルの入手方法は、前章の「プロファイルのダウンロード」を参照してください。

VPN 接続プロファイルをメールの添付ファイルで送信し、iPhone/iPad で受け取ります。

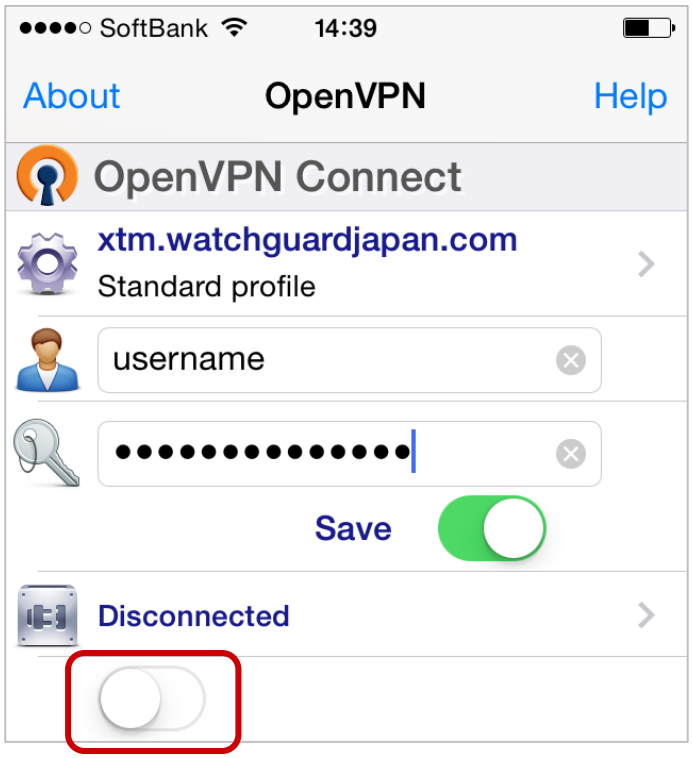
添付されたプロファイルをタップします。

添付ファイルをどのアプリで開くか候補が出るので、「OpenVPN で開く」をタップします。

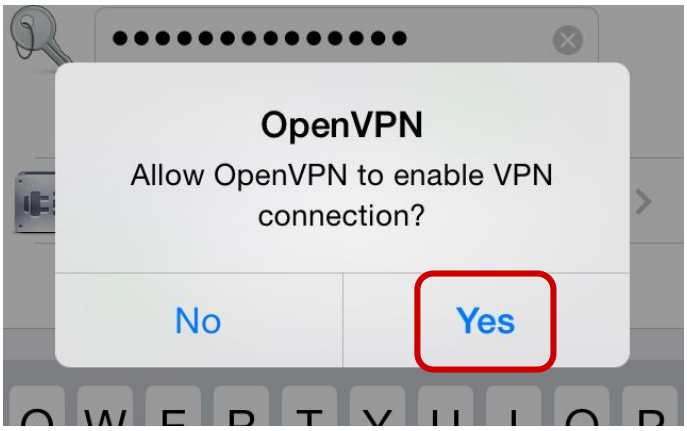
OpenVPN が新しいプロファイルが読み込み可能であることを表示します。接続先が正しいことを確認し、問題なければ ⊕ をタップしてインポートします。



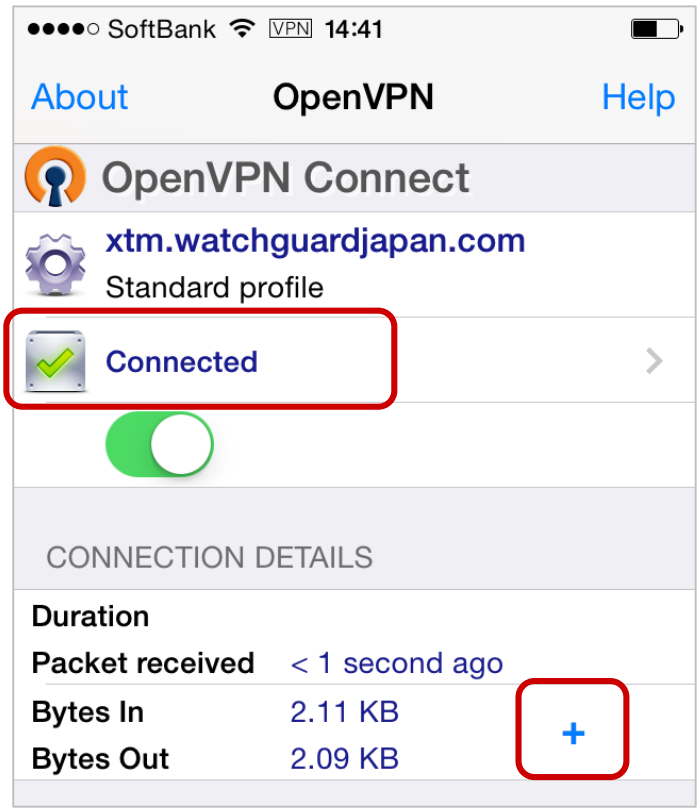
ユーザー名とパスワードを入力します。問題なければ Save も有効にします。Disconnected の下のスライドを右に移動し、接続します。



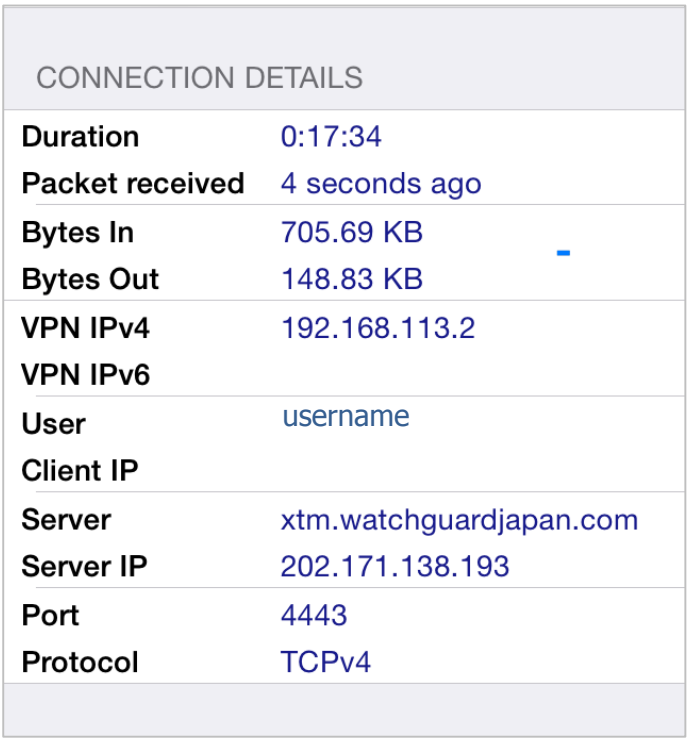
接続を許可するかたずねられたら、Yes をタップします。



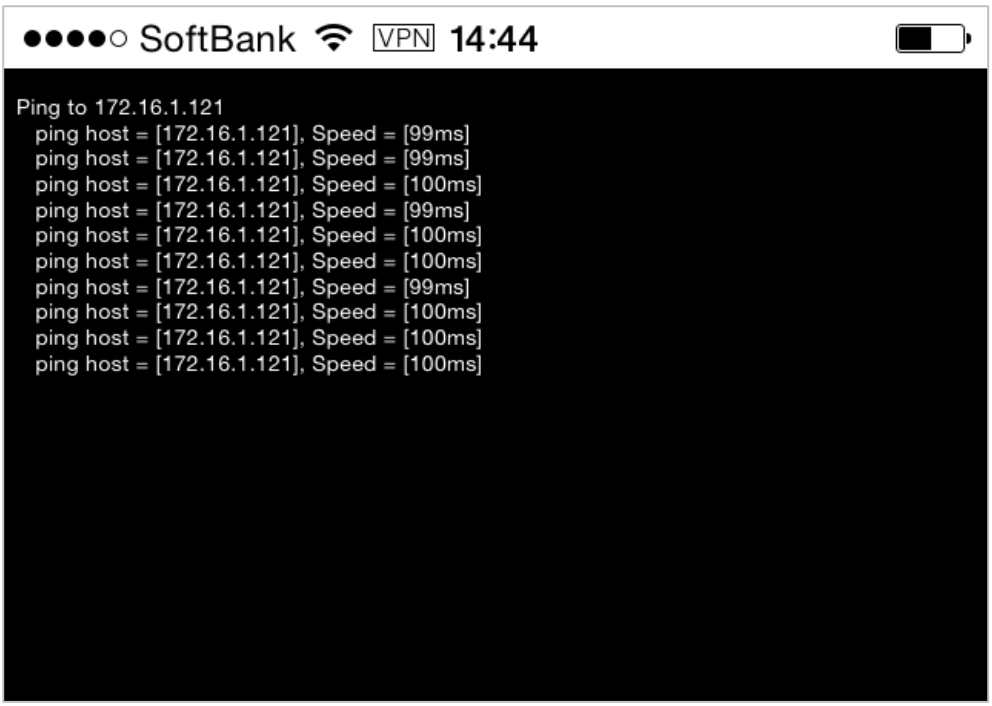
Connected と表示されたら、正常に接続できています。下方の+ をタップすると、VPN の接続状況の詳細が確認できます。



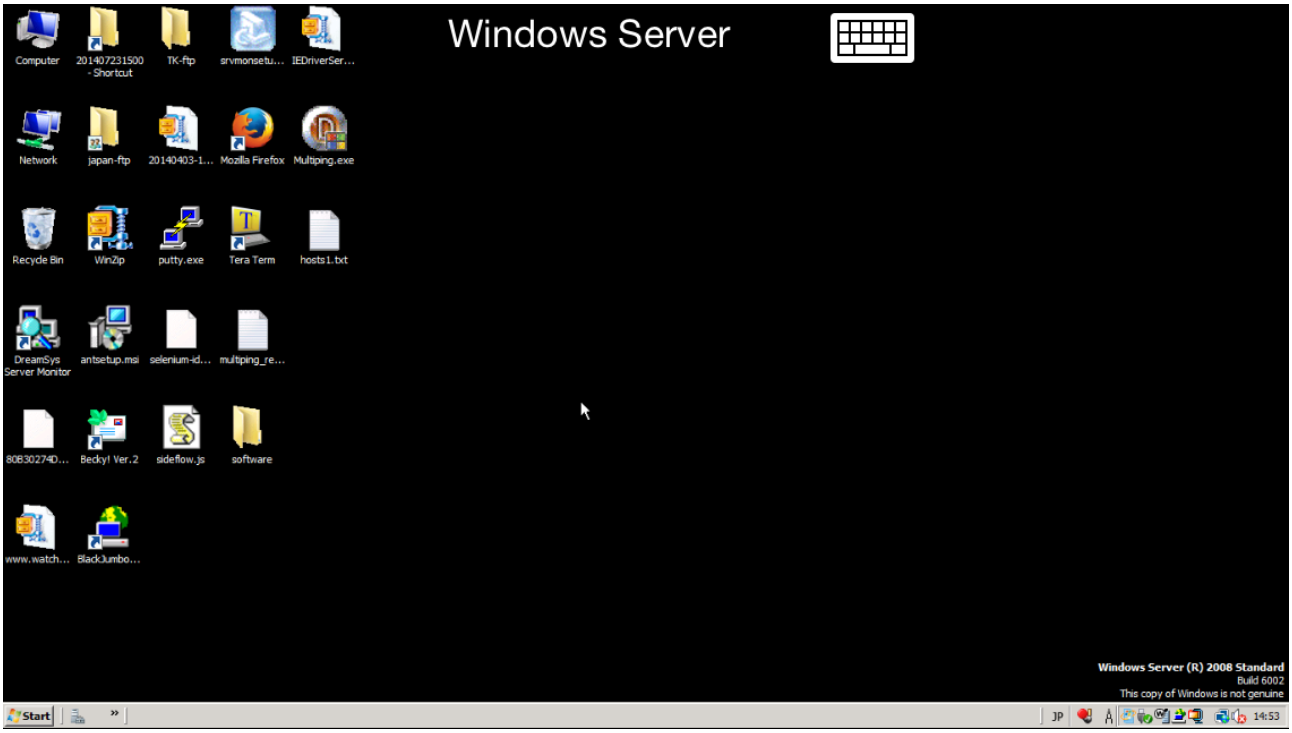
VPN 接続でクライアントデバイスが取得した IP アドレスなどが確認できます。



Ping コマンドを実行するアプリで、応答を確認できます。



RDP アプリで Windows マシンにアクセスできます。



おわりに

VPN かんたん接続ガイドをご活用いただき、ありがとうございます。

このガイドを通して、WatchGuard 製品によっていかにモバイル VPN の接続環境の構築が容易か、実感していただけたと思います。

WatchGuard XTM が御社のセキュリティにお役に立てれば幸いです。