



GlobalProtect 設定ガイド(PAN-OS 8.1) V1.0

Palo Alto Networks K.K.
2019/7

目次

1. はじめに	4
2. GlobalProtect の動作概要	5
2.1. External Gateway への接続	5
2.2. Internal Gateway への接続	7
3. GlobalProtect の動作検証用ネットワーク構成	9
4. 初期設定	10
5. L3 Firewall としての基本的な設定	11
5.1. ネットワーク設定	11
5.2. ポリシーの設定	14
6. Active Directory Domain Services の設定	15
6.1. ADDS と DNS Server のインストール	15
6.2. ADDS の設定	19
6.3. [参考]パスワードの複雑さの変更	22
6.4. Active Directory ユーザーの作成	23
7. GlobalProtect の基本的な設定	25
7.1. ネットワーク設定	25
7.2. ユーザー認証の設定	30
7.3. SSL 証明書の生成	39
7.4. SSL / TLS サービスプロファイルの設定	42
7.5. Gateway の設定	43
7.6. 内部 DNS の設定	47
7.7. ポリシーの設定	57
7.8. GP Agent の設定	58
8. クライアント証明書認証の設定	67
8.1. 全ユーザー共通のクライアント証明書で認証	67
8.2. 各ユーザー個別のクライアント証明書で認証 (SCEP 利用による配布)	72
8.3. CRL によるクライアント証明書の失効管理	96
8.4. OCSP によるクライアント証明書の失効管理	113
8.5. 新規ユーザーだけにクライアント証明書を配布する方法	127
9. ワンタイムパスワード認証の設定	132
9.1. Google Authenticator のインストール	132
9.2. OTP サーバーのインストールと設定	132
9.3. RADIUS 認証の設定	143
9.4. GP Agent からのアクセス	148
9.5. 外部からの接続はパスワードと OTP 両方の入力を強制する設定	149
9.6. VPN の再接続時に一定時間は OTP の再入力を必要としない設定	150
10. macOS からの接続	151
10.1. GP Agent (v4.1.10) のダウンロードとインストール	151
10.2. Portal & Gateway へのアクセス	153
10.3. クライアント証明書の失効	156
11. User-ID でアクセス制御	157
11.1. ユーザー名でアクセス制御	157
11.2. グループでアクセス制御	159
12. Host Information Profile で制御	162

12.1.	HIP 検証用の事前設定	162
12.2.	HIP オブジェクトとHIP プロファイルの設定	162
12.3.	HIP マッチログの確認	164
12.4.	セキュリティポリシーの設定	165
12.5.	動作確認	165
12.6.	[参考]各種端末のHIP	166
13.	スマートデバイスからの接続.....	168
13.1.	SCEP によるクライアント証明書のインポート	168
13.2.	手動によるクライアント証明書のインポート.....	174
14.	おわりに.....	191

1. はじめに

本ガイドにて、GlobalProtect の設定方法をご紹介します。

GlobalProtect には以下のような特徴があり、それぞれの設定と動作確認の方法を記載しています。

- ① リモートアクセス VPN (IPSec または SSL)
- ② ユーザー識別 (リモートアクセス VPN 時だけでなく、社内 LAN でも)
- ③ クライアント証明書の発行・認証・失効管理 (認証局サーバーとの連携)
- ④ ワンタイムパスワード認証 (OTP サーバーとの連携)
- ⑤ 検疫: Host Information Profile(HIP)でのアクセス制御 (アンチウィルスの有無、HDD 暗号化の有無等で制御)

PA Firewall の機能と共に GlobalProtect を使うことで、外部からのリモートアクセス機能だけでなく、社内 LAN におけるユーザー識別や検疫が可能となるので、PA Firewall をより有効に、より強力にご利用いただくことができます。

また、Windows と macOS に限定されますが、本ガイドで紹介するほとんどの機能は PA Firewall の標準機能としてご利用いただけます。

○: PA Firewall の標準機能 / ●: GlobalProtect サブスクリプション(有償)

↓機能	OS→	Windows	macOS	iOS	Android	Linux
① リモートアクセス VPN		○	○	●	●	●
② ユーザー識別		○	○	●	●	●
③ クライアント証明書認証		○	○	●	●	●
④ ワンタイムパスワード認証		○	○	●	●	●
⑤ HIP 制御		●	●	●	●	●

本ガイドを弊社提供の正式ドキュメントと併用して頂き、新規設置作業や日々の運用時の設定変更作業時の参考ドキュメントとしてご活用ください。

※) 本ガイドは、以下の OS バージョンを利用しています。

- PAN-OS: 8.1.7
- GP Agent: 4.1.10 (Windows & macOS)
5.0.5 (iOS & Android)

適用する OS バージョンが異なる場合は、該当する OS のドキュメントを参照してください。

2. GlobalProtect の動作概要

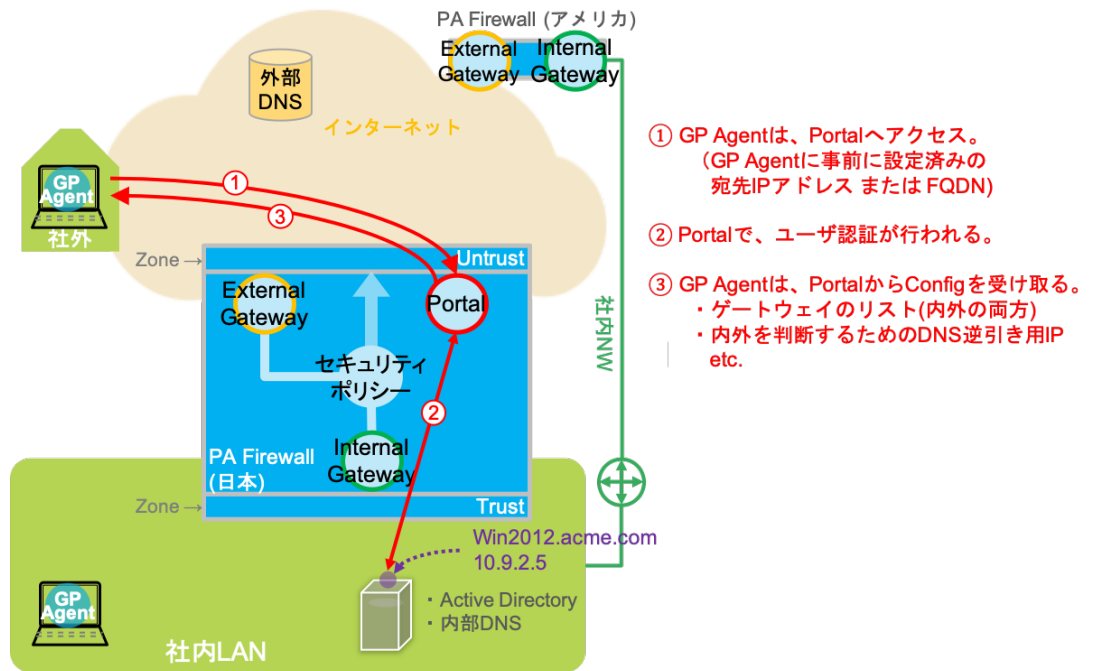
設定の解説に入る前に、GlobalProtect の動作を説明します。

ここで説明する動作については、GlobalProtect Agent (以降、GP Agent) ソフトウェアがクライアント PC へインストール済みである前提とします。

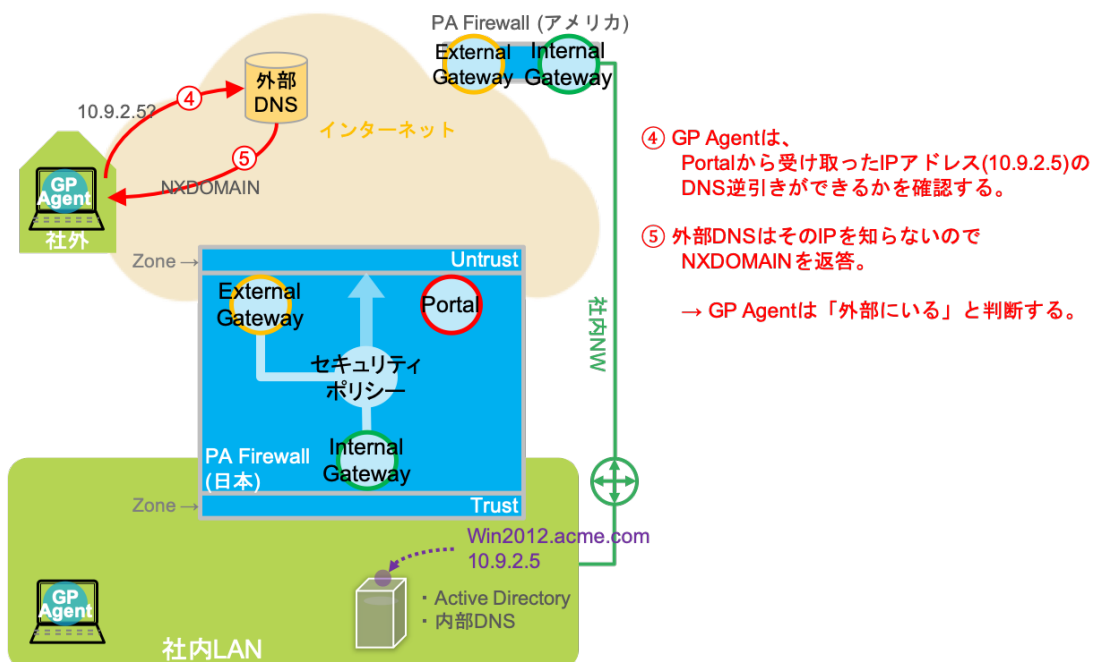
2.1. External Gateway への接続

GP Agent が、社外=インターネットから自社内 LAN に接続するときの動作フローです。

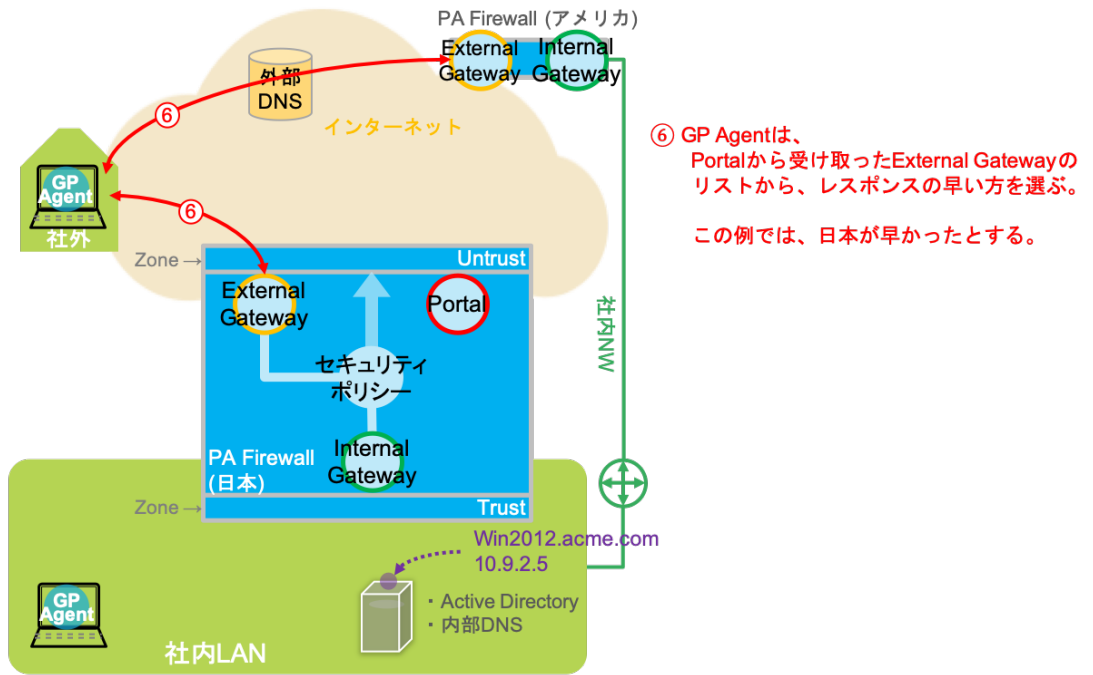
(1) ポータルへのアクセス



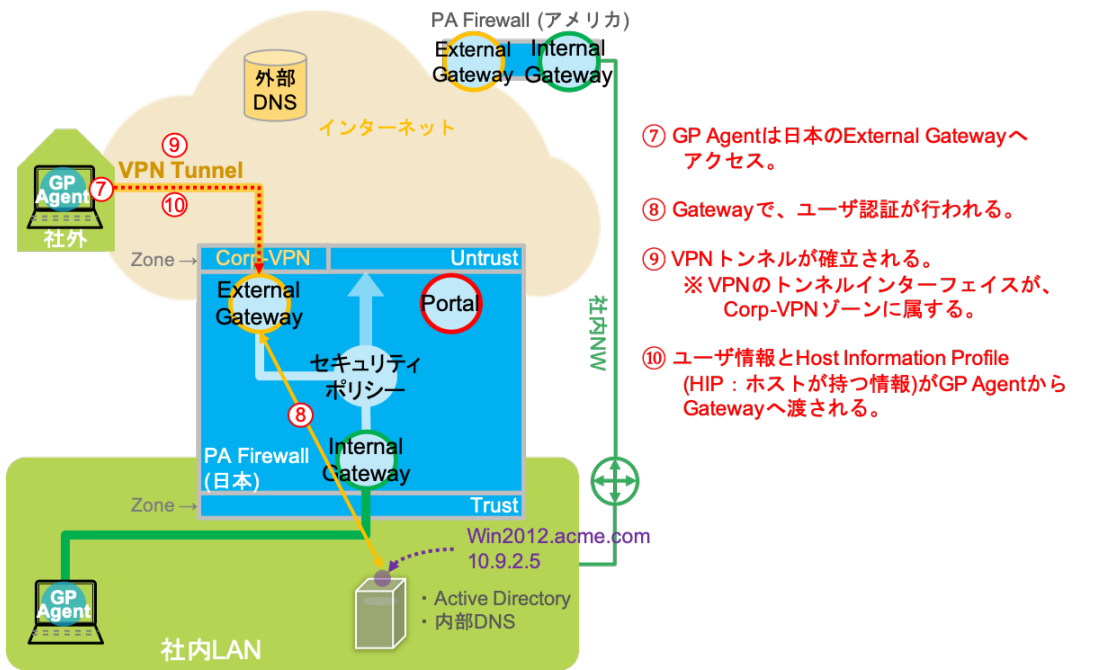
(2) DNS を使って、GP Agent が今どこにいるのか(外部 or 内部)を判断



(3) 世界に複数存在する External Gateway のうち、近い方を選択



(4) External Gateway へのログイン&VPNトンネル確立と、検疫情報(HIP)の送信



VPNトンネル確立後のクライアント PC は、LAN 端末と同様の扱いが可能となり、PA Firewall のセキュリティポリシーの適用が可能です。

ユーザー認証を実施済みなので、ユーザーID 情報を持つログ出力や、ユーザー名(グループ名)でのポリシーコントロールが可能です。

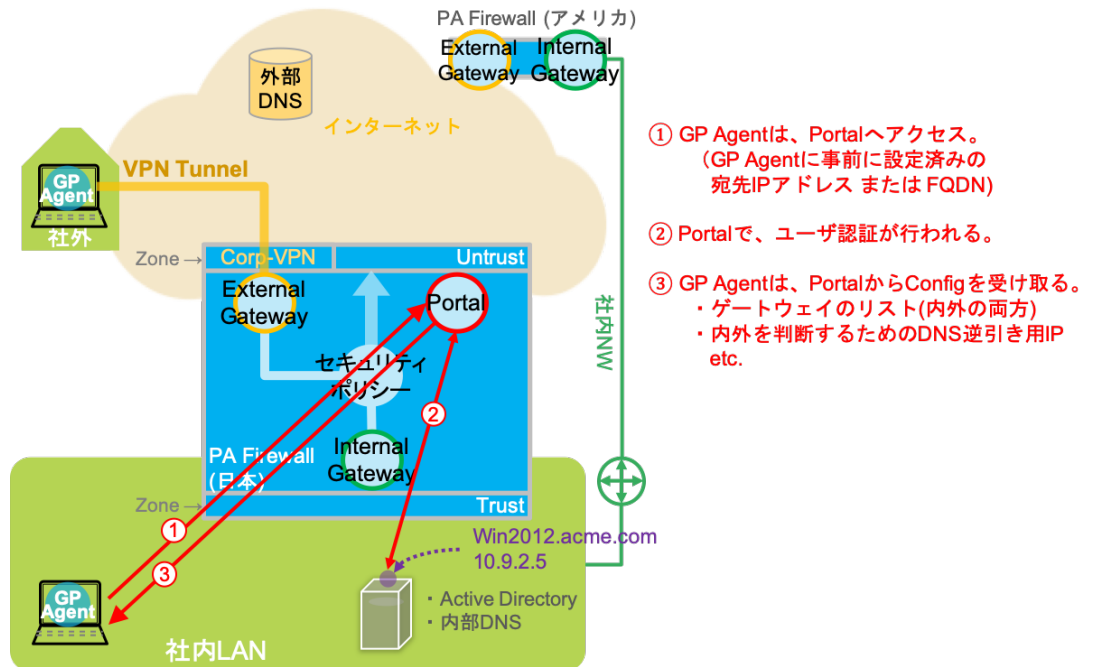
検疫によるポリシーコントロールも可能であり、例えば「ディスクが暗号化されていない PC は特定サーバーへアクセスさせない」という制御も可能です。

2.2. Internal Gateway への接続

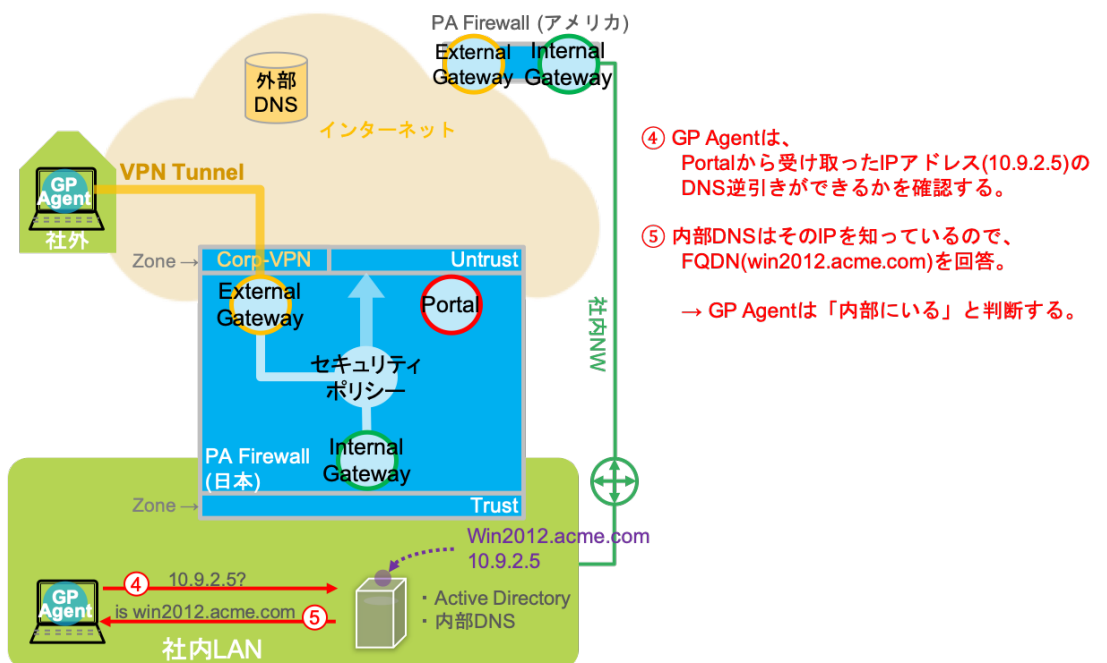
次は、GP Agent が社内 LAN に接続されたときの動作フローです。

基本的な動作は、「External Gateway への接続」で示したフローと同じで、異なるのは「VPNトンネルを確立しない」点です。

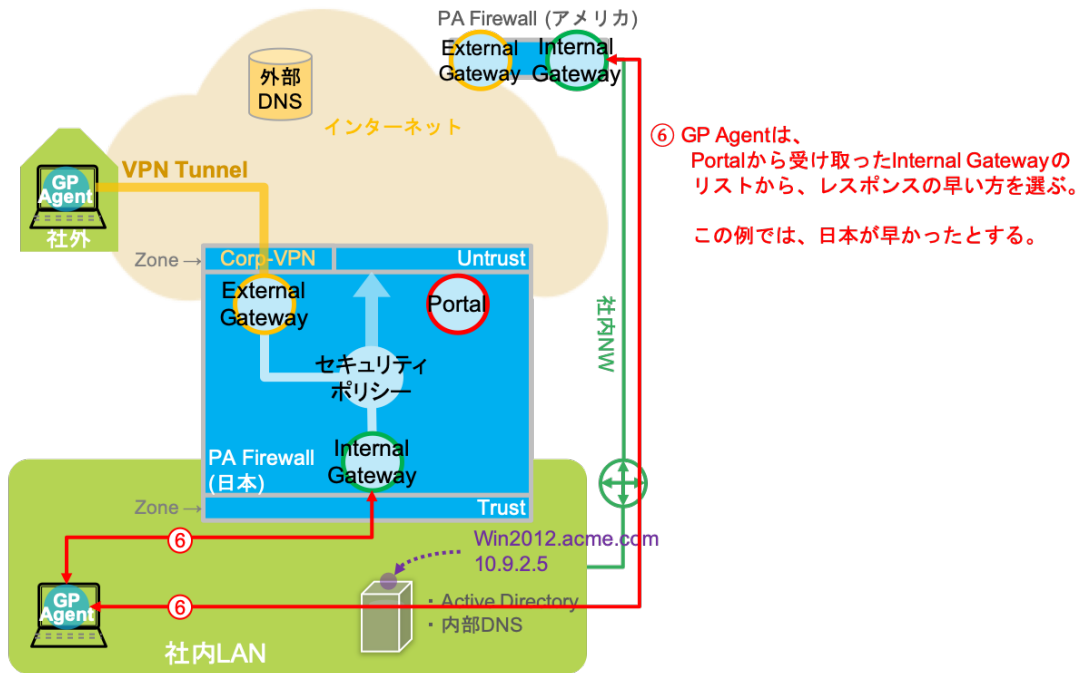
(1) ポータルへのアクセス



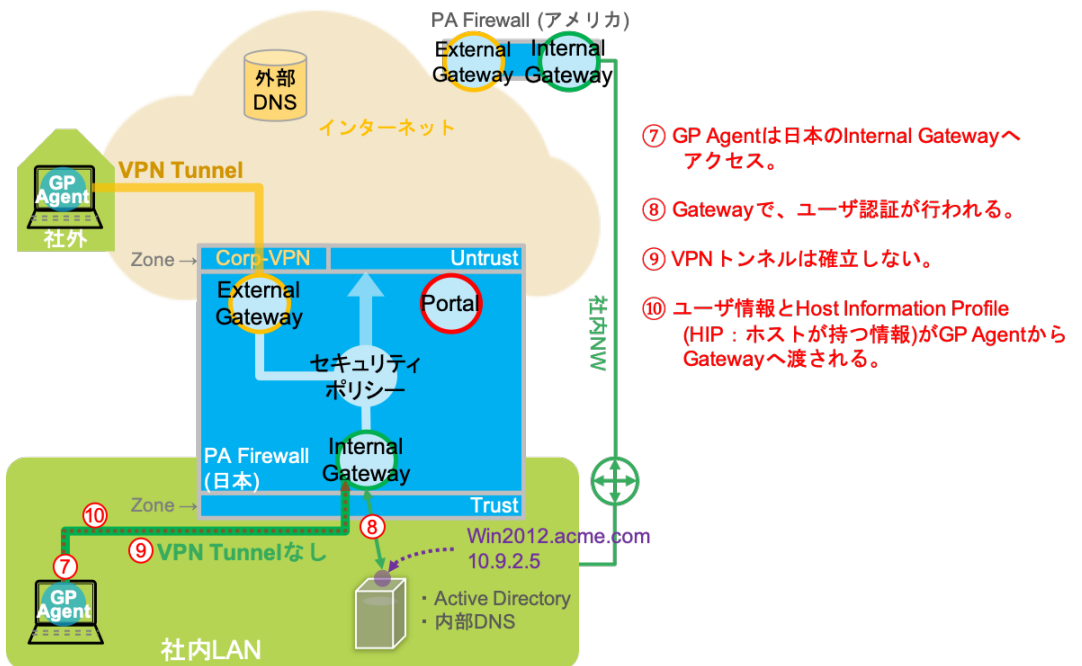
(2) DNS を使って、GP Agent が今どこにいるのか(外部 or 内部)を判断



(3) 世界に複数存在する Internal Gateway のうち、近い方を選択



(4) Internal Gateway へのログインと、検疫情報(HIP)の送信 (VPNトンネルは確立しない)

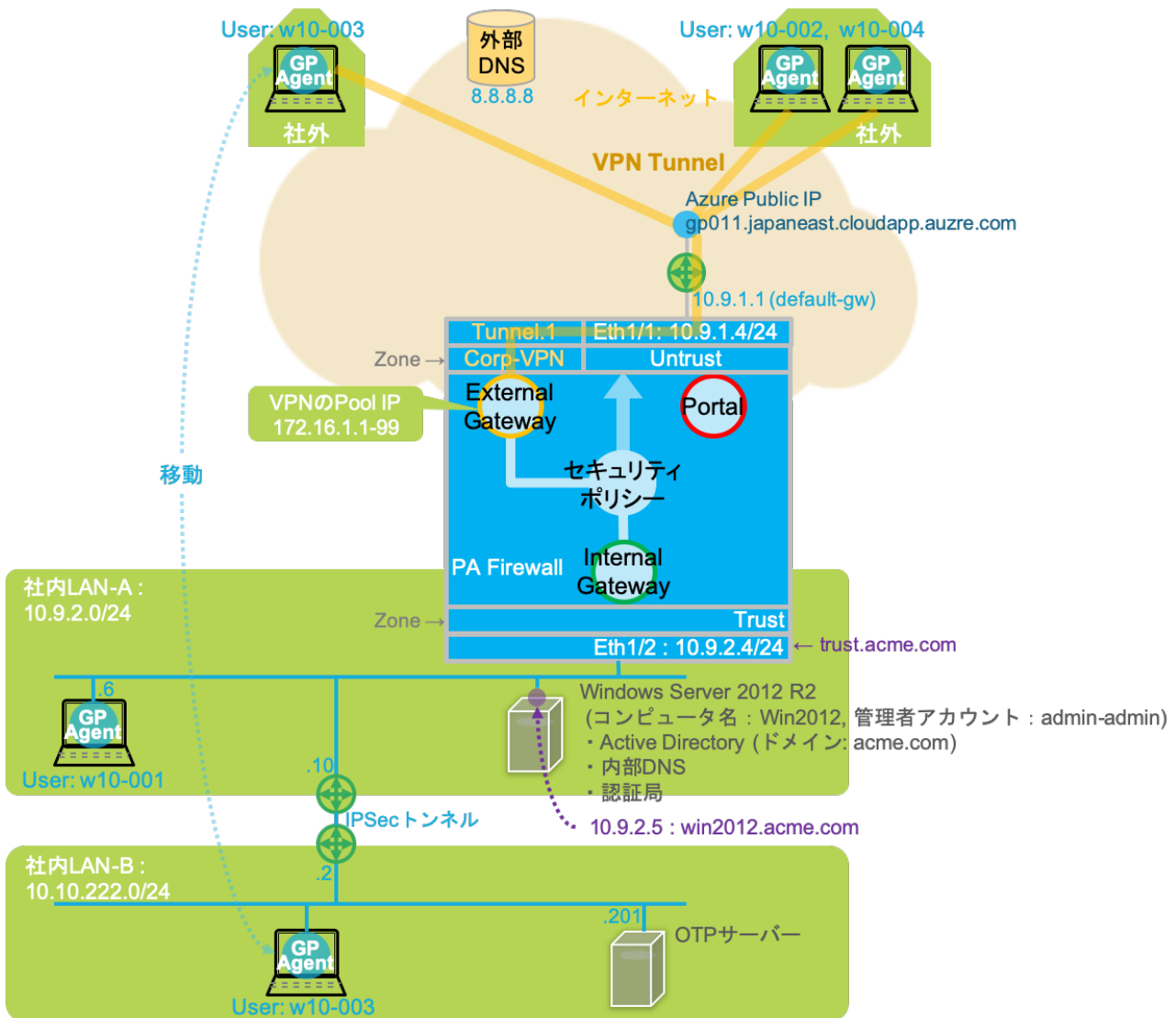


Internal Gateway ログイン後は、LAN 端末として、PA Firewall のセキュリティポリシーの適用が可能です。ユーザー認証を実施済みなので、ユーザーID 情報を持つログ出力や、ユーザー名(グループ名)でのポリシーコントロールが可能です。

社内 LAN においても検疫によるポリシーコントロールが可能であり、例えば「ディスクが暗号化されていない PC は特定サーバーへアクセスさせない」という制御も可能です。

3. GlobalProtect の動作検証用ネットワーク構成

以下のネットワーク構成にて、GlobalProtect の動作を確認します。



検証用ネットワーク構成の概要:

- GlobalProtect 設定を行う PA-Firewall は、パブリッククラウド: Microsoft Azure(以降、Azure)上に設置しています。
 - Azure から提供される Public IP アドレスと、Untrust 側のプライベート IP アドレスは 1 対 1 NAT です。
 - その Public IP アドレスは、Azure の DNS に「gp011.japaneast.cloudapp.azure.com」として登録しています。
- Windows Server 2012 R2(以降、Win2012)を Trust ゾーン側(Azure 内)に設置し、以下の役割をインストールします。
 - Active Directory Domain Services (ドメイン: acme.com)
 - 内部 DNS (正引き/逆引き)
 - Active Directory Certificate Services (認証局: クライアント証明書の発行及び管理)
- GP Agent がインストールされたクライアント PC は 4 台あり、以下の状態です。
 - 全て Windows10 です。
 - ドメイン: acme.com のクライアントです。
 - ユーザー: w10-003 だけは内部と外部の移動ができるようにしていますが、それ以外は図の通り固定です。
- 「社内 LAN-B」はオンプレミスであり、Azure の「社内 LAN-A」との間を IPsec トンネルで接続しています。
 - VyOS(仮想ルーター)を利用して、IPsec トンネル接続しています。
 - 理由:
 - ◇ オンプレミスの仮想版 OTP サーバーを利用するため。
 - ◇ 社内 LAN サブネットとインターネットを容易に移動できる端末(w10-003)を用意するため。

4. 初期設定

以下の初期設定は実施済みであるものとします。

これらは、下記 Link からダウンロードできる「PA Series Firewall 設定ガイド(PAN-OS 8.1)」に詳細を記載していますので、必要に応じてご参照ください。

<https://live.paloaltonetworks.com/t5/ナレッジドキュメント/PA-Series-Firewall-設定ガイド-PAN-OS-8-1/ta-p/209905>

- (1) マネージメント IP の設定
- (2) ライセンス投入
- (3) シグネチャのダウンロードとインストール
- (4) OS アップグレード

5. L3 Firewall としての基本的な設定

本ガイドでは、インターネット・ゲートウェイとして設置済みの PA Firewall に GlobalProtect 機能を追加する、という状況を想定し、まずは PA Firewall が、基本的な L3 ルーティングが行える状態まで設定します。

5.1. ネットワーク設定

ネットワークに関わる設定を行います。

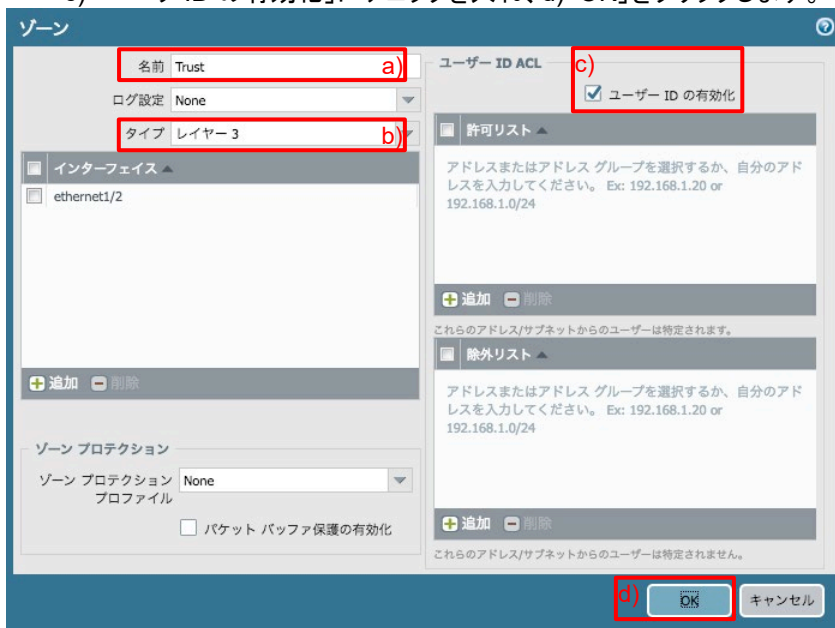
5.1.1. ゾーンの設定

Untrust (インターネット側) と Trust (社内 LAN 側)のゾーンを設定します。

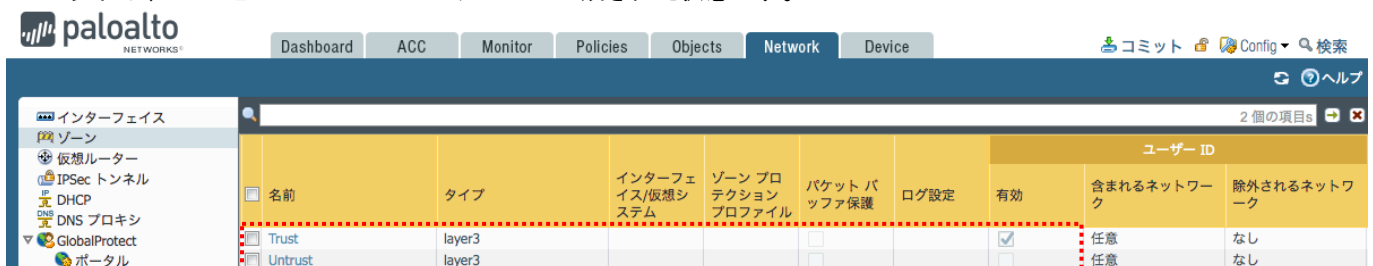
(1) a)「Network」 → b)「ゾーン」 → c)「追加」をクリックします。



(2) a)名前に「Trust」、b)タイプで「レイヤー3」を選択します。
c)「ユーザー ID の有効化」にチェックを入れ、d)「OK」をクリックします。



(3) 同様の方法で Untrust ゾーンも設定します。(ただし、Untrust は、ユーザーID は無効化のままでよいです。)
以下は、Trust と Untrust の 2 つのゾーンが生成された状態です。



5.1.2. Ethernet インターフェイスの設定

インターフェイスにゾーン、IP アドレス、仮想ルーターを割り当てます。

また、インターフェイスへの Ping 応答を許可するように、インターフェイス管理プロファイルの設定も合わせて行います。

(1) a)「Network」 → b)「インターフェイス」にて、「ethernet1/1」および「ethernet1/2」を、以下の c)のように設定します。

The screenshot shows the Palo Alto Networks configuration interface. The 'Network' tab is selected. In the left sidebar, 'インターフェイス' (Interfaces) is highlighted with a red box labeled 'b)'. The main content area shows a table of Ethernet interfaces. The table has columns: インターフェイス (Interface), インターフェイス タイプ (Interface Type), 管理プロファイル (Management Profile), リンク状態 (Link Status), IP アドレス (IP Address), 仮想ルーター (Virtual Router), タグ (Tag), VLAN / バーチャル ワイヤー (VLAN / Virtual Wire), and セキュリティ ゾーン (Security Zone). The first two rows, for 'ethernet1/1' and 'ethernet1/2', are highlighted with a red box labeled 'c)'. Both are configured with 'Layer3' type, 'IF-MGMT' profile, 'default' virtual router, and 'Trust' security zone.

インターフェイス	インターフェイス タイプ	管理プロファイル	リンク状態	IP アドレス	仮想ルーター	タグ	VLAN / バーチャル ワイヤー	セキュリティ ゾーン
ethernet1/1	Layer3	IF-MGMT		10.9.1.4/24	default	Untagged	none	Untrust
ethernet1/2	Layer3	IF-MGMT		10.9.2.4/24	default	Untagged	none	Trust
ethernet1/3				none	none	Untagged	none	none

(2) インターフェイス管理プロファイル: a)「IF-MGMT」は、b)Ping のみ許可します。

The screenshot shows the 'Interface Management Profile' configuration window for 'IF-MGMT'. The name field is highlighted with a red box labeled 'a)'. Under 'Management Services Management', 'HTTP', 'HTTPS', 'Temperature', and 'SSH' are unchecked. Under 'Network Services', 'Ping' is checked with a red box labeled 'b)', while 'HTTP OCSP', 'SNMP', 'Response Page', 'User ID', 'User ID Syslog Listener SSL', and 'User ID Syslog Listener UDP' are unchecked. The 'Access Allowed IP Address' field is empty. The window has 'OK' and 'キャンセル' (Cancel) buttons at the bottom.

5.1.3. 仮想ルーターの設定

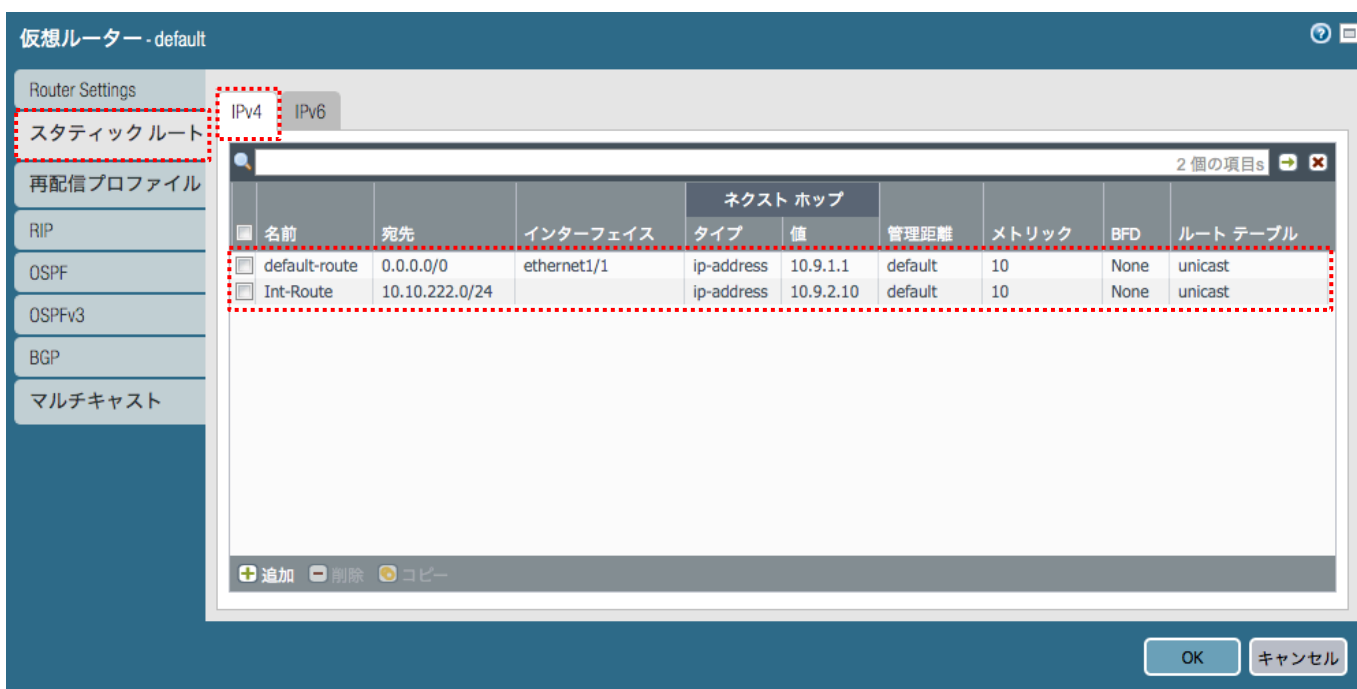
仮想ルーターに、デフォルトルートを設定します。

加えて、社内 LAN-B へのスタティックルートも設定します。

(1) a)「Network」 → b)「仮想ルーター」 → c)「default」をクリックします。



(2) 「スタティックルート」タブ → 「IPv4」タブで、以下のように 2 つのルートを設定します。



5.2. ポリシーの設定

Trust ゾーンのクライアント PC が、インターネットにアクセスするためのポリシーを設定します。

5.2.1. セキュリティポリシー

簡易的に、Trust から Untrust は全て許可する設定にしておきます。

(1) a)「Policies」 → b)「セキュリティ」 → c)「追加」をクリックします。



(2) a) 以下のように、Trust→Untrust 方向への全許可ポリシーを追加します。

名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	送信元	宛先	アプリケーション	サービス	アクション
1 outbound	none	universal	Trust	any	any	any	Untrust	any	any	any	許可 a)
5 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	許可
6 interzone-default	none	interzone	any	any	any	any	any	any	any	any	拒否

5.2.2. NAT ポリシー

Trust 発のパケットの送信元 IP アドレスを、eth1/1 の IP アドレスに変換する NAT ポリシーを設定します。

eth1/1 の IP アドレスは、Azure の Public IP と 1 対 1 で紐付けられているので、この設定によって、送信元は Global IP アドレスに変換されます。

(1) a)「Policies」 → b)「NAT」 → c)「追加」をクリックします。



(2) a) 以下のように、Trust→Untrust 方向への送信元 NAT ポリシーを追加します。

名前	タグ	送信元ゾーン	宛先ゾーン	宛先インターフェイス	送信元アドレス	宛先アドレス	サービス	送信元変換	宛先変換
1 outbound	none	Trust	Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1 10.9.1.4/24	なし a)

(3) 「コミット」を実施します。

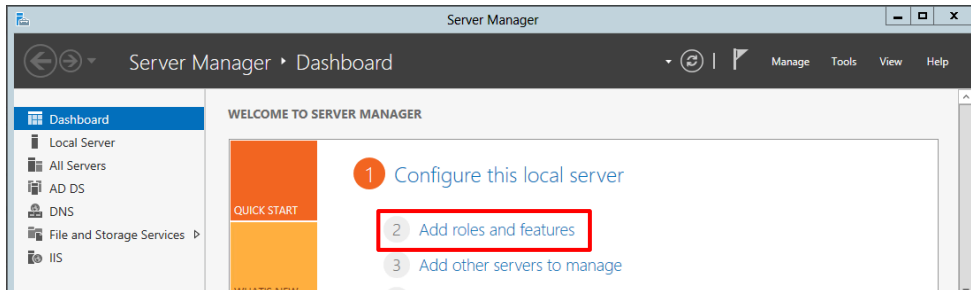
L3 Firewall としての基本的な設定は以上です。

6. Active Directory Domain Services の設定

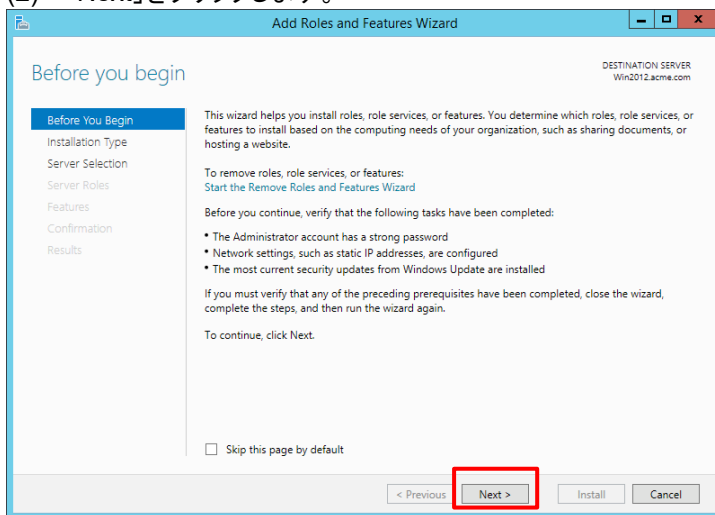
本ガイドでは、Win2012 に Active Directory Domain Services (以降、ADDS)を認証サーバーとして利用しますので、その設定を行います。

6.1. ADDS と DNS Server のインストール

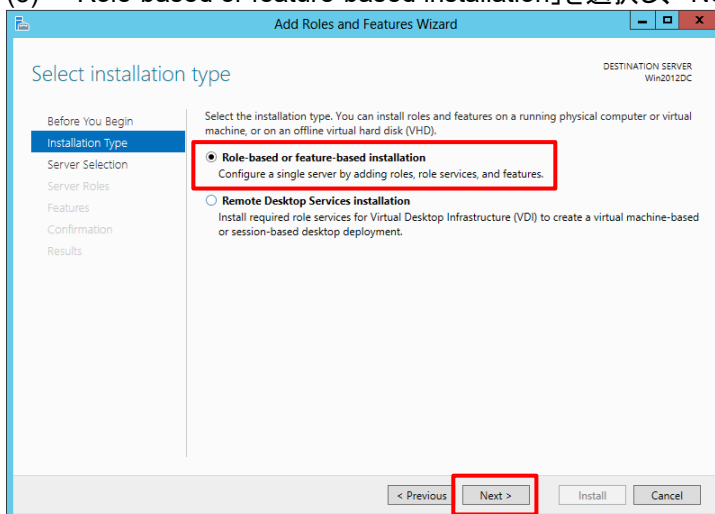
(1) Server Manager で、「Add roles and features」をクリックします。



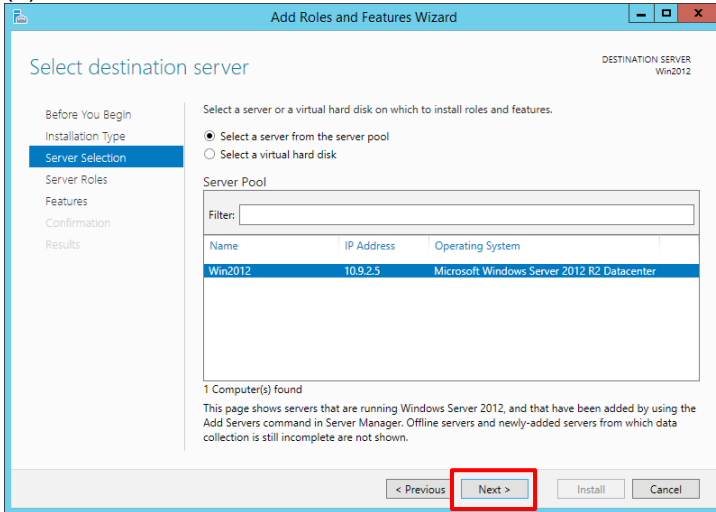
(2) 「Next」をクリックします。



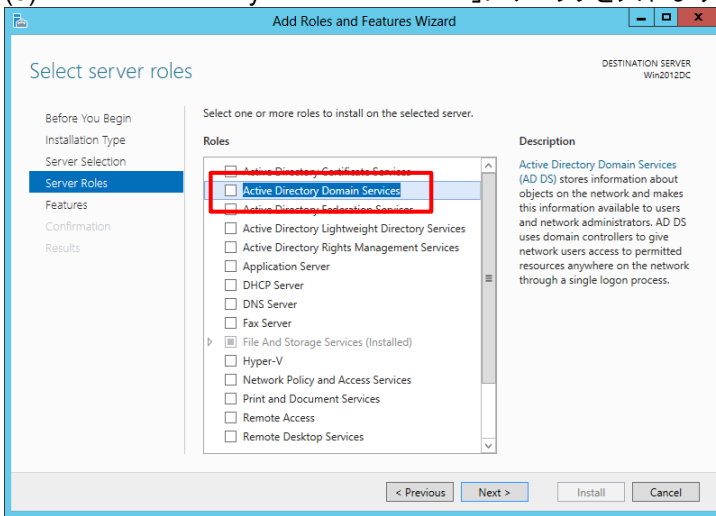
(3) 「Role-based or feature-based installation」を選択し、「Next」をクリックします。



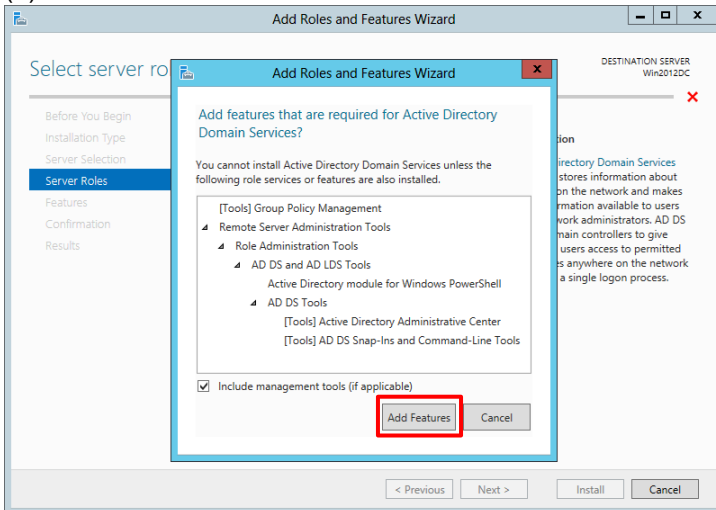
(4) 「Next」をクリックします。



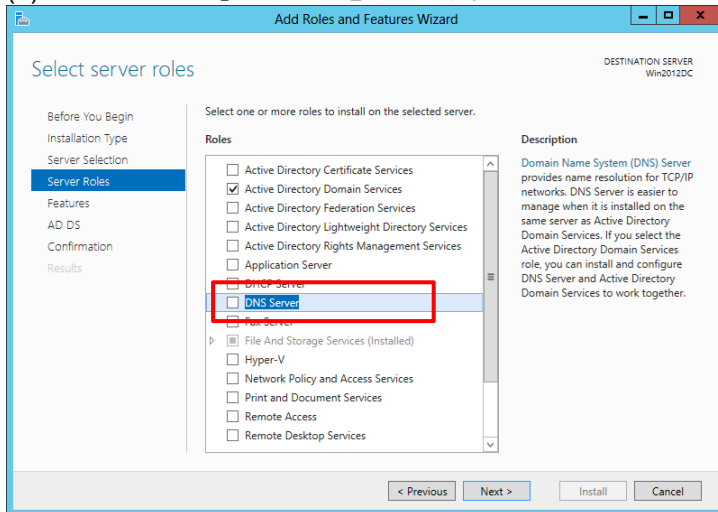
(5) 「Active Directory Domain Services」にチェックを入れます。



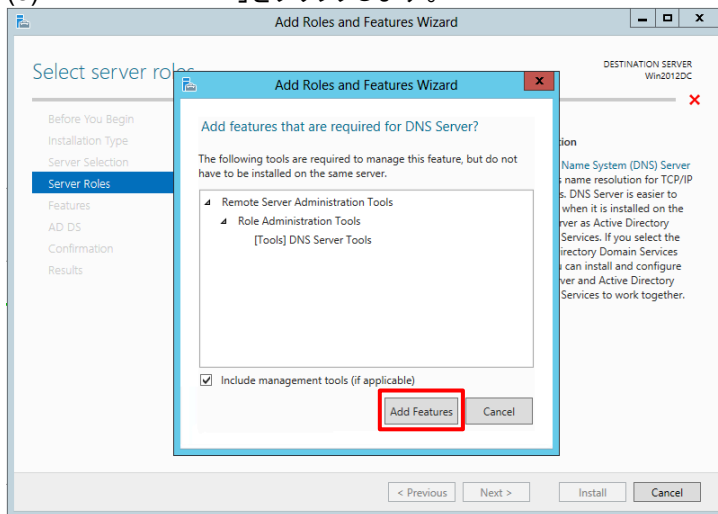
(6) 「Add Features」をクリックします。



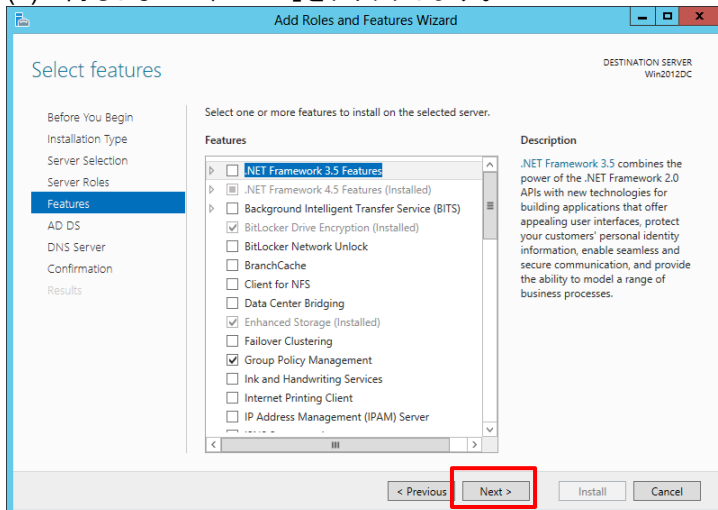
(7) 「DNS Server」にチェックを入れます。



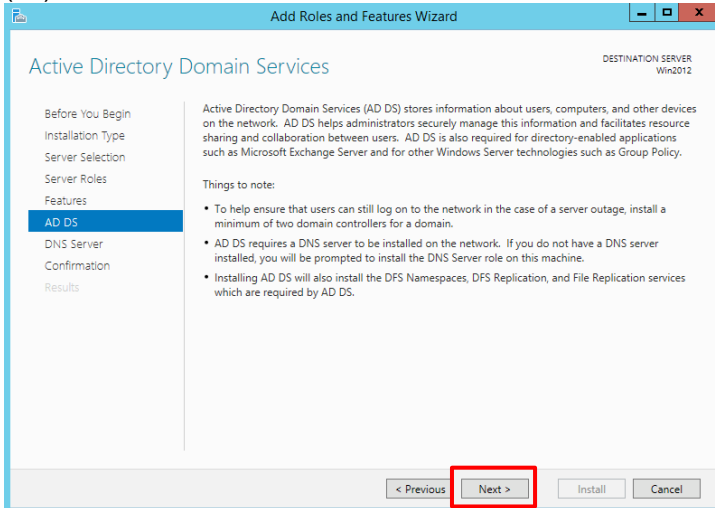
(8) 「Add Features」をクリックします。



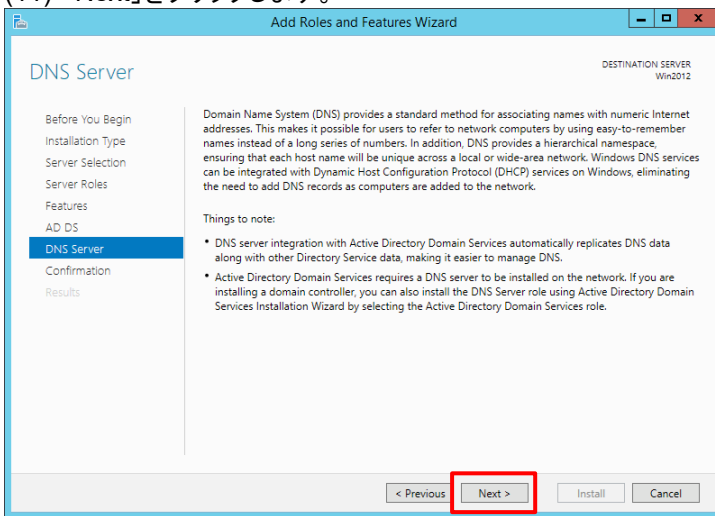
(9) 何もしないで、「Next」をクリックします。



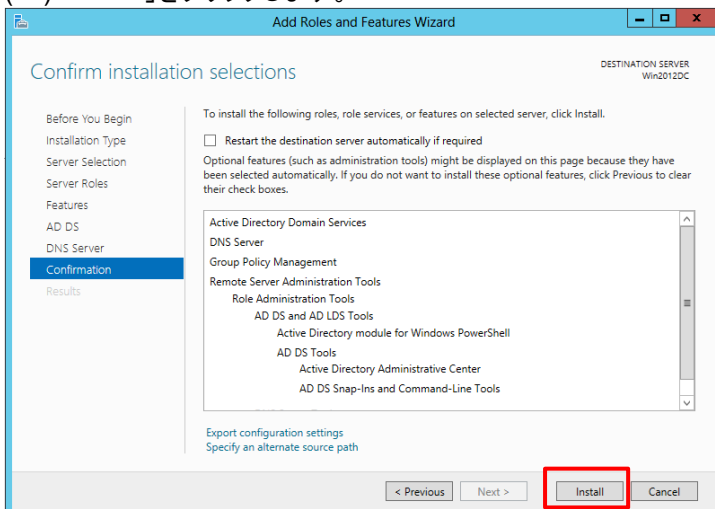
(10) 「Next」をクリックします。



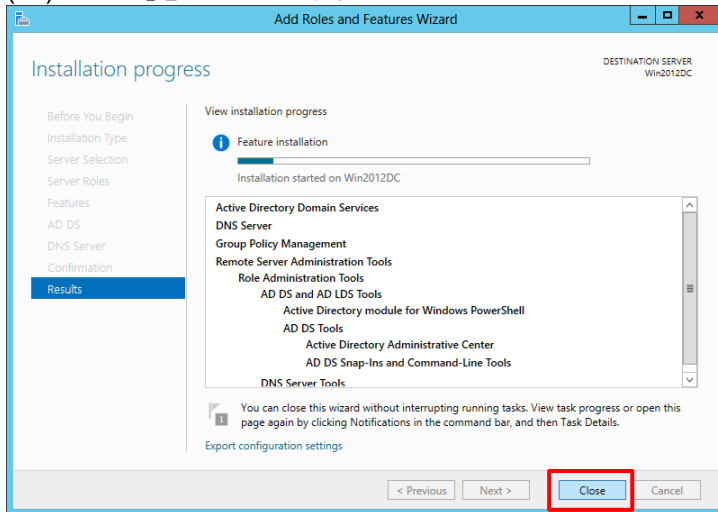
(11) 「Next」をクリックします。



(12) 「Install」をクリックします。



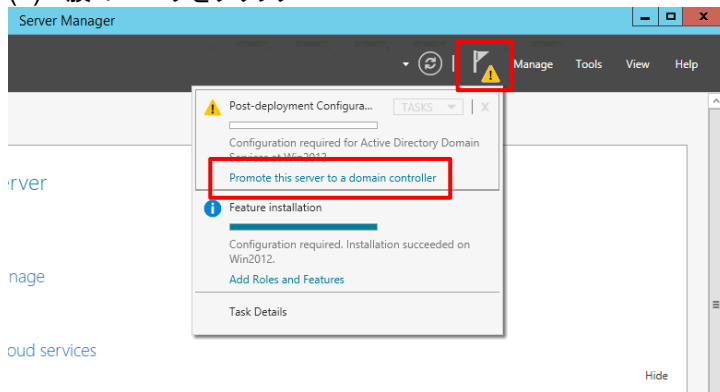
(13) 「Close」をクリックします。



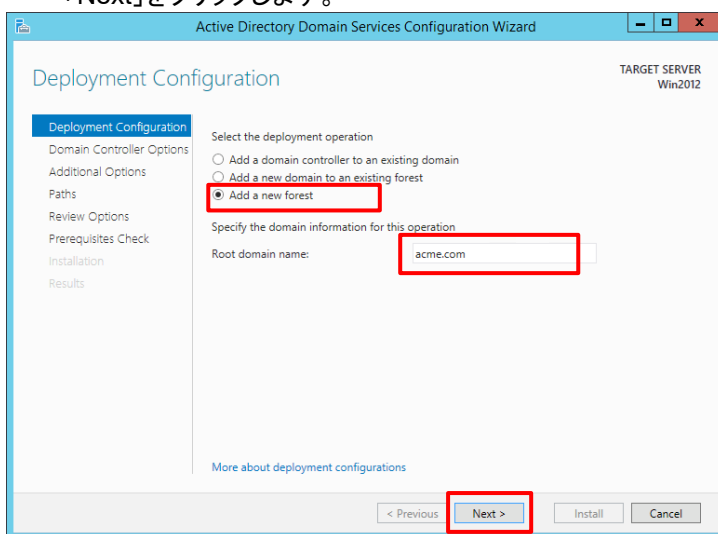
6.2. ADDS の設定

ドメイン名は「acme.com」として設定していきます。

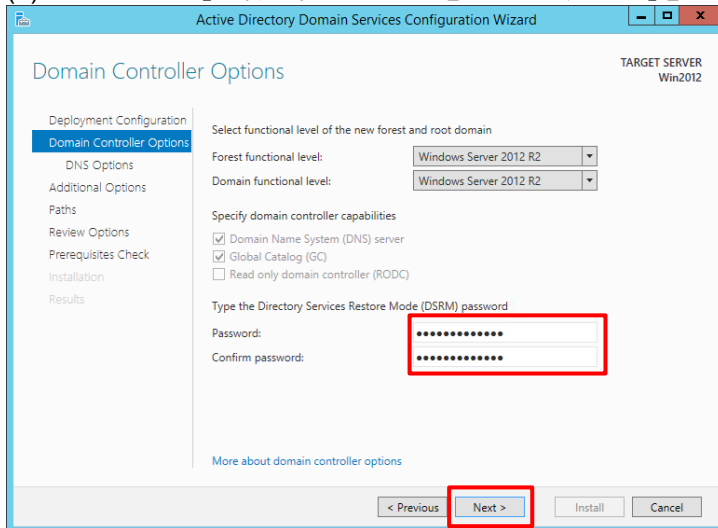
(1) 旗のマークをクリック → 「Promote this server to a domain controller」をクリックします。



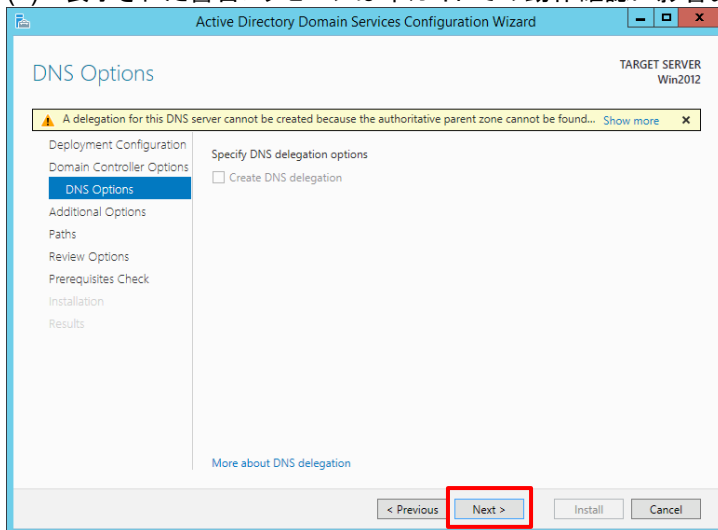
(2) 「Add a new forest」を選択して、「Root domain name:」に、「acme.com(任意)」と入力します。「Next」をクリックします。



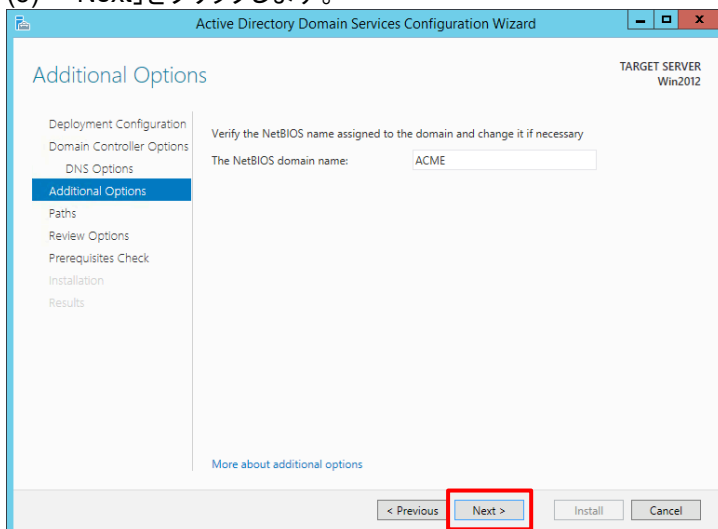
(3) 「Password:」に管理者パスワードを入力して、「Next」をクリックします。



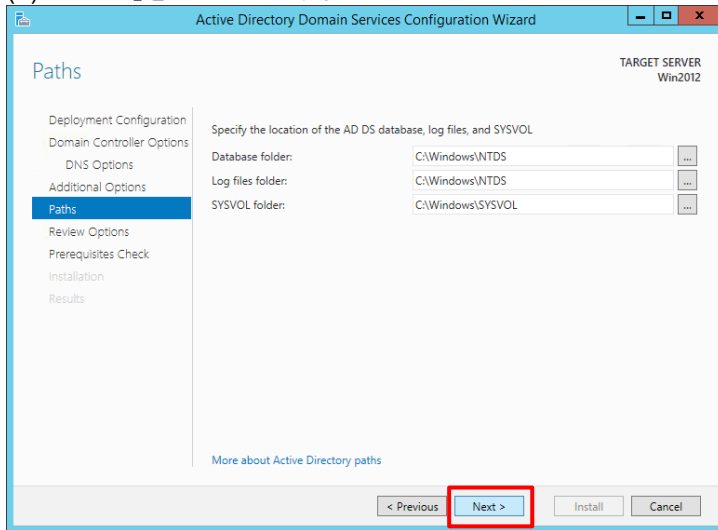
(4) 表示された警告メッセージは本ガイドでの動作確認に影響ありませんので、「Next」をクリックします。



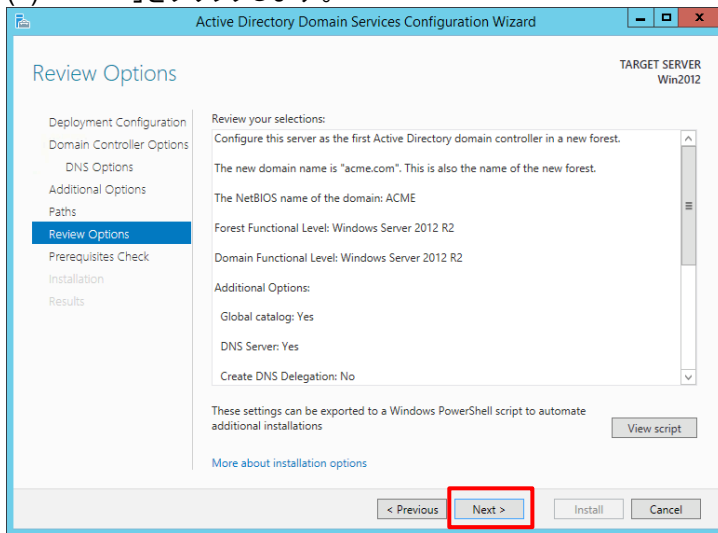
(5) 「Next」をクリックします。



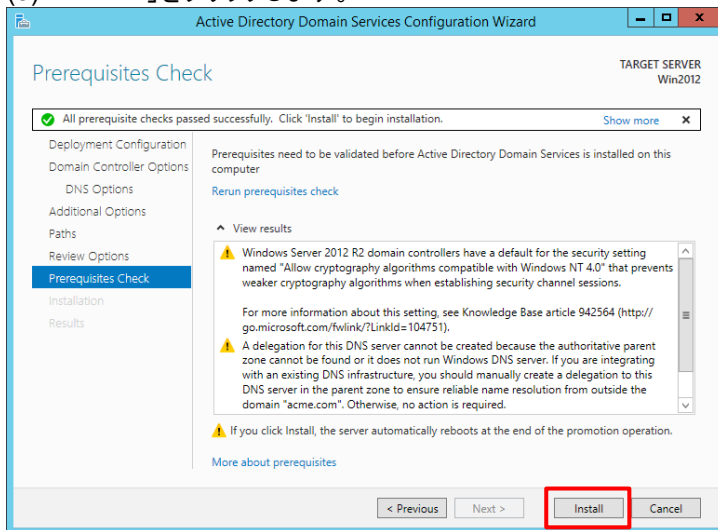
(6) 「Next」をクリックします。



(7) 「Next」をクリックします。



(8) 「Install」をクリックします。

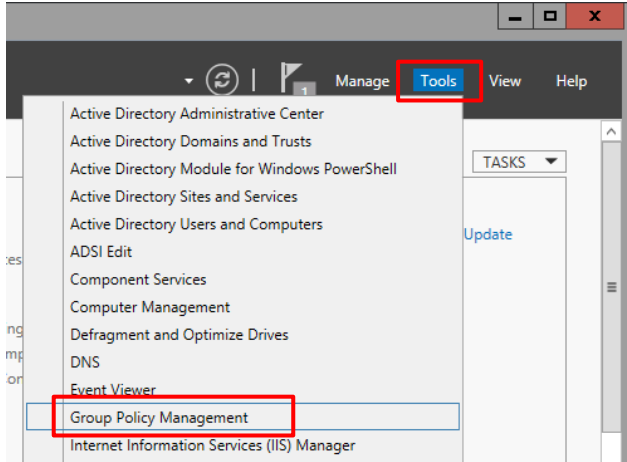


(9) インストール後、自動的に再起動が行われます。

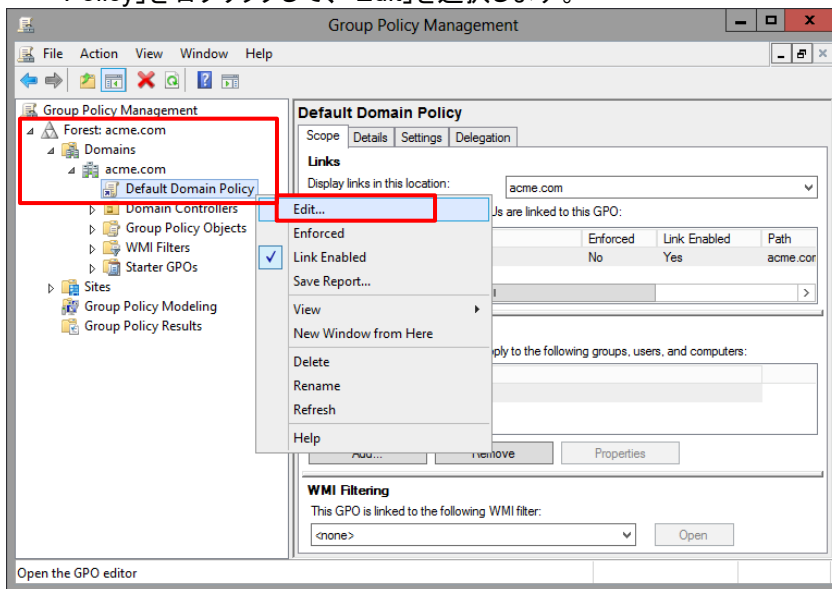
6.3. [参考]パスワードの複雑さの変更

検証環境においては、Active Directory ユーザのデフォルトパスワードポリシーが複雑すぎて、検証しづらい場合があります。その場合は、以下のステップで、変更できます。

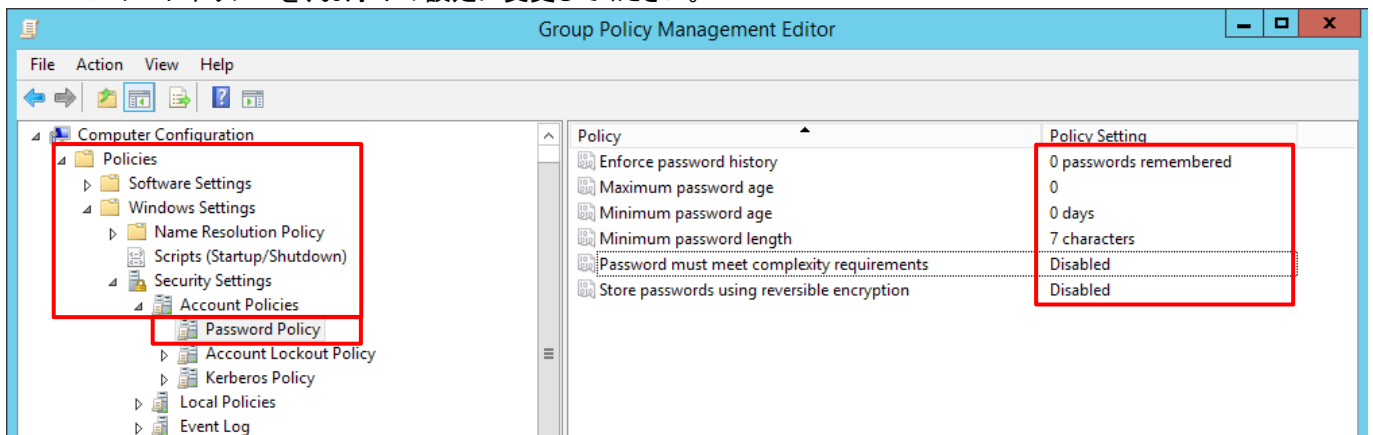
(1) 「Server Manager」の右上にある「Tools」 → 「Group Policy Management」を選択します。



(2) 「Group Policy Management」の下に「Forest: acme.com」→「Domains」→「acme.com」→「Default Domain Policy」を右クリックして、「Edit」を選択します。



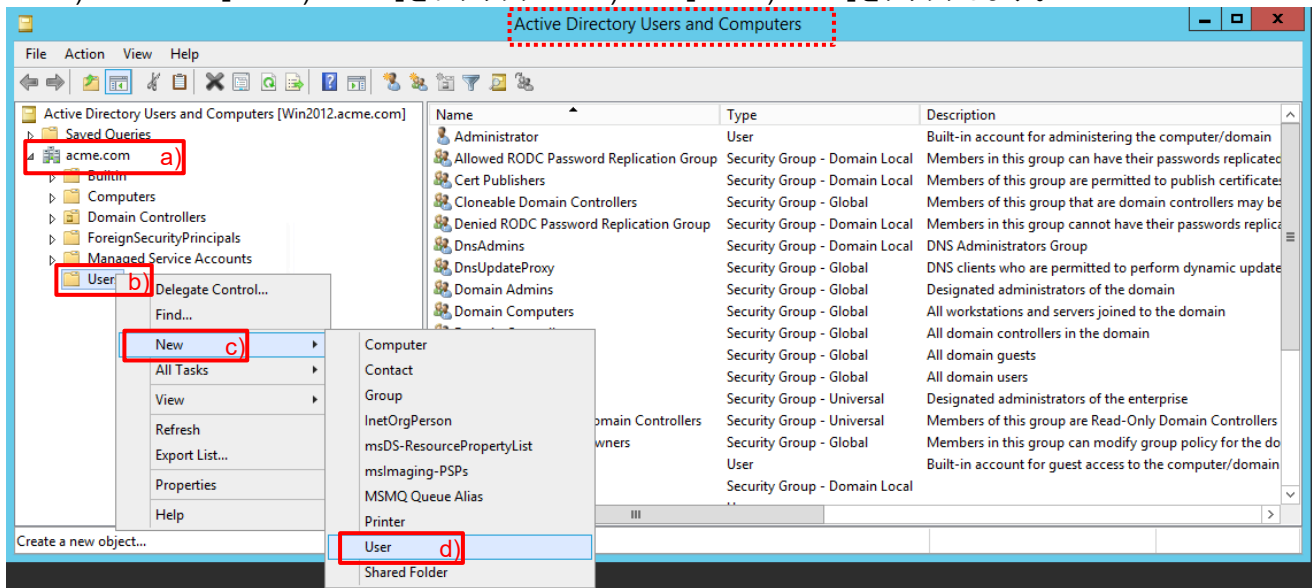
(3) 「Policies」→「Windows Settings」→「Security Settings」→「Account Policies」→「Password Policy」で表示されたパスワードポリシーを、お好みの設定に変更してください。



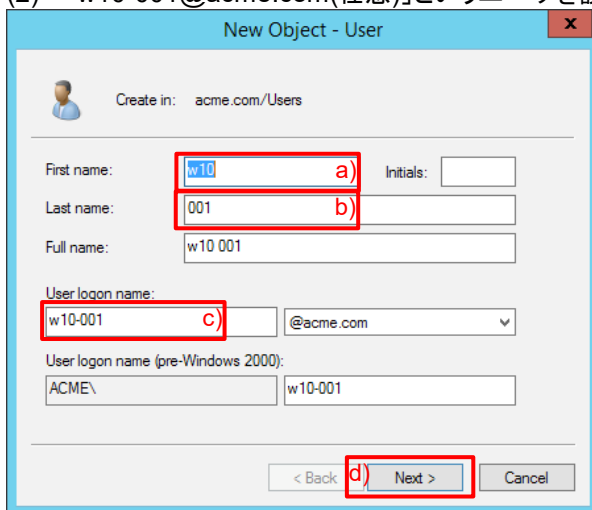
6.4. Active Directory ユーザーの作成

本ガイドのクライアント PC × 4 台分の AD ユーザーを登録します。

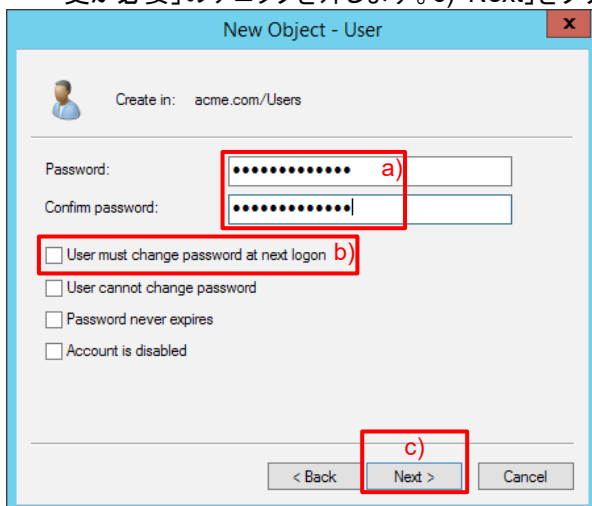
- (1) Win2012 の「Administrative Tools」 → 「Active Directory Users and Computers」を開きます。
a)「acme.com」 → b)「Users」を右クリック → c)「New」 → d)「User」をクリックします。



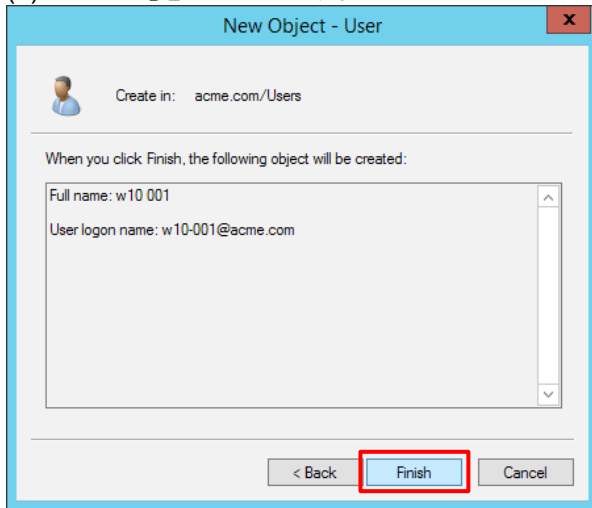
- (2) 「w10-001@acme.com(任意)」というユーザを設定します。



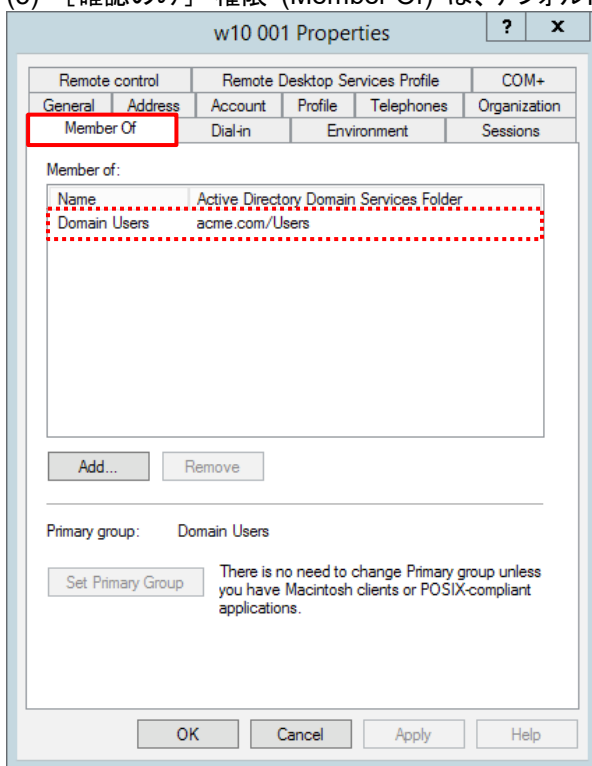
- (3) a)パスワードを入力し、b)「User must change password ad next login/ユーザーは次回ログイン時にパスワードの変更が必要」のチェックを外します。c)「Next」をクリックします。



(4) 「Finish」をクリックします。



(5) [確認のみ] 権限 (Member Of) は、デフォルトの「Domain Users」のままで OK です。



(6) 同様の方法で、後 3 つのユーザーを登録＝合計 4 つのユーザー登録を行います。

- ① w10-001
- ② w10-002
- ③ w10-003
- ④ w10-004

7. GlobalProtect の基本的な設定

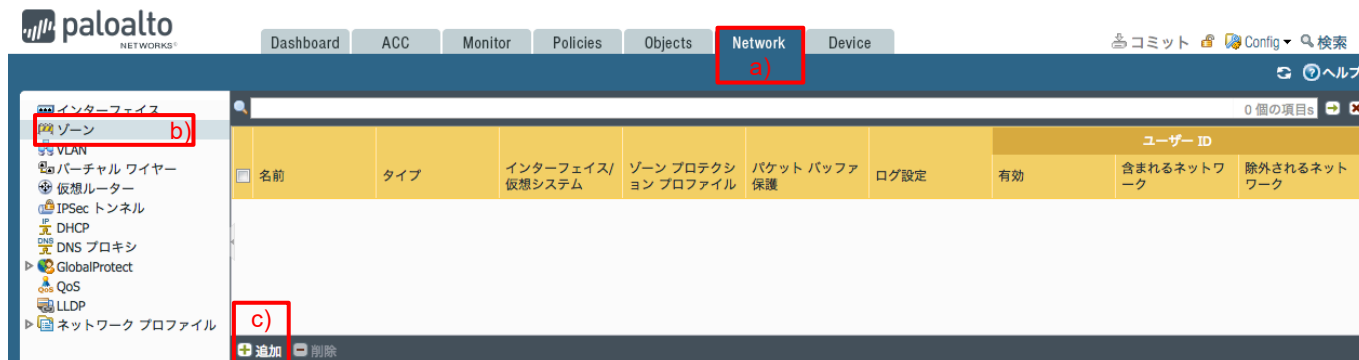
7.1. ネットワーク設定

7.1.1. ゾーンの設定

PA Firewall に Corp-VPN ゾーンを新しく追加し、GlobalProtect Agent が VPN 接続すると、そのトンネルインターフェイスが Corp-VPN ゾーンに割り当てられるようにします。

Trust ゾーンを利用することもできますが、制御のしやすさの観点から、VPN 用のゾーンを生成することを推奨します。

(1) a)「Network」 → b)「ゾーン」 → c)「追加」をクリックします。



(2) 表示された画面で、a)名前に「Corp-VPN」、b) タイプで「レイヤー3」を選択します。
c)「ユーザーIDの有効化」にチェックを入れ、d)「OK」をクリックします。



(3) [確認のみ] 以下は、Corp-VPN ゾーンが追加された状態です。



7.1.2. トンネルインターフェイスの設定

GP Agent が外部から VPN 接続するためのトンネルインターフェイスを設定し、それを Corp-VPN ゾーンに割り当てます。

複数の Agent が VPN 接続する場合でも、トンネルインターフェイスは一つだけでよいです。

(1) a)「Network」 → b)「インターフェイス」 → c)「トンネル」タブ → d)「追加」をクリックします。



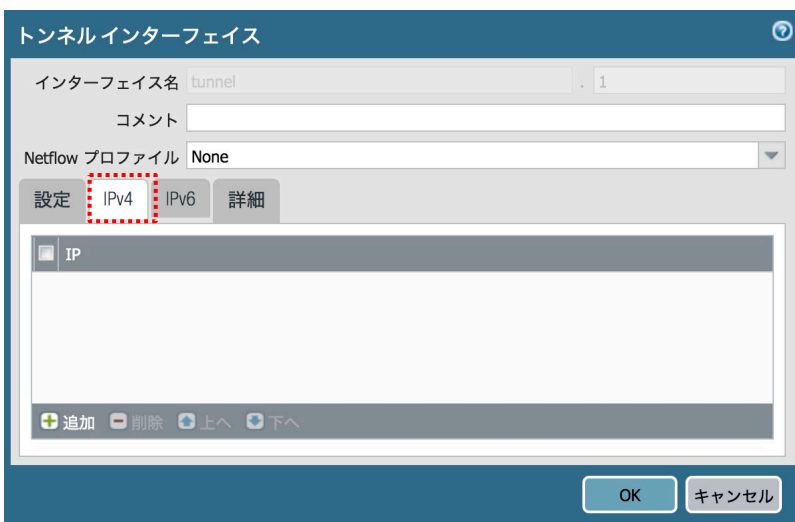
(2) a) インターフェイス名の末尾に、「1」(任意)を入力します。
まず、b)「設定」タブ内の設定を行います。

c) 仮想ルーターで「default」を選択します。

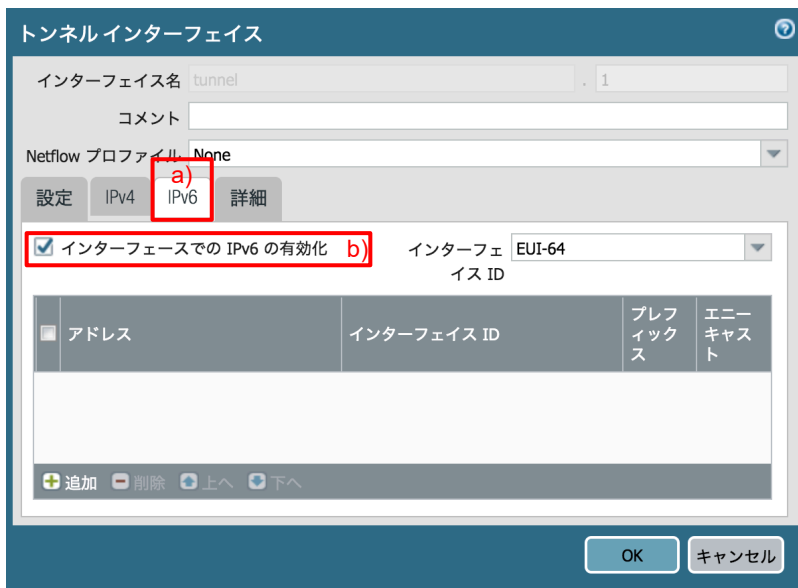
d) セキュリティゾーンは「Corp-VPN」を選択します。



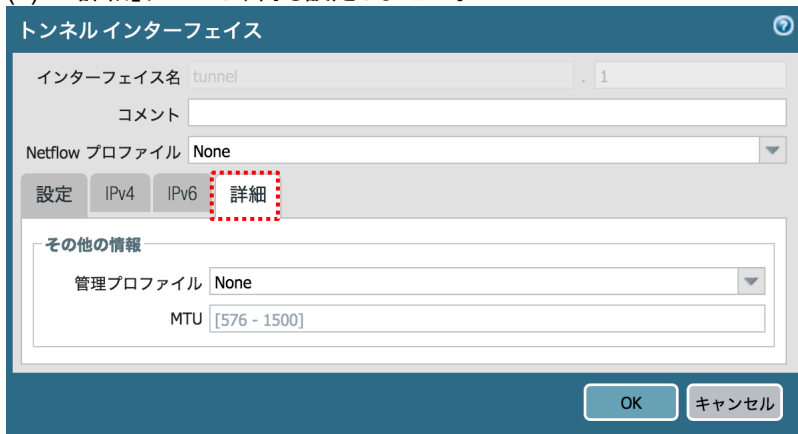
(3) 「IPv4」タブでは、何も設定しません。



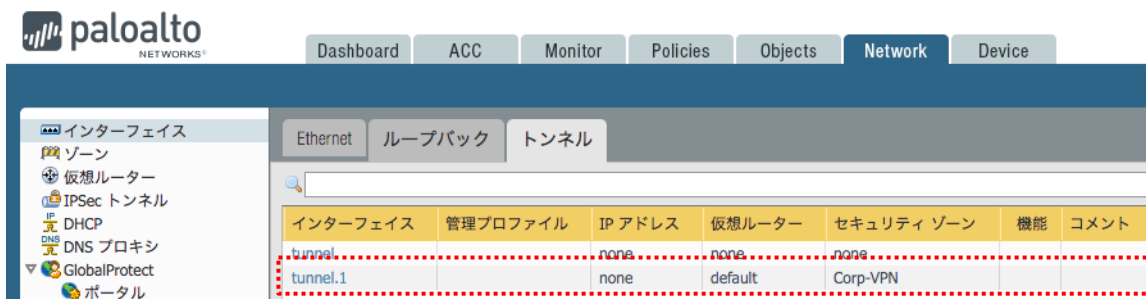
- (4) a)「IPv6」タブでは、b)「インターフェイスでの IPv6 有効化」にチェックを入れます。
 (コミット時の Warning メッセージを回避するためだけの目的であり、本ガイドでは IPv6 は使いません。)



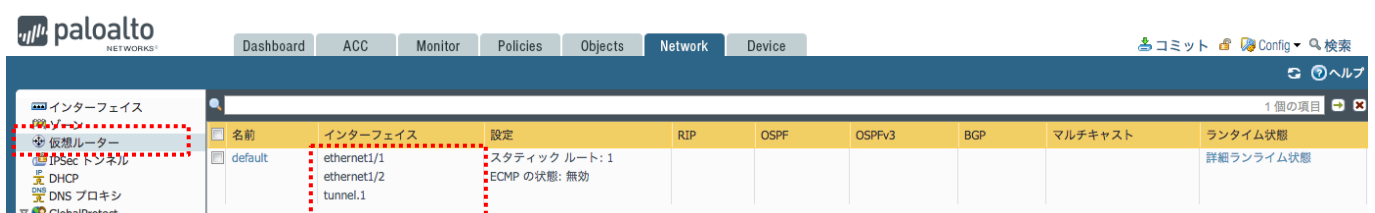
- (5) 「詳細」タブでは、何も設定しません。



- (6) 以下は、トンネルインターフェイスが一つ生成された状態です。



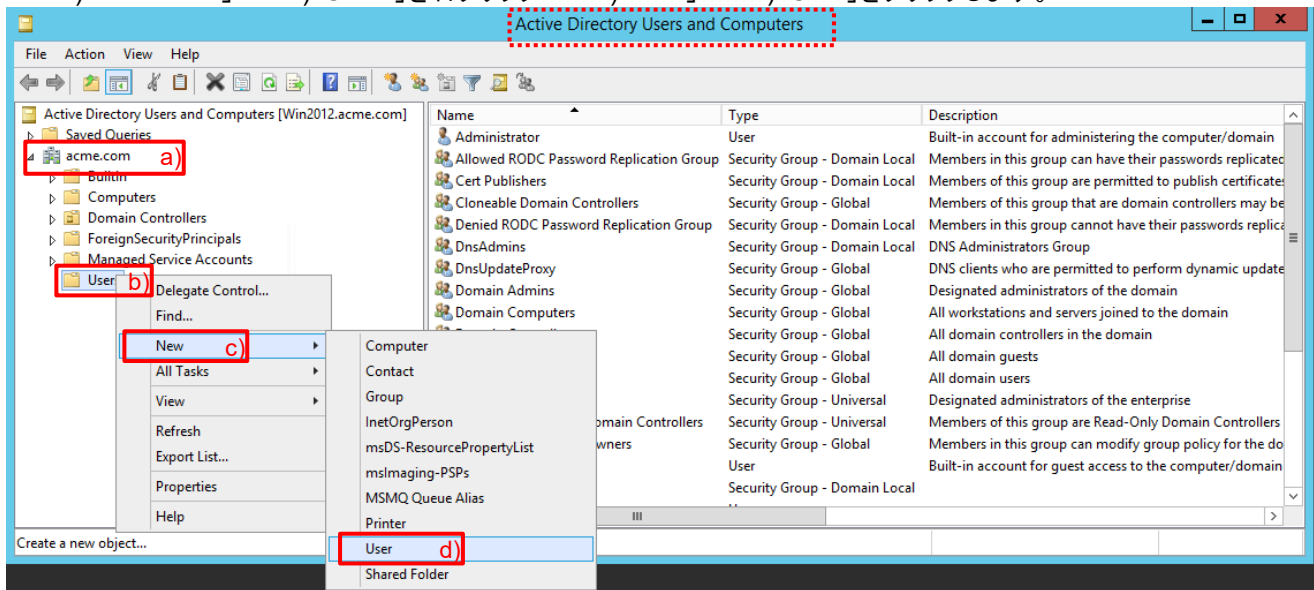
- (7) [確認のみ] 仮想ルーターにトンネルインターフェイスが加わります。
 このことで、VPN 接続したクライアントのインターフェイスが仮想ルーターのインターフェイスとなり、Trust や Untrust ゾーンとのルーティングが可能になります。



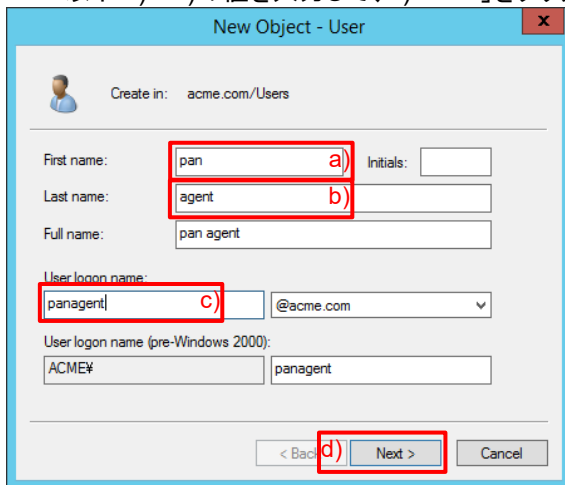
7.1.3. Active Directory への BIND 用ユーザーの設定

PA Firewall が Active Directory からユーザー情報を取得するためのアカウントを、1つ生成します。

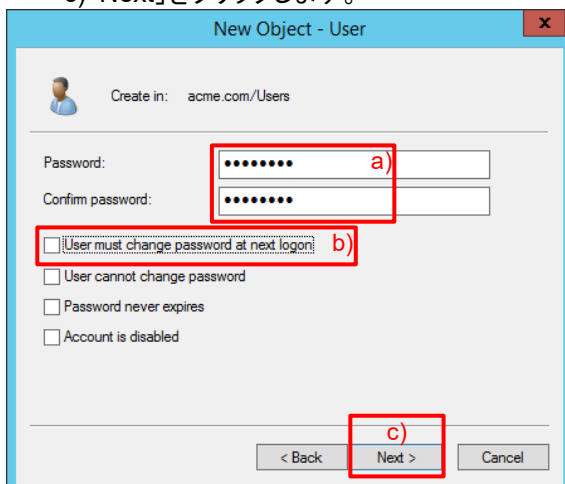
- (1) Win2012 の「Administrative Tools」 → 「Active Directory Users and Computers」を開きます。
a)「acme.com」 → b)「Users」を右クリック → c)「New」 → d)「User」をクリックします。



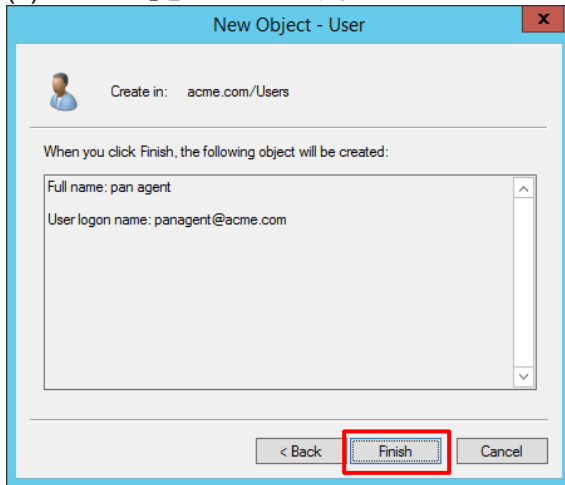
- (2) 「panagent@acme.com(任意)」というユーザーを生成します。
以下 a)~c)の値を入力して、d)「Next」をクリックします。



- (3) a)パスワードを入力し、b)「User must change password at next login」のチェックを外します。
c)「Next」をクリックします。

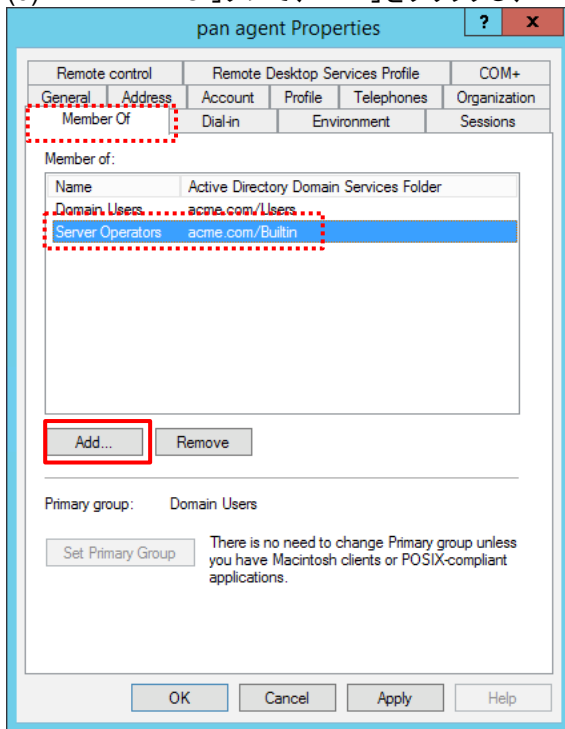


(4) 「Finish」をクリックします。



(5) 設定した panagent ユーザーを開きます。

(6) 「Member Of」タブで、「Add」をクリックし、「Server Operators」を追加します。



7.2. ユーザー認証の設定

PA Firewall が、Win2012 を認証サーバーとして利用できるように設定します。


7.2.1. サービスルートおよび DNS の設定

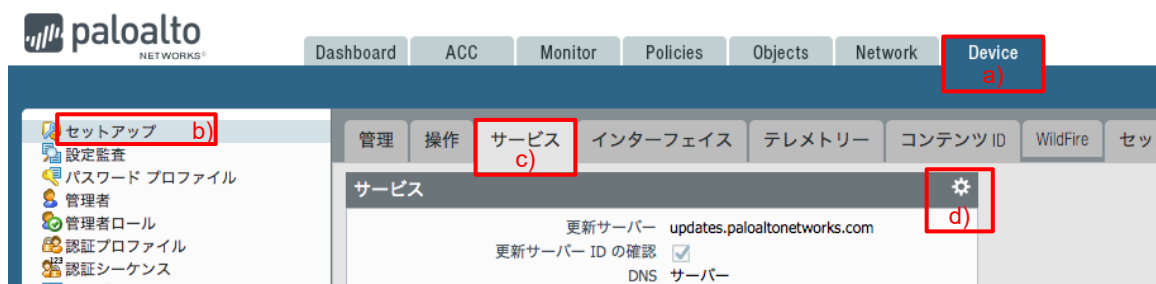
PA Firewall デフォルト状態では、DNS および LDAP の参照先はマネージメントインターフェイス側になっています。

本ガイドの構成では、Win2012 は Trust ゾーン(eth1/2)側に設置されているので、その方向に DNS と LDAP の参照先を変更します。

7.2.1.1. DNS サーバーの参照設定

まず、PA Firewall が参照する DNS サーバーを、Win2012 に設定します。

(1) a)「Device」 → b)「セットアップ」 → c)「サービス」 で表示された「サービス」の d)  をクリックします。



(2) a)「プライマリ DNS サーバー」に、Win2012 の IP アドレスを設定します。
b) 「OK」をクリックします。



7.2.1.2. サービスルートの設定

PA Firewall の LDAP と DNS のサービスルートを eth1/2 へ変更します。

- (1) a)「Device」 → b)「セットアップ」 → c)「サービス」 → d)「サービスルートの設定」で表示された画面で、e)のように、DNS および LDAP の送信元インターフェイスおよび送信元アドレスを eth1/2 に変更します。
f)「OK」をクリックします。

The screenshot shows the Palo Alto Networks management console. The 'Device' tab is selected (a). In the left sidebar, 'Setup' (b) is highlighted. The 'Services' section is active (c). The 'Service Route Settings' dialog box (d) is open, showing a table of service routes. The 'DNS' and 'LDAP' rows are selected, and their 'Source Interface' and 'Source Address' are set to 'ethernet1/2' and '10.9.2.4/24' respectively (e). The 'OK' button is highlighted (f).

サービス	送信元インターフェイス	送信元アドレス
<input type="checkbox"/> AutoFocus	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> CRL Status	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Panorama のプッシュさ	デフォルトを使用	デフォルトを使用
<input checked="" type="checkbox"/> DNS	ethernet1/2	10.9.2.4/24
<input type="checkbox"/> 外部ダイナミック リス	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> 電子メール	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> HSM	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> HTTP	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Kerberos	デフォルトを使用	デフォルトを使用
<input checked="" type="checkbox"/> LDAP	ethernet1/2	10.9.2.4/24
<input type="checkbox"/> MDM	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Mfa	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Netflow	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> NTP	デフォルトを使用	デフォルトを使用

- (2) 「コミット」します。

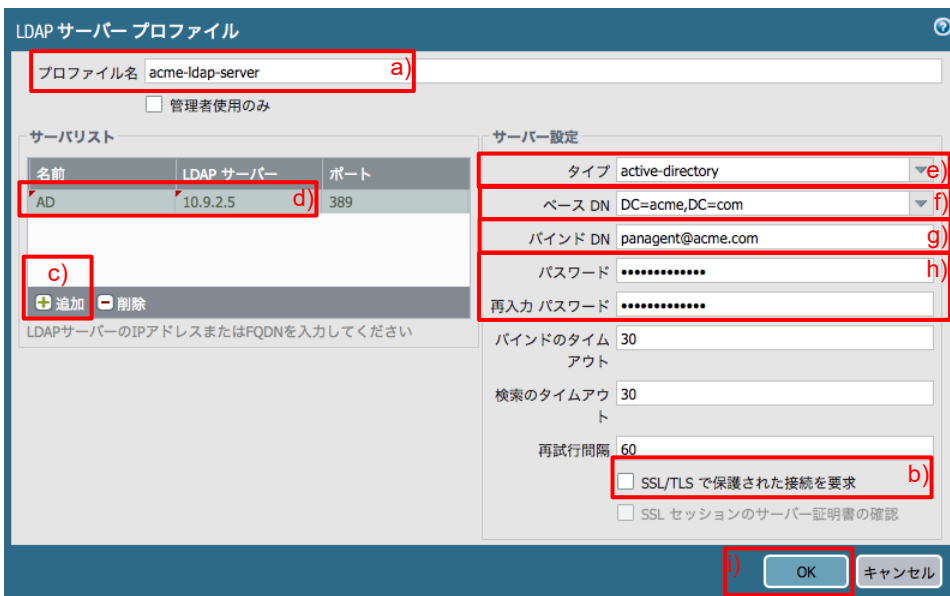
7.2.2. LDAP サーバーとの接続設定

認証サーバーとして利用する Active Directory (Win2012)との接続設定を行います。

(1) a)「Device」 → b)「LDAP」 → c)「追加」をクリックします。



(2) a)名前に「acme-ldap-server(任意)」と入力します。
b)「SSL/TLS で保護された接続を要求」のチェックを外します。(AD 側の設定に依存します。)
c)「追加」をクリックし、d)名前に「AD(任意)」、LDAP サーバーに「10.9.2.5」と入力します。
e)タイプで「active-directory」を選択し、f)ベース DN は「DC=acme,DC=com」を選択します。
(LDAP サーバーとの接続ができていなければ、ベース DN が取得できないので、選択できません。)
g)に AD 上で生成済みのユーザー「panagent@acme.com」、h)にそのパスワードを設定します。
i)「OK」をクリックします。



7.2.3. グループマッピングの設定

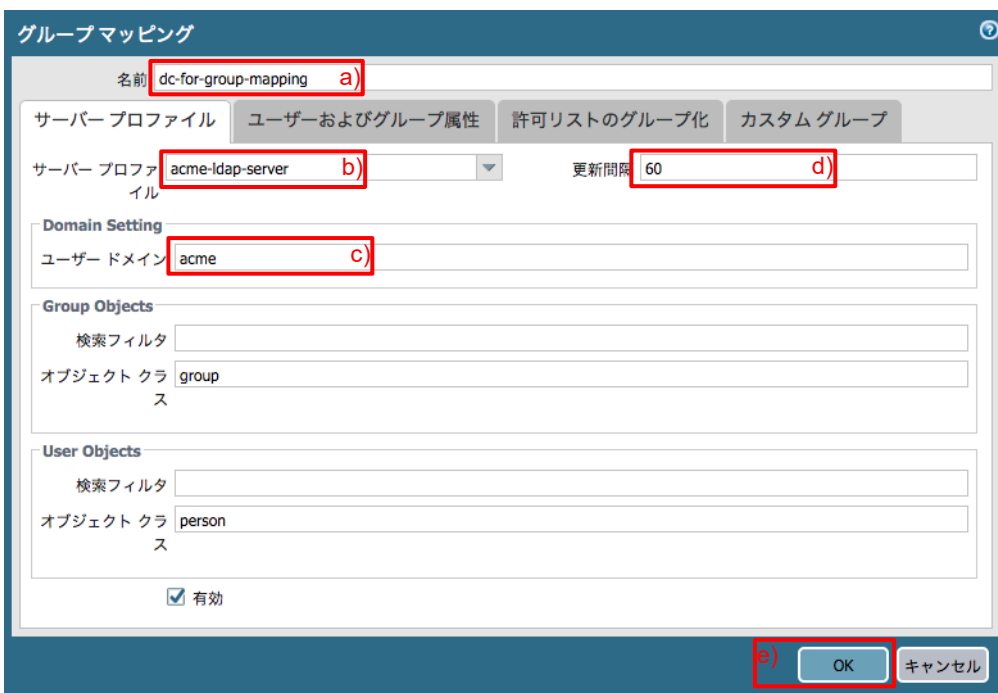
Active Directory (LDAP サーバー)から、ユーザーとグループのマッピング情報を取得します。

グループマッピングは、ある特定のグループだけ認証して VPN 接続させたい場合や、グループ単位のセキュリティポリシーを設定したい、という場合に必要となる設定です。

(1) a)「Device」 → b)「ユーザーID」 → c)「グループマッピング設定」 → d)「追加」をクリックします。

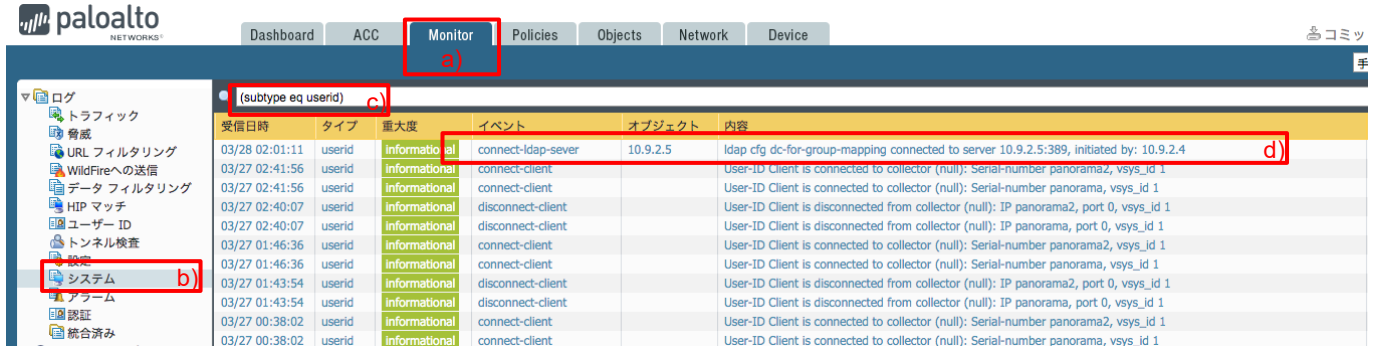


- (2) a) 名前に「dc-for-group-mapping(任意)」を入力します。
b) サーバープロファイルは設定済みの「acme-ldap-server」を選択します。
c) ドメインに「acme」を入力します。
d) LDAP との更新間隔のデフォルトは 3600 秒と長いので、検証用に最短の「60」秒にしておきます。(任意)
e) 「OK」をクリックします。

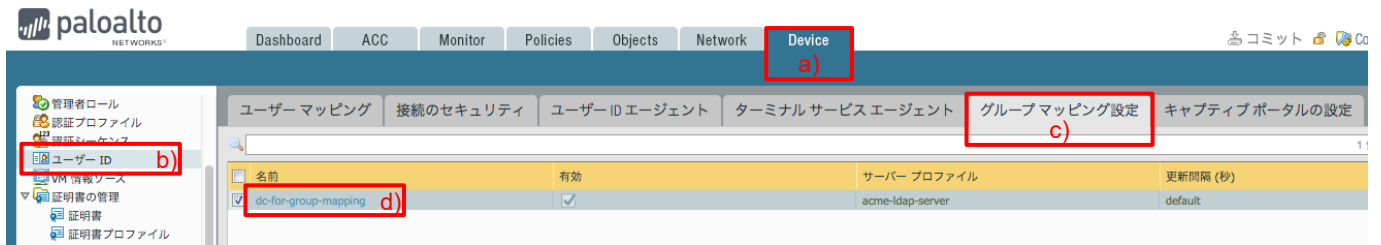


(3) 「コミット」を実施します。

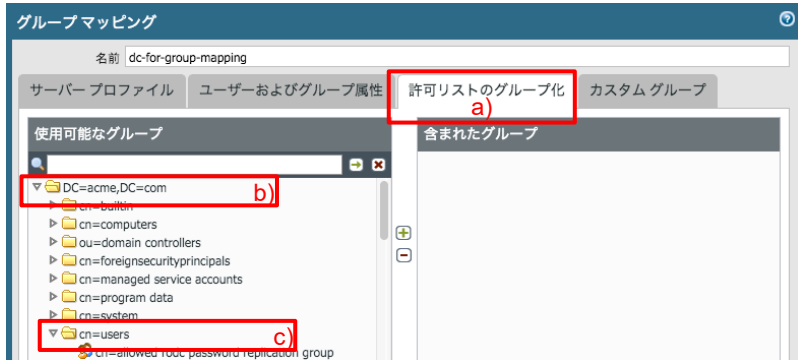
- (4) a)「Monitor」 → b)「システム」の c)検索フォームに「(subtype eq userid)」と入力します。
 d)のログが出力されていれば OK です。
 イベント:「connect-ldap-server」
 オブジェクト:「10.9.2.5」(AD(LDAP)サーバーの IP アドレス)
 内容:「ldap cfg dc-for-group-mapping connected to server 10.9.2.5:389, initiated by:10.9.2.4」
 (10.9.2.4: PA Firewall の eth1/2 の IP アドレス)




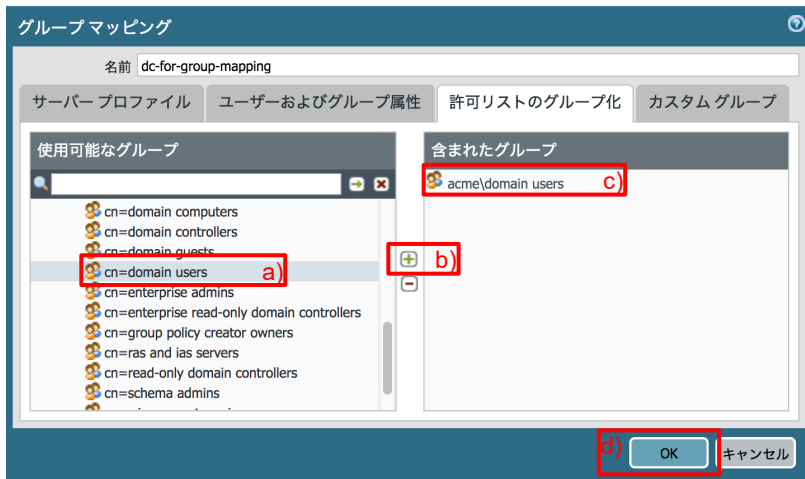
- (5) a)「Device」 → b)「ユーザーID」 → c)「グループマッピング設定」 → d)「dc-for-group-mapping」をクリックします。



- (6) a)「許可リストのグループ化」 → b)「DC=acme,DC=com」 → c)「cn=users」を展開します。



- (7) スクロールダウンして、a)「cn=domain users」を選択 → b)  をクリック → c)の状態にして、d)「OK」をクリックします。



- (8) 「コミット」を実施します。

- (9) [確認のみ] CLI で以下のコマンドを実行して、グループマッピング状態を確認できます。

```
admin-admin@PA-VM> show user group-mapping state all
```

```
Group Mapping(vsys1, type: active-directory): dc-for-group-mapping
  Bind DN      : panagent@acme.com
  Base        : DC=acme,DC=com
  Group Filter: (None)
  User Filter : (None)
  Servers     : configured 1 servers
                10.9.2.5(389)
                Last Action Time: 1733 secs ago(took 0 secs)
                Next Action Time: In 1867 secs
  Number of Groups: 1
  cn=domain users, cn=users, dc=acme, dc=com
```

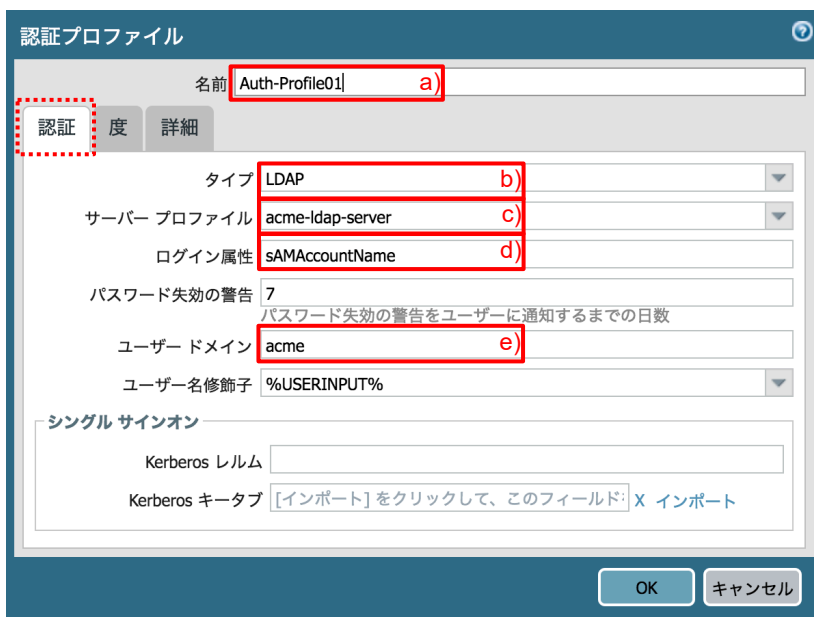
7.2.4. 認証プロファイルの設定

認証プロファイルを設定して、GlobalProtect Portal および Gateway が、Active Directory(=LDAP サーバー)をユーザー認証サーバーとして利用できるにします。

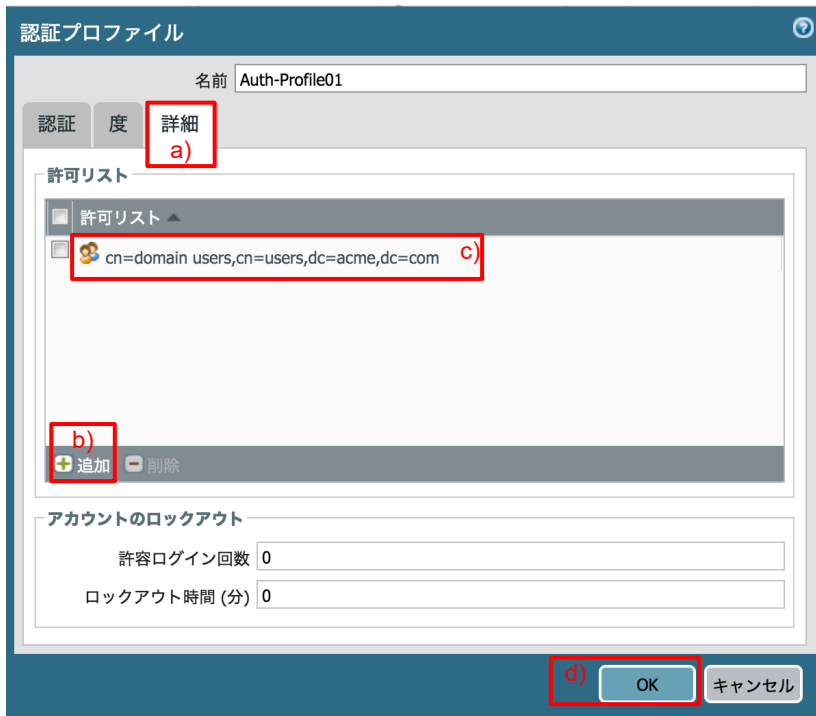
(1) a)「Device」 → b)「認証プロファイル」 → c)「追加」をクリックします。



(2) a)名前に「Auth-Profile01(任意)」を入力します。
「認証」タブで、
b)タイプは「LDAP」を選択します。
c)サーバープロファイルは設定済みの「acme-ldap-server」を選択します。
d)ログイン属性に「sAMAccountName」と入力します。
e)ドメインに「acme」と入力します。



- (3) a)「詳細」タブ → 許可リストの b)「追加」をクリックします。
- c)グループマッピングの「許可リストのグループ化」で指定したグループ「domain users」を選択します。
- d)「OK」をクリックします。



- (4) 「コミット」を実施します。

7.2.5. 認証テスト

認証プロファイルの設定が正しく動作するかを、CLI でテストできます。

- (1) ユーザーグループを確認します。

```
admin-admin@Azure-PA-VM> show user group list
```

```
cn=domain users, cn=users, dc=acme, dc=com
```

```
Total: 1
```

```
* : Custom Group
```

- (2) グループ内のユーザーを確認します。

```
admin-admin@Azure-PA-VM> show user group name "cn=domain users, cn=users, dc=acme, dc=com"
```

```
short name: acme¥domain users
```

```
source type: ldap
```

```
source: dc-for-group-mapping
```

```
[1 ] acme¥admin-admin
[2 ] acme¥panagent
[3 ] acme¥w10-001
[4 ] acme¥w10-002
[5 ] acme¥w10-003
[6 ] acme¥w10-004
```

(3) 試しに、acme¥w10-003 をテストしてみます。

```
admin-admin@Azure-PA-VM> test authentication authentication-profile Auth-Profile01 username acme¥w10-003 password
```

Enter password : (パスワードを入力します)

Target vsys is not specified, user "acme¥w10-003" is assumed to be configured with a shared auth profile.

Do allow list check before sending out authentication request...

user "acme¥w10-003" is a member of allowed group "cn=domain users,cn=users,dc=acme,dc=com" on vsys "vsys1"

Authentication to LDAP server at 10.9.2.5 for user "acme¥w10-003"

Egress: 10.9.2.4

Type of authentication: plaintext

Starting LDAP connection...

Succeeded to create a session with LDAP server

DN sent to LDAP server: CN=w10 003,CN=Users,DC=acme,DC=com

User expires in days: never

Authentication succeeded for user "acme¥w10-003" (←認証が成功したことを示しています。)

(4) [参考] グループマッピングのデフォルトの更新間隔は 3600 秒 = 1 時間です。

(本ガイドでは既述の設定で、60 秒に短縮しました。)

AD ユーザーを新しく追加したとき、即座にグループマッピングに反映させたい場合には、PA Firewall の以下のコマンドで、強制的に再読み込みする必要があります。

```
admin-admin@Azure-PA-VM> debug user-id refresh group-mapping all
```

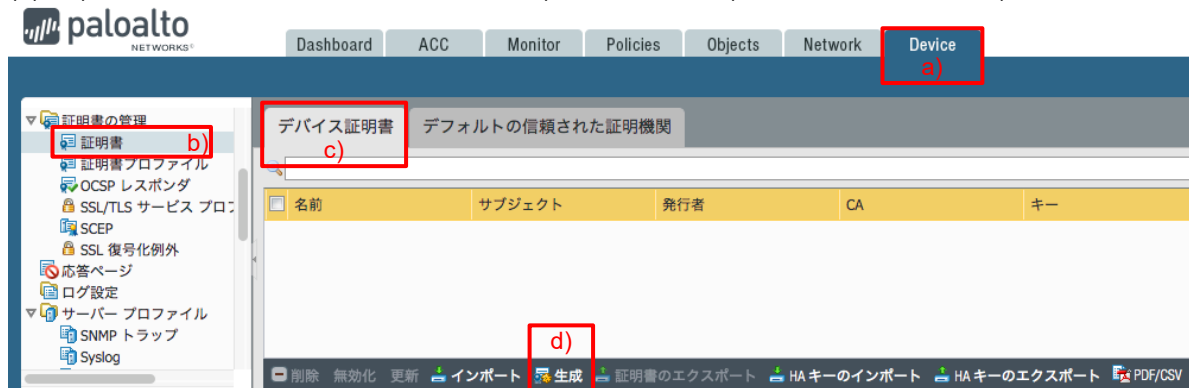
group mapping 'dc-for-group-mapping' in vsys1 is marked for refresh.

7.3. SSL 証明書の生成

GP Agent から Portal や Gateway への接続には HTTPS が使われるので、そのためには SSL 証明書が必要です。それらを PA Firewall 内で生成します。

7.3.1. 認証局証明書の生成

(1) a)「Device」 → 「証明書の管理」の下の b)「証明書」 → c)「デバイス証明書」→ d)「生成」をクリックします。



(2) a)証明書名に「PA-Certificate-Authority(任意)」と入力します。
b)共有名にも「PA-Certificate-Authority(任意)」と入力します。
c)認証局にチェックを入れます。
d)「生成」をクリックします。

The screenshot shows the '証明書の生成' (Generate Certificate) dialog box. The '証明書タイプ' (Certificate Type) is set to 'ローカル' (Local). The '証明書名' (Certificate Name) field contains 'PA-Certificate-Authority' and is labeled 'a)'. The '共通名' (Common Name) field also contains 'PA-Certificate-Authority' and is labeled 'b)'. The '署名者' (Issuer) dropdown menu is set to '認証局' (CA) and is labeled 'c)'. The 'OCSP レスポンダ' (OCSP Responder) field is empty. Under the '暗号設定' (Encryption Settings) section, 'アルゴリズム' (Algorithm) is set to 'RSA', 'ビット数' (Bit Length) is '2048', 'ダイジェスト' (Digest) is 'sha256', and '有効期限(日)' (Validity Period) is '365'. At the bottom, the '生成' (Generate) button is highlighted with a red box and labeled 'd)', and the 'キャンセル' (Cancel) button is also visible.

(3) 生成が成功したことを示すメッセージが出力されたら、「OK」をクリックします。

7.3.2. GlobalProtect 用のサーバー証明書の生成

生成した認証局証明書を使って、GlobalProtect Portal および Gateway に設定するサーバー証明書を生成します。

7.3.2.1. 外部用サーバー証明書の生成 (Portal と External Gateway 兼用)

本ガイドの構成では、Portal と External Gateway で同じ IP アドレスを共有するので、サーバー証明書も共有することにし、外部用に 1 つだけサーバー証明書を生成します。(それぞれ、別々のサーバー証明書を発行しても問題ありません。)

- (1) a) 証明書名に「External-Gateway(任意)」と入力します。
- b) 共有名は、ネットワーク構成に従い、「gp011.japaneast.cloudapp.azure.com」と入力します。
- c) 署名者は生成した認証局「PA-Certificate-Authority」を選択します。
- d) 「追加」をクリックして、e)「Host Name」を選択し、「gp011.japaneast.cloudapp.azure.com」を入力します。
- f) 「生成」をクリックします。

証明書の生成

証明書タイプ ローカル SCEP

証明書名 External-Gateway a)

共通名 gp011.japaneast.cloudapp.azure.com b)

署名者 PA-Certificate-Authority c)

認証局

OCSP レスポンダ

暗号設定

アルゴリズム RSA

ビット数 2048

ダイジェスト sha256

有効期限 (日) 365

証明書の属性

タイプ	値
<input checked="" type="checkbox"/> Host Name	gp011.japaneast.cloudapp.azure.com e)

d)

- (2) 生成が成功したことを示すメッセージが出力されたら、「OK」をクリックします。

※ Portal のサーバー証明書の共通名:「gp011.japaneast.cloudapp.azure.com」と、クライアント PC 上の GP Agent に、宛先として設定する Portal の FQDN が一致する必要があります。(理由: GP Agent は、Web ブラウザと同様に、サーバー証明書の共通名: Common Name (CN) をチェックしており、宛先 FQDN と CN が一致しなければ証明書エラーとなって、接続できません。)

よって、この FQDN:「gp011.japaneast.cloudapp.azure.com」は、外部 DNS でアドレス解決できる状態になっている必要があります。

本ガイドでは、Azure を使用しており、この FQDN が Azure の DNS サーバーにエントリーされるように設定しています。

7.3.2.2. 内部用サーバー証明書の生成 (Internal Gateway 用)

Internal Gateway が利用するサーバー証明書を生成します。

- (1) a) 証明書名に「Internal-Gateway(任意)」と入力します。
- b) 共有名は、ネットワーク構成に従い、「trust.acme.com」と入力します。
- c) 署名者は生成した認証局「PA-Certificate-Authority」を選択します。
- d) 「追加」をクリックして、e)「Host Name」を選択し、「gp011.japaneast.cloudapp.azure.com」を入力します。
- f) 「生成」をクリックします。

証明書の生成

証明書タイプ ローカル SCEP

証明書名 Internal-Gateway a)

共通名 trust.acme.com b)

署名者 PA-Certificate-Authority c)

認証局

OCSF レスポンダ

暗号設定

アルゴリズム RSA

ビット数 2048

ダイジェスト sha256

有効期限 (日) 365

証明書の属性

タイプ	値
<input checked="" type="checkbox"/> Host Name	trust.acme.com e)

d) + 追加 - 削除

f) 生成 キャンセル

- (2) 生成が成功したことを示すメッセージが出力されたら、「OK」をクリックします。

※ Internal Gateway のサーバー証明書の共通名 : 「trust.acme.com」と、Portal から GP Agent に送られる Internal Gateway の FQDN が一致する必要があります。(理由: GP Agent は、Web ブラウザと同様に、サーバー証明書の共通名 : Common Name (CN) をチェックしており、宛先 FQDN と CN が一致しなければ証明書エラーとなって、接続できません。)

よって、FQDN : 「trust.acme.com」は、内部 DNS でアドレス解決できる状態になっている必要があります。

7.4. SSL / TLS サービスプロファイルの設定

SSL / TLS サービスプロファイルを使用して、GP Agent~GP Portal/Gateway 間で使用するサーバー証明書の指定と、許可する SSL/TLS のプロトコルバージョンを指定することができます。

本ガイドでは、SSL/TLS プロトコルバージョンはデフォルトのままとします。

(1) a)「Device」 → 「証明書の管理」の下の b)「SSL/TLS サービス プロファイル」 → c)「追加」をクリックします。



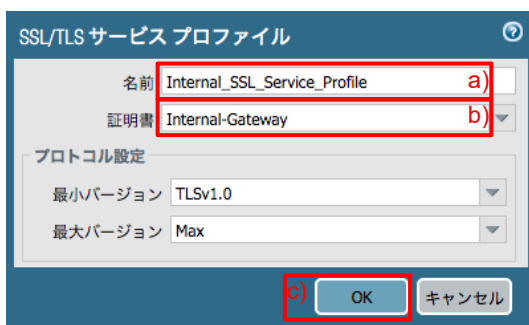
(2) Portal と External-Gateway 用の SSL/TLS サービスプロファイルを生成します。

- a) 名前に「External_SSL_Service_Profile(任意)」と入力します。
- b) 証明書は作成済みの「External-Gateway」を選択します。
- c) 「OK」をクリックします。



(3) Internal-Gateway 用の SSL/TLS サービスプロファイルを生成します。

- a) 名前に「Internal_SSL_Service_Profile(任意)」と入力します。
- b) 証明書は作成済みの「Internal-Gateway」を選択します。
- c) 「OK」をクリックします。



7.5. Gateway の設定

2 つの Gateway (External と Internal) を設定します。

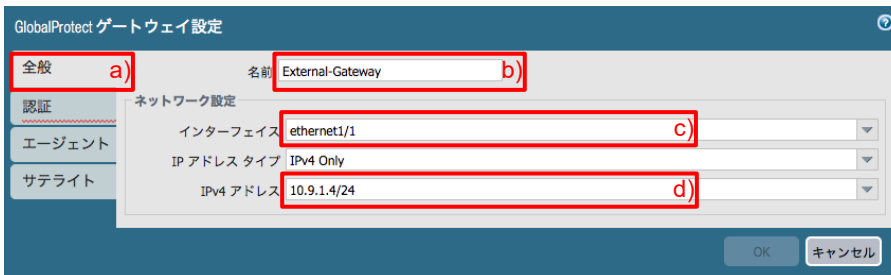
7.5.1. External Gateway の設定

インターネット側から VPN 接続する対象となる Gateway の設定です。

(1) a)「Network」 → 「GlobalProtect」の下の b)「ゲートウェイ」 → c)「追加」をクリックします。



(2) a)「全般」タブで、b)名前に「External-Gateway(任意)」と入力します。
c)インターフェイスは「ethernet1/1」を選択します。
d)IPv4 アドレスは「10.9.1.4/24」を選択します。



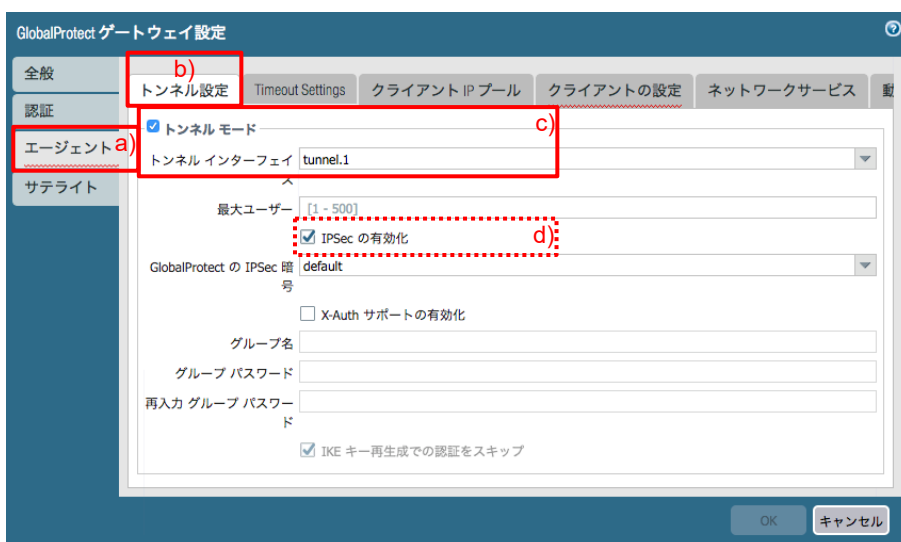
(3) a)「認証」タブで、b)SSL/TLS サービスプロファイルで設定済みの「External_SSL_Service_Profile」を選択します。
c)「追加」をクリックします。



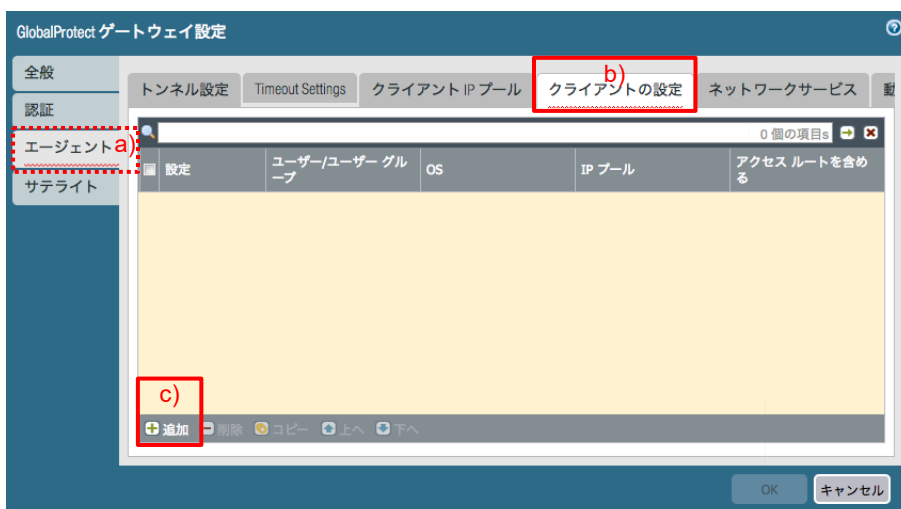
- (4) a)名前に「ADAuth(任意)」と入力し、b)認証プロファイルは設定済みの「Auth-Profile01」を選択します。
c)「OK」をクリックします。



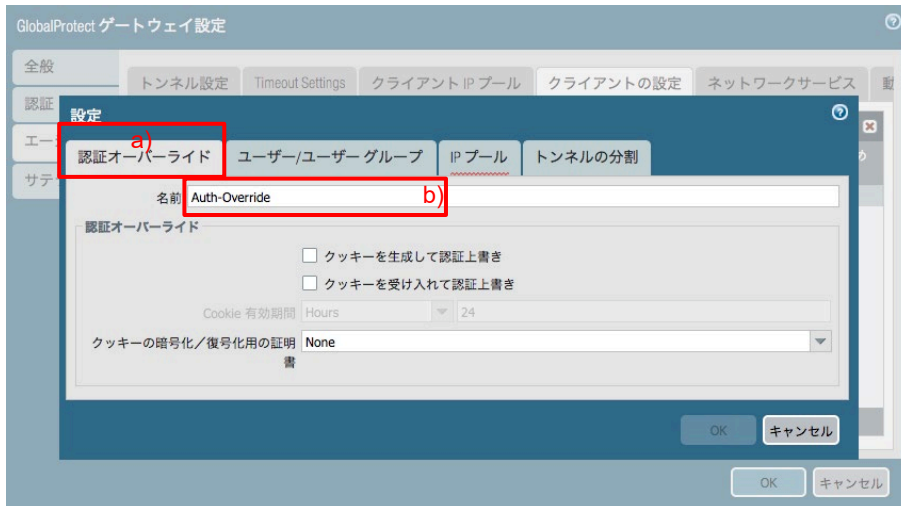
- (5) a)「エージェント」タブ → b)「トンネル設定」タブで、c)「トンネルモード」にチェックを入れ、「tunnel.1」を選択します。
d)「IPSecの有効化」にチェックが入っていることを確認します。
このことで、SSL-VPN よりも IPSec が優先的に使われます。



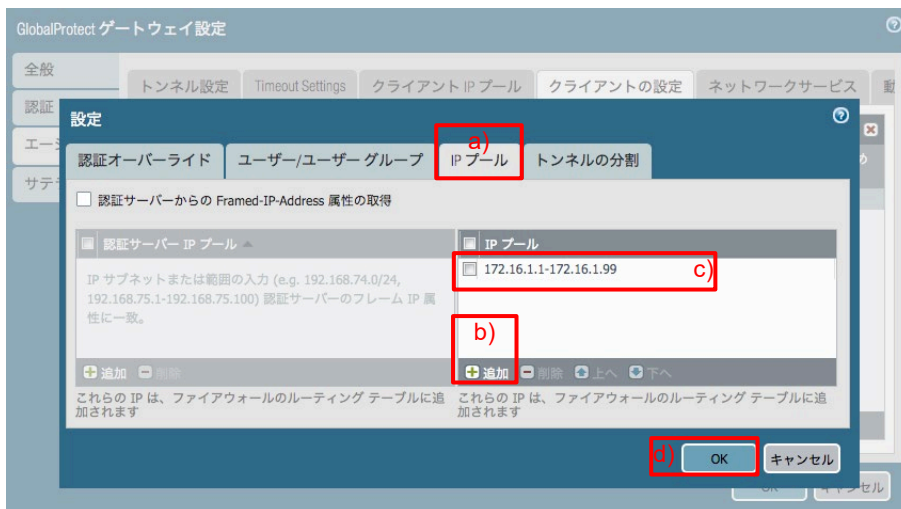
- (6) a)「エージェント」タブ → b)「クライアントの設定」タブで、c)「追加」をクリックします。



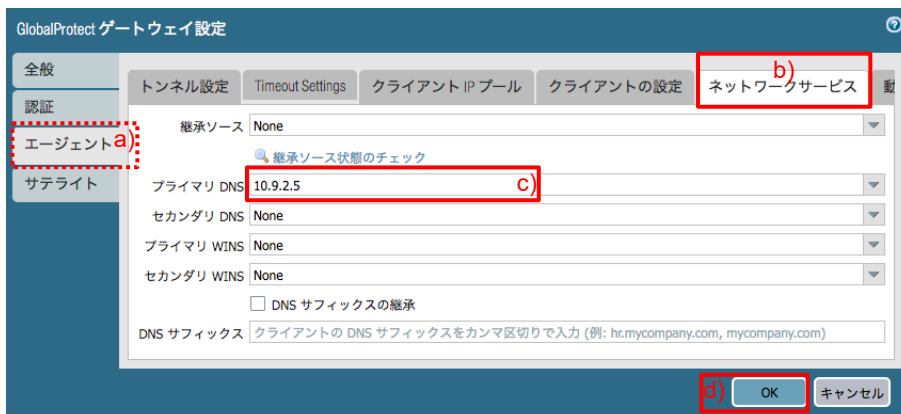
(7) a)「認証オーバーライド」タブで、b)名前に「Auth-Override(任意)」と入力します。



(8) a)「IP プール」タブ → b)「追加」をクリック → c)プールアドレス「172.16.1.1-172.16.1.99」と入力します。この IP アドレスが、GP Agent の VPN 確立後、クライアント PC の VPN インターフェイスに割り当てられます。d)「OK」をクリックします。



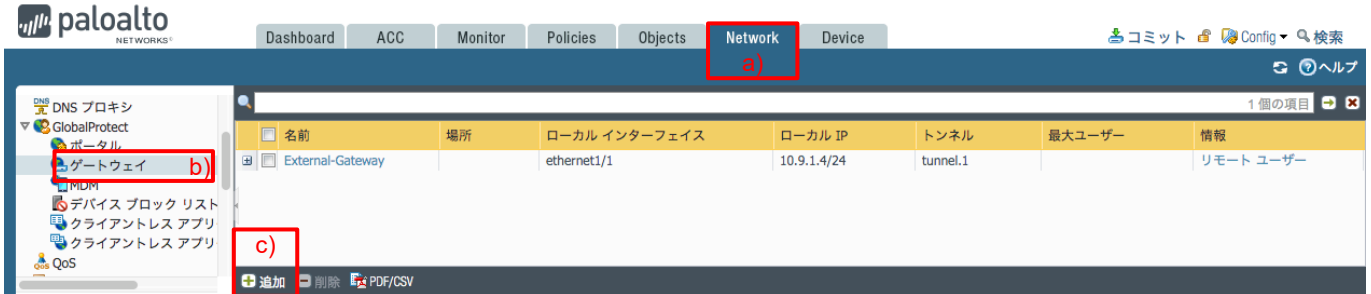
(9) a)「エージェント」タブ → b)「ネットワークサービス」タブで、c)プライマリ DNS に「10.9.2.5」と入力します。この設定が、GP Agent の VPN 確立後、クライアント PC の VPN インターフェイスに割り当てられます。d)「OK」をクリックします。



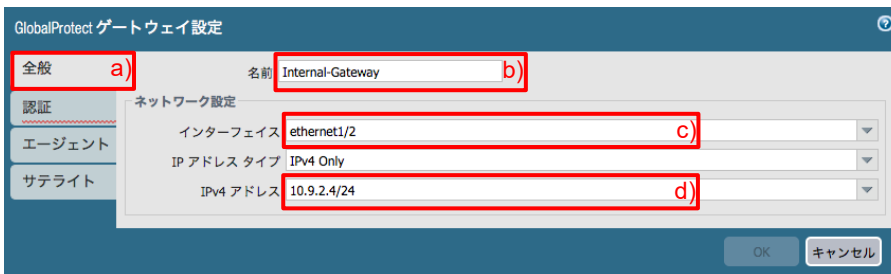
7.5.2. Internal Gateway の設定

社内 LAN から GP Agent が接続する Gateway の設定です。
VPN トンネルは確立しないのが特徴です。(VPN トンネルを確立する設定も可能です。)

(1) a)「Network」 → 「GlobalProtect」の下での b)「ゲートウェイ」 → c)「追加」をクリックします。



(2) a)「全般」タブで、b)名前に「Internal-Gateway(任意)」と入力します。
c) インターフェイスは「ethernet1/2」を選択します。
d) IPv4 アドレスは「10.9.2.4/24」を選択します。



(3) a)「認証」タブで、b)SSL/TLS サービスプロファイルで設定済みの「Internal_SSL_Service_Profile」を選択します。
c)「追加」をクリックして、d) External-Gateway と同様の方法で、認証サーバーを指定します。
e)「OK」をクリックします。



(4) 「コミット」を実施します。

7.6. 内部 DNS の設定

Portal 設定の前に、内部 DNS の設定を行います。

GP Agent は、自身が今いる場所が外部か内部かの特定や、Gateway のサーバー証明書の CN と自身が接続しようとしている宛先 FQDN が一致しているかどうかをチェックする際に DNS を利用するので、DNS 設定にも注意を払う必要があります。

本ガイドでは、Win2012 を内部 DNS として利用しており、Internal Gateway との接続時には、この DNS が正しく設定されている必要があります。

7.6.1. DNS の逆引き設定

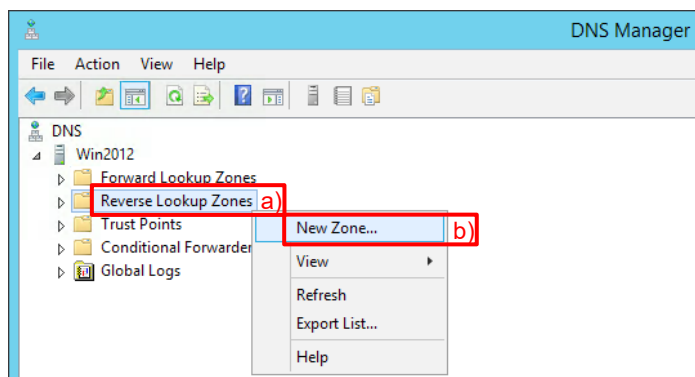
GP Agent は、現在外部にいるのか内部にいるのかの判断をするために、DNS の逆引きを利用します。

GP Agent が Portal にアクセスした際に、Portal から DNS 逆引き用 IP アドレスを受け取り、その IP アドレスの逆引きが成功することによって、GP Agent は、「内部にいる」と判断します。

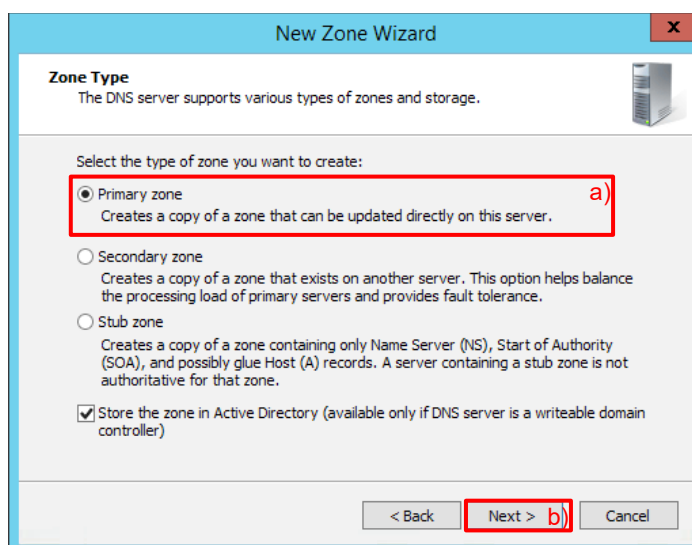
よって、内部 DNS が逆引きに応答できるように設定しておきます。

(1) Win2012 で、「Administration Tools」 → 「DNS」を選択します。

(2) 表示された DNS Manager で、a)「Reverse Lookup Zones」を右クリック → b)「New Zone」を選択します。



(3) a)「Primary zone」を選んで、b)「Next」をクリックします。



(4) a)「To all DNS servers running on domain controllers in this domain」を選択して、b)「Next」をクリックします。

The screenshot shows the 'New Zone Wizard' dialog box with the title 'Active Directory Zone Replication Scope'. Below the title, it says 'You can select how you want DNS data replicated throughout your network.' There are four radio button options: 'To all DNS servers running on domain controllers in this forest: acme.com', 'To all DNS servers running on domain controllers in this domain: acme.com' (which is selected and highlighted with a red box and labeled 'a)'), 'To all domain controllers in this domain (for Windows 2000 compatibility): acme.com', and 'To all domain controllers specified in the scope of this directory partition:'. Below the last option is a text input field. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box and labeled 'b)'), and 'Cancel'.

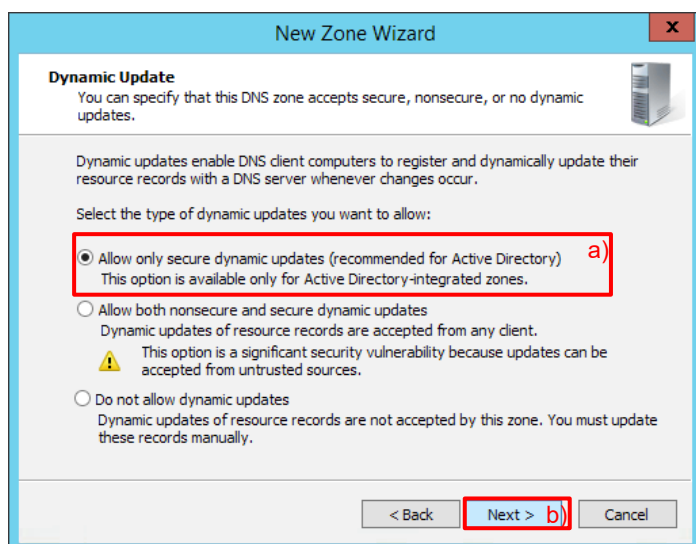
(5) a)「IPv4 Reverse Lookup Zone」を選択して、b)「Next」をクリックします。

The screenshot shows the 'New Zone Wizard' dialog box with the title 'Reverse Lookup Zone Name'. Below the title, it says 'A reverse lookup zone translates IP addresses into DNS names.' There are two radio button options: 'IPv4 Reverse Lookup Zone' (selected and highlighted with a red box and labeled 'a') and 'IPv6 Reverse Lookup Zone'. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box and labeled 'b)'), and 'Cancel'.

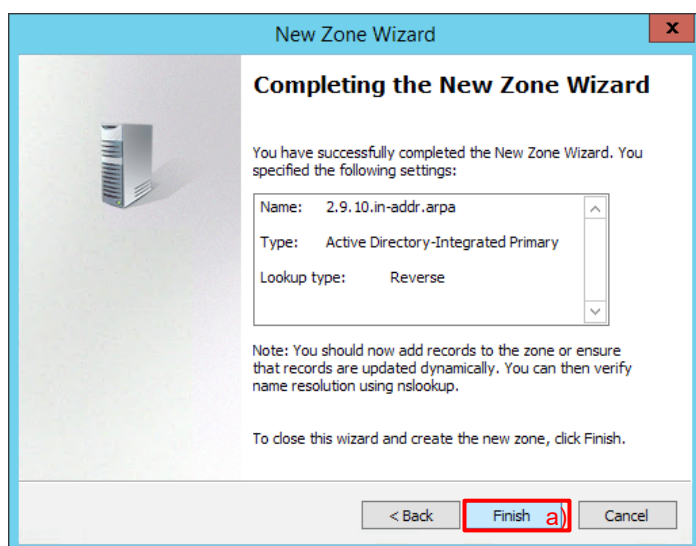
(6) a) Network ID を選択して、「10.9.2.」と入力し、b)「Next」をクリックします。

The screenshot shows the 'New Zone Wizard' dialog box with the title 'Reverse Lookup Zone Name'. Below the title, it says 'A reverse lookup zone translates IP addresses into DNS names.' There are two main sections. The first section is titled 'To identify the reverse lookup zone, type the network ID or the name of the zone.' It has two radio button options: 'Network ID:' (selected and highlighted with a red box and labeled 'a') and 'Reverse lookup zone name:'. The 'Network ID:' option has a text input field containing '10 .9 .2 .' (highlighted with a red box). Below this, it says 'The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.' The 'Reverse lookup zone name:' option has a text input field containing '2.9.10.in-addr.arpa'. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box and labeled 'b)'), and 'Cancel'.

(7) a)「Allow only secure dynamic updates」を選択して、b)「Next」をクリックします。



(8) a)「Finish」で完了です。

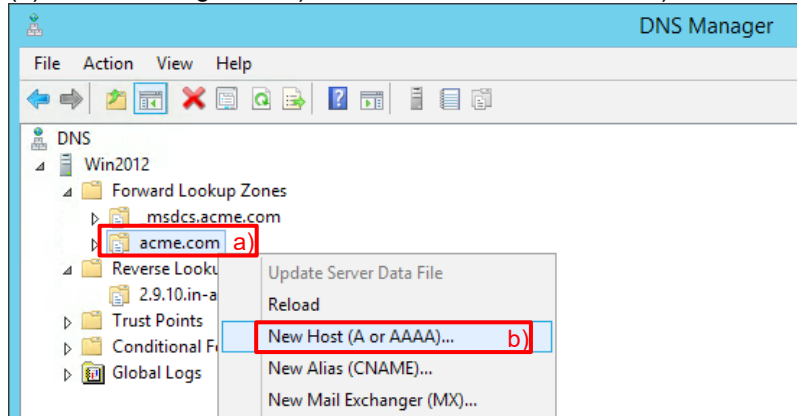


7.6.2. DNS の正引き設定

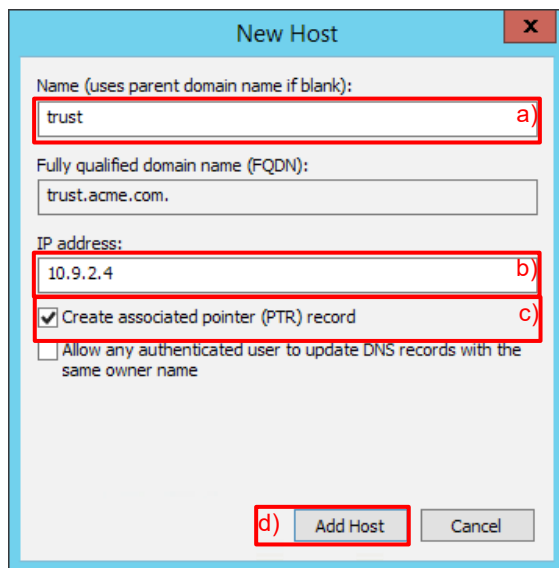
GP Agent が Internal Gateway へ接続する際には、Internal Gateway が持つサーバー証明書の Common Name: 「trust.acme.com」と、GP Agent が Portal から受け取った Internal Gateway の FQDN が一致する必要があります。

そのためには、GP Agent が「trust.acme.com」の DNS 問合せを行い、その IP アドレス解決ができる必要があるため、その設定を行います。

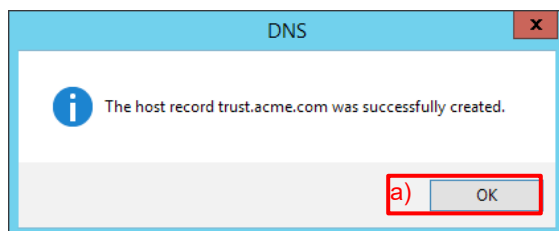
(1) DNS Manager で、a)「acme.com」を右クリック → b)「New Host (A or AAAA)」を選択します。



- (2) a) Name に「trust」と入力します。
b) IP address に「10.9.2.4」と入力します。
c) 逆引き生成するために「Create associated point (PTR) record」にチェックを入れます(必須ではありません)。
d) 「Add Host」をクリックします。



(3) a)「OK」をクリックします。



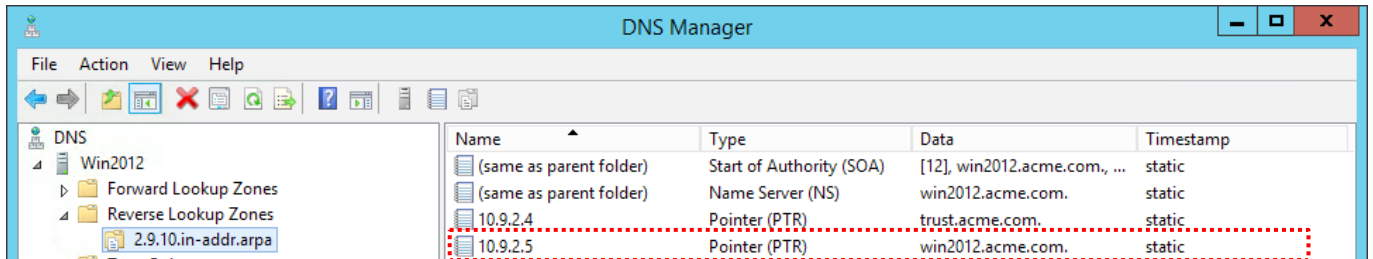
(4) Win2012 で、「Administration Tools」 → 「Services」 を選択して起動します。
一覧から「DNS Server」を見つけ出し、右クリックして「Restart」を選択して、サービスを再起動します。

7.6.3. 内部 DNS ゾーンの確認

設定された DNS ゾーン内容を確認しておきます。

(1) 逆引きゾーンの確認

本ガイドでは、逆引きは「10.9.2.5 Pointer (PTR) win2012.acme.com」を使います。

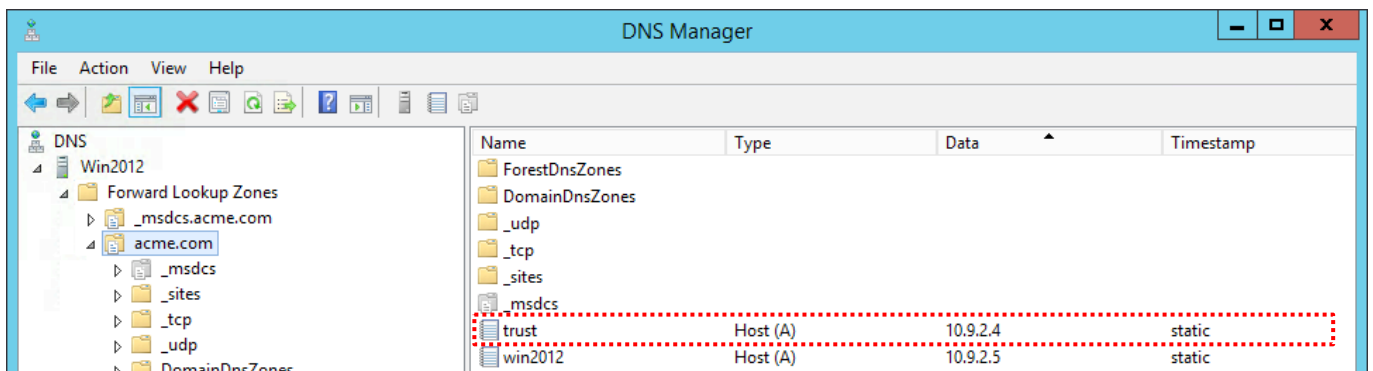


The screenshot shows the DNS Manager interface. The left pane shows the tree structure under 'Win2012' with 'Reverse Lookup Zones' expanded to show '2.9.10.in-addr.arpa'. The main pane displays a table of DNS records:

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[12], win2012.acme.com., ...	static
(same as parent folder)	Name Server (NS)	win2012.acme.com.	static
10.9.2.4	Pointer (PTR)	trust.acme.com.	static
10.9.2.5	Pointer (PTR)	win2012.acme.com.	static

(2) 正引きゾーンの確認

本ガイドでは、Internal Gateway への接続に、「trust.acme.com : 10.9.2.4」を使います。



The screenshot shows the DNS Manager interface. The left pane shows the tree structure under 'Win2012' with 'Forward Lookup Zones' expanded to show 'acme.com'. The main pane displays a table of DNS records:

Name	Type	Data	Timestamp
ForestDnsZones			
DomainDnsZones			
_udp			
_tcp			
_sites			
_msdcs			
trust	Host (A)	10.9.2.4	static
win2012	Host (A)	10.9.2.5	static

- (3) [参考] 本ガイドでは、Portal および External Gateway の FQDN:「gp011.japaneast.cloudapp.azure.com」への接続時に参照する外部 DNS は、Azure の公開 DNS を利用します。

7.6.4. Portal の設定

GP Agent が最初にアクセスする、Portal の設定を行います。

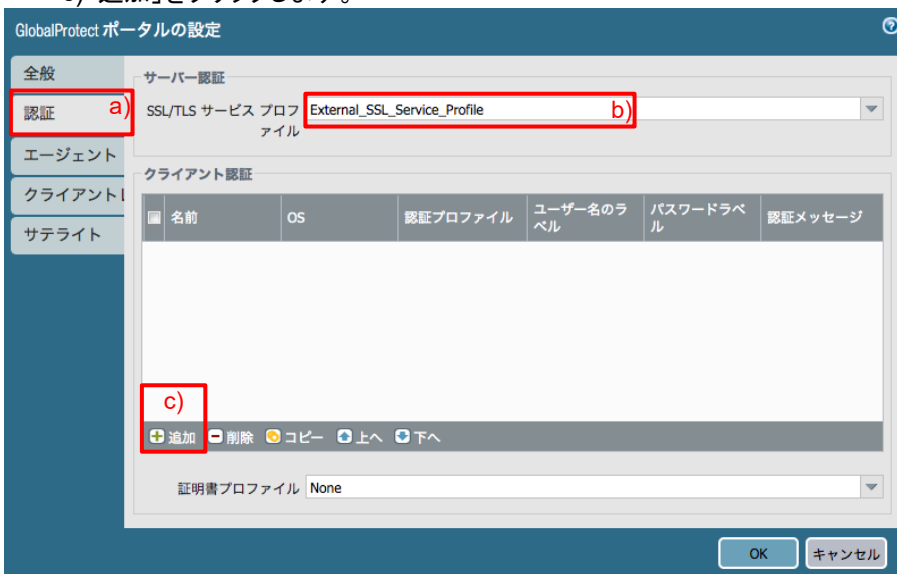
(1) a)「Network」 → 「GlobalProtect」の下の b)「ポータル」 → c)「追加」をクリックします。



(2) a)「全般」タブで、b)名前に「Portal(任意)」と入力します。
c)インターフェイスは「ethernet1/1」を選択します。
d)IPv4 アドレスは「10.9.1.4/24」を選択します。



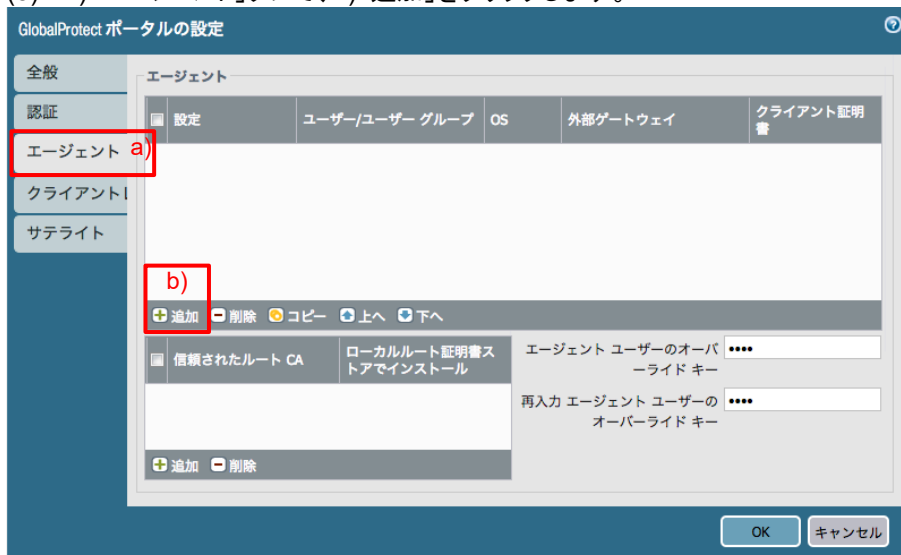
(3) a)「認証」タブで、b)SSL/TLS サービスプロファイルで「External_SSL_Service_Profile」を選択します。
c)「追加」をクリックします。



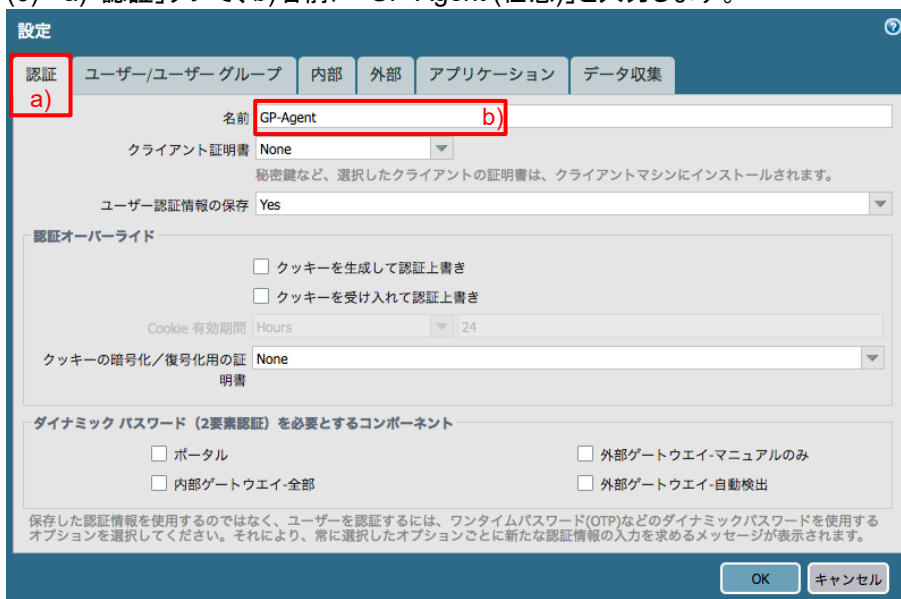
- (4) a) 名前に「ADAuth(任意)」と入力し、b) 認証プロファイルは設定済みの「Auth-Profile01」を選択します。
c) 「OK」をクリックします。



- (5) a) 「エージェント」タブで、b) 「追加」をクリックします。



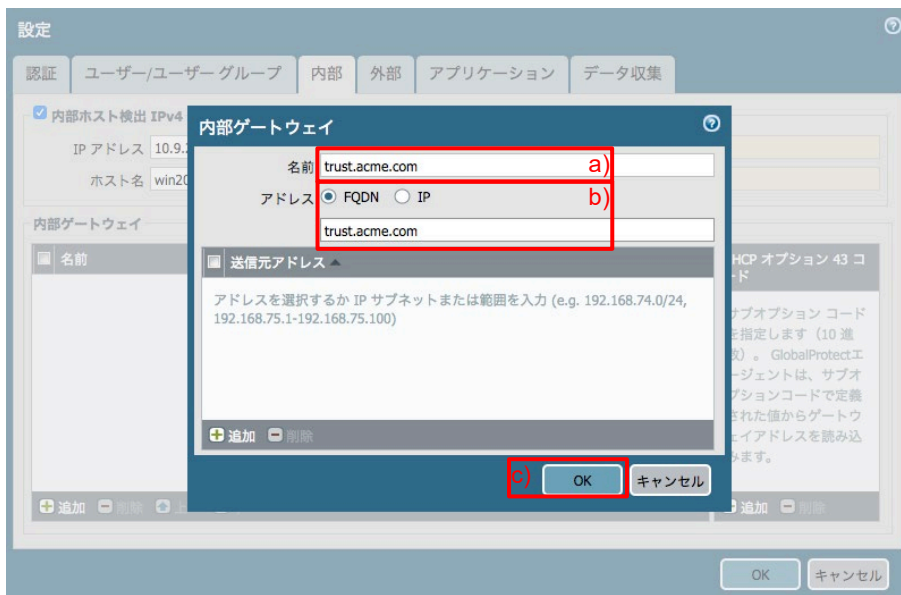
- (6) a) 「認証」タブで、b) 名前に「GP-Agent (任意)」と入力します。



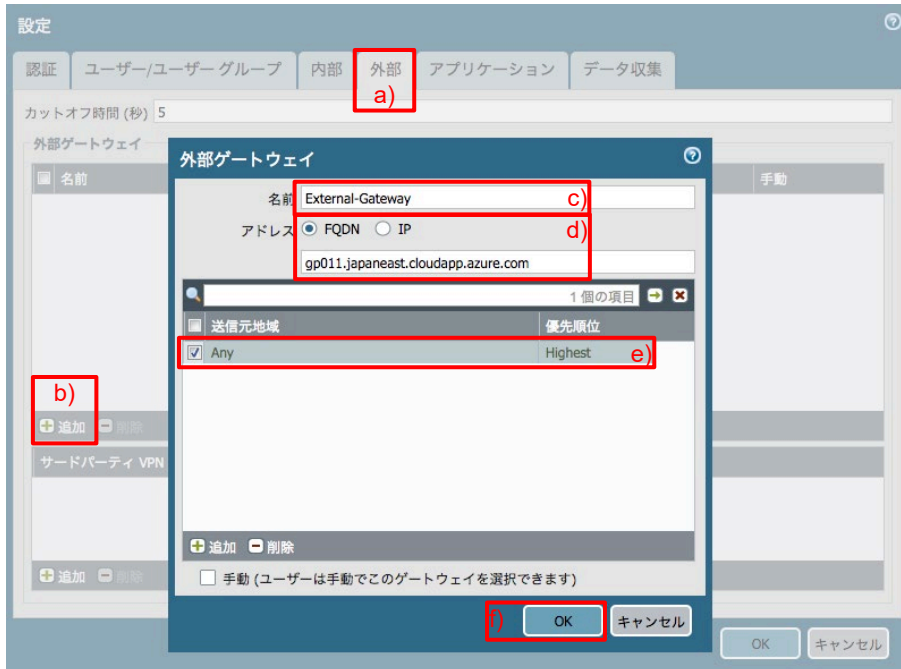
- (7) a) 「内部」タブをクリックします。
 GP Agent が社内 LAN に接続されていることを検出するために、内部 DNS の逆引きを利用しますが、その設定をこの「内部ホスト検出 IPv4」で行います。
 b) 「内部ホスト検出 IPv4」にチェックを入れます。
 c) 内部 DNS の逆引きができる IP アドレス「10.9.2.5」を入力します。
 d) 内部 DNS の逆引きで返答されるホスト名「win2012.acme.com」を入力します。
 e) 「追加」をクリックします。



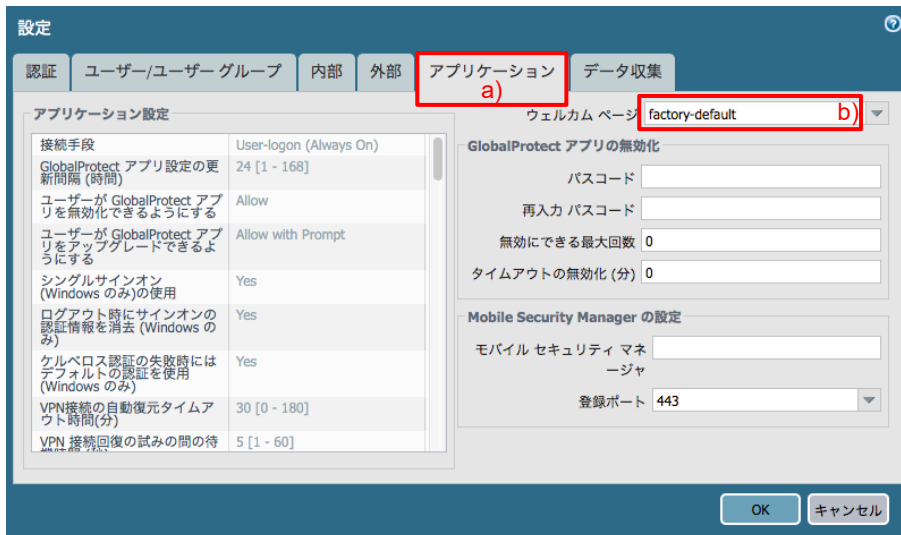
- (8) a) 名前に「trust.acme.com(任意)」と入力します。
 b) アドレスは「FQDN」を選択し、「trust.acme.com」と入力します。
 ※この FQDN が、Internal Gateway 用 SSL/TLS サービスプロファイルに設定したサーバー証明書の Common Name と一致する必要があります。
 c) 「OK」をクリックします。



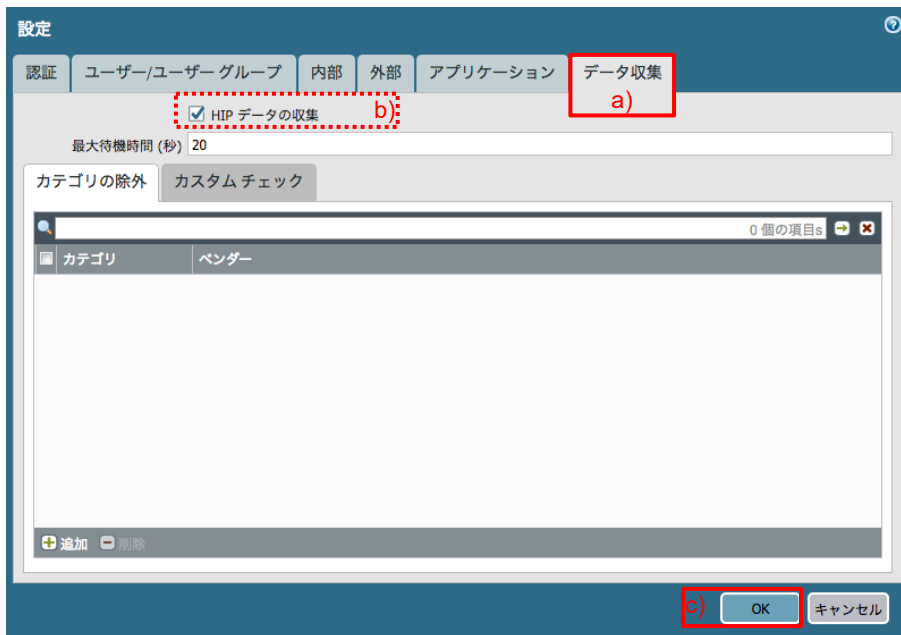
- (9) a) 「外部」タブをクリックします。
 b) 「追加」をクリックします。
 c) 名前に「External-Gateway(任意)」と入力します。
 d) FQDN を選択し、「gp011.japaneast.cloudapp.azure.com」と入力します。
 ※この FQDN が、External Gateway 用 SSL/TLS サービスプロファイルに設定したサーバー証明書の Common Name と一致する必要があります。
 e) 「送信元地域」で「Any」を選択します。
 f) 「OK」をクリックします。



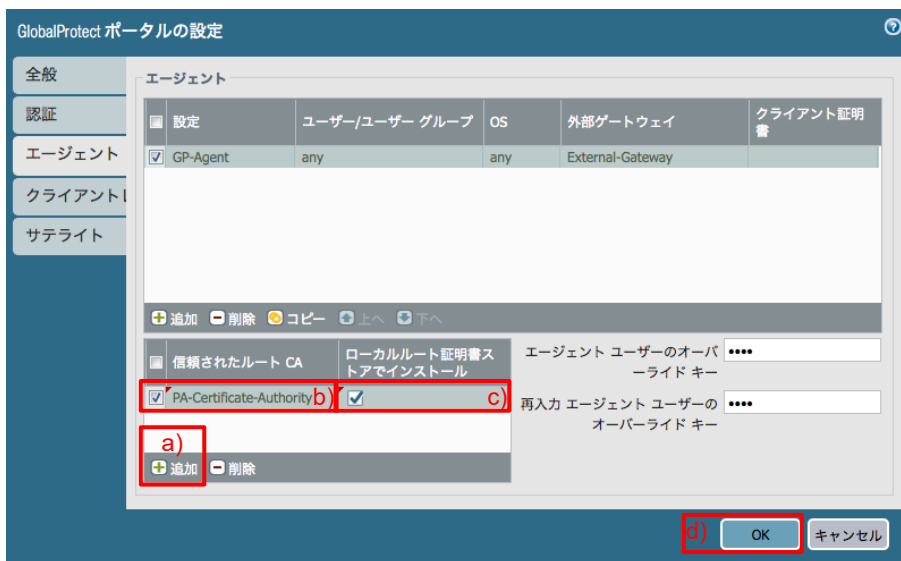
- (10) a) 「アプリケーション」タブをクリックします。
 b) ウェルカムページで「factory-default」を選択します。



- (11) a) 「データ収集」タブでは、何も設定しません。
 b) HIP データの収集が有効になっていることを確認します。
 c) 「OK」をクリックします。



- (12) a)「追加」 → b)信頼されたルート CA に、生成済みの「PA-Certificate-Authority」を選択し、c)「ローカルルート証明書ストアでインストール」にチェックを入れます。
 d)「OK」をクリックします。



※ この設定をするだけで、GP Agent がインストールされたクライアント PC(Windows)の「信頼されたルート証明書発行機関」フォルダ(macOS の場合は「キーチェーンアクセス」)に、ルート証明書をインポートすることができます。

PA Firewall が生成した証明書以外のルート証明書であっても、ここに指定すれば、クライアント PC へインポートできます。(その場合は、そのルート証明書を事前に PA Firewall へインポートしておく必要があります。)

- (13) 「コミット」を実施します。

7.7. ポリシーの設定

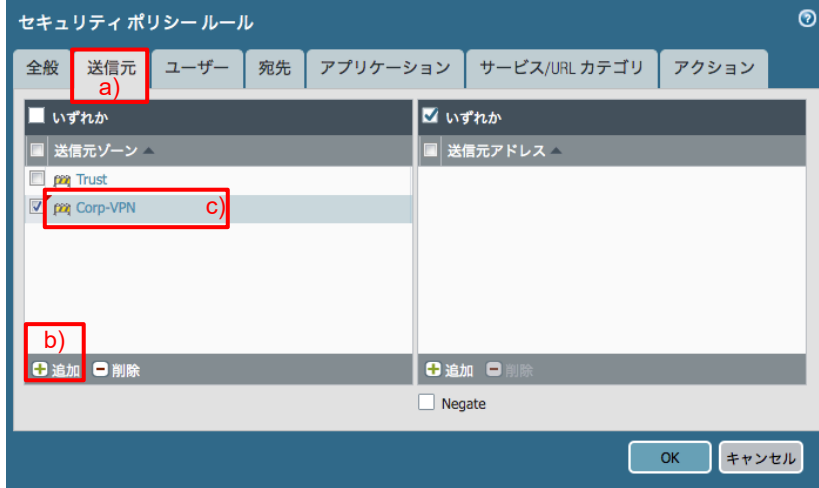
Trust→Untrust 方向の既存ポリシーに、Corp-VPN ゾーンを加えます。
Corp-VPN→Trust ゾーンへの通信も許可したいので、そのポリシーも追加します。

7.7.1. セキュリティポリシー

(1) a)「Policies」 → b)「セキュリティ」 → c)「outbound」をクリックします。



(2) a)「送信元」タブ → b)「追加」をクリックして、c)「Corp-VPN」ゾーンを追加します。



(3) a) は、outbound ポリシーの送信元ゾーンに、Trust と Corp-VPN の 2 つが設定された状態です。
加えて、b) のように、Corp-VPN→Trust 方向のポリシーも追加します。

名前	タグ	タイプ	送信元				宛先		アプリケーション	サービス	アクション
			ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス			
1 outbound	none	universal	Corp-VPN Trust	any	any	any	Untrust	any	any	any	許可
2 VPN-to-Trust	none	universal	Corp-VPN	any	any	any	Trust	any	any	any	許可
3 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	許可
4 interzone-default	none	interzone	any	any	any	any	any	any	any	any	拒否

7.7.2. NAT ポリシー

NAT の outbound ポリシーにも、送信元ゾーンに Corp-VPN を加えて、PA Firewall 経由でインターネットへ通信できるようにし、「コミット」を実施します。



7.8. GP Agent の設定

GP Agent をクライアント PC にインストールする際には、PA Firewall の Portal に Web ブラウザでアクセスし、PA Firewall からダウンロードします。

そのためには、事前に PA Firewall に GP Agent をダウンロード & アクティベーションしておく必要があります。

7.8.1. GlobalProtect Agent のダウンロード&アクティベーション

- (1) a)「Device」 → b)「GlobalProtect クライアント」 → c)「今すぐチェック」をクリックします。
現在リリースされている GlobalProtect Agent のバージョンの一覧が得られます。
本ガイドでは、d) 4.1.10 を利用することになります。アクション列の「ダウンロード」をクリックします。

バージョン	サイズ	リリース日	ダウンロード済み	現在アクティベーション済み	アクション
5.0.1	59 MB	2019/03/11 16:23:18			ダウンロード リリース ノート
5.0.0	58 MB	2019/02/11 14:22:59			ダウンロード リリース ノート
4.1.11	59 MB	2019/04/08 13:58:42			ダウンロード リリース ノート
4.1.10	58 MB	2019/02/20 14:50:25			ダウンロード リリース ノート
4.1.9	58 MB	2019/01/23 08:39:38			ダウンロード リリース ノート
4.1.8	58 MB	2018/12/11 16:06:53			ダウンロード リリース ノート
4.1.7	58 MB	2018/11/27 06:18:49			ダウンロード リリース ノート
4.1.6	57 MB	2018/10/15 16:26:22			ダウンロード リリース ノート
4.1.5	57 MB	2018/09/10 12:47:13			ダウンロード リリース ノート
4.1.4	57 MB	2018/08/06 17:42:34			ダウンロード リリース ノート

- (2) 「アクティベーション」をクリックします。

バージョン	サイズ	リリース日	ダウンロード済み	現在アクティベーション済み	アクション
5.0.1	59 MB	2019/03/11 16:23:18			ダウンロード リリース ノート
5.0.0	58 MB	2019/02/11 14:22:59			ダウンロード リリース ノート
4.1.11	59 MB	2019/04/08 13:58:42			ダウンロード リリース ノート
4.1.10	58 MB	2019/02/20 14:50:25	✓		アクティベーション リリース ノート
4.1.9	58 MB	2019/01/23 08:39:38			ダウンロード リリース ノート
4.1.8	58 MB	2018/12/11 16:06:53			ダウンロード リリース ノート
4.1.7	58 MB	2018/11/27 06:18:49			ダウンロード リリース ノート
4.1.6	57 MB	2018/10/15 16:26:22			ダウンロード リリース ノート
4.1.5	57 MB	2018/09/10 12:47:13			ダウンロード リリース ノート
4.1.4	57 MB	2018/08/06 17:42:34			ダウンロード リリース ノート

- (3) 「はい」をクリックします。

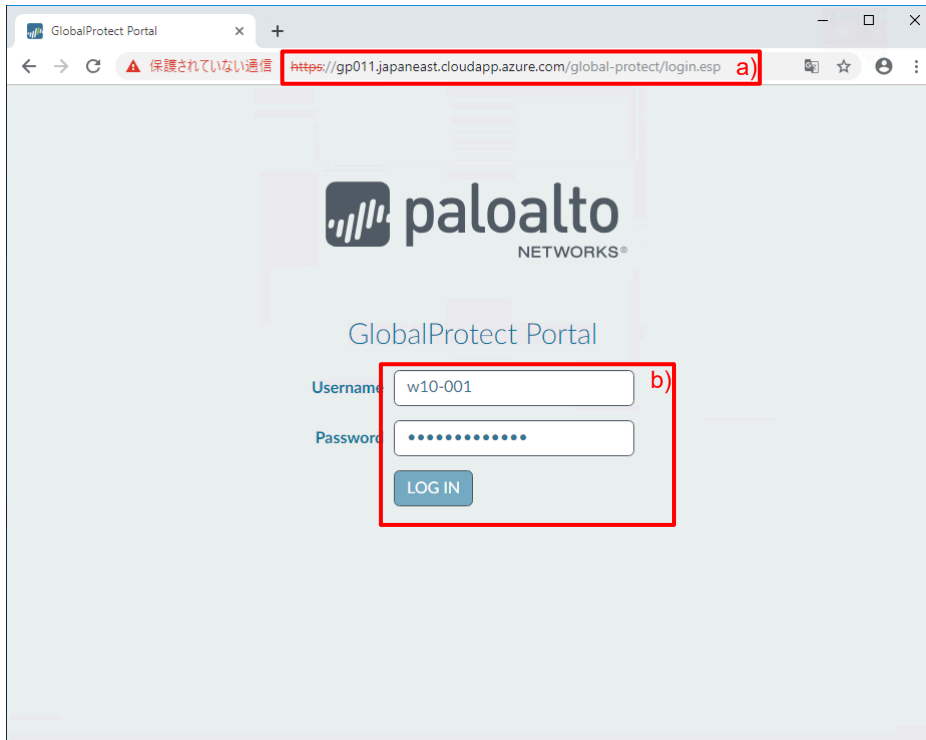
GlobalProtect クライアント バージョン 4.1.10 のアクティベーション

これにより、次の接続時に GlobalProtect ユーザーのコンピュータにダウンロードされる GlobalProtect クライアント ソフトウェアの新しいバージョンがアクティベーションされます。続行しますか？

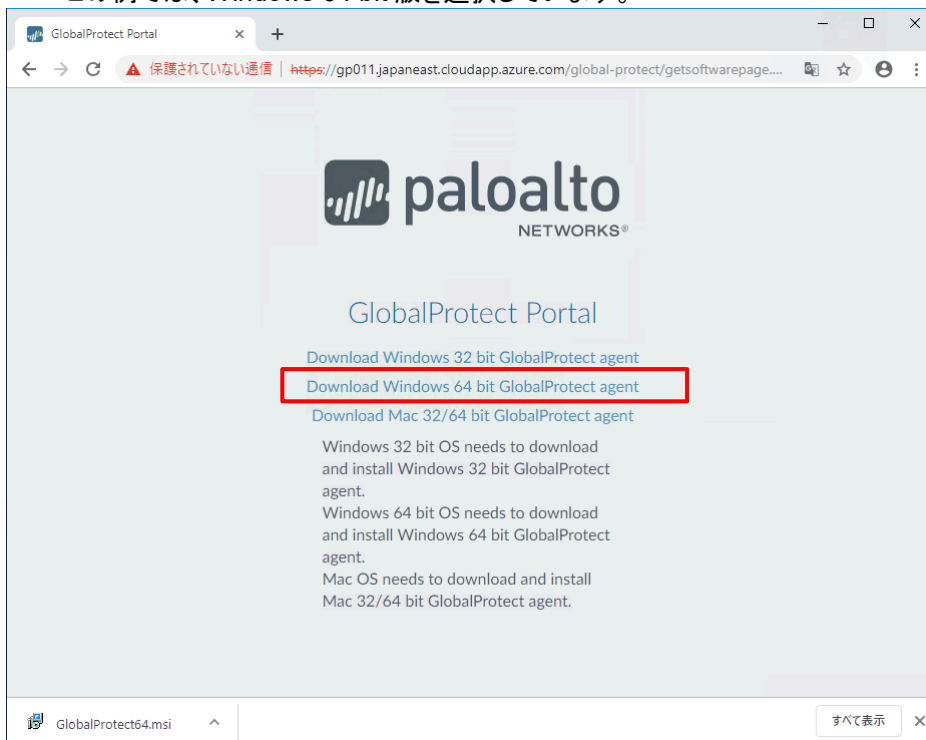
- (4) 成功を示すメッセージが出たら、「閉じる」をクリックします。

7.8.2. クライアント PC への GP Agent のインストール

- (1) a) GP Agent をインストールするクライアント PC (例: Windows10) から、Web ブラウザを使って、Portal (gp011.japaneast.cloudapp.azure.com) へアクセスします。
b) Active Directory に登録されているユーザー名(例: w10-001)とパスワードを入力し「LOG IN」をクリックします。

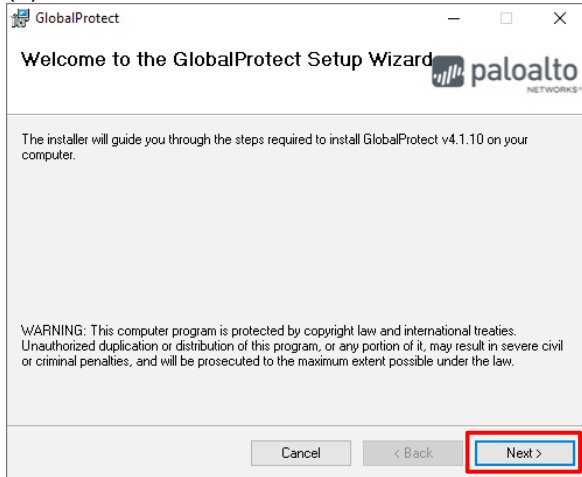


- (2) OS 環境に合う GlobalProtect Agent をダウンロードします。
この例では、Windows 64 bit 版を選択しています。

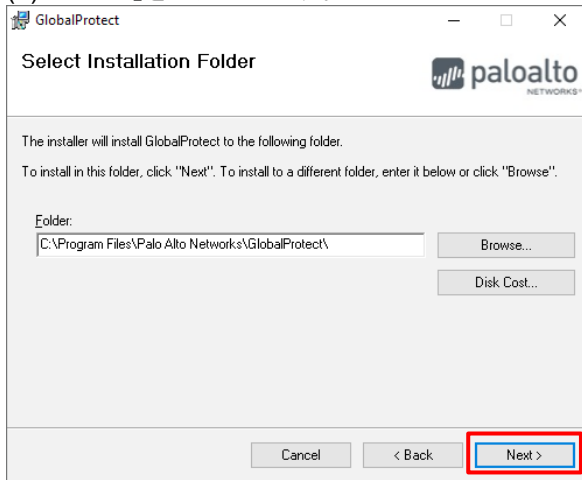


- (3) ダウンロードした msi 形式ファイルを実行します。

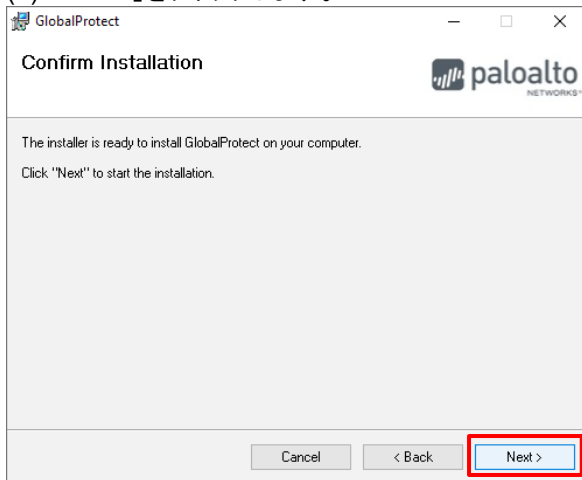
(4) 「Next」をクリックします。



(5) 「Next」をクリックします。

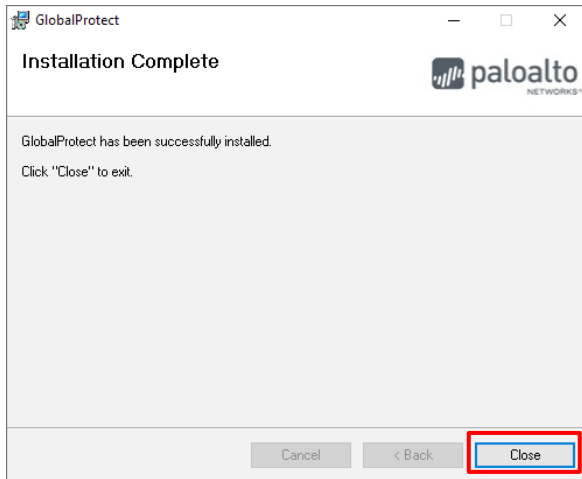


(6) 「Next」をクリックします。



(7) ユーザー権限でログインしている Windows クライアント PC の場合、ここで管理者権限を求められます。管理者 ID およびパスワードの入力が必要です。

(8) 「Close」をクリックします。GP Agent のインストールは完了です。



(9) Windows10 へのインストールが完了すると、GP Agent は常駐プログラムとしてタスクトレイに入ります。

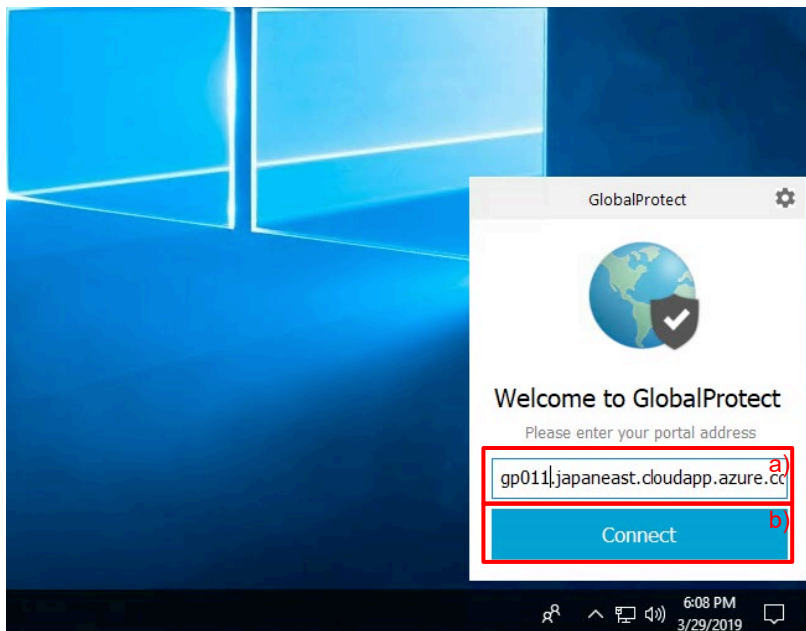
7.8.3. Portal & Gateway へのアクセス

インストールが完了した GP Agent から、まずは Portal、その後 Gateway へ接続できることを確認します。

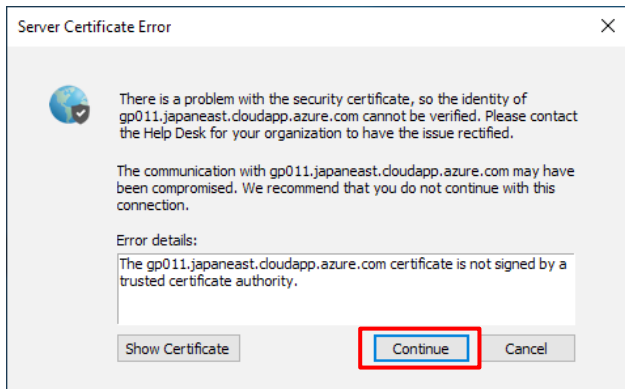
7.8.3.1. Internal Gateway へログイン

社内 LAN 上の Windows10 (ユーザー:w10-003) から接続する例です。

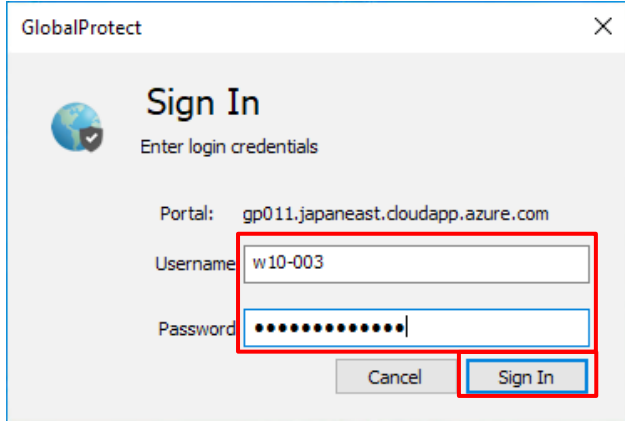
- (1) 表示された以下の GP Agent の画面で、a) Portal の FQDN:「gp011.japaneast.cloudapp.azure.com」を入力します。
- b) 「Connect」をクリックします。



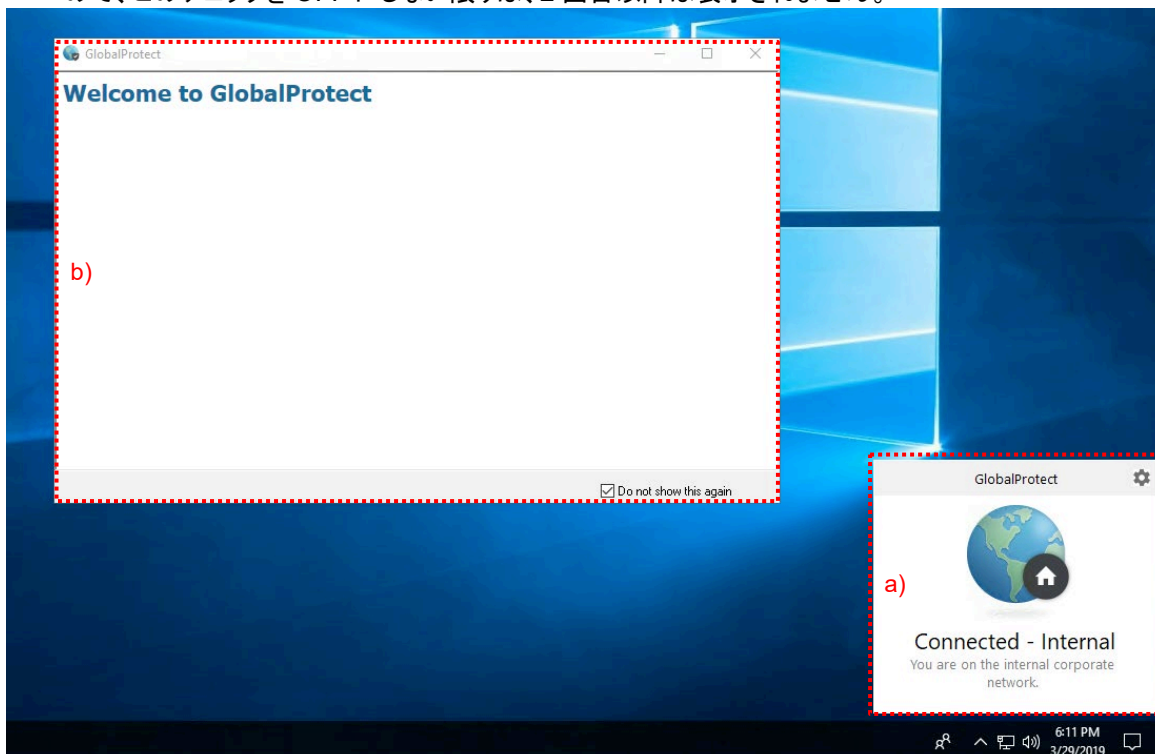
- (2) 初めて Portal にアクセスした際には、以下の「Server Certificate Error」が出ます。「Continue」をクリックします。
 (Portal の設定で、Portal からルート証明書:「PA-Certificate-Authority」がインポートされるように設定したので、2 回目以降にこのエラーメッセージを見ることはありません。)



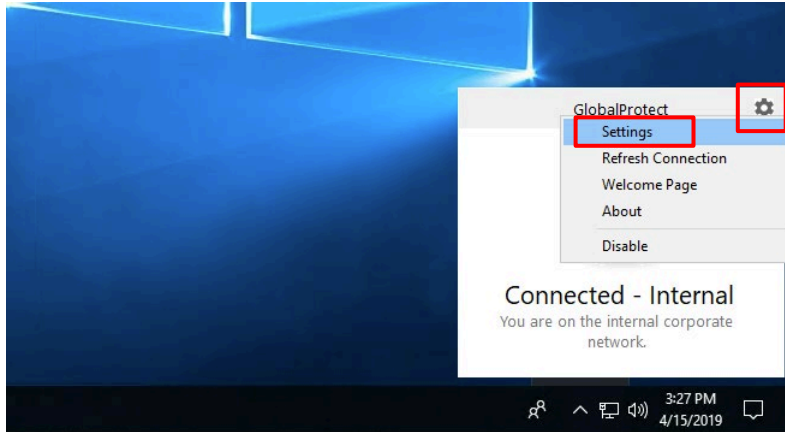
- (3) Active Directory に登録されているユーザー名(例: w10-003)とパスワードを入力し「Sign In」をクリックします。



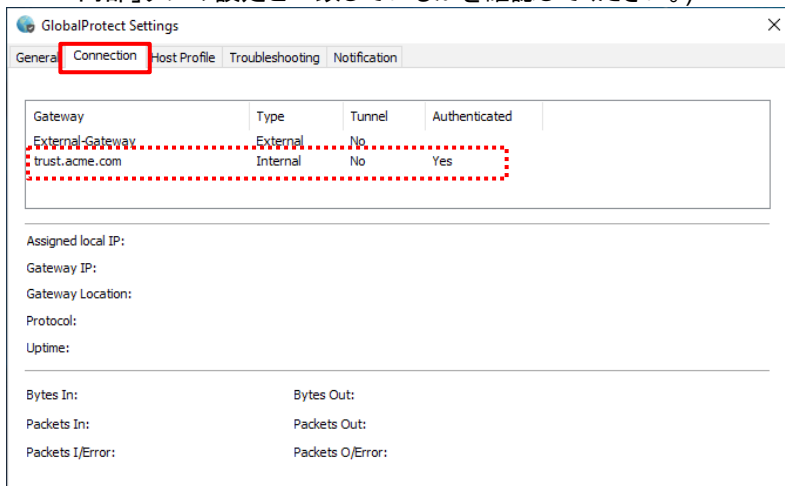
- (4) 内部接続(Internal-Gateway への接続)の場合には、a)のように「Connected - Internal」と表示されます。b)の Welcome メッセージは、初回は表示されますが、デフォルトで「Do not show this again」にチェックが入っているため、このチェックを OFF にしない限りは、2 回目以降は表示されません。



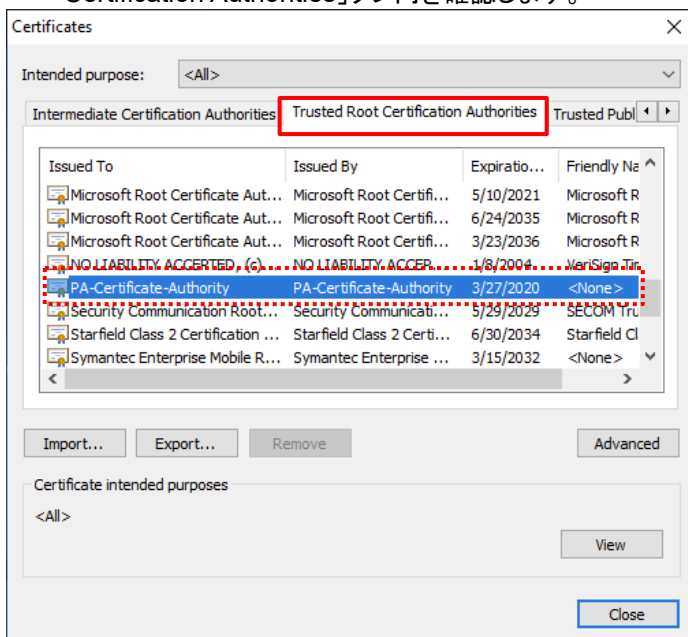
(5) [確認のみ] GP Agent の右上にある  をクリックして、「Settings」を選択します。



(6) 「Connection」タブをクリックして、Internal-Gateway である「trust.acme.com」の Authenticated が「Yes」であることを確認します。
 (Internal Gateway の場合、「Connected - Internal」と表示されても、Internal Gateway へのログインができていない場合があります。その場合、まずは内部 Gateway のサーバー証明書 CN の FQDN が、Portal の「エージェント」→「内部」タブの設定と一致しているかを確認してください。)



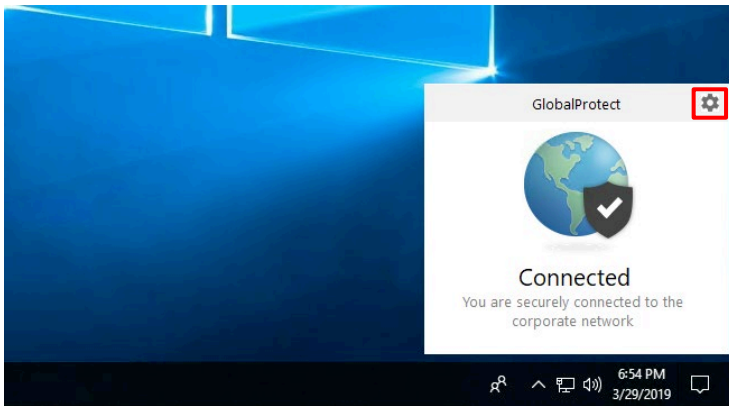
(7) [確認のみ] PA Firewall で生成したルート証明書がインポートされていることを確認します。
 例: Chrome ブラウザ → 「設定」 → 「詳細設定」 → 「証明書の管理」で表示された画面で、「Trusted Root Certification Authorities」タブ内を確認します。



7.8.3.2. External Gateway へのログイン

インターネット上の Windows10 (ユーザー:w10-003) から接続する例です。

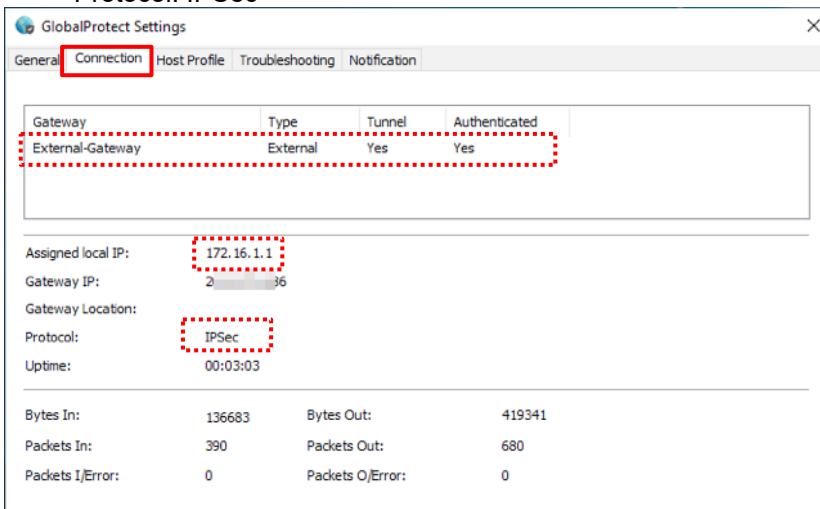
- (1) 最初に Portal へログインする際に、Username と Password を入力したので、社外へ持ち出した場合は、デフォルトでは、Username と Password を入力することなく、自動的に接続されます。




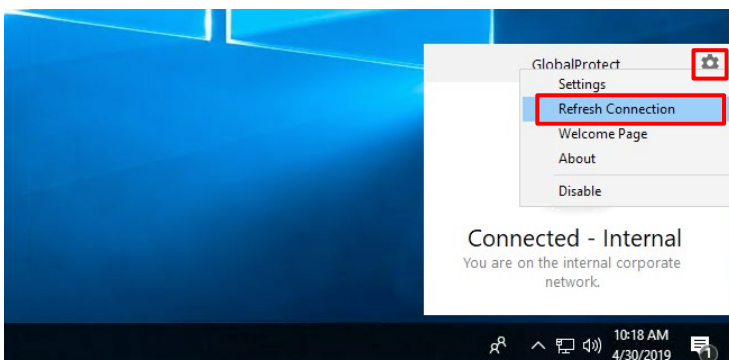
- (2) [確認のみ]GP Agent の右上にある  をクリックして、「Settings」を選択します。

「Connection」タブをクリックして、以下の状態を確認します。

- External-Gateway で、Tunnel が Yes
- Assigned local IP: 172.16.1.x (Pool 設定した IP アドレス)
- Protocol: IPSec



- (3) 再接続して挙動を確かめたい場合には、GP Agent の右上にある  をクリックして、「Refresh Connection」をクリックしてください。



GlobalProtect の基本的な設定は以上です。

7.8.4. [参考] GP Agent のアップグレード

GlobalProtect Agent を、4.1.10→4.1.11 へアップグレードする手順です。

7.8.4.1. PA Firewall 側の準備

(1) a)「Device」 → b)「GlobalProtect クライアント」 で 4.1.11 をダウンロード後、c)「アクティベーション」をクリックします。

バージョン	サイズ	リリース日	ダウンロード済み	現在アクティベーション済み	アクション
5.0.1	59 MB	2019/03/11 16:23:18			ダウンロード
5.0.0	58 MB	2019/02/11 14:22:59			ダウンロード
4.1.11	59 MB	2019/04/08 13:58:42	✓		アクティベーション c)
4.1.10	58 MB	2019/02/20 14:50:25	✓	✓	再アクティビ化
4.1.9	58 MB	2019/01/23 08:39:38			ダウンロード
4.1.8	58 MB	2018/12/11 16:06:53			ダウンロード
4.1.7	58 MB	2018/11/27 06:18:49			ダウンロード
4.1.6	57 MB	2018/10/15 16:26:22			ダウンロード
4.1.5	57 MB	2018/09/10 12:47:13			ダウンロード
4.1.4	57 MB	2018/08/06 17:42:34			ダウンロード

(2) 「はい」をクリックします。

GlobalProtect クライアントバージョン 4.1.11 のアクティベーション

これにより、次の接続時に GlobalProtect ユーザーのコンピュータにダウンロードされる GlobalProtect クライアント ソフトウェアの新しいバージョンがアクティベーションされます。続行しますか?

7.8.4.2. クライアント側の動作

(1) クライアントが Gateway へ再接続した際に、以下の画面が出力されます。「Yes」をクリックします。

GlobalProtect Update

There is a newer version (4.1.11-9) of GlobalProtect available for download. Download will begin in the background. You will be prompted to install once the download is successfully completed. Download now ?

(2) 数秒後に、以下のメッセージが出力されます。「Yes」をクリックすると、新しい GP Agent が自動的にインストールされて、GP Agent の再起動が行われます。よって、GP Agent のアップデートを行うクライアントは、一時的な通信停止を伴います。

GlobalProtect Update

GlobalProtect version 4.1.11-9 is ready for installation. During the installation VPN connection will be terminated and reestablished. Install now ?

7.8.5. [参考] GP Agent の挙動の変更方法

GP Agent の挙動を変更する方法について、記載しておきます。

例えば、GP Agent のデフォルトの挙動は、「User-logon(Always On)」となっており、Windows にログオンすると同時に、常に PA Firewall に接続した状態を維持するようになっています。

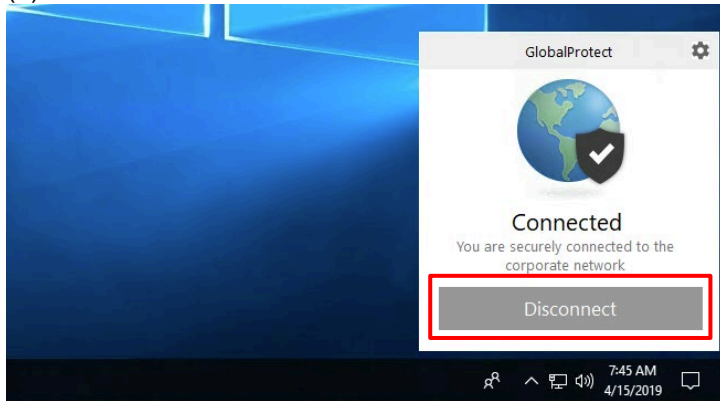
この挙動を、「ユーザーが VPN 接続したい時だけ、手動で接続させるようにしたい。」という場合には、Portal の設定で変更することができます。

- (1) 「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリック → a)「アプリケーションタブ」で表示される以下の画面で、「接続手段」を b)「On-demand (Manual user initiated connection)」に変更し、c)「OK」をクリックします。

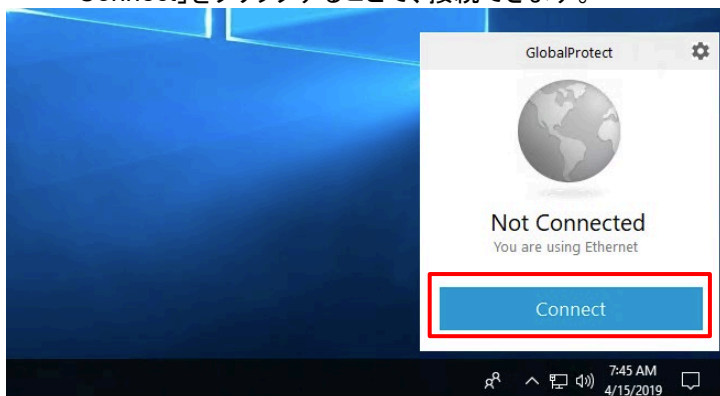


- (2) 「コミット」を実施します。

- (3) クライアントが再ログインすると、「Disconnect」が現れるようになります。クリックすると切断されます。



- (4) この設定によって、GP Agent が自動接続することなく、以下の状態で待機するようになります。「Connect」をクリックすることで、接続できます。



8. クライアント証明書認証の設定

前セクションまでで設定したユーザー名とパスワードによる認証に加え、2要素目としてのクライアント証明書認証を追加する方法を示します。

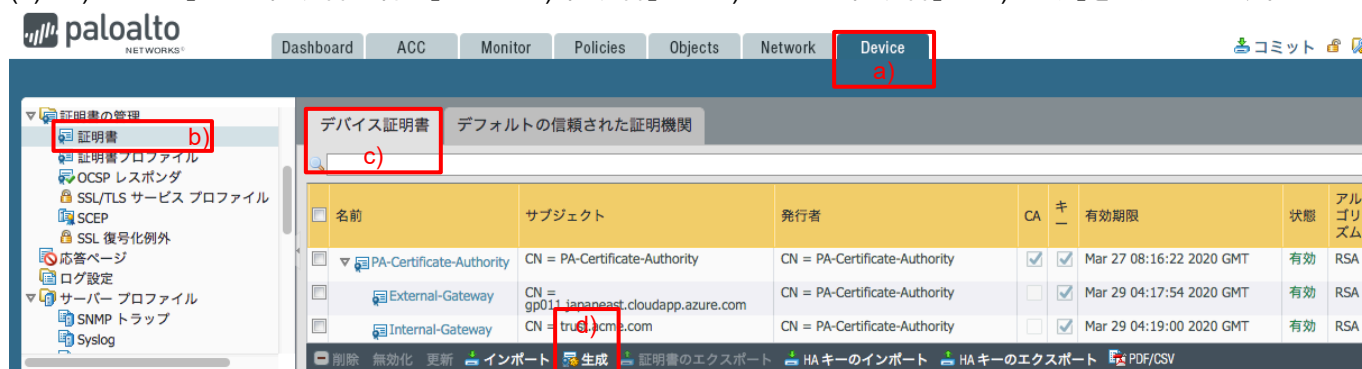
8.1. 全ユーザー共通のクライアント証明書で認証

簡易的な方法として、「全ユーザーが共通のクライアント証明書を持ち、そのクライアント証明書を持たないクライアント PC は接続させない」という設定を行います。

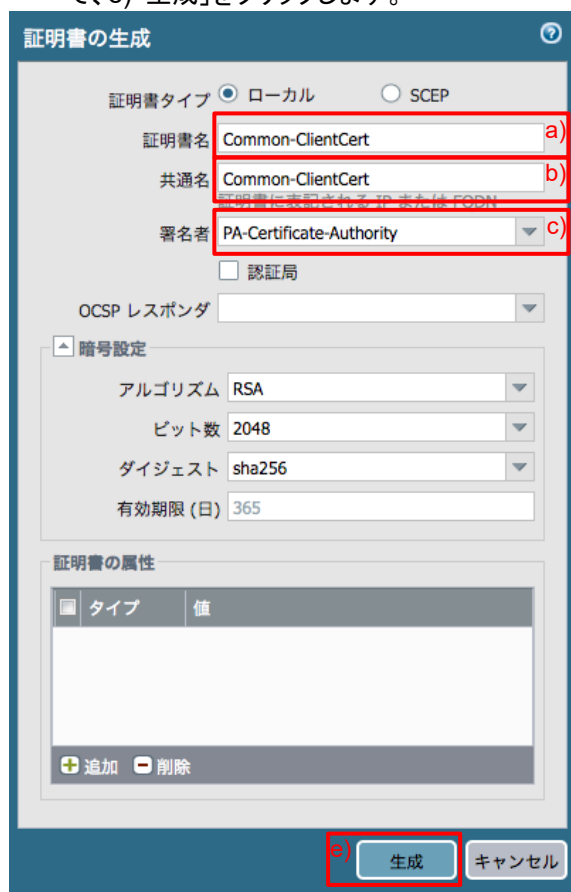
「各ユーザーにその共通クライアント証明書を配布して、インポート作業をしてもらう」というのも一つの手段ですが、その手間を省く目的で、GlobalProtect では、「ユーザ名とパスワード認証の際に、同時にクライアント証明書を配布する」という機能が提供されていますので、その設定を行います。

8.1.1. 全ユーザー共通のクライアント証明書の生成

(1) a)「Device」 → 「証明書の管理」の下に b)「証明書」 → c)「デバイス証明書」 → d)「生成」をクリックします。



(2) a)証明書名および共通名に「Common-ClientCert(任意)」と入力し、c)署名者に「PA-Certificate-Authority」を選択して、e)「生成」をクリックします。



(3) Gateway用のサーバー証明書と同じ形で、クライアント証明書が生成されます。



8.1.2. 証明書プロファイルの設定とGatewayへの割当て

証明書プロファイル設定し、それをPortalやGatewayに割当てることで、クライアント証明書認証が可能になります。このプロファイルでは、クライアント証明書認証に使用する、証明書発行機関の証明書(ルート証明書)を指定します。

(1) a)「Device」 → 「証明書の管理」の下の b)「証明書プロファイル」 → c)「追加」をクリックします。



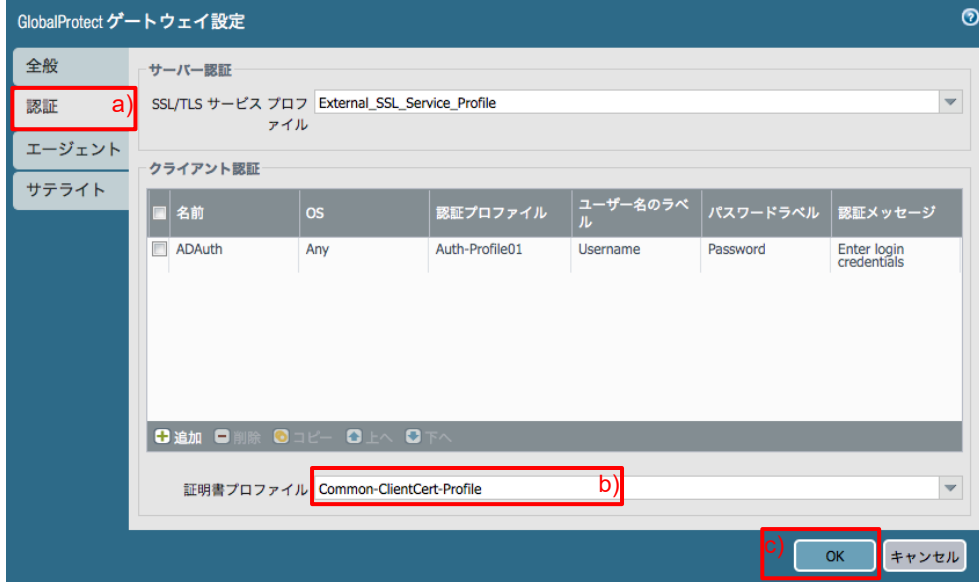
(2) a)名前に「Common-ClientCert-Profile(任意)」と入力し、b)「追加」をクリックします。表示された画面で c)CA 証明書「PA-Certificate-Authority」を選択し、d)「OK」をクリックします。e)「OK」をクリックします。



(3) a)「Network」 → b)「ゲートウェイ」 → c)「External-Gateway」をクリックします。



(4) a)「認証」タブ → b)証明書プロファイルで「Common-ClientCert-Profile」を選択し、d)「OK」をクリックします。



(5) 同様の方法で、Internal-Gateway にも証明書プロファイルを割り当てます。

8.1.3. Portal から共通クライアント証明書を配布する設定

(1) 「Network」タブ → GlobalProtect の下の「Portal」 → 設定済みの Portal をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブの「クライアント証明書」で、b)「ローカル」を選択し、c)「Common-ClientCert」を選択します。

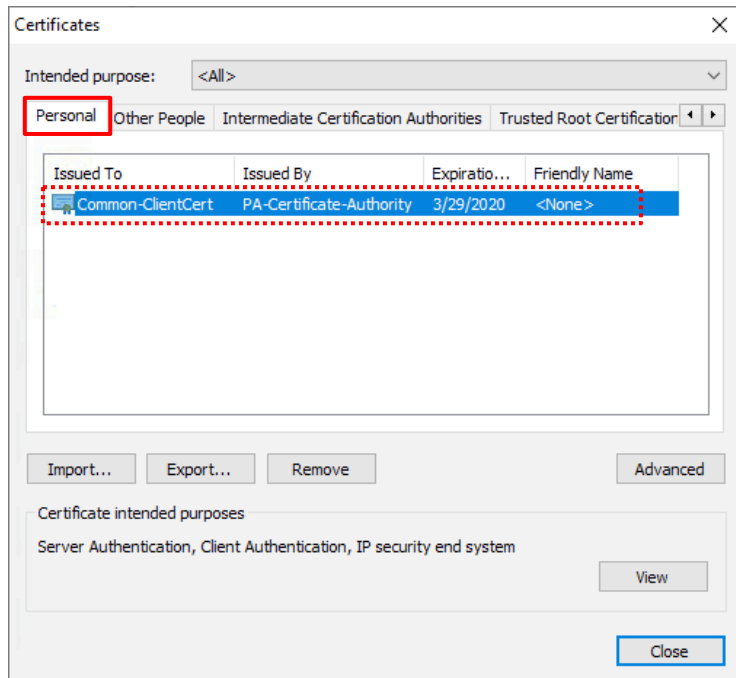


(2) 「コミット」を実施します。

8.1.4. GP Agent からのログイン(1)

GP Agent (例えば、w10-001, w10-002) から Portal へログインすると、Personal の証明書ストアへ、共通クライアント証明書がインポートされます。

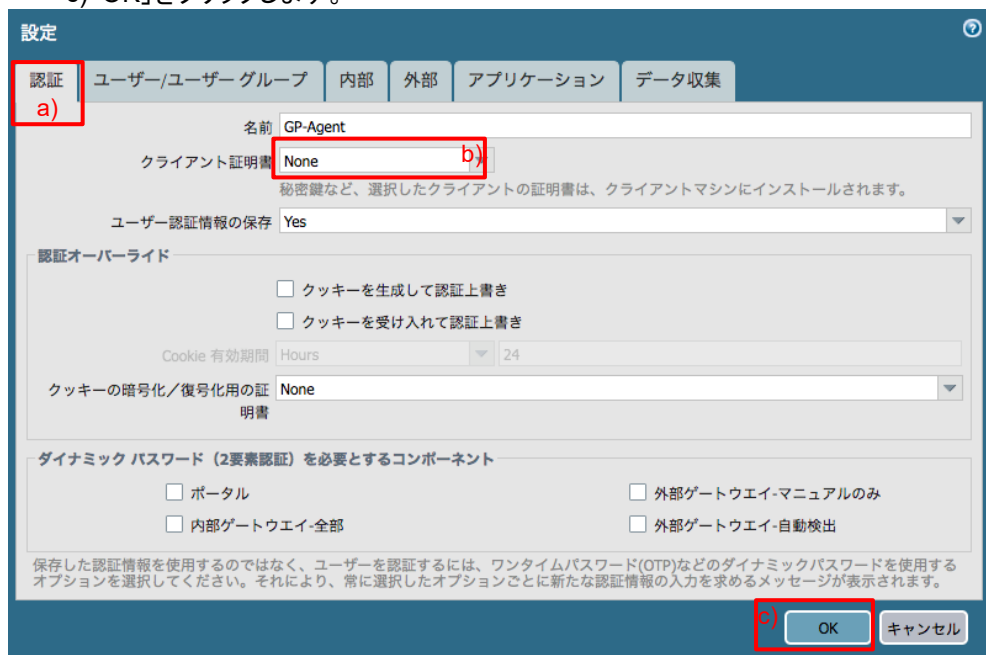
[確認のみ] 例:Chrome ブラウザ → 「設定」 → 「詳細設定」 → 「証明書の管理」で表示された画面で、「Personal」タブをクリックし、クライアント証明書がインポートされていることを確認します。



8.1.5. 共通クライアント証明書配布の解除

GP Agent への共通クライアント証明書の配布が完了したら、配布設定を解除します。

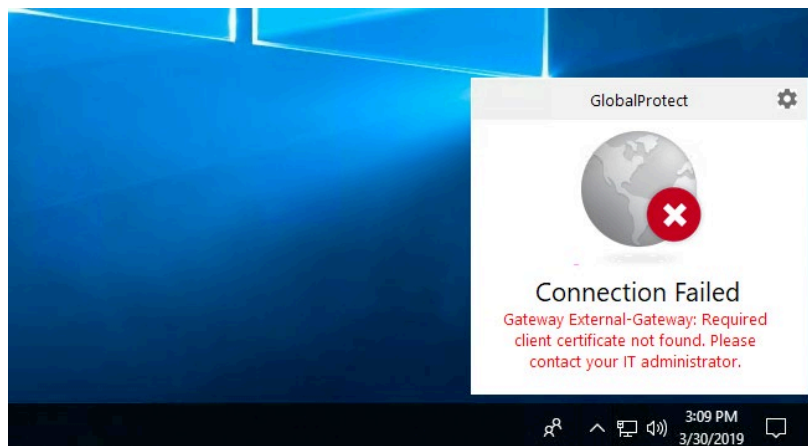
(1) 「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブの「クライアント証明書」で、b)「None」を選択し、c)「OK」をクリックします。



(2) 「コミット」を実施します。

8.1.6. GP Agent からのログイン(2)

クライアント証明書を配布されていないクライアント (例:w10-003) からは接続できません。



8.2. 各ユーザー個別のクライアント証明書で認証 (SCEP 利用による配布)

今回は、「各ユーザーが個別のクライアント証明書を持ち、そのクライアント証明書を持たないクライアント PC は接続させない」という設定を行います。

「各ユーザーに個別のクライアント証明書を渡して、インポート作業をしてもらう」というのも一つの手段ですが、その手間を省く目的で、GlobalProtect では、SCEP (Simple Certificate Enrollment Protocol) を利用して、「ユーザ名とパスワード認証と同時に、ユーザ毎のクライアント証明書を配布する」という機能が提供されていますので、その設定を行います。

8.2.1. SCEP サーバーのインストール

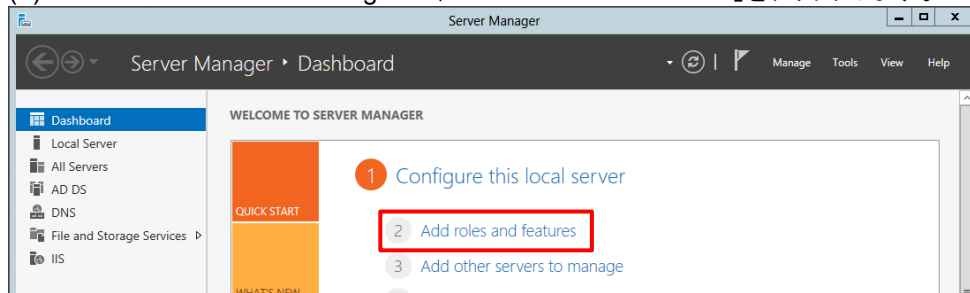
本ガイドでは、認証サーバーとして Win2012 の Active Directory を利用しているため、このサーバーを Certification Authority (認証局) として設定し、このサーバーから、ユーザー認証と同時にクライアント証明書を発行するのが効率的です。

Win2012 の Active Directory Certificate Services (以降、ADCS) は SCEP に対応しているため、その設定を行って利用することになります。

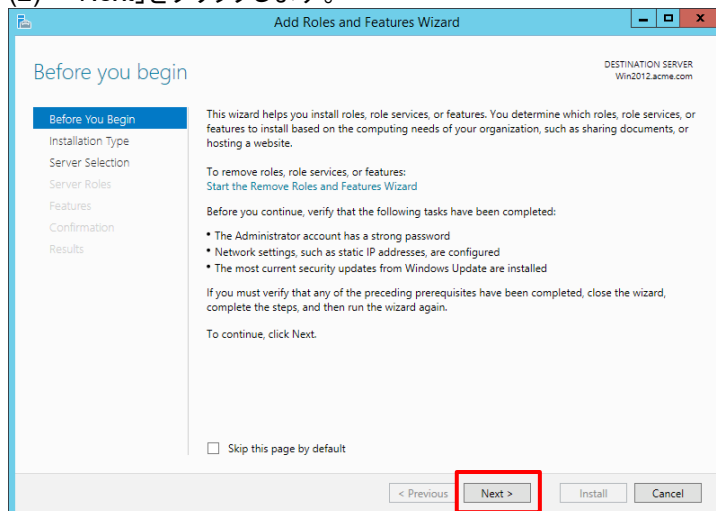
8.2.1.1. IIS のインストール

SCEP でクライアント証明書を発行する際に利用されるプロトコルは HTTP であり、Win2012 では IIS (Internet Information Service) が利用されます。よって IIS をインストールします。

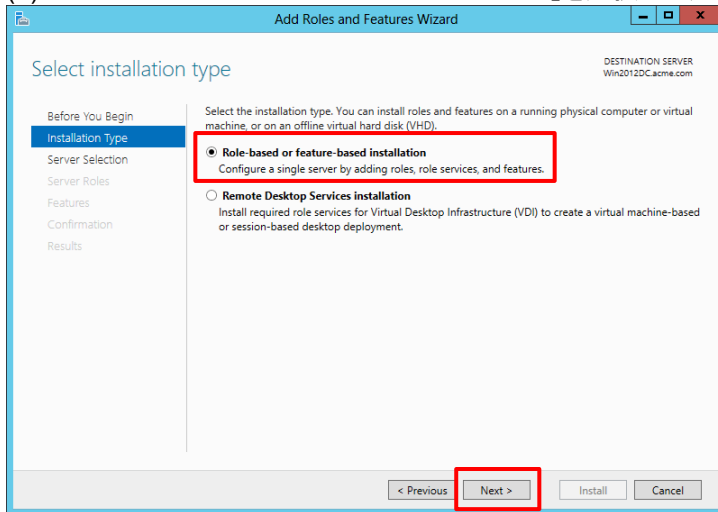
(1) Win2012 の Server Manager で、「Add roles and features」をクリックします。



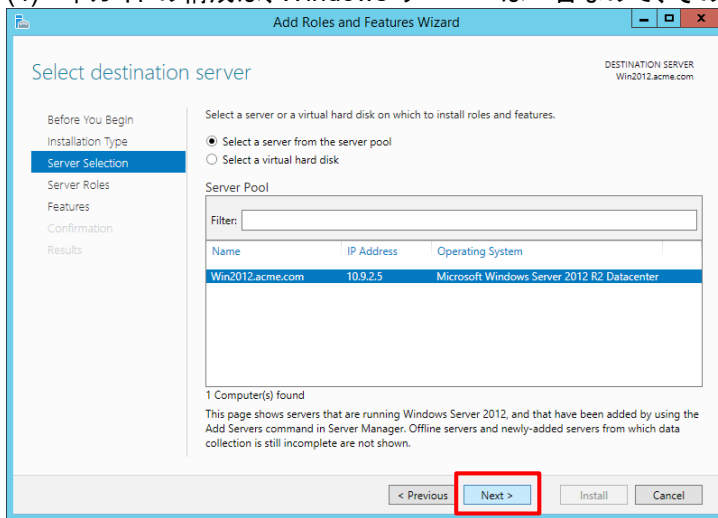
(2) 「Next」をクリックします。



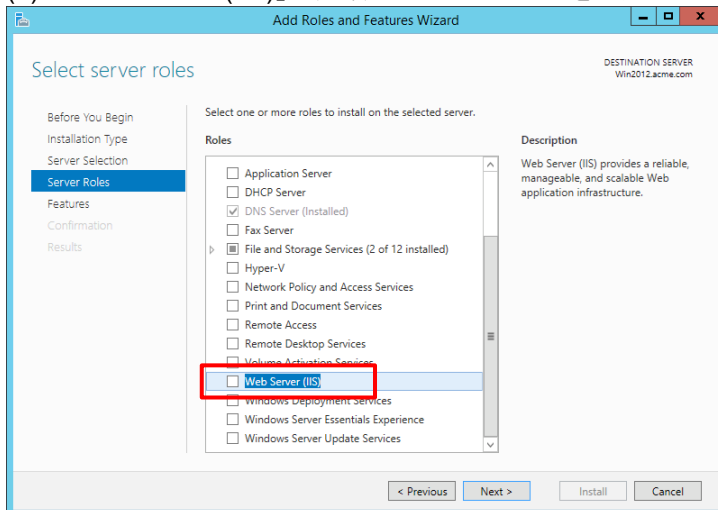
(3) 「Role-based or feature-based installation」を選択して、「Next」をクリックします。



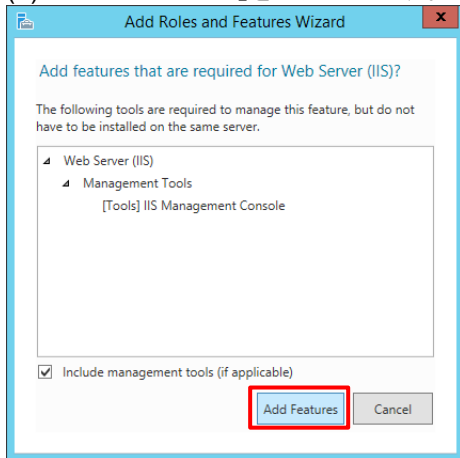
(4) 本ガイドの構成は、Windows サーバーは一台なので、そのまま「Next」をクリックします。



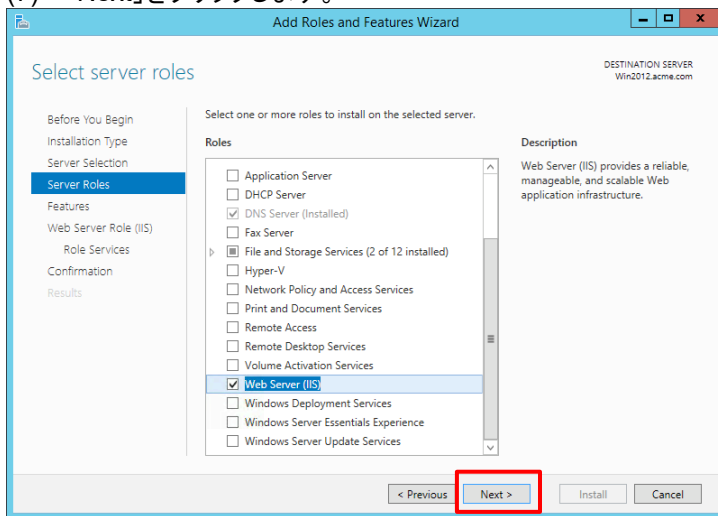
(5) 「Web Server (IIS)」の先頭のチェックボックスをクリックします。



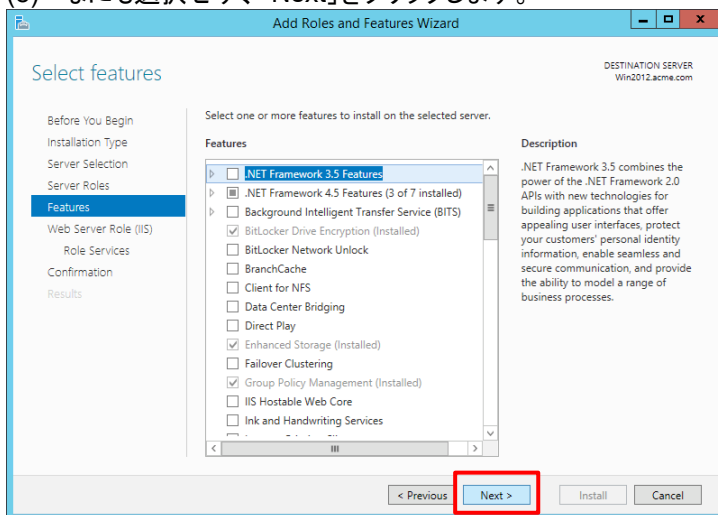
(6) 「Add Features」をクリックします。



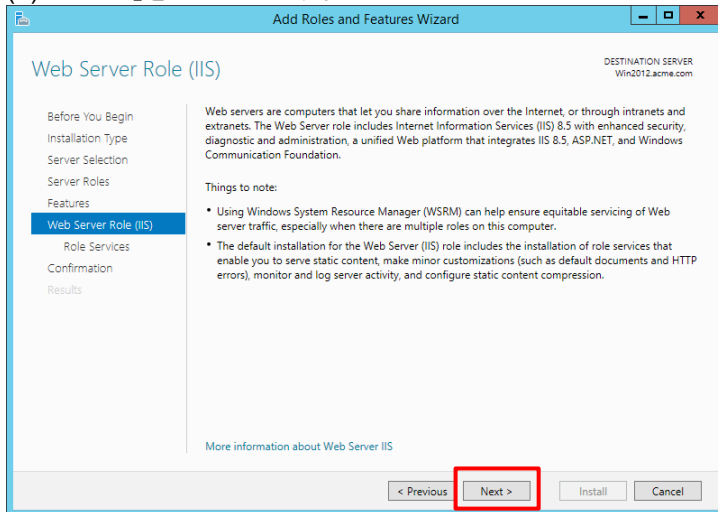
(7) 「Next」をクリックします。



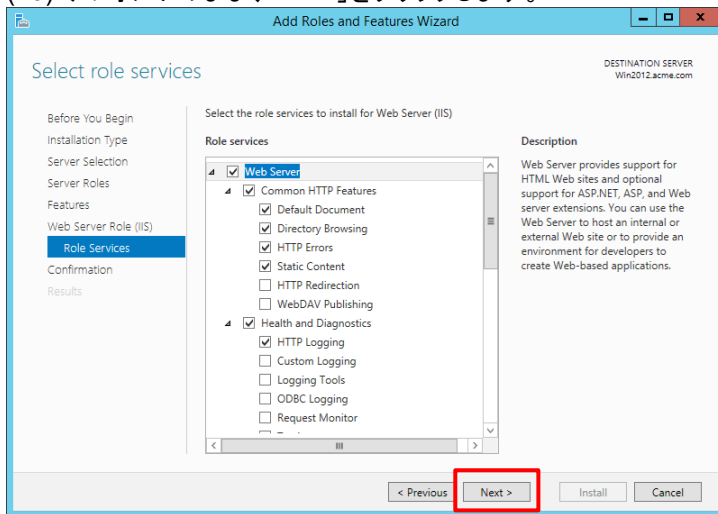
(8) なんにも選択せず、「Next」をクリックします。



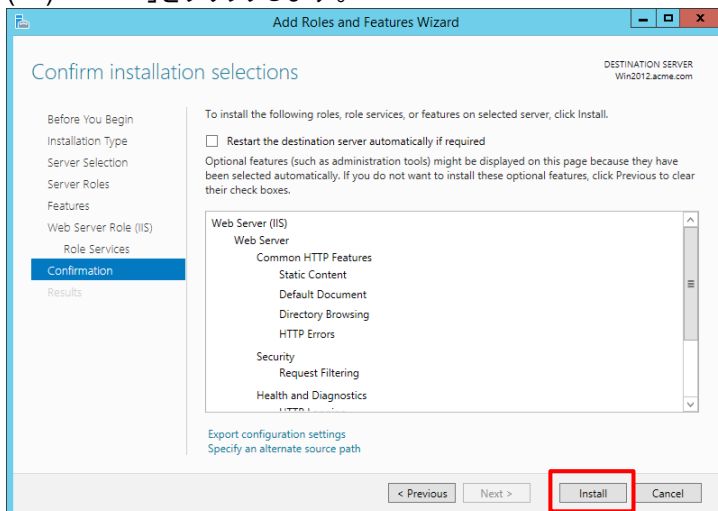
(9) 「Next」をクリックします。



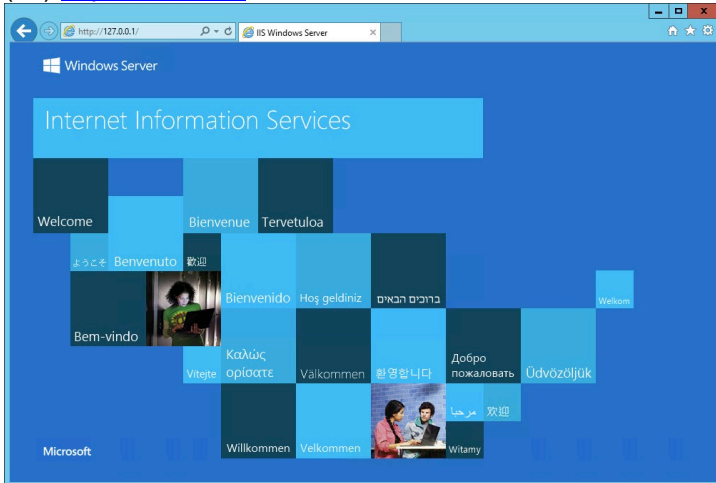
(10) デフォルトのまま、「Next」をクリックします。



(11) 「Install」をクリックします。



(12) <http://127.0.0.1> にアクセスして、IIS が動作することを確認します。



8.2.1.2. ADCS のインストール

ADCS にはいくつかの役割がありますが、ここでは以下 2 つが必要です。

- Certification Authority (以降、CA)
- Network Device Enrollment Service (以降、NDES)

加えて、以下も同時にインストールしておきます(*)。

- Certification Authority Web Enrollment (以降、CAWE)

(*) NDES インストール後に CAWE をインストールすると、Web ブラウザを使ったクライアント証明書発行機能が期待通りに動作しませんでした(Web ブラウザで IIS へアクセスしても、ユーザー単位の認証画面が表示されませんでした)。

この 2 つの機能はどちらも、IIS の「Windows Authentication」を使うので、そこで何らかの問題が発生していると思われるのですが、この事象のトラブルシューティングは、本ガイドの本質ではないので、それ以上は追求しておりません。

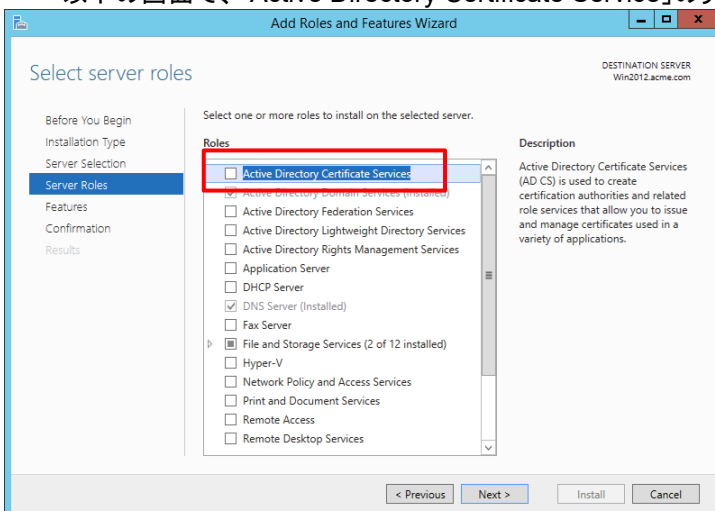
[利用 OS]: Windows Server 2012R2 Version 6.3 (build 9600)

そのため、CAWE は、後章の「スマートデバイスからの接続」で必要になりますので、先にインストールしておきます。

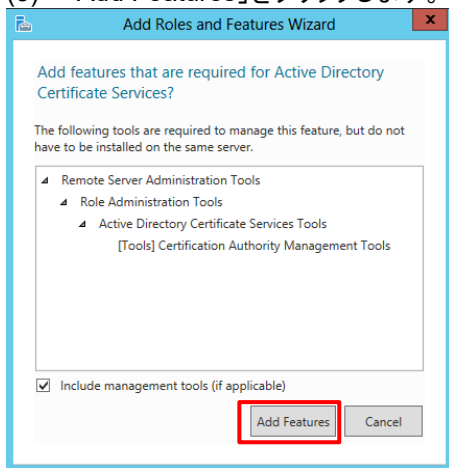
(1) IIS と同様に、Win2012 の Server Manager で、「Add roles and features」をクリックします。

(2) 以下の画面までは「Next」をクリックして進めます。

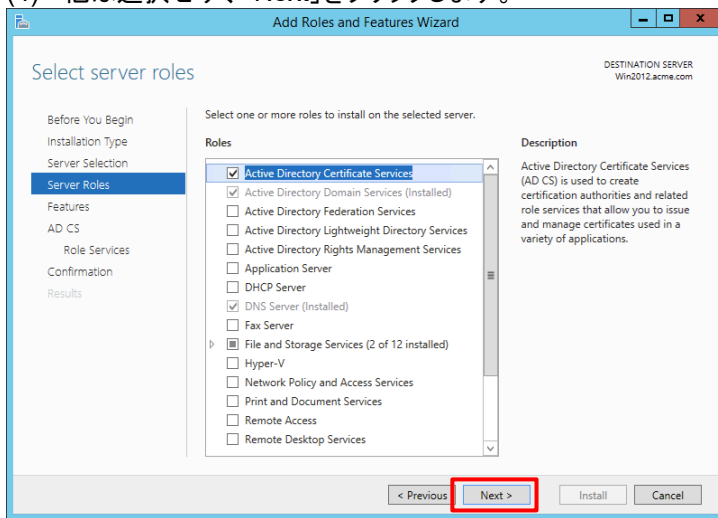
以下の画面で、「Active Directory Certificate Service」の先頭のチェックボックスをクリックします。



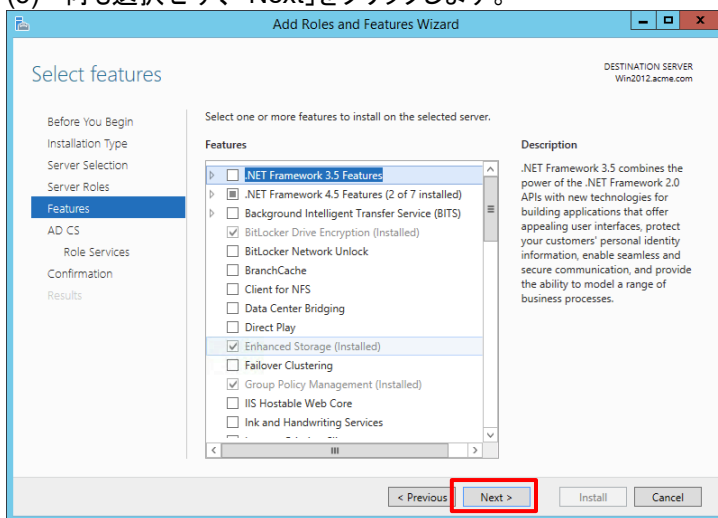
(3) 「Add Features」をクリックします。



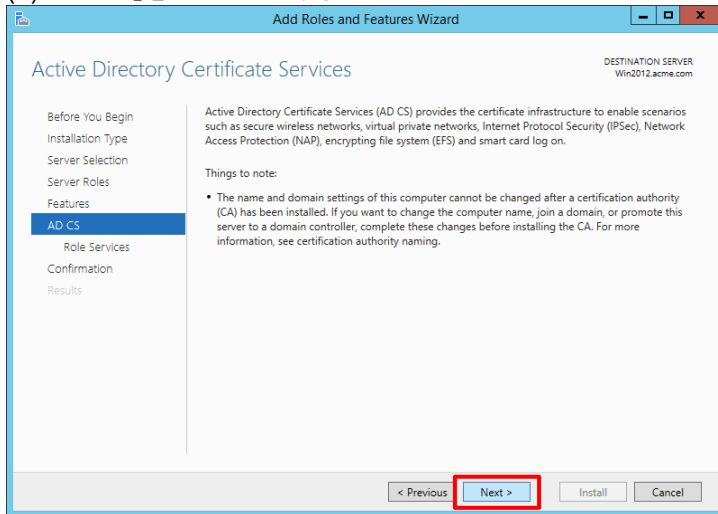
(4) 他は選択せず、「Next」をクリックします。



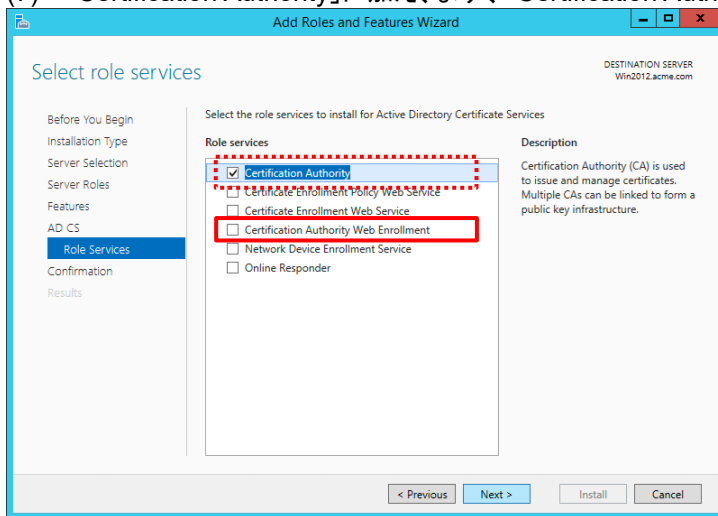
(5) 何も選択せず、「Next」をクリックします。



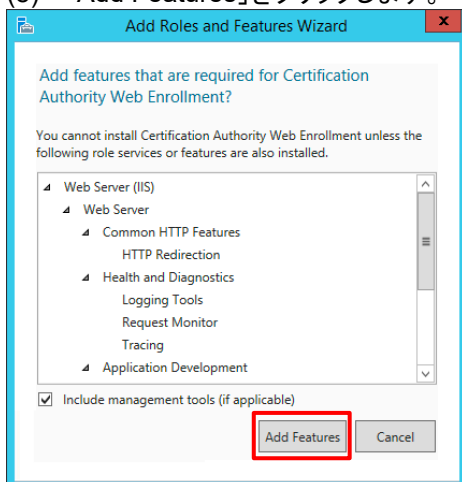
(6) 「Next」をクリックします。



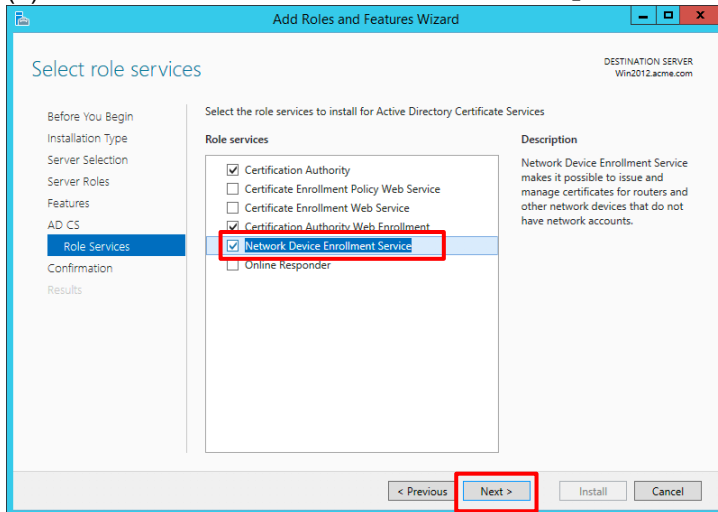
(7) 「Certification Authority」に加え、まず、「Certification Authority Web Enrollment」にチェックを入れます。



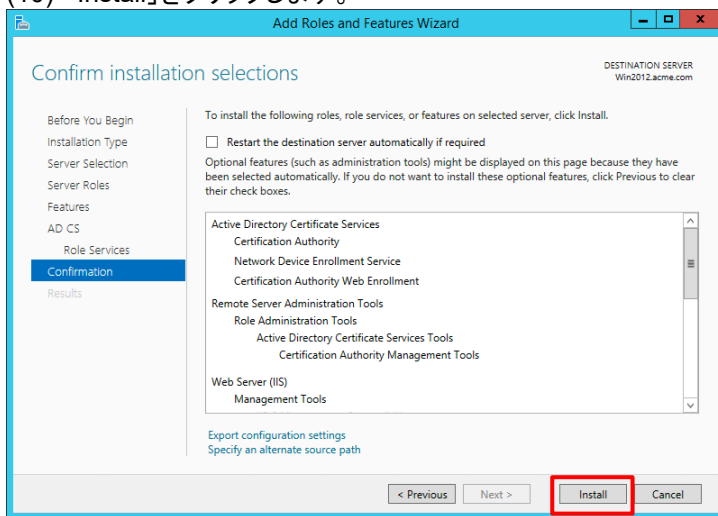
(8) 「Add Features」をクリックします。



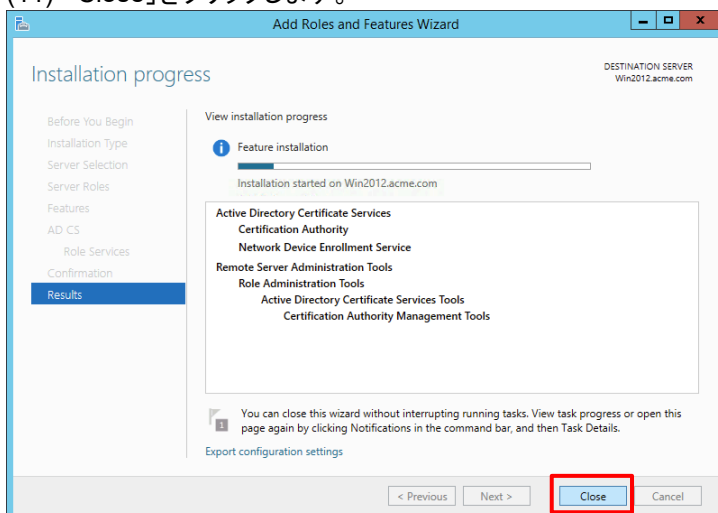
(9) さらに「Networks device Enrollment Service」にもチェックを入れ、「Next」をクリックします。



(10) 「Install」をクリックします。



(11) 「Close」をクリックします。



8.2.2. NDES 用のアカウント設定

PA Firewall が各ユーザー個別のクライアント証明書を NDES に要求する際には、その権限を持つアカウントの設定が必要です。

NDES を設定する際にも、その権限アカウントが要求されるので、事前に「panagent」に権限を設定しておきます。

- (1) Win2012 の「Administrative Tools」 → 「Active Directory Users and Computers」を開きます。
「acme.com」 → 「Users」で、設定済みの「panagent」をダブルクリックします。

The screenshot shows the 'pan agent Properties' dialog box with the 'Account' tab selected. The 'User logon name' field contains 'panagent' and the domain dropdown is set to '@acme.com'. The 'User logon name (pre-Windows 2000)' field contains 'ACME\panagent'. The 'Account expires' section has the 'Never' radio button selected. The 'Add...' button is highlighted with a red box.

- (2) そのアカウントの「Member of」タブで「Add」をクリックし、「IIS_IUSRS」権限を加え、「OK」をクリックします。

The screenshot shows the 'pan agent Properties' dialog box with the 'Member of' tab selected. The 'Add...' button is highlighted with a red box. The 'Member of' list shows 'Domain Users', 'IIS_IUSRS', and 'Server Operators'. The 'OK' button is highlighted with a red box.

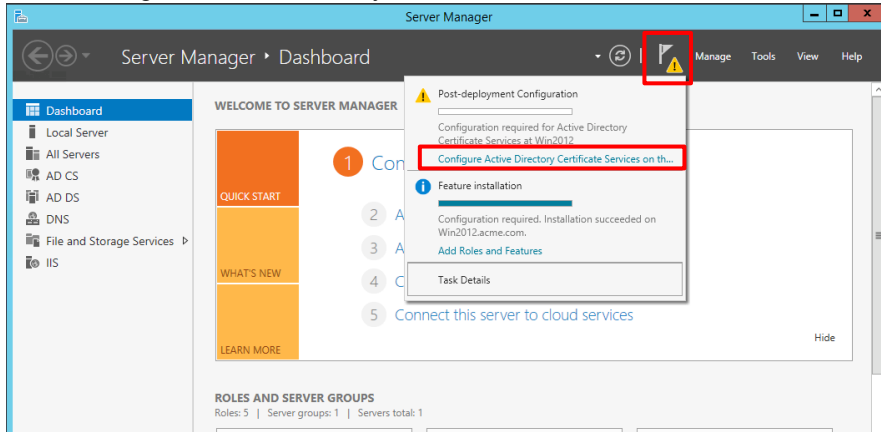
8.2.3. ADCS の設定

ADCS の CA と NDES のインストールが完了し、「panagent」へ必要な権限を付与しましたので、次は設定を行います。

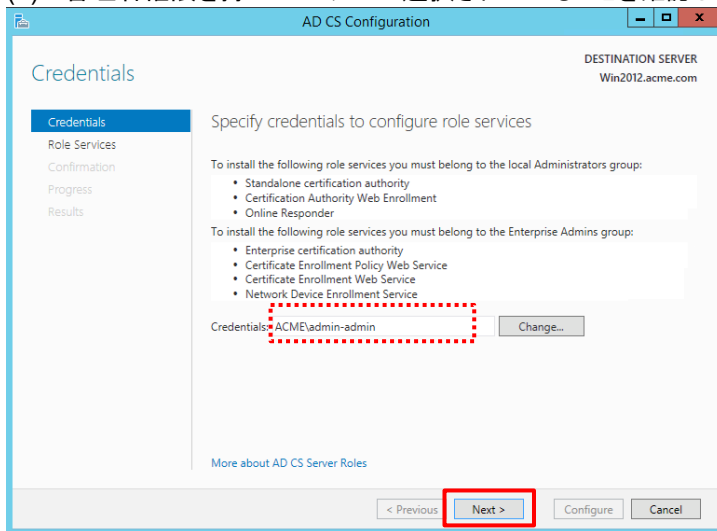
8.2.3.1. CA の設定

(1) Server Manager で警告を示すマークをクリックします。

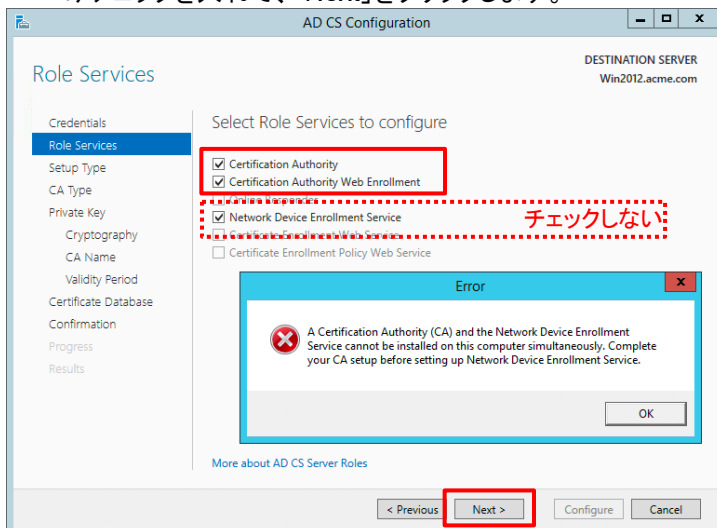
「Configure Active Directory Certificate Service on the destination server」をクリックします。



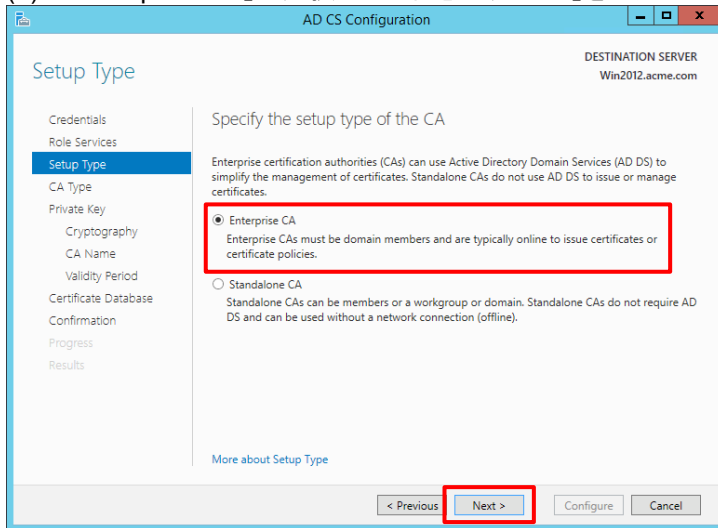
(2) 管理者権限を持つユーザーが選択されていることを確認して、「Next」をクリックします。



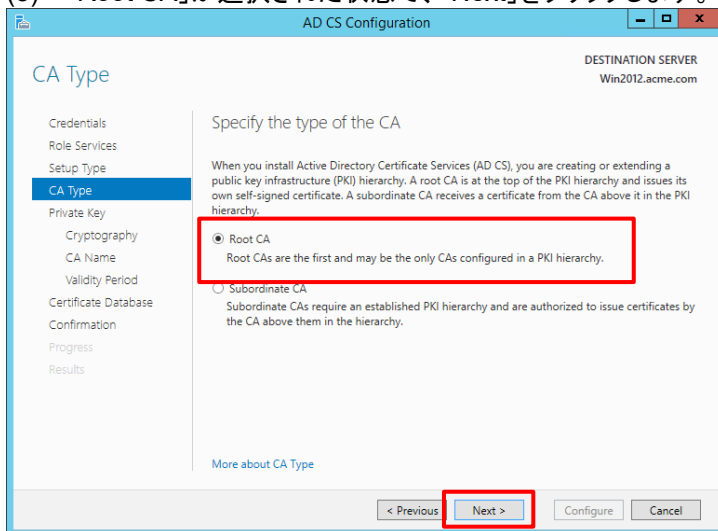
(3) 「Network Device Enrollment Service」も同時にチェックを入れると、以下のように「Certification Authority」を先にインストールするように警告が出ますので、「Certification Authority」と「Certification Authority Web Enrollment」にだけチェックを入れて、「Next」をクリックします。



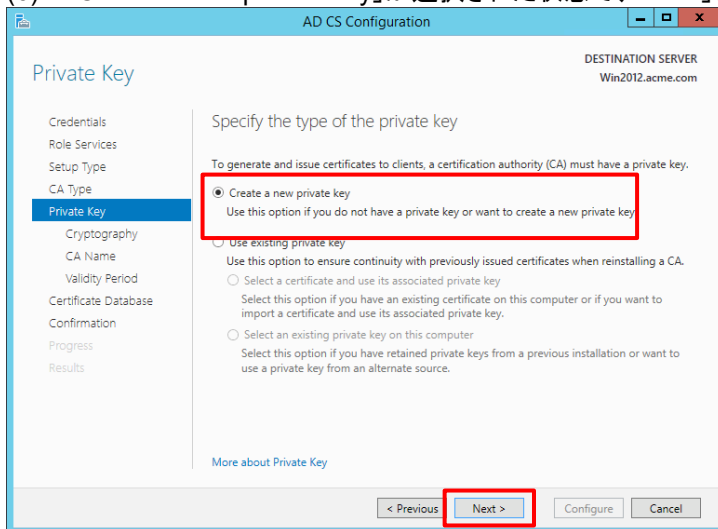
(4) 「Enterprise CA」が選択された状態で、「Next」をクリックします。



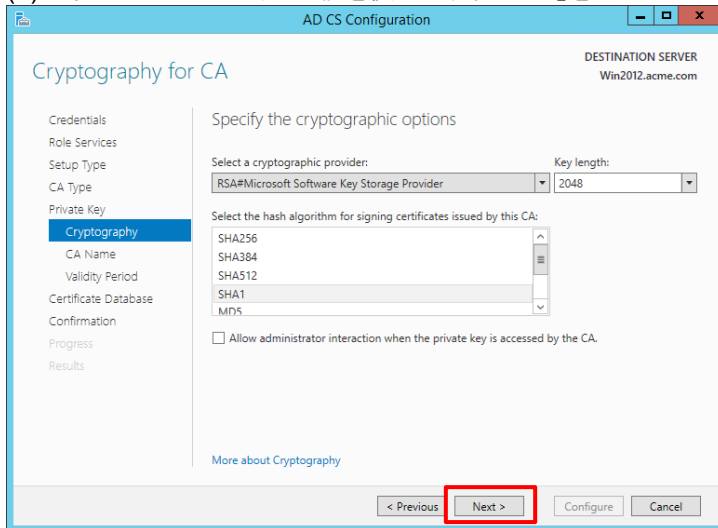
(5) 「Root CA」が選択された状態で、「Next」をクリックします。



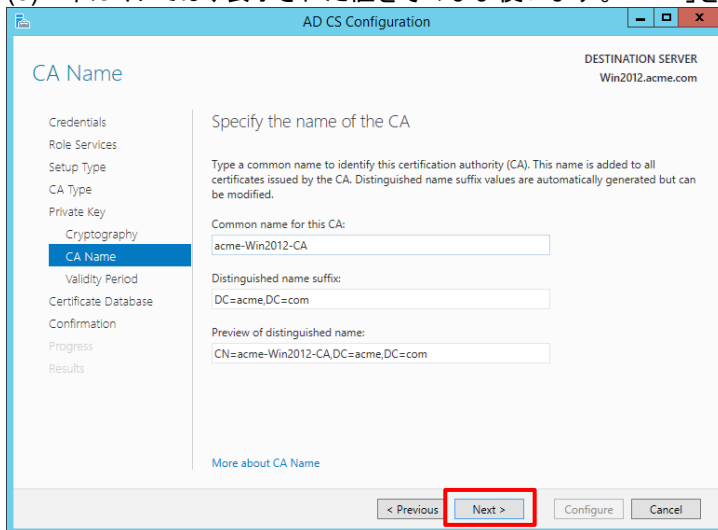
(6) 「Create a new private key」が選択された状態で、「Next」をクリックします。



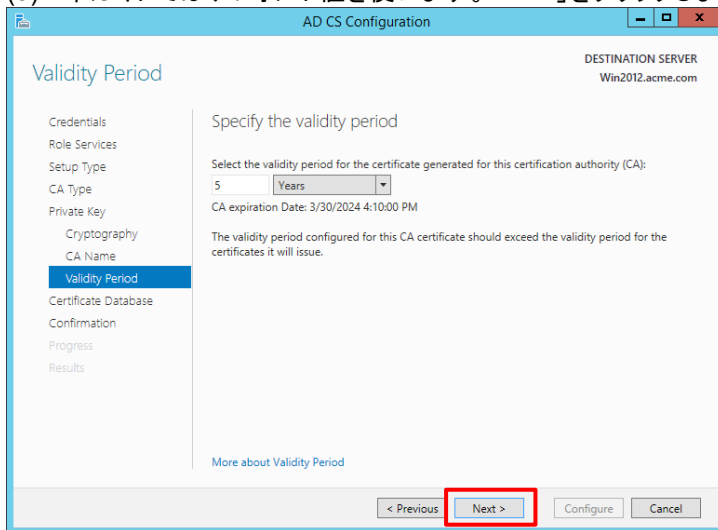
(7) 本ガイドではデフォルト値を使います。「Next」をクリックします。



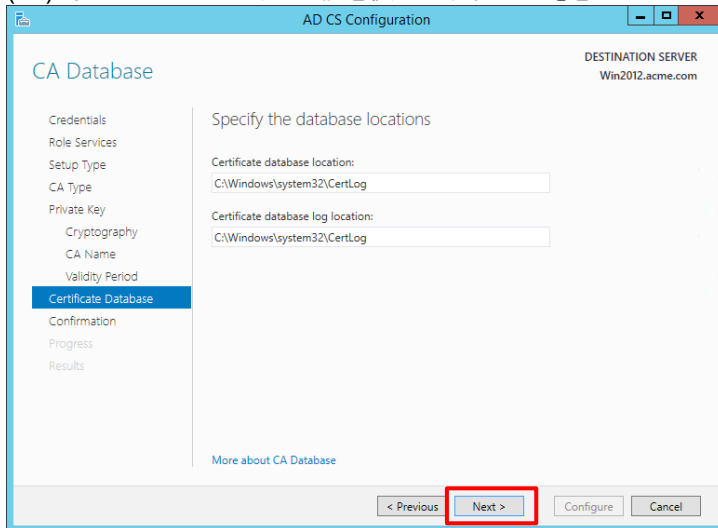
(8) 本ガイドでは、表示された値をそのまま使います。「Next」をクリックします。



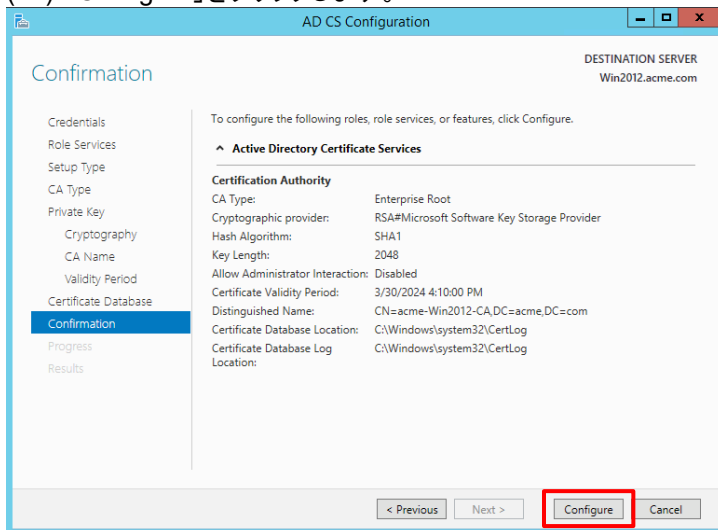
(9) 本ガイドではデフォルト値を使います。「Next」をクリックします。



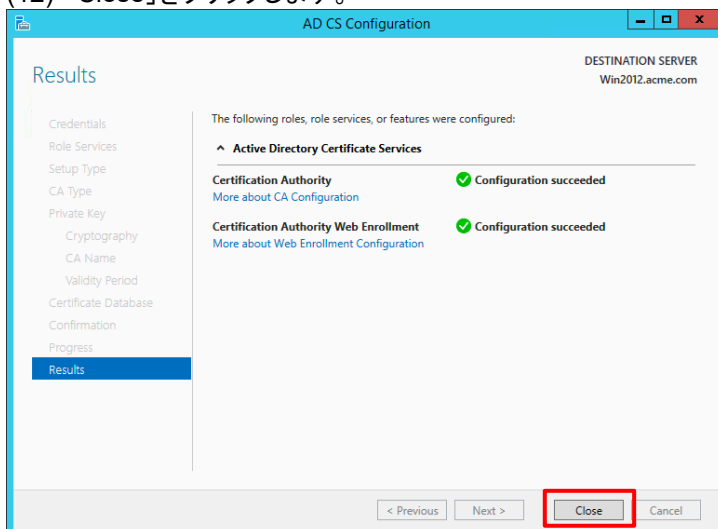
(10) 本ガイドではデフォルト値を使います。「Next」をクリックします。



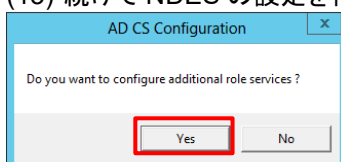
(11) 「Configure」をクリックします。



(12) 「Close」をクリックします。

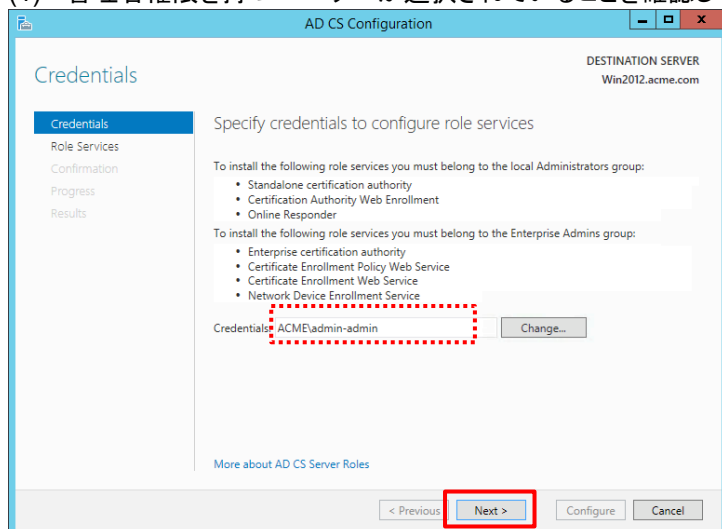


(13) 続けて NDES の設定を行いますので、「Yes」をクリックします。

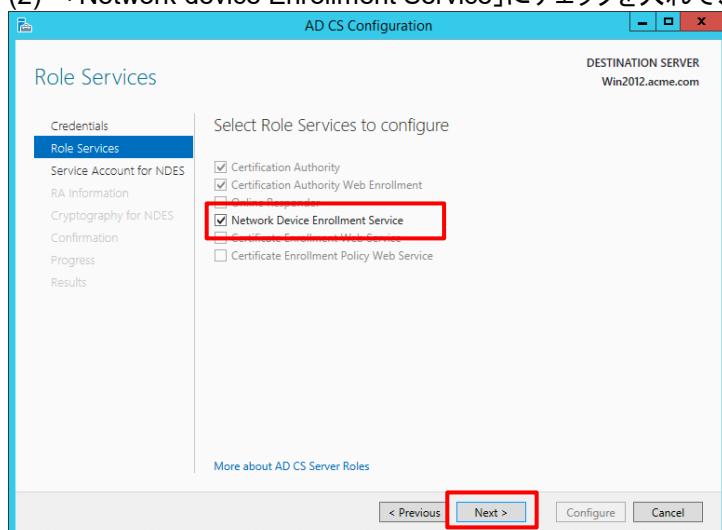


8.2.3.2. NDES の設定

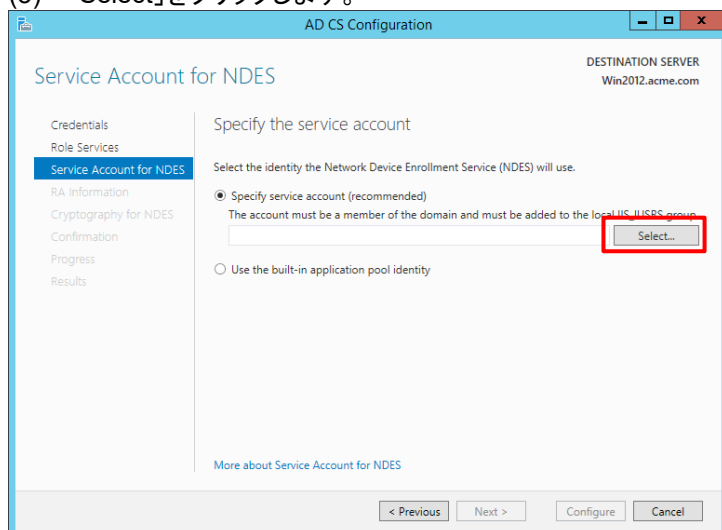
(1) 管理者権限を持つユーザーが選択されていることを確認して、「Next」をクリックします。



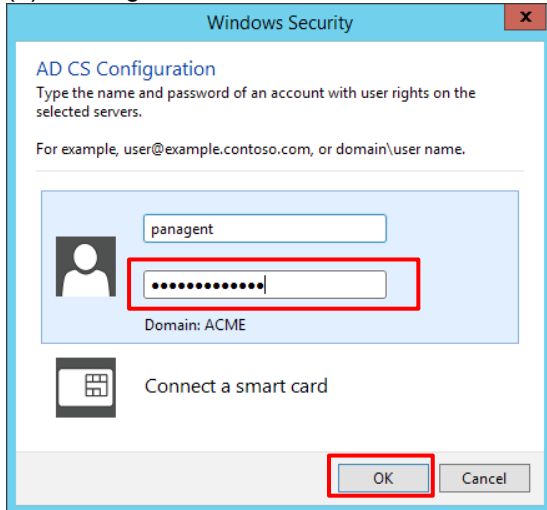
(2) 「Network device Enrollment Service」にチェックを入れて、「Next」をクリックします。



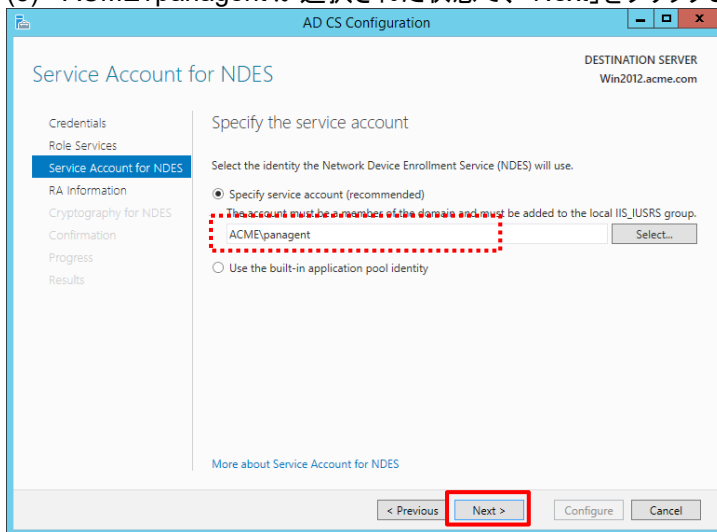
(3) 「Select」をクリックします。



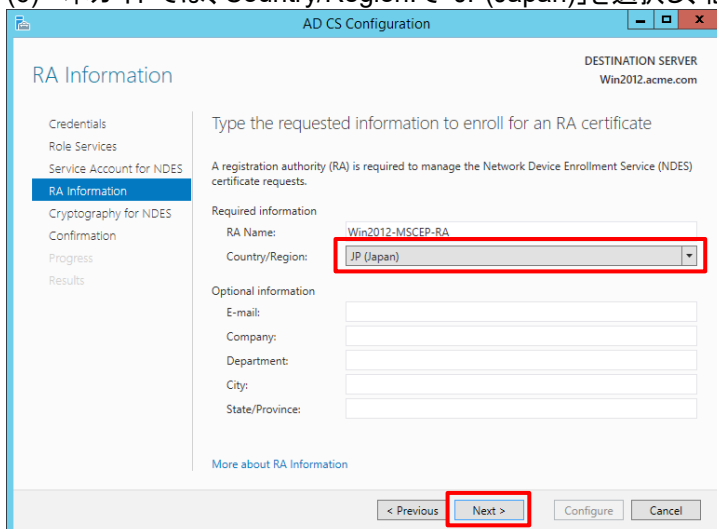
(4) Panagent の認証が必要です。パスワードを入力して、「OK」をクリックします。



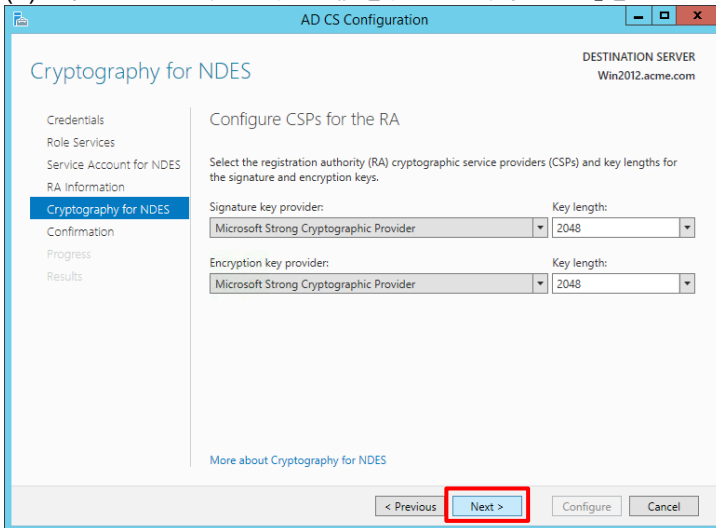
(5) ACME\panagent が選択された状態で、「Next」をクリックします。



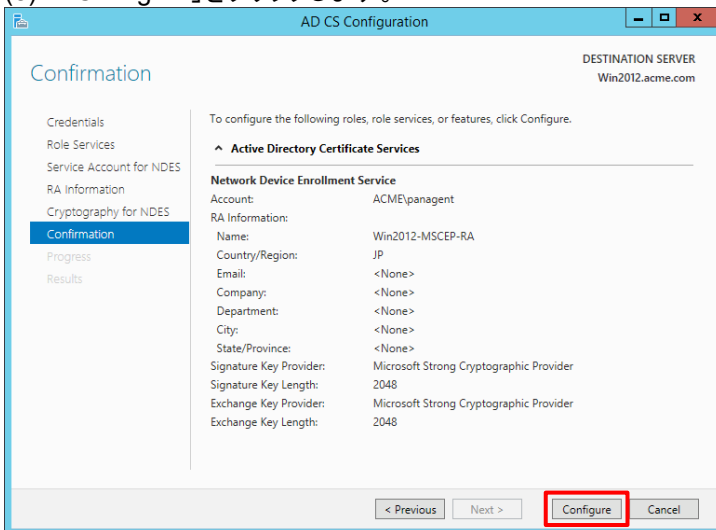
(6) 本ガイドでは、Country/Region:で「JP(Japan)」を選択し、他はブランクのまま、「Next」をクリックします。



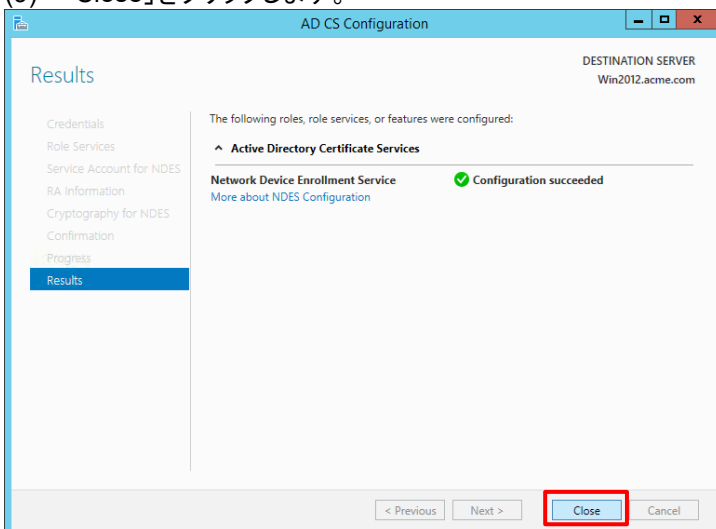
(7) 本ガイドでは、デフォルト値を利用します。「Next」をクリックします。



(8) 「Configure」をクリックします。



(9) 「Close」をクリックします。



8.2.3.3. NDES の動作確認

設定した NDES が動作することを確認します。

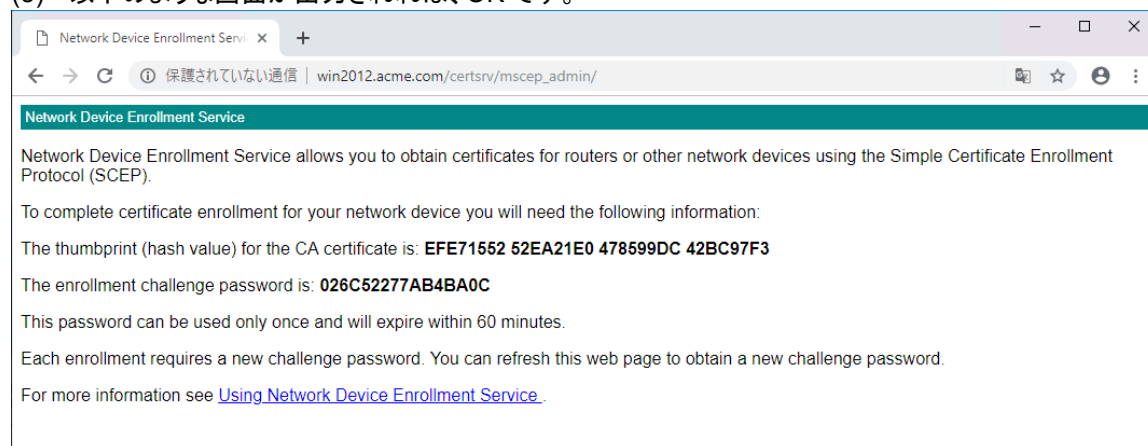
- (1) NDES 設定を行った Win2012 へ到達できる IP アドレスを持つ端末 (例:w10-001) から、下記 Link へアクセスします。

http://win2012.acme.com/certsrv/mscep_admin

- (2) panagent アカウントでログインします。



- (3) 以下のような画面が出力されれば、OK です。



8.2.4. PA Firewall の SCEP 設定

SCEP を使って、PA Firewall が ADCS と接続し、GP Agent の各ユーザーに個別のクライアント証明書が配布できるまでの設定を行います。

8.2.4.1. サービスルートの変更

本ガイドの環境では、ADCS(Win2012)が Trust ゾーンに設置されているので、サービスルートを変更します。

- (1) a)「Device」 → b)「セットアップ」 → c)「サービス」 → d)「サービスルートの設定」で表示された画面で、e)のように、SCEP の送信元インターフェイスおよび送信元アドレスを eth1/2 に変更します。
f)「OK」をクリックします。

The screenshot shows the Palo Alto Networks management console. The 'Device' tab is selected at the top. In the left sidebar, 'セットアップ' (Setup) is highlighted. The main area shows the 'サービス' (Services) configuration page. The 'サービス機能' (Service Features) section has 'サービス ルートの設定' (Service Route Configuration) highlighted. A modal window titled 'サービス ルートの設定' (Service Route Configuration) is open, showing a table of services and their configurations. The 'SCEP' service is selected, and its '送信元インターフェイス' (Source Interface) is set to 'ethernet1/2' and '送信元アドレス' (Source Address) is set to '10.9.2.4/24'. The 'OK' button is highlighted at the bottom right of the modal.

サービス	送信元インターフェイス	送信元アドレス
<input type="checkbox"/> Mia	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Netflow	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> NTP	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Palo Alto Networks サービス	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Panorama	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> プロキシ	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Radius	デフォルトを使用	デフォルトを使用
<input checked="" type="checkbox"/> SCEP	ethernet1/2	10.9.2.4/24
<input type="checkbox"/> SNMP トラップ	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Syslog	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Tacplus	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> UID Agent	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> URL Updates	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> VM モニター	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Wildfire Private	デフォルトを使用	デフォルトを使用

- (2) 「コミット」を実施します。

8.2.4.2. SCEP の設定

(1) a)「Device」 → 「証明書の管理」の下の b)「SCEP」 → c)「追加」をクリックします。



- (2) a) 名前に「WIN2012_SCEP(任意)」と入力します。
ワンタイムパスワード(チャレンジ):
b) SCEP チャレンジで「ダイナミック」を選択します。
c) サーバー URL に「http://win2012.acme.com/certsrv/mscep_admin/」と入力します。
d) ユーザー名:「acme\panagent」と入力します。
e) パスワードおよび再入力パスワードに、panagent のパスワードを入力します。
設定:
f) サーバー URL に「http://win2012.acme.com/certsrv/mscep/mscep.dll」と入力します。
g) CA-IDENT 名に「WIN2012-CA(任意)」と入力します。
暗号設定:
h) ビット数は「2048」を選択します。
i) CSR のダイジェストは「sha1」を選択します。
j) 「OK」をクリックします。

The screenshot shows the 'SCEP 設定' (SCEP Configuration) form. The fields are as follows:
- 名前 (Name): WIN2012_SCEP (labeled a)
- ワンタイムパスワード (チャレンジ) (One-time password (challenge)):
 - SCEP チャレンジ (SCEP challenge): ダイナミック (Dynamic) (labeled b)
 - サーバー URL (Server URL): http://win2012.acme.com/certsrv/mscep_admin/ (labeled c)
 - ユーザー名 (Username): acme\panagent (labeled d)
 - パスワード (Password): (labeled e)
 - 再入力パスワード (Re-enter password): (labeled e)
- 設定 (Settings):
 - サーバー URL (Server URL): http://win2012.acme.com/certsrv/mscep/mscep.dll (labeled f)
 - CA-IDENT 名 (CA-IDENT name): WIN2012-CA (labeled g)
 - サブジェクト (Subject): CN=\$USERNAME
 - サブジェクトの代替名タイプ (Subject alternate name type): None
- 暗号設定 (Encryption settings):
 - ビット数 (Bits): 2048 (labeled h)
 - CSR のダイジェスト (CSR digest): sha1 (labeled i)
 - デジタル署名として使用 (Use as digital signature):
 - 鍵の暗号化に使用 (Use for key encryption):
 - CA 証明書フィンガープリント (CA certificate fingerprint):
- SCEP Server SSL Authentication:
 - CA 証明書 (CA certificate): None
 - クライアント証明書 (Client certificate): None
At the bottom right, the 'OK' button is highlighted with a red box labeled 'j)'.

8.2.4.3. ルート証明書が自動的にインポートされたことの確認

[確認のみ] a)「Device」 → 「証明書の管理」の下の b)「証明書」をクリックします。
 実施した SCEP 設定により、c) Win2012 の CA のルート証明書が自動的に取り込まれます。



8.2.4.4. 証明書プロファイルの設定

Win2012 のルート証明書を使った証明書プロファイルを設定します。

(1) a)「Device」 → 「証明書の管理」の下の b)「証明書プロファイル」 → c)「追加」をクリックします。



(2) a) 名前に「WIN2012-CA-Profile(任意)」と入力します。
 b) 「追加」をクリックして、c)「WIN2012_SCEP」を選択します。
 d) 「OK」をクリックします。



8.2.4.5. Portal の設定

- (1) 「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブの「クライアント証明書」で、b)「SCEP」を選択し、c)設定済みの SCEP 設定:「WIN2012_SCEP」を選択します。

設定

認証 a) ユーザー/ユーザーグループ 内部 外部 アプリケーション データ収集

名前 GP-Agent

クライアント証明書 SCEP b) WIN2012_SCEP c)

秘密鍵など、選択したクライアントの証明書は、クライアントマシンにインストールされます。

ユーザー認証情報の保存 Yes

認証オーバーライド

クッキーを生成して認証上書き

クッキーを受け入れて認証上書き

Cookie 有効期間 Hours 24

クッキーの暗号化/復号化用の証明書 None

ダイナミック パスワード (2要素認証) を必要とするコンポーネント

ポータル 外部ゲートウェイ-マニュアルのみ

内部ゲートウェイ-全部 外部ゲートウェイ-自動検出

保存した認証情報を使用するのではなく、ユーザーを認証するには、ワンタイムパスワード(OTP)などのダイナミックパスワードを使用するオプションを選択してください。それにより、常に選択したオプションごとに新たな認証情報の入力を求めるメッセージが表示されます。

OK キャンセル

- (2) a)「アプリケーション」タブ→b)「クライアントの証明書ストアの検索」で「User」を選択します(*)。
- c)「OK」をクリックします。

設定

認証 ユーザー/ユーザーグループ 内部 外部 アプリケーション a) データ収集

アプリケーション設定

ウェルカム ページ factory-default

GlobalProtect アプリの無効化

パスコード

再入力 パスコード

無効にできる最大回数 0

タイムアウトの無効化(分) 0

Mobile Security Manager の設定

モバイル セキュリティ マネージャ

登録ポート 443

クライアントの証明書ストアの検索 b) User

SCEP 証明書更新期間 (日) User

クライアント証明書向けの拡張キー使用OID Machine

スマートカードの取り外し時に接続を維持 (Windows のみ) User and Machine

OK キャンセル

(*) Windows ドメインに参加しているクライアント PC の場合、マシン証明書を持っている場合があります。

GP 設定のデフォルトでは、「User and Machine」=「個人(Personal)ストアとマシン証明書の両方」を検索するようになっています。

この設定のままでは、「SCEP で配布したクライアント証明書の有無で接続許可・拒否をコントロールしたいのに、マシン証明書があればクライアント証明書がなくても接続できてしまう」という状況になってしまいます。

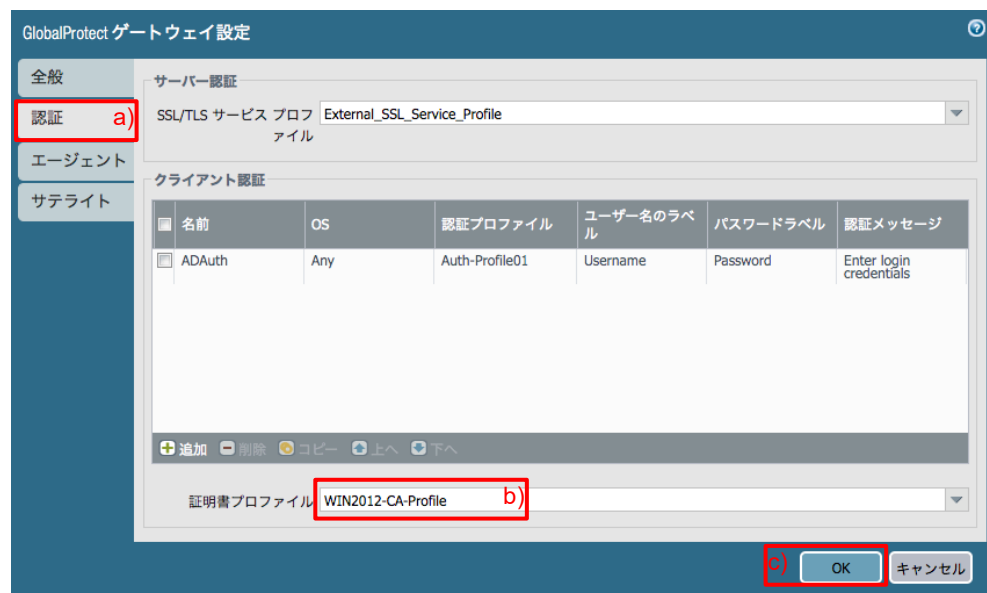
よって、「User」=「個人(Personal)ストア」だけを参照するように、この設定変更を行います。

- (3) GlobalProtect Portal の設定を、「OK」をクリックして閉じます。

8.2.4.6. Gateway の設定

Portal から SCEP で配布したクライアント証明書で、各 Gateway がクライアント証明書認証を行うためには、設定済みの証明書プロファイルを Gateway に割り当てる必要があります。

- (1) 「Network」タブ → GlobalProtect の下の「ゲートウェイ」 → 設定済みの「External-Gateway」をクリック → a)「認証」タブ → b)証明書プロファイルで、「WIN2012-CA-Profile」を選択します。
c)「OK」をクリックします。



- (2) 同様の方法で、Internal-Gateway にも、同じ証明書プロファイルを割り当てます。



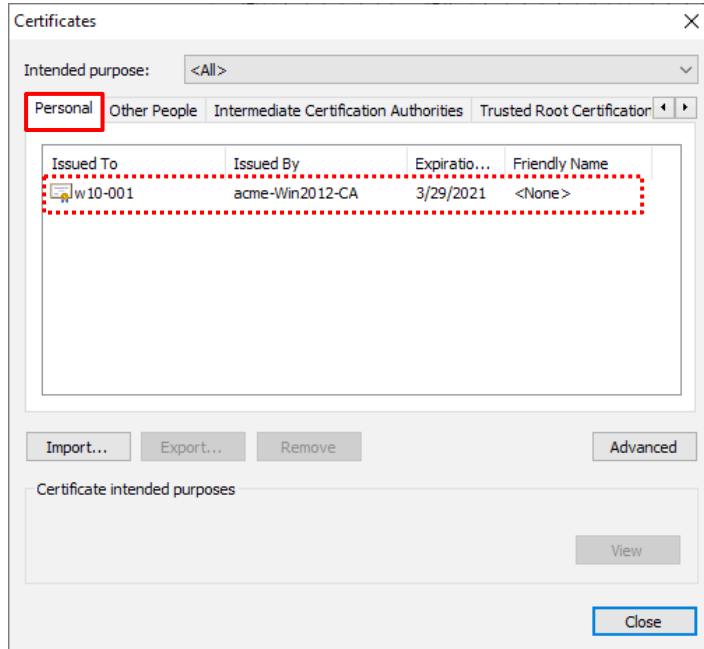
- (3) 「コミット」を実施します。

8.2.5. GP Agent からのログイン(1)

GP Agent から Portal へログインすると、「Personal」証明書ストアへ、ユーザー毎のクライアント証明書がインポートされます。本ガイドでは、w10-001~w10-003 の3つのクライアントからログインします。

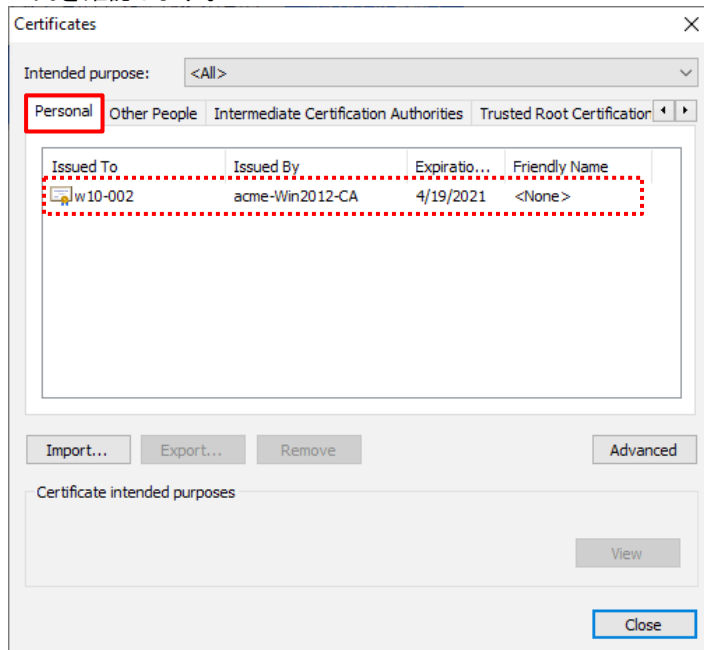
(1) Trust に接続された GP Agent (w10-001)

[確認のみ] 例:Chrome ブラウザ → 「設定」 → 「詳細設定」 → 「証明書の管理」で表示された画面で、「Personal」タブ内を確認します。



(2) インターネットからアクセスした GP Agent (w10-002)

[確認のみ] 例:Chrome ブラウザ → 「設定」 → 「詳細設定」 → 「証明書の管理」で表示された画面で、「Personal」タブ内を確認します。



(3) インターネット側の GP Agent (w10-003)

GP Agent からアクセスして、同様の方法で、クライアント証明書を確認します。

8.2.6. クライアント証明書配布の解除

GP Agent への共通クライアント証明書の配布が完了したら、SCEP による配布設定を解除します(*)。

(*) SCEP サーバ側でクライアント証明書の再発行をコントロールすることが可能であれば、ここで行う SCEP 配布設定の解除は必要ないと思われます。

しかし、本ガイドの作成時点では、SCEP サーバである ADCS で、その方法が見つけられないため、GlobalProtect 側で制御することにします。

- (1) 「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブの「クライアント証明書」で、b)「None」を選択し、c)「OK」をクリックします。

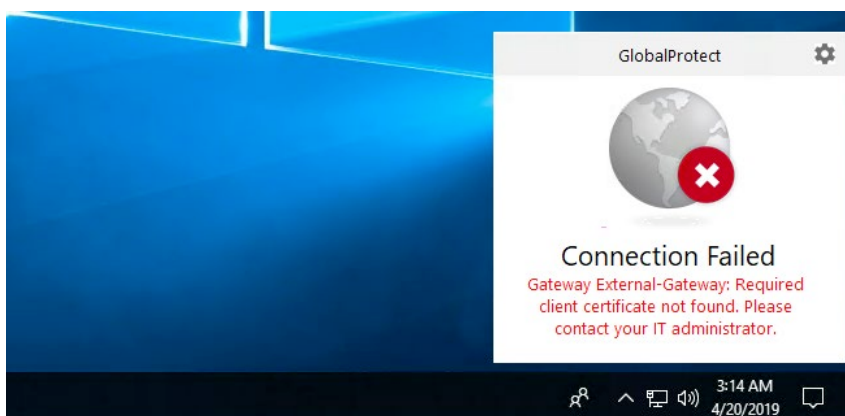
The screenshot shows the '設定' (Settings) window for the 'GP-Agent' portal. The '認証' (Authentication) tab is selected. The 'クライアント証明書' (Client Certificate) dropdown menu is set to 'None'. The 'OK' button is highlighted with a red box.

- (2) 「コミット」を実施します。

8.2.7. GP Agent からのログイン(2)

クライアント証明書を配布されていないユーザーを想定して、一つのクライアント PC(例:w10-002)からクライアント証明書を削除します。

下記のように接続ができないことを確認します。



(Portal で再度 SCEP 設定し、もう一度 GP Agent からアクセスすれば、再びクライアント証明書は配布されます。)

8.3. CRL によるクライアント証明書の失効管理

配布したクライアント証明書を失効させることで、クライアント証明書を持っていても GlobalProtect に接続できないように制御する方法の一つとして、CRL (Certificate Revocation List) があります。

例えば、「退社する社員」や「過ぎて紛失してしまった」クライアント PC を接続できないようにしたい場合に有効です。

CRL は名前の通り、失効した証明書の一覧であり、テキストファイルです。
そのテキストファイルを、PA Firewall が認証局から、例えば HTTP を使って取得する、という単純なものです。

その CRL テキストファイルを取得するには、クライアント証明書内に、CRL の配布元である CRL Distribution Point (以降、CDP) が記載されている必要があります。

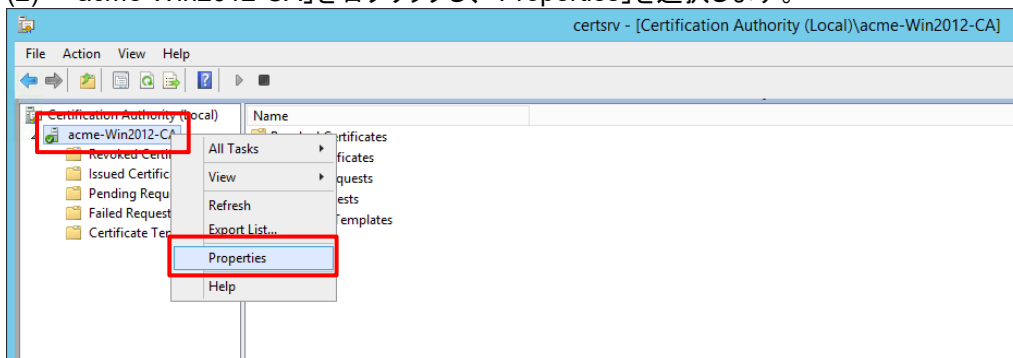
本ガイドでは、Win2012 を CDP として設定し、クライアント証明書に CDP 値を書き込みます。
PA Firewall が、クライアント証明書内の CDP 宛にアクセスして、CRL を取得する、という設定を行います。

8.3.1. CDP の設定

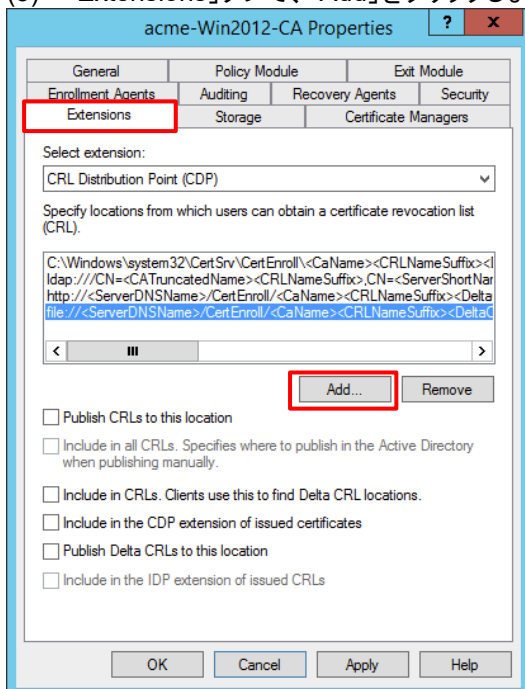
8.3.1.1. CA の設定

(1) Win2012 の Administration Tools から「Certification Authority」を開きます。

(2) 「acme-Win2012-CA」を右クリックし、「Properties」を選択します。



(3) 「Extensions」タブで、「Add」をクリックします。



(4) 「Location:」に、「http://win2012.acme.com/crld/」と入力し、「Variable:」で、以下の 4 ステップを行います。

- 「<CaName>」を選択して、「Insert」をクリックします。
- 「<CRLNameSuffix>」を選択して、「Insert」をクリックします。
- 「<DeltaCRLAllowed>」を選択して、「Insert」をクリックします。
- 末尾に「.crf」と入力します。

結果、「Location:」が以下の文字列になります。

<http://win2012.acme.com/crld/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crf>

「OK」をクリックします。

The screenshot shows the 'Add Location' dialog box. The 'Location:' field contains the URL 'http://win2012.acme.com/crld/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crf'. The 'Variable:' dropdown is set to '<DeltaCRLAllowed>' and the 'Insert' button is highlighted. The 'OK' button is also highlighted.

(5) 以下 2 つにチェックを入れます。

- Include in CRLs. Clients use this to find Delta CRL locations.
- Include in the CDP extension of issued certificates

「Apply」をクリックします。

The screenshot shows the 'acme-Win2012-CA Properties' dialog box, 'Extensions' tab. The 'CRL Distribution Point (CDP)' extension is selected. The 'Specify locations from which users can obtain a certificate revocation list (CRL)' field contains the URL 'http://win2012.acme.com/crld/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crf'. The 'Include in CRLs. Clients use this to find Delta CRL locations.' and 'Include in the CDP extension of issued certificates' checkboxes are checked. The 'Apply' button is highlighted.

(6) 一旦、「No」をクリックします。

The screenshot shows the 'Certification Authority' dialog box. A warning message says 'You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now?'. The 'No' button is highlighted.

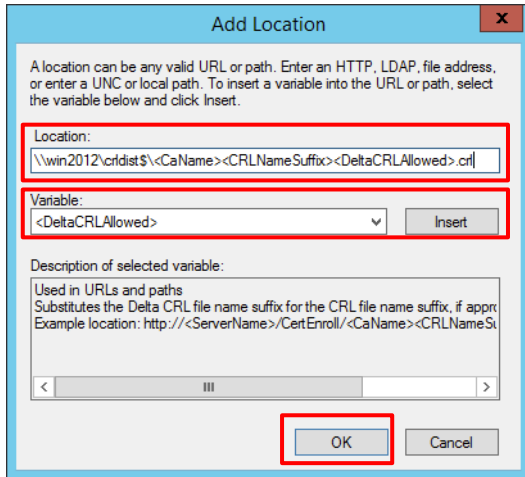
(7) 再度、「Extensions」タブで、「Add」をクリックします。

- (8) 「Location:」に、「¥¥win2012¥crldist¥¥」と入力し、「Variable:」で、以下の 4 ステップを行います。
 (「win2012」は、本ガイドの Win2012 のコンピューター名です。)
- 「<CaName>」を選択して、「Insert」をクリックします。
 - 「<CRLNameSuffix>」を選択して、「Insert」をクリックします。
 - 「<DeltaCRLAllowed>」を選択して、「Insert」をクリックします。
 - 末尾に「.crl」と入力します。

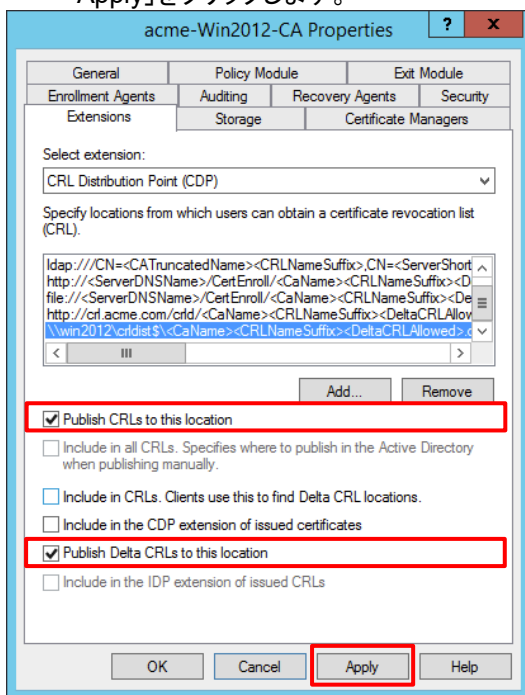
結果、「Location:」が以下の文字列になります。

[¥¥win2012¥crldist¥¥<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl](#)

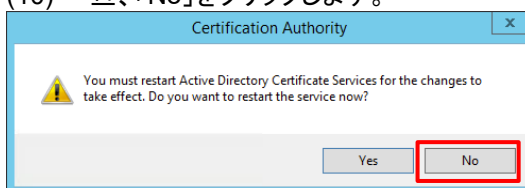
「OK」をクリックします。



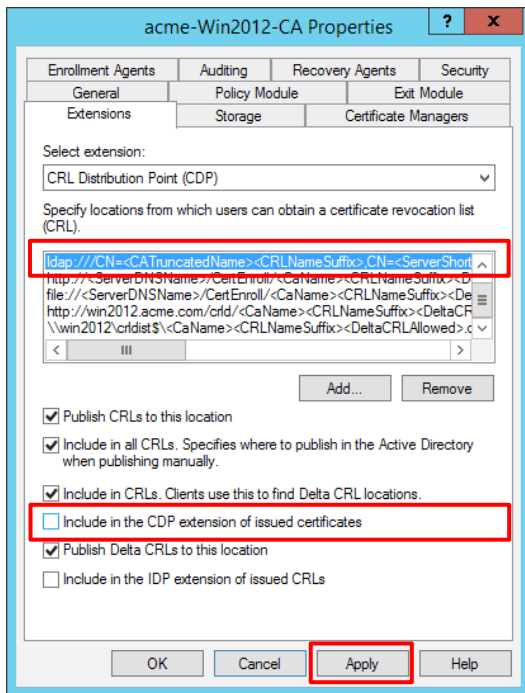
- (9) 以下 2 つにチェックを入れます。
- Publish CRLs to this location
 - Publish Delta CRLs to this location
- 「Apply」をクリックします。



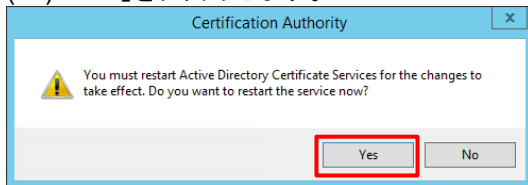
- (10) 一旦、「No」をクリックします。



- (11) 「ldap://～」で始まるものを選んで、「Include in the CDP extension of issued certificates」のチェックを外します。
(デフォルトでは、クライアント証明書の CDP 値に、これを書き込まれていますので、書き込まれないようにします。)
「Apply」をクリックします。



- (12) 「Yes」をクリックします。

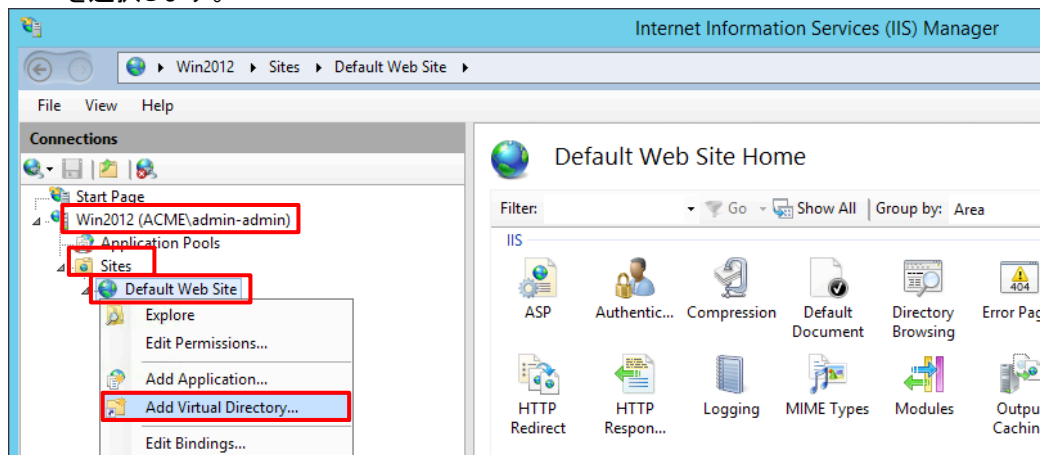


- (13) Certification Authority を閉じます。

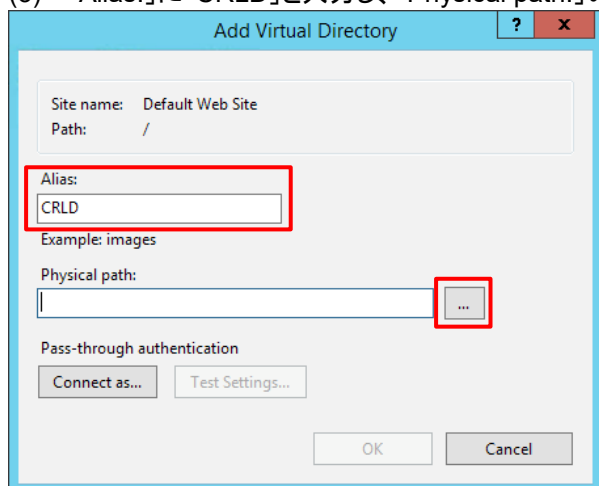
8.3.1.2. IIS の設定

CRL を HTTP で配布できるように、IIS を設定します。

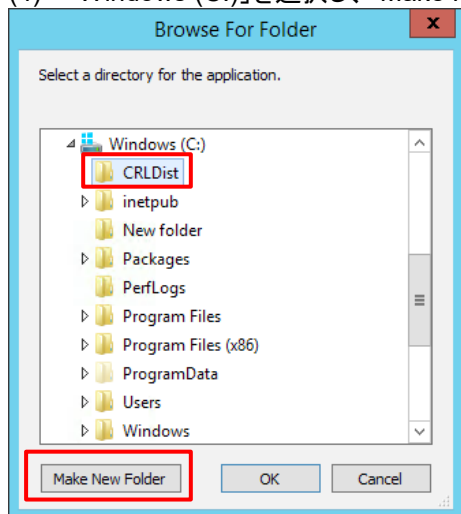
- (1) Win2012 の Administration Tools から「Internet Information Services (IIS) Manager」を開きます。
- (2) 「Win2012」を展開 → 「Sites」を展開して表示された「Default Web Site」を右クリックして、「Add Virtual Directory」を選択します。



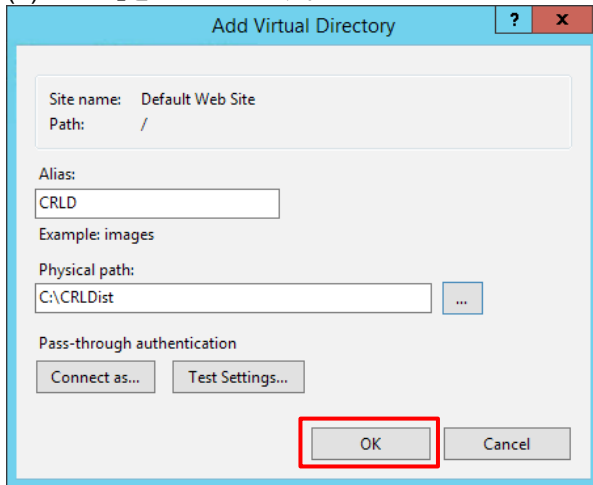
- (3) 「Alias:」に「CRLD」と入力し、「Physical path:」の「...」をクリックします。



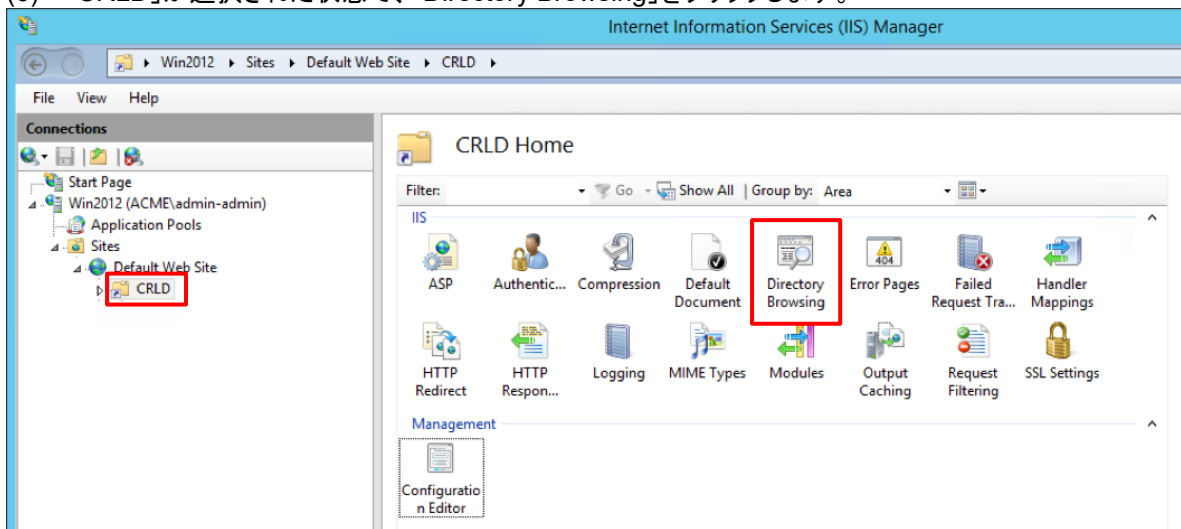
- (4) 「Windows (C:)」を選択し、「Make New Folder」をクリックして、「CRLDist」フォルダを生成します。



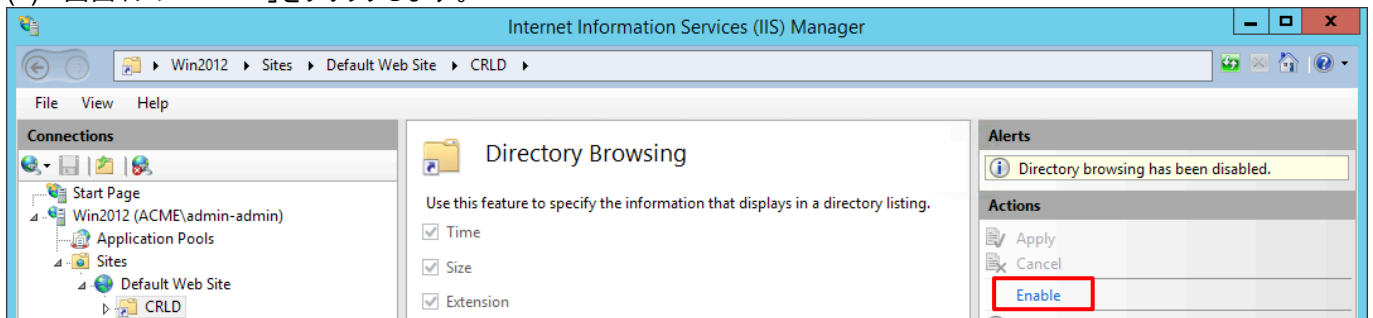
(5) 「OK」をクリックします。



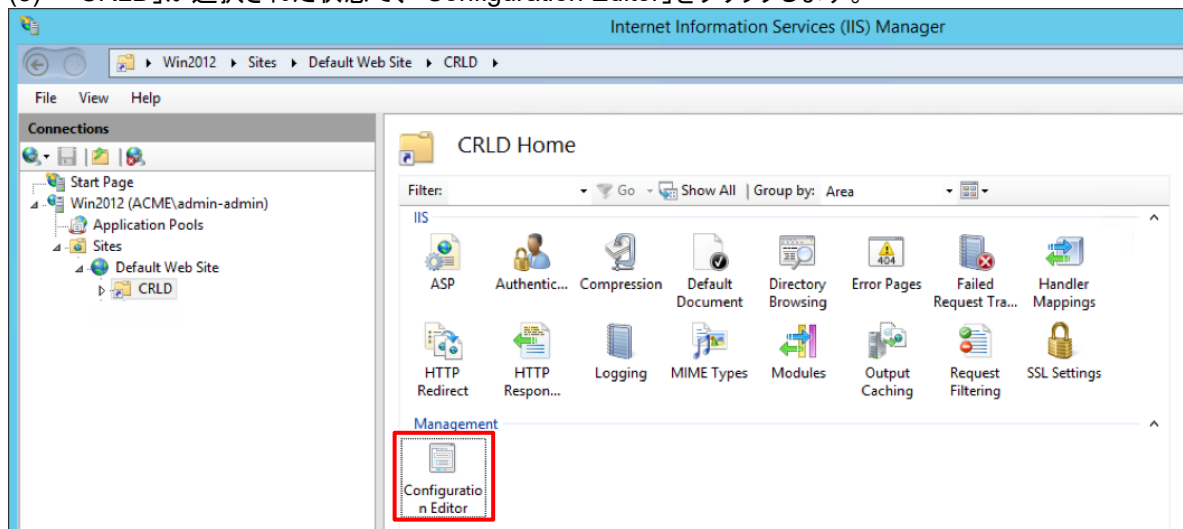
(6) 「CRLD」が選択された状態で、「Directory Browsing」をクリックします。



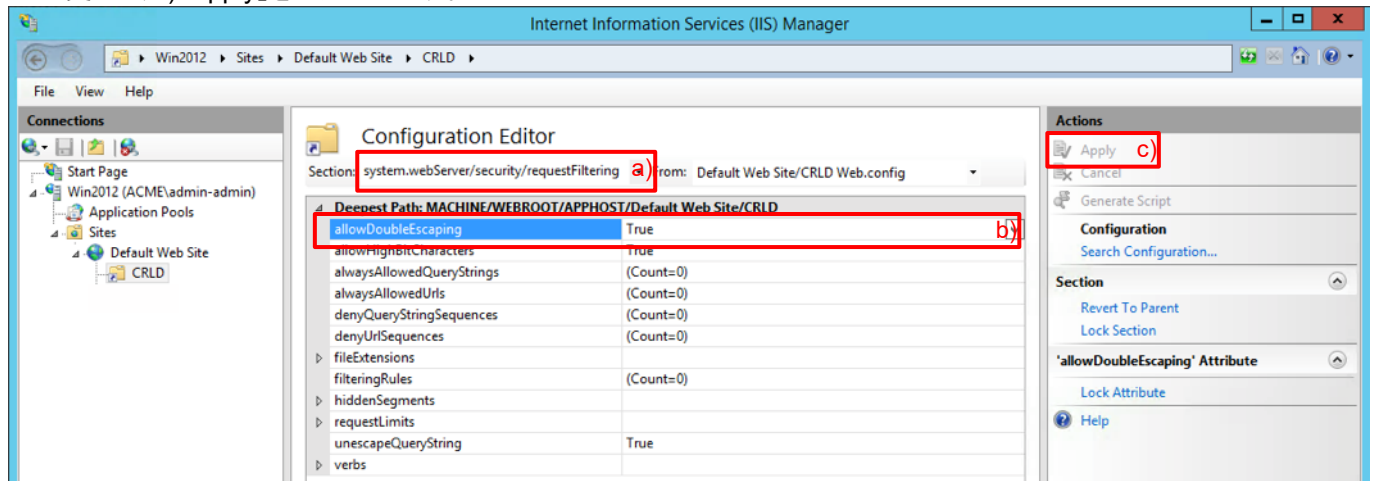
(7) 画面右の「Enable」をクリックします。



(8) 「CRLD」が選択された状態で、「Configuration Editor」をクリックします。



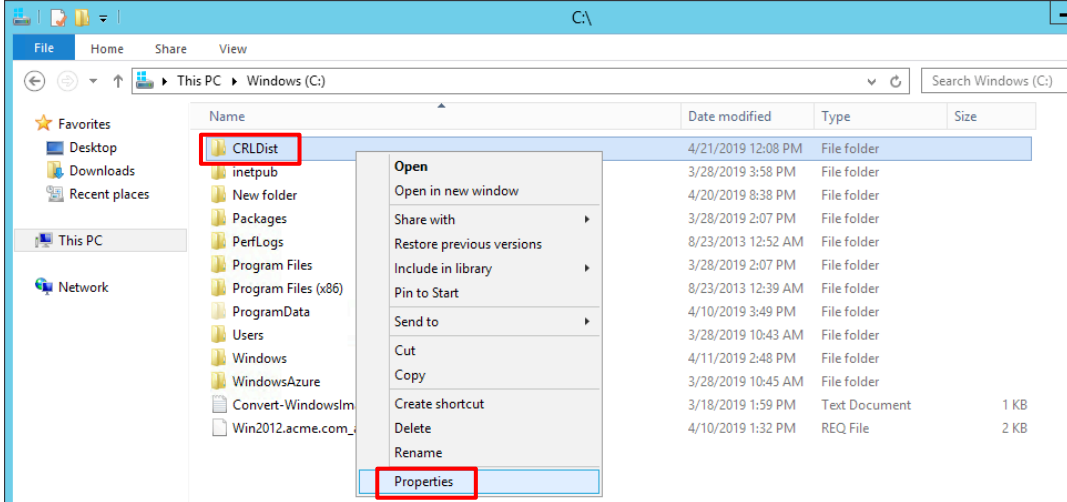
(9) a) Section: で「system.webServer/security/requestFiltering」を選択 → b)「allowDoubleEscaping」を「True」に変更して、c)「Apply」をクリックします。



8.3.1.3. フォルダの設定

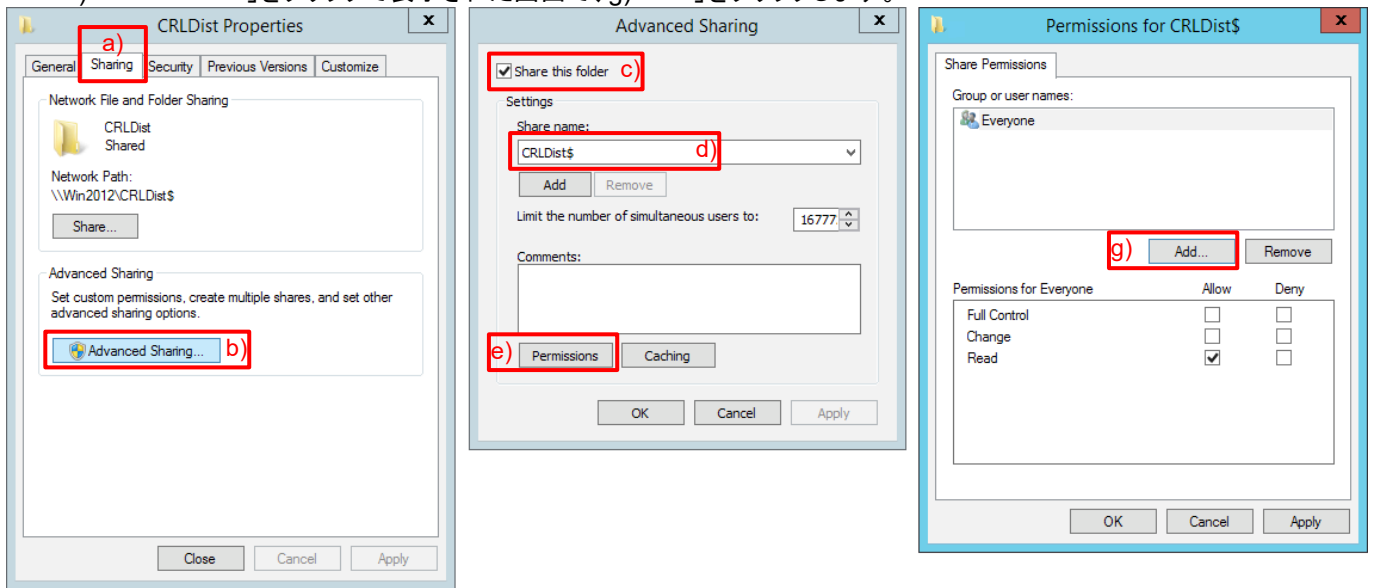
CRL ファイルが置かれるフォルダ:「CRLDist」に、適切なアクセス権を設定します。

(1) File Explorer を開き、C:ドライブ直下の「CRLDist」を右クリックし、「Properties」を選択します。

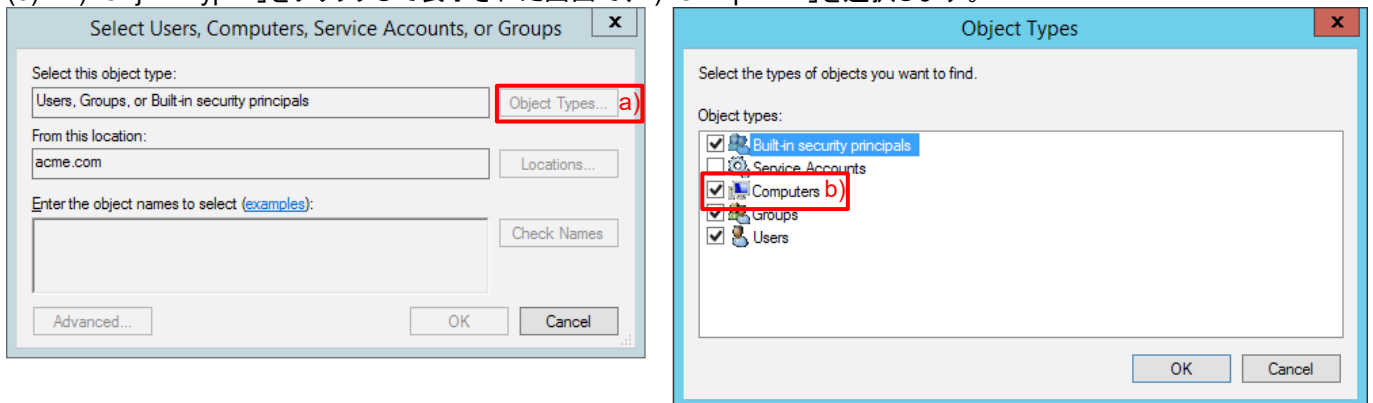


(2) a)「Sharing」 → b)「Advanced Sharing」で表示された画面で、c)「Share this folder」にチェック → d)CRLDist の末尾に\$を入力します。

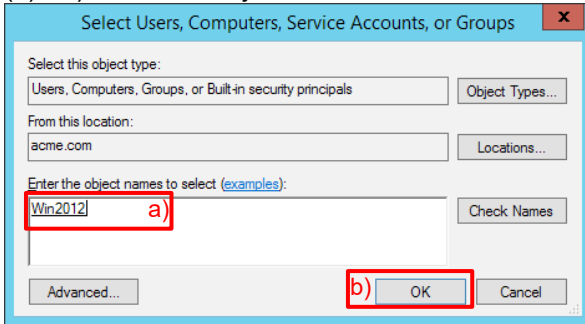
e)「Permissions」をクリックで表示された画面で、g)「Add」をクリックします。



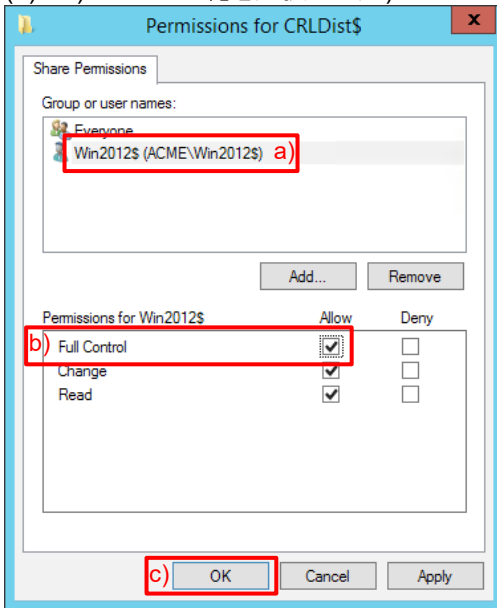
(3) a)「Object Types」をクリックして表示された画面で、b)「Computers」を選択します。



(4) a)「Enter the object names to select」の下に「Win2012」と入力し、b)「OK」をクリックします。



(5) a)「Win2012\$」を選択して、b)「Full Control」にチェックを入れ、c)「OK」をクリックします。

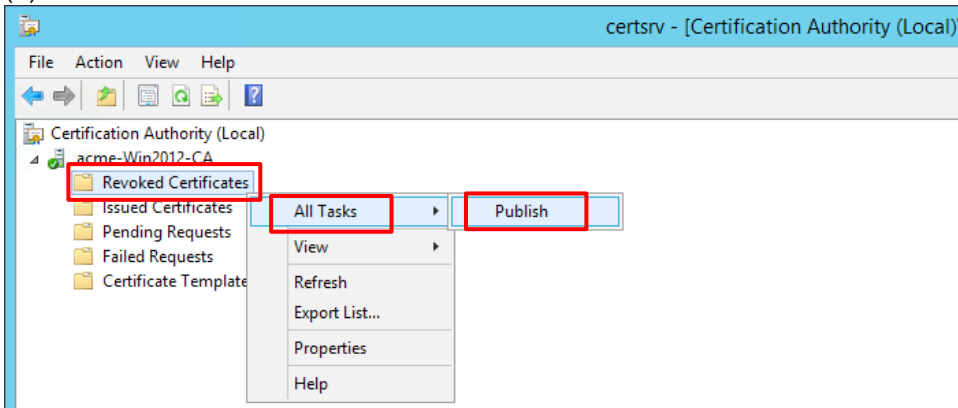


(6) 全て「OK」 → 「Close」をクリックして、フォルダ設定を終了します。

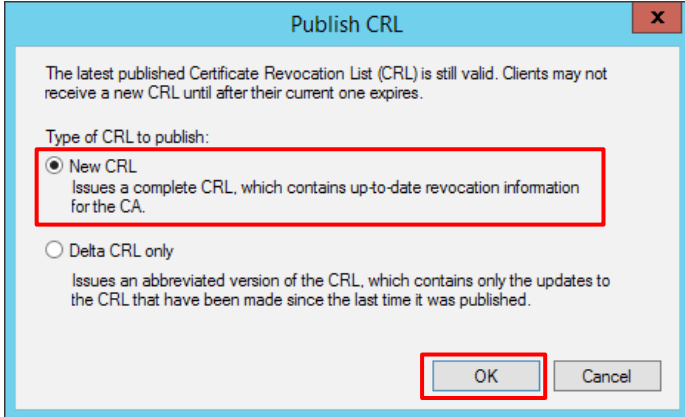
8.3.2. CRL の発行

(1) Win2012 の Administration Tools から「Certification Authority」を開きます。

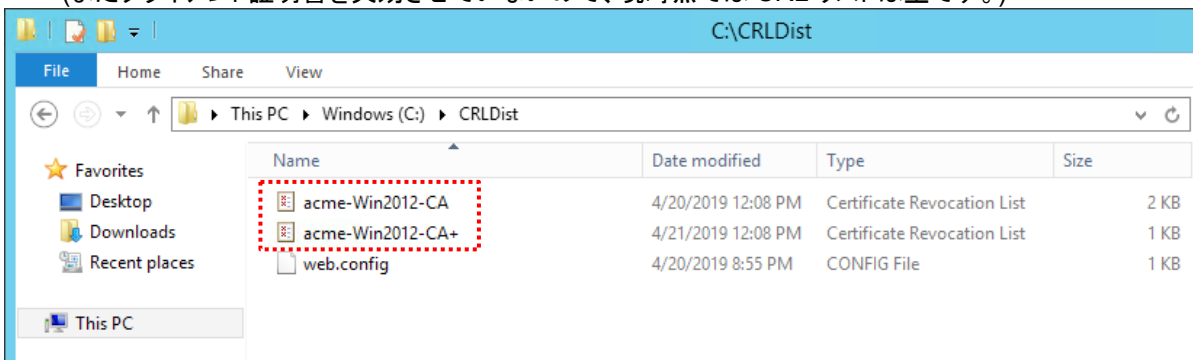
(2) 「acme-Win2012-CA」の下の「Revoked Certificates」を右クリック → 「All Tasks」 → 「Publish」を選択します。



(3) 「New CRL」が選択された状態で、「OK」をクリックします。



(4) File Explorer で「C:\%CRLDist」フォルダを開くと、以下のような CRL ファイルが生成されて入れば OK です。
(まだクライアント証明書を失効させていないので、現時点では CRL リストは空です。)

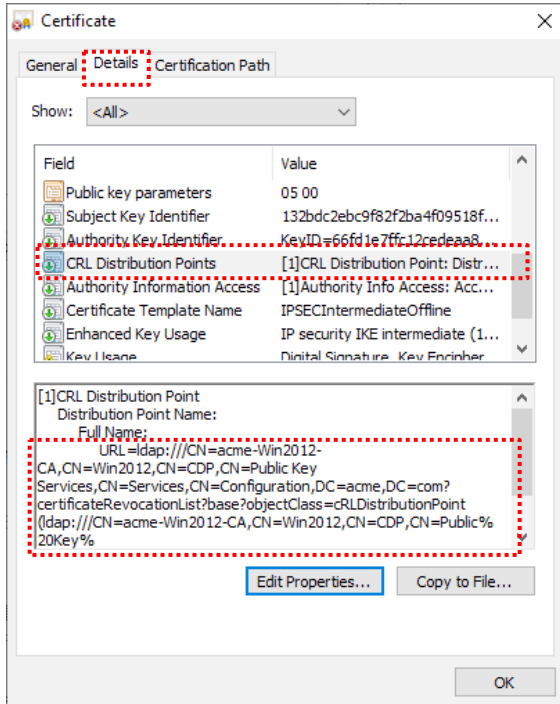


8.3.3. クライアント証明書の再発行

SCEP でクライアント PC へ配布済みのクライアント証明書を一旦削除して、再発行します。

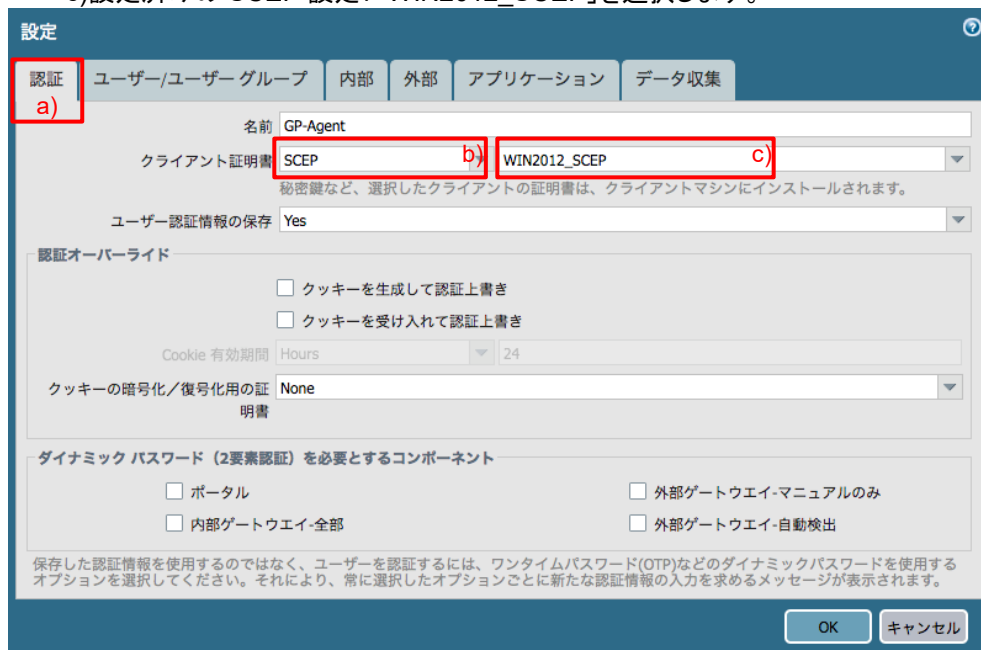
[理由]

CRL 設定の前に SCEP で配布したクライアント証明書の CDP は、以下のように「URL=ldap://～」となっています。



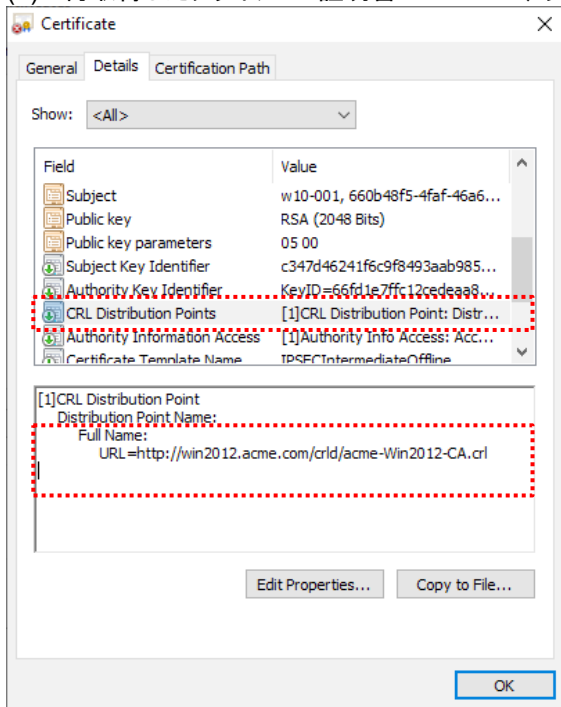
本ガイドの設定では、HTTP を使って CRL ファイルを取得する形にしたので、この証明書では CRL 取得ができません。よって、一旦削除して、新たにクライアント証明書を取り直します。

- (1) クライアント証明書を持つクライアント PC へログインします。(w10-001~w10-003)
- (2) 例: Chrome ブラウザ → 「設定」 → 「詳細設定」 → 「証明書の管理」で表示された画面で、「Personal」タブをクリックし、SCEP により個別に発行されたクライアント証明書を削除します。
- (3) SCEP でクライアント証明書を再発行します。
「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブの「クライアント証明書」で、b)「SCEP」を選択し、c)設定済みの SCEP 設定:「WIN2012_SCEP」を選択します。



(4) 各クライアント PC(w10-001~w10-003)の GP Agent で、Portal へ再ログインします。

(5) 再取得したクライアント証明書の CDP が、以下のように「URL=http://」になります。



(6) SCEP によるクライアント証明書の再発行を停止します。

「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブの「クライアント証明書」で、b)「None」を選択し、c)「OK」をクリックします。



8.3.4. 証明書プロファイルの CRL 設定

PA Firewall の証明書プロファイルを設定変更して、CRL による失効管理ができるようにします。

- (1) 「Device」タブ→「証明書の管理」の下の「証明書プロファイル」で表示された、設定済みの「WIN2012-CA-Profile」をクリックします。
- (2) a)「CRL の使用」にチェックを入れ、b)「OK」をクリックします。

証明書プロファイル

名前 WIN2012-CA-Profile

ユーザー名フィールド None

ユーザードメイン

名前	デフォルト OCSP URL	OCSP 検証証明書
WIN2012_SCEP		

追加 削除

デフォルト OCSP URL (http:// または https:// で開始する必要あり)

CRL の使用 a)

OCSP の使用
CRL より OCSP を優先

CRL 受信の有効期限 (秒) 5

OCSP 受信の有効期限 (秒) 5

証明書の有効期限 (秒) 5

証明書状態が不明な場合にセッションをブロック

タイムアウト時間内に証明書状態を取得できない場合にセッションをブロック

証明書が認証側デバイスに発行されなかった場合セッションをブロック

期限切れ証明書のセッションをブロック

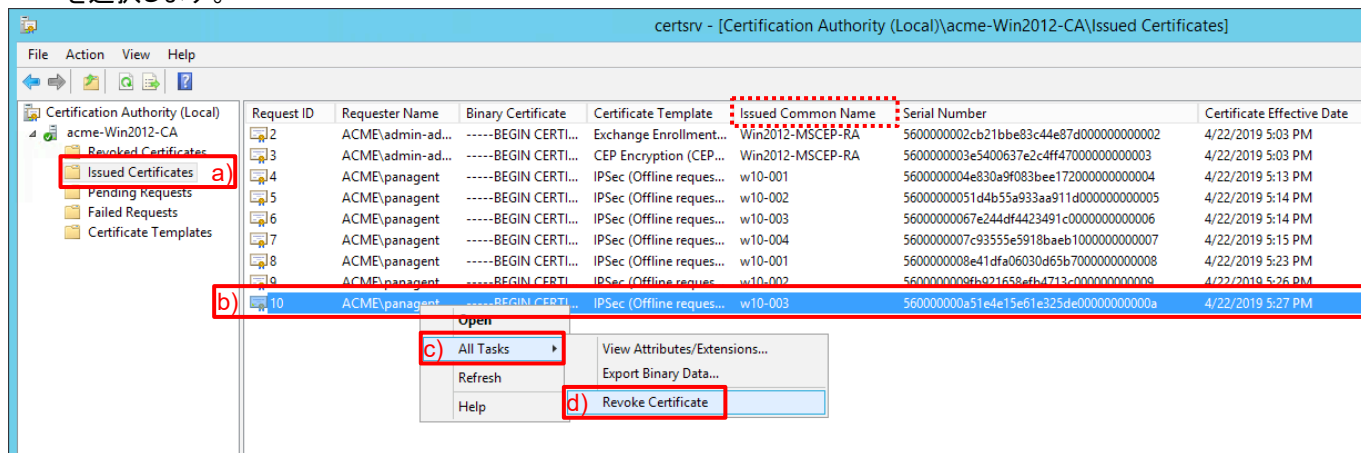
b) OK キャンセル

- (3) 「コミット」を実施します。

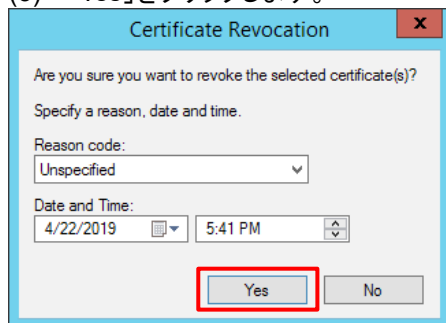
8.3.5. クライアント証明書の失効と CRL の発行

試しに、w10-003 に発行済みのクライアント証明書を失効させます。

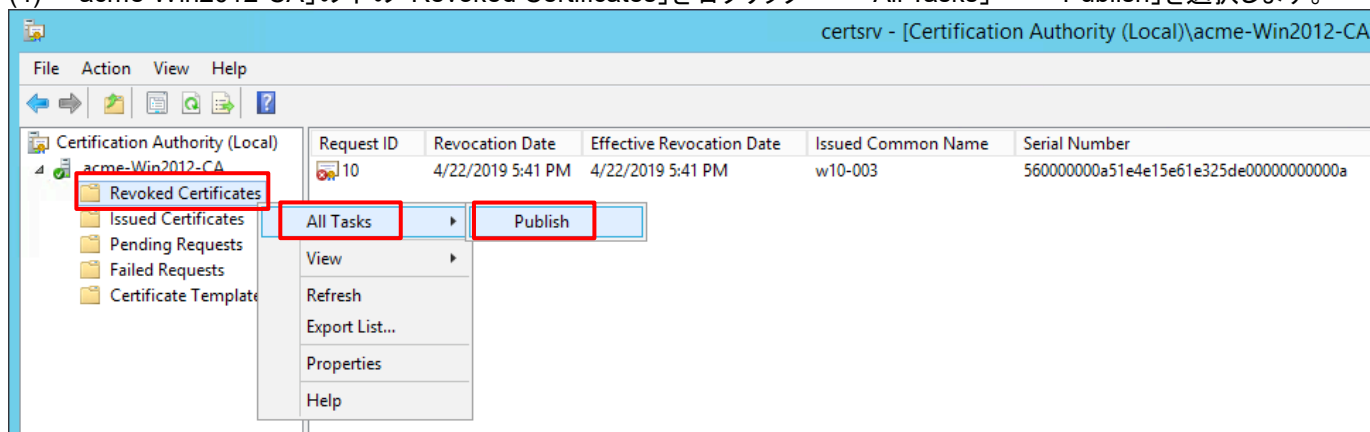
- (1) Win2012 の Administration Tools から「Certification Authority」を開きます。
- (2) 「acme-Win2012-CA」の下の a)「Issued Certificates」をクリックします。
b)「Issued Common Name」が「w10-003」で最新のものを右クリック → c)「All Tasks」 → d)「Revoke Certificate」を選択します。



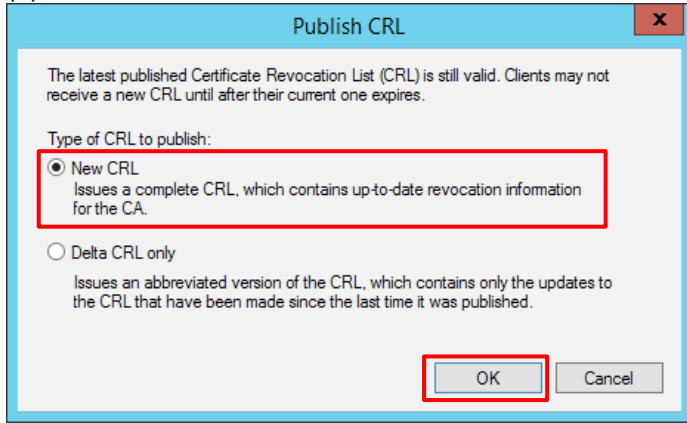
- (3) 「Yes」をクリックします。



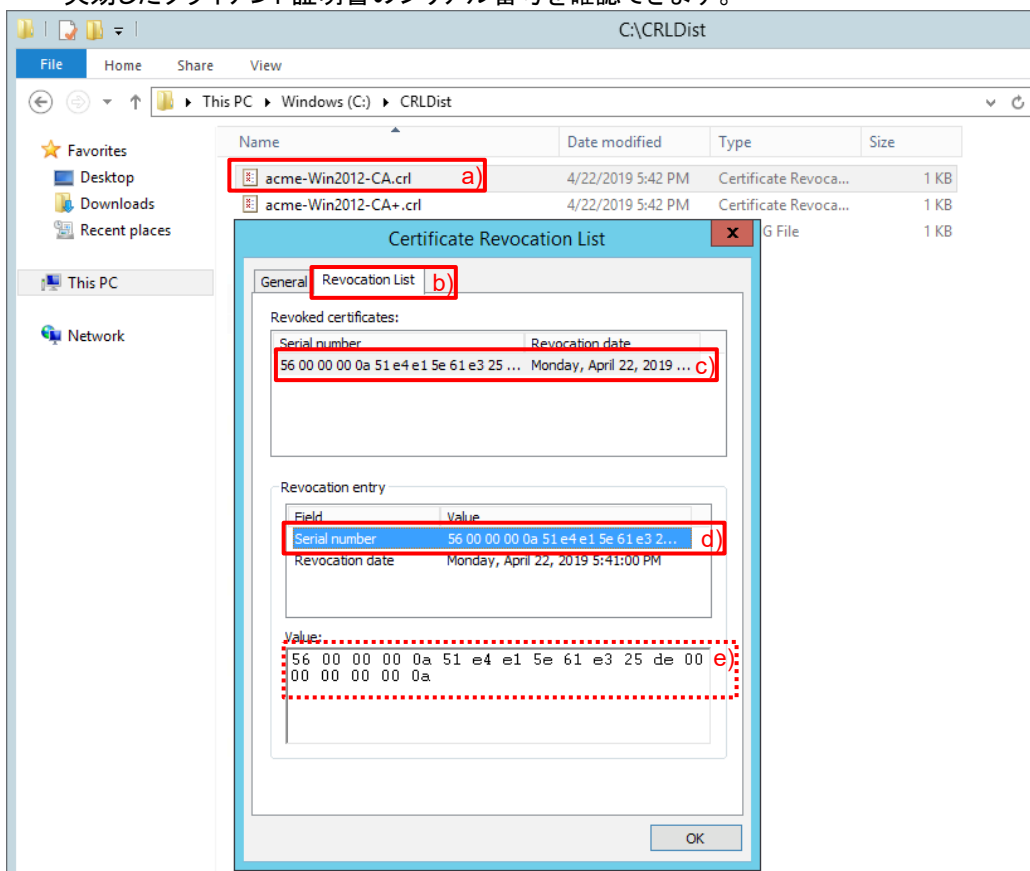
- (4) 「acme-Win2012-CA」の下「Revoked Certificates」を右クリック → 「All Tasks」 → 「Publish」を選択します。



(5) 「New CRL」が選択された状態で、「OK」をクリックします。



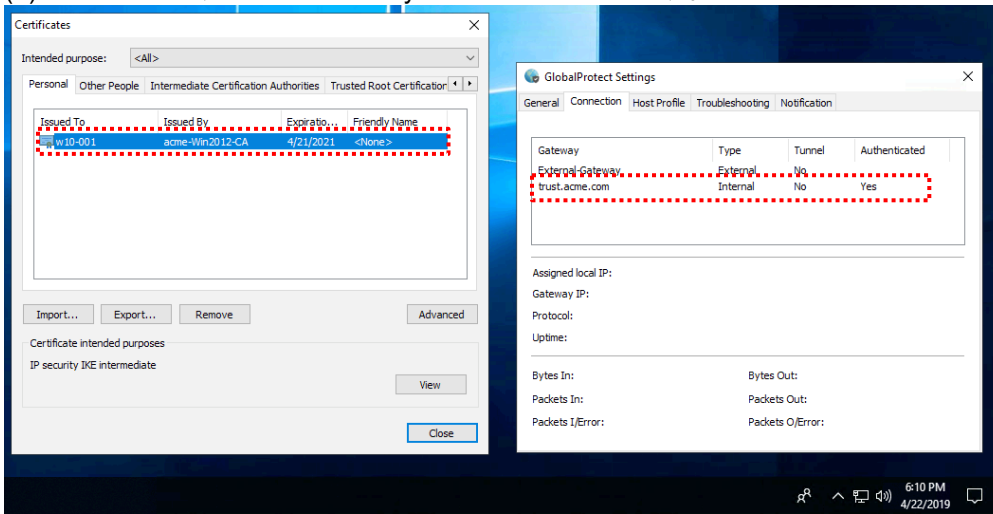
(6) [確認のみ] File Explorer で「C:\CRLDist」フォルダの a)「acme-Win2012-CA.crl」をダブルクリックで開きます。
b)「Revocation List」タブ →「Revoked Certificates」下の c)をクリック → d)「Serial Number」をクリックすると、e)で失効したクライアント証明書のシリアル番号を確認できます。



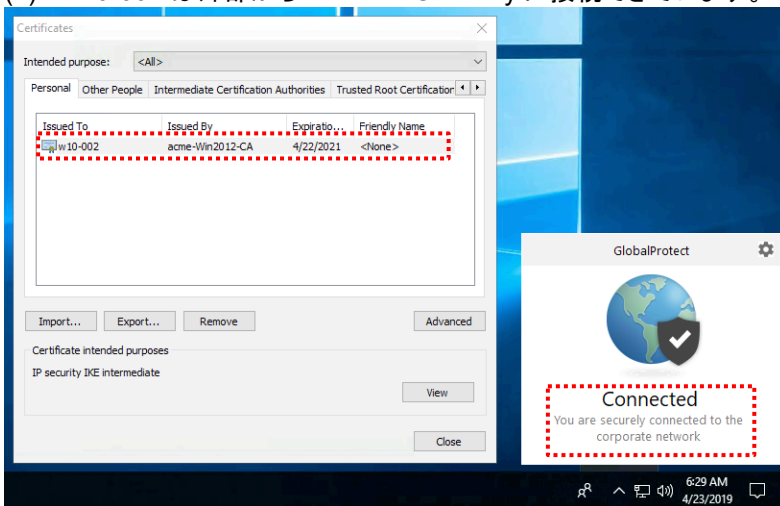
8.3.6. GP Agent からのアクセス

クライアント PC(w10-001~w10-003)の GP Agent からアクセスして、失効した w10-003 だけが接続できない状況を確認します。

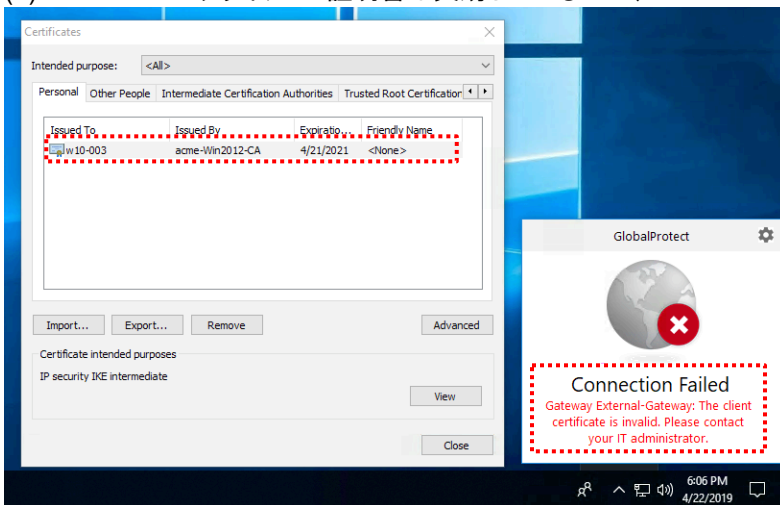
(1) w10-001 は、Internal Gateway にログインできています。



(2) w10-002 は外部から External-Gateway に接続できています。



(3) w10-003 のクライアント証明書は失効しているので、External-Gateway に接続できません。



8.3.7. PA Firewall の CLI コマンド

PA Firewall の CLI コマンドで、CRL 取得状況を確認できます。

(1) 取得した CRL の確認

```
admin-admin@Azure-PA-VM> debug sslmgr view crl http://win2012.acme.com/crld/acme-Win2012-CA.crl
```

```
Current time is: Mon Apr 22 08:48:59 2019
```

```
Next update time is Apr 29 20:52:50 2019 GMT
```

Count	Serial Number	Revocation Date
[1]	560000000A51E4E15E61E325DE0000000000A	Apr 22 08:41:00 2019 GMT

(2) 取得した CRL キャッシュの消去

一旦取得した CRL はしばらくキャッシュされますが、CRL の挙動を確認するために、CRL キャッシュを消去したい場合があります。

CRL キャッシュを消去するには、以下 2 つのコマンドを実行する必要があります。

```
admin-admin@Azure-PA-VM> debug sslmgr delete crl all
```

```
All cached CRLs deleted
```

```
admin-admin@Azure-PA-VM> debug dataplane reset ssl-decrypt certificate-cache
```

```
deleted 1 cert entries.
```

8.4. OCSP によるクライアント証明書の失効管理

次に OSCP による失効管理の動作を確認します。

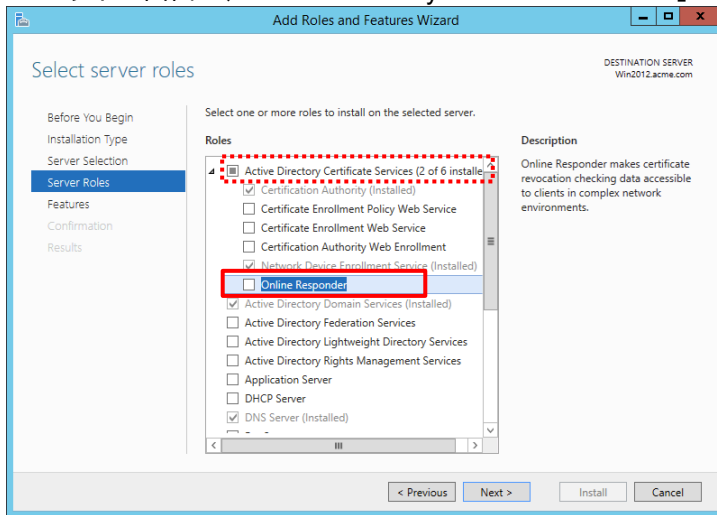
OCSP の動作を確認するには、ADCS の役割の一つである「Online Responder」が必要です。

8.4.1. Online Responder のインストール

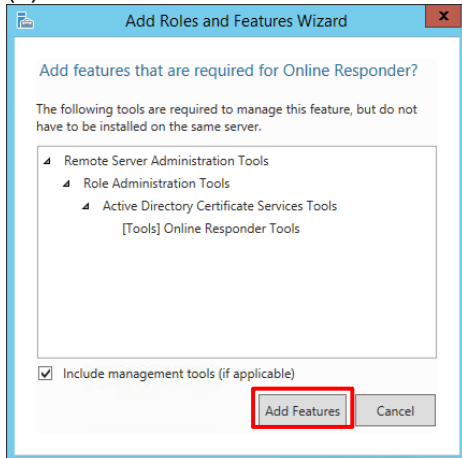
(1) IIS と同様に、Win2012 の Server Manager で、「Add roles and features」をクリックします。

(2) 以下の画面までは「Next」をクリックして進めます。

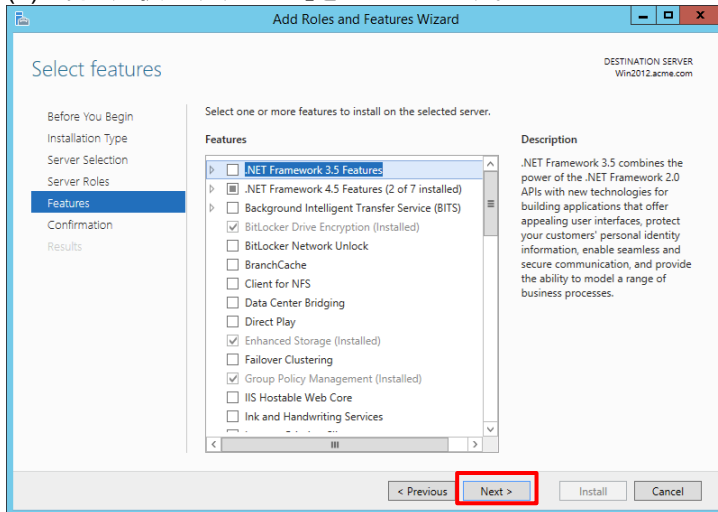
以下の画面で、「Active Directory Certificate Services」の下の「Online Responder」を選択します。



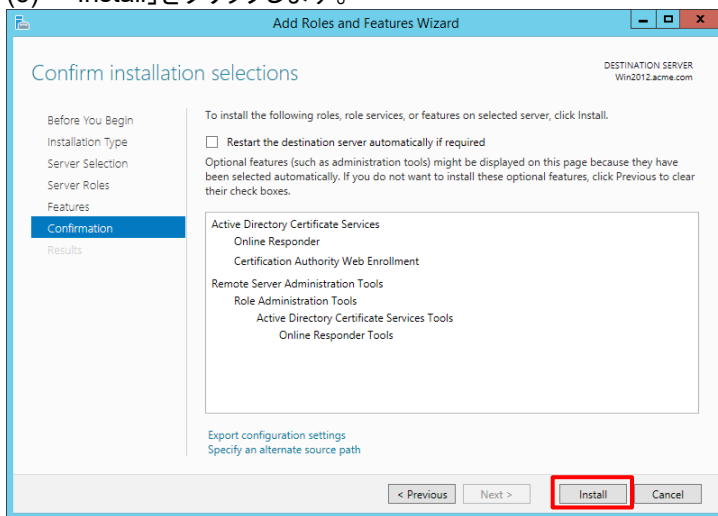
(3) 「Add Features」をクリックします。



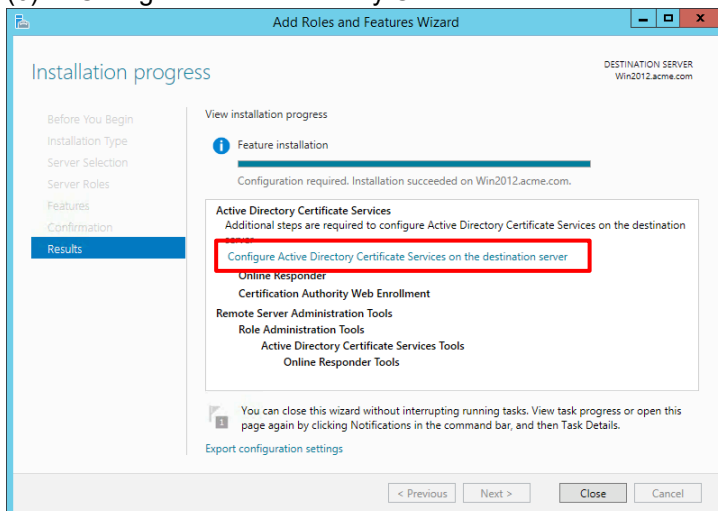
(4) 何も選択せず、「Next」をクリックします。



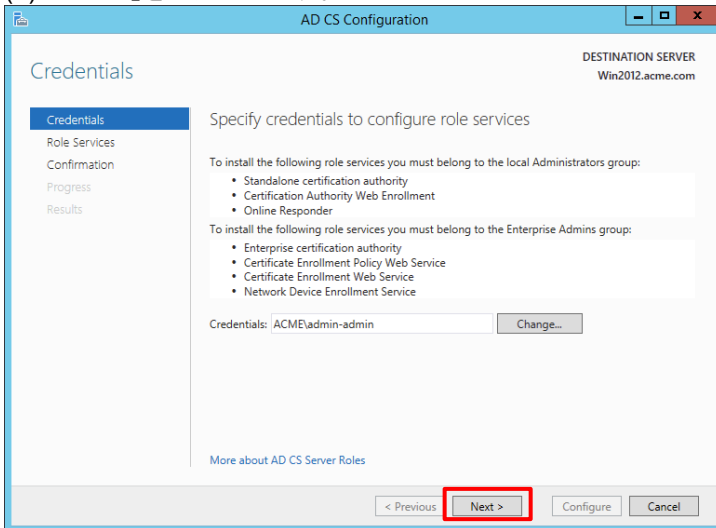
(5) 「Install」をクリックします。



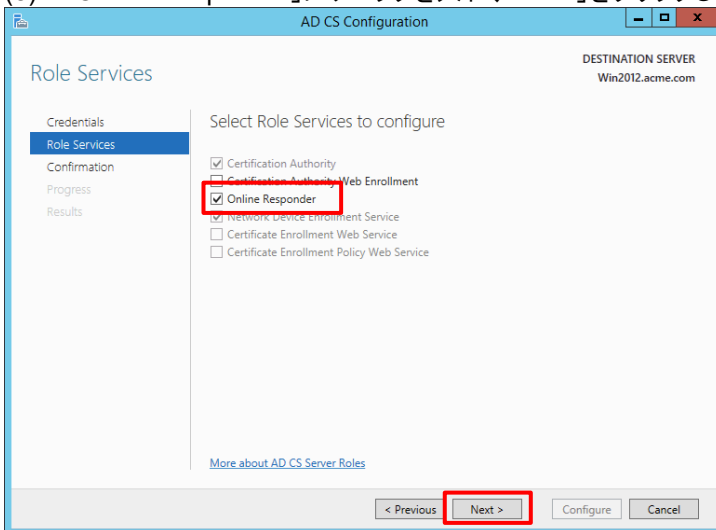
(6) 「Configure Active Directory Certificate Services on the destination server」をクリックします。



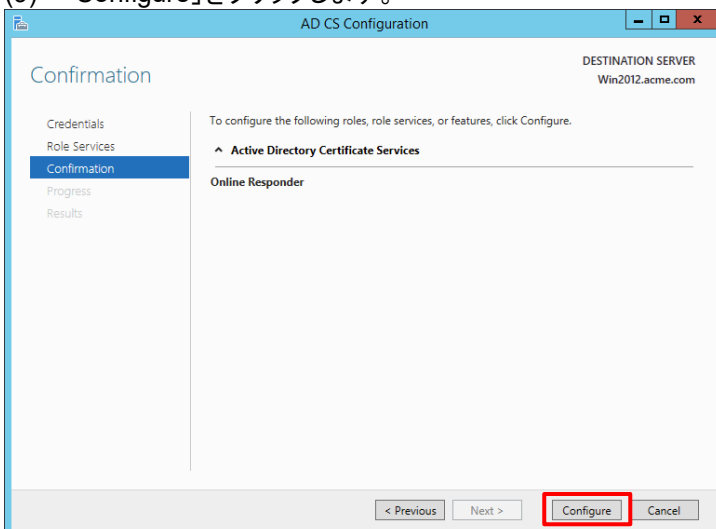
(7) 「Next」をクリックします。



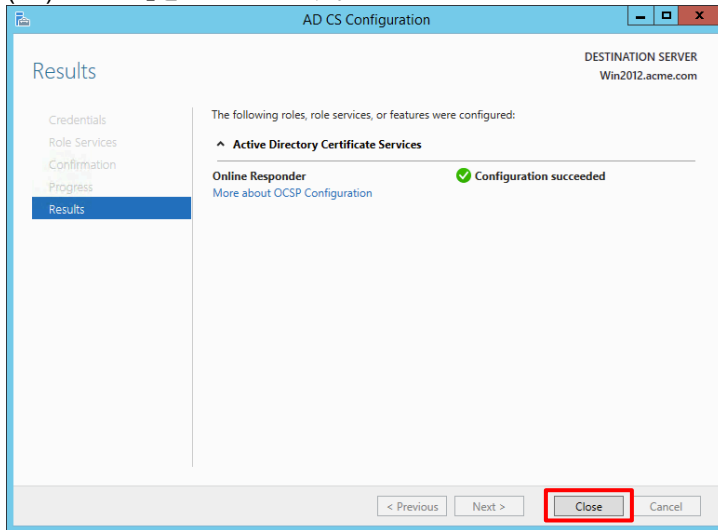
(8) 「Online Responder」にチェックを入れ、「Next」をクリックします。



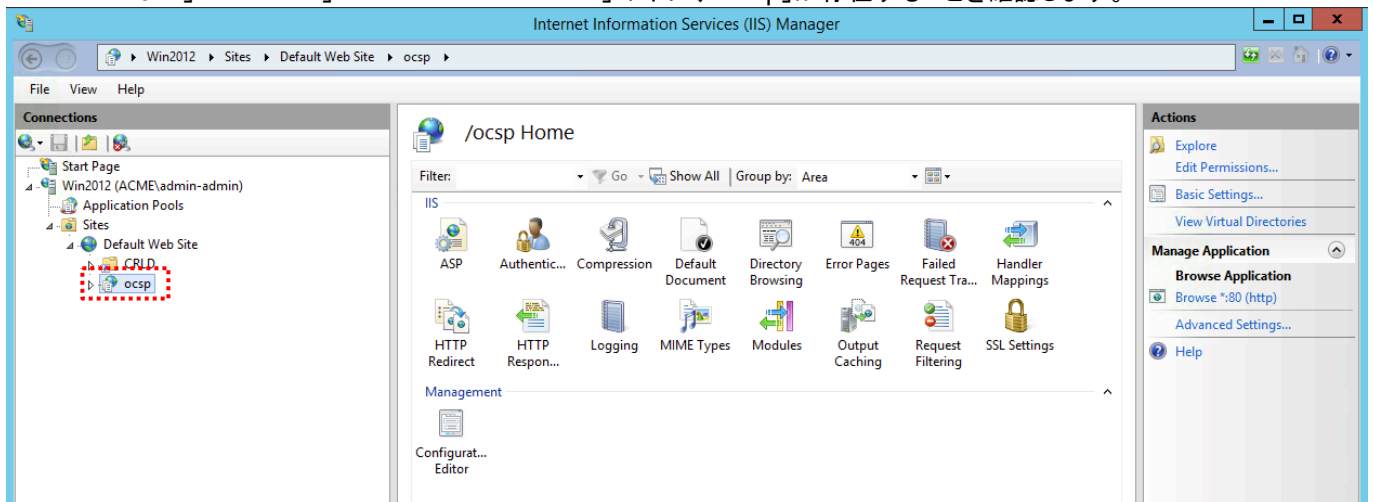
(9) 「Configure」をクリックします。



(10) 「Close」をクリックします。

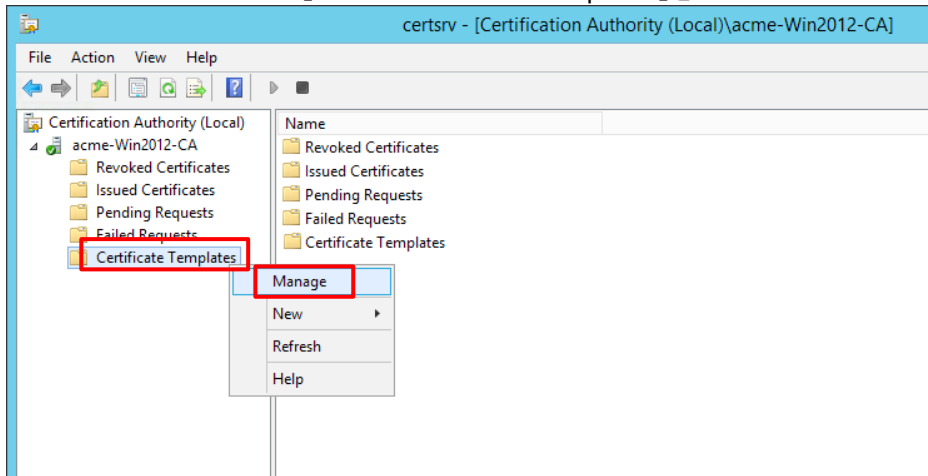


(11) [確認のみ] 「Administrative Tools」 → 「Internet Information Services (IIS) Manager」を開きます。
「Win2012」 → 「Sites」 → 「Default Web Site」の下に、「ocsp」が存在することを確認します。

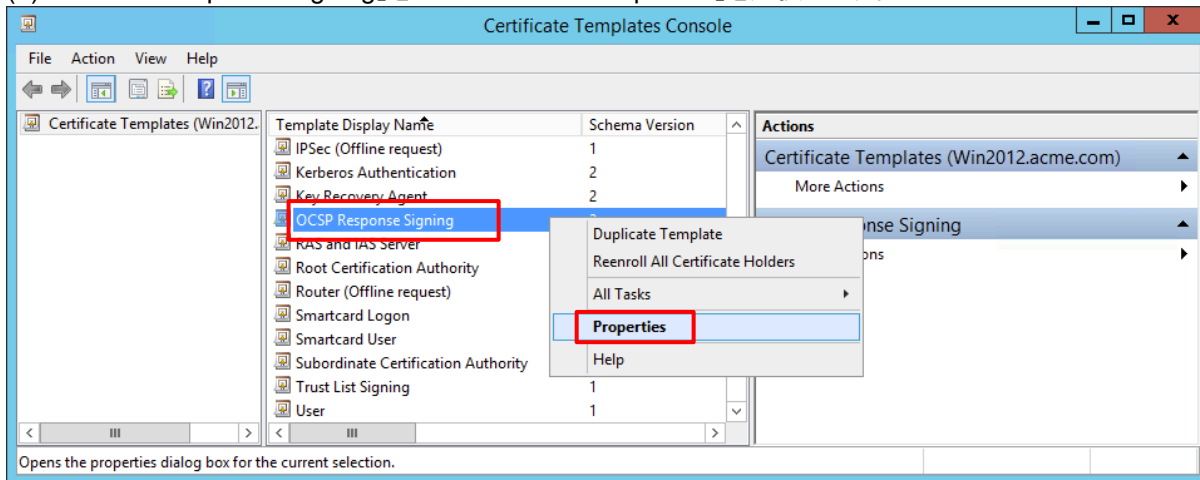


8.4.2. CA のテンプレート設定

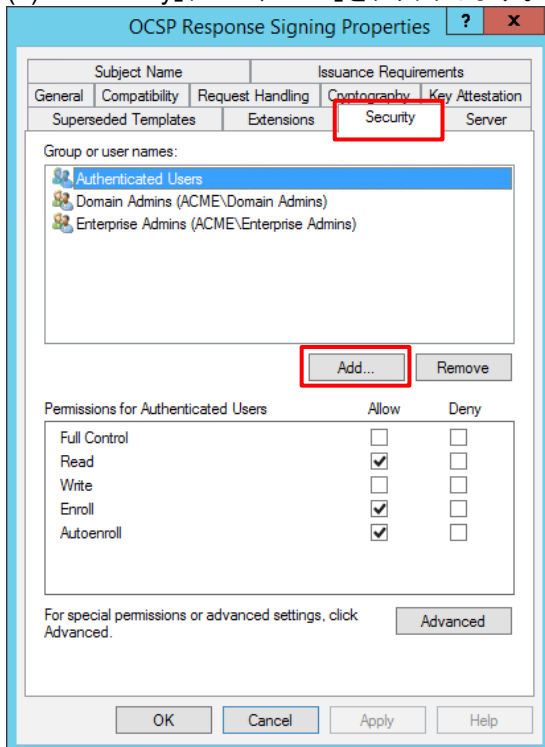
- (1) Win2012 の「Administrative Tools」 → 「Certification Authority」を開きます。
「acme-Win2012-CA」の下の「Certificate Templates」を右クリック → 「Manage」を選択します。



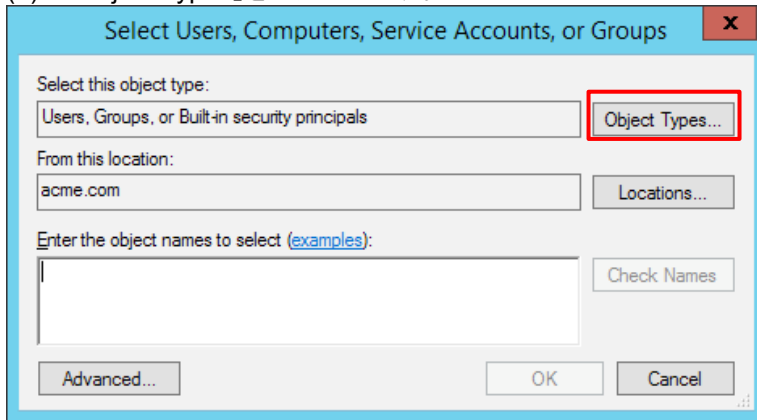
- (2) 「OCSP Response Signing」を右クリック → 「Properties」を選択します。



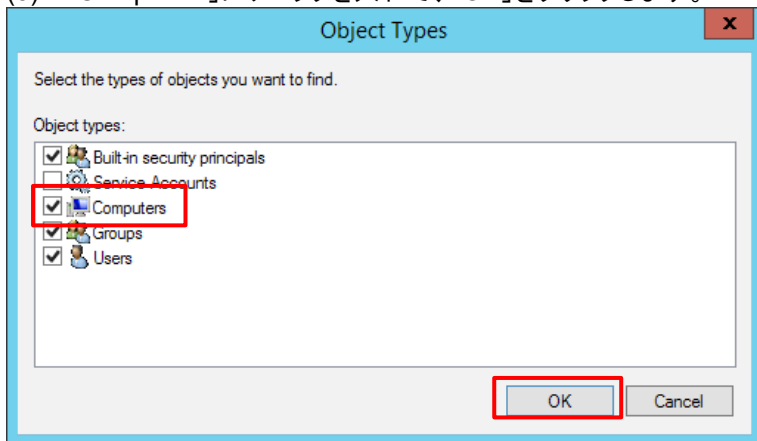
- (3) 「Security」タブで、「Add」をクリックします。



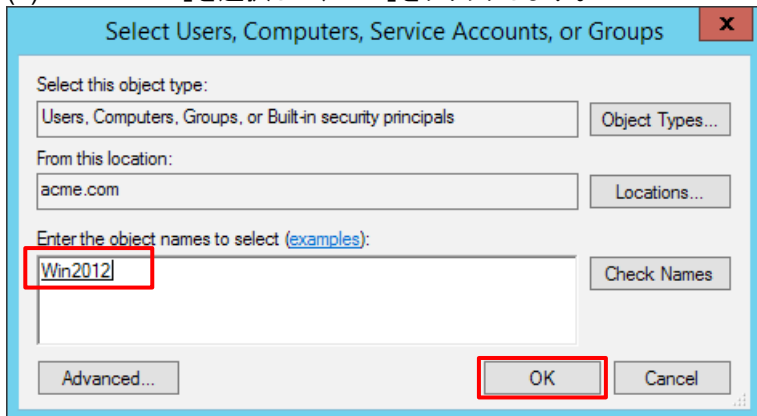
(4) 「Object Types」をクリックします。



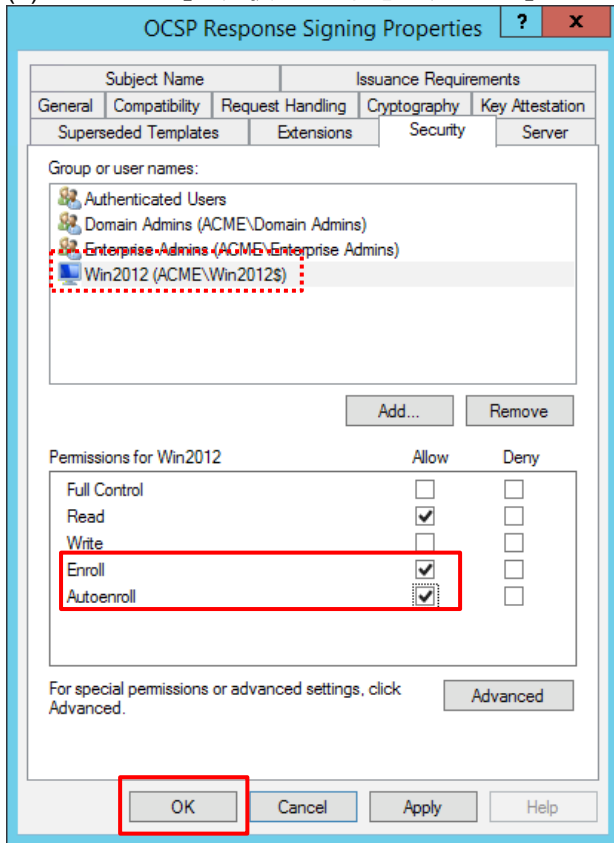
(5) 「Computers」にチェックを入れて、「OK」をクリックします。



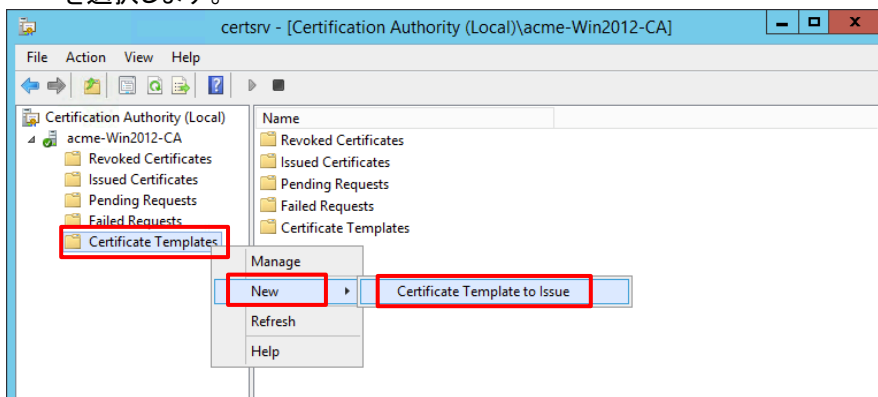
(6) 「Win2012」を選択して、「OK」をクリックします。



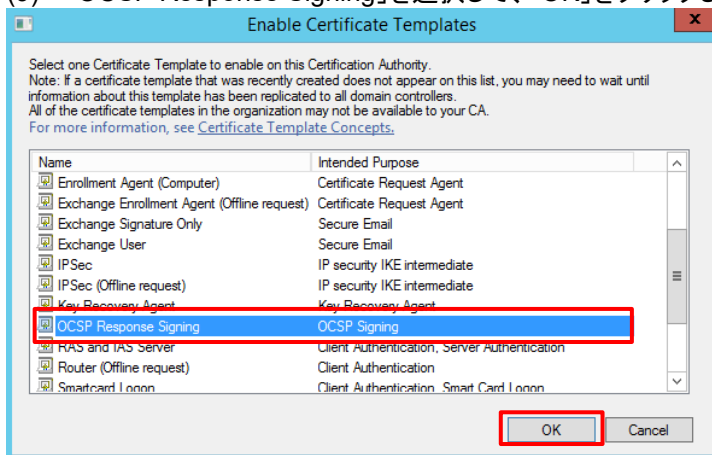
(7) 「Win2012」が選択された状態で、「Enroll」と「Autoenroll」にチェックを入れ、「OK」をクリックします。



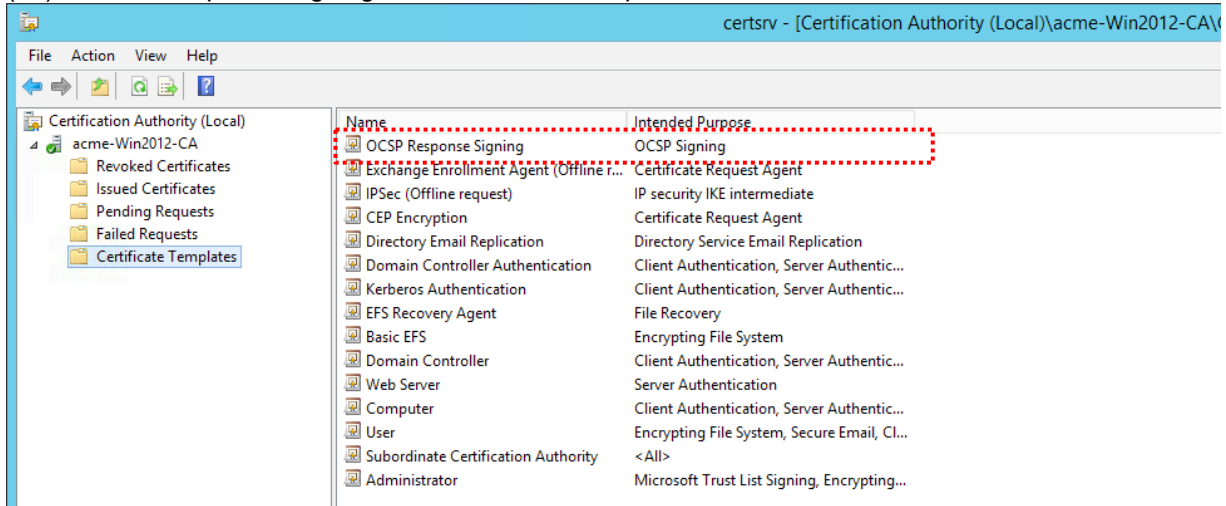
(8) 「acme-Win2012-CA」の下の「Certificate Templates」を右クリック → 「New」 → 「Certificate Template to Issue」を選択します。



(9) 「OCSP Response Signing」を選択して、「OK」をクリックします。

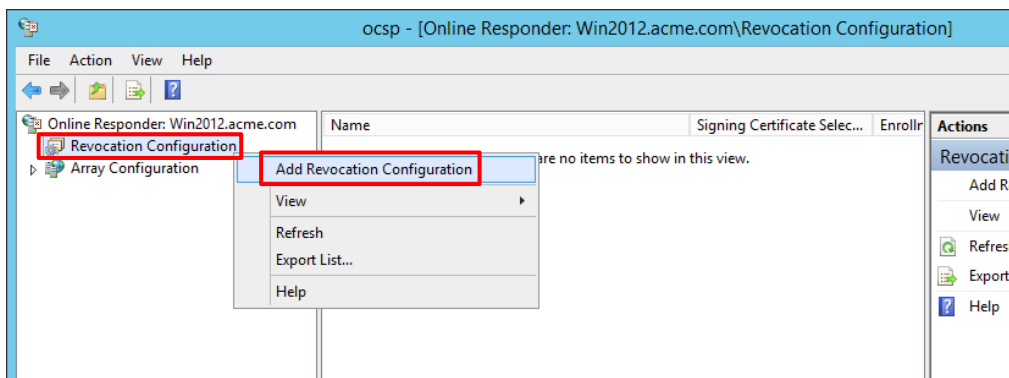


(10) 「OSCP Response Signing」が、「Certificate Templates」に加わります。

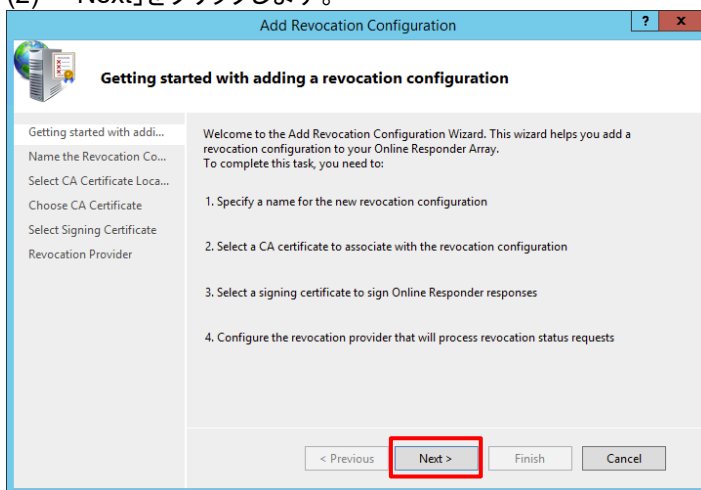


8.4.3. OCSP Responder の Revocation 設定

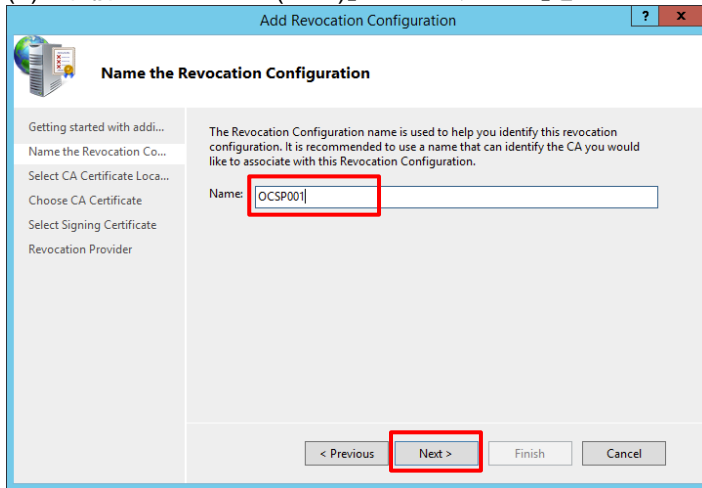
(1) Win2012 の「Administrative Tools」 → 「Online Responder Management」を開きます。
「Online Responder: Win2012.acme.com」の下の「Revocation Configuration」を右クリック → 「Add Revocation Configuration」を選択します。



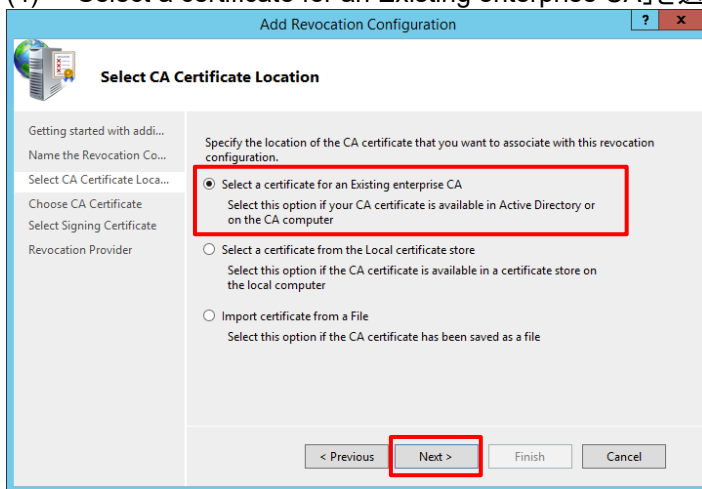
(2) 「Next」をクリックします。



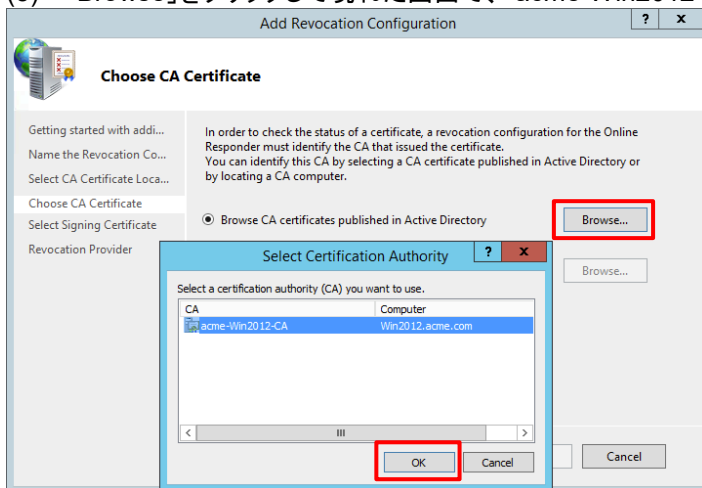
(3) 名前に「OCSP001(任意)」と入力し、「Next」をクリックします。



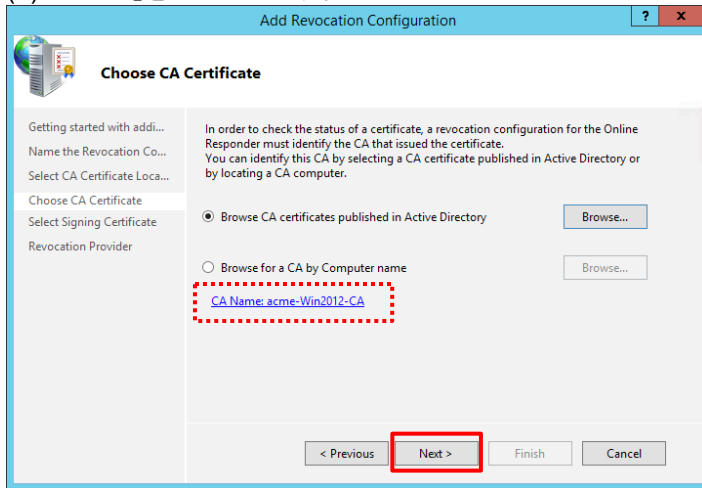
(4) 「Select a certificate for an Existing enterprise CA」を選択して、「Next」をクリックします。



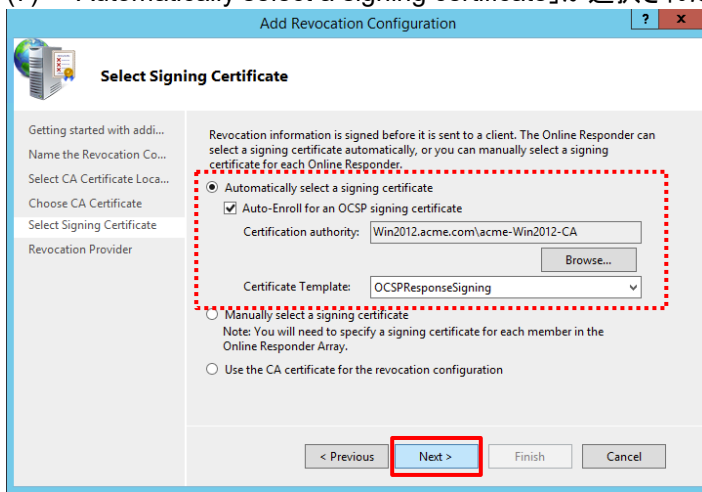
(5) 「Browse」をクリックして現れた画面で、「acme-Win2012-CA」が選択された状態で、「OK」をクリックします。



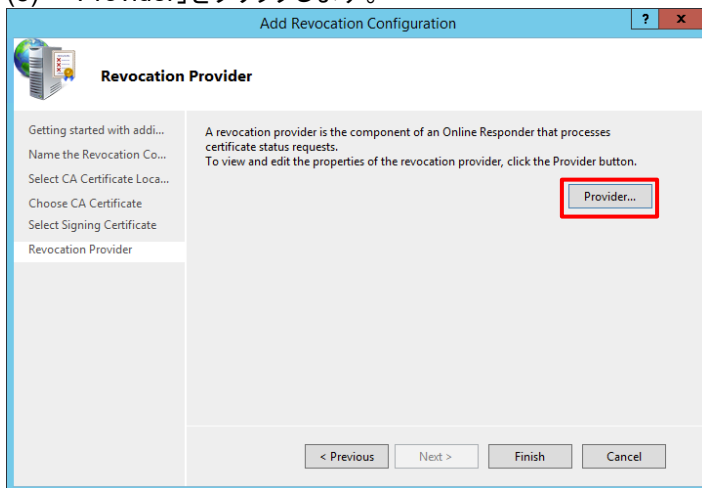
(6) 「Next」をクリックします。



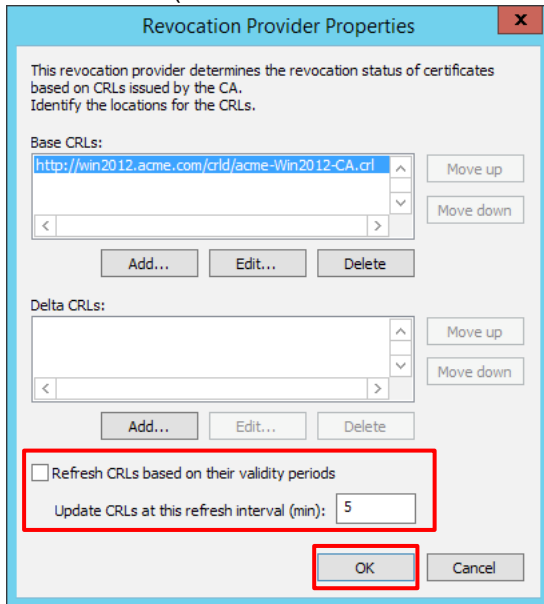
(7) 「Automatically select a signing certificate」が選択された状態で、「Next」をクリックします。



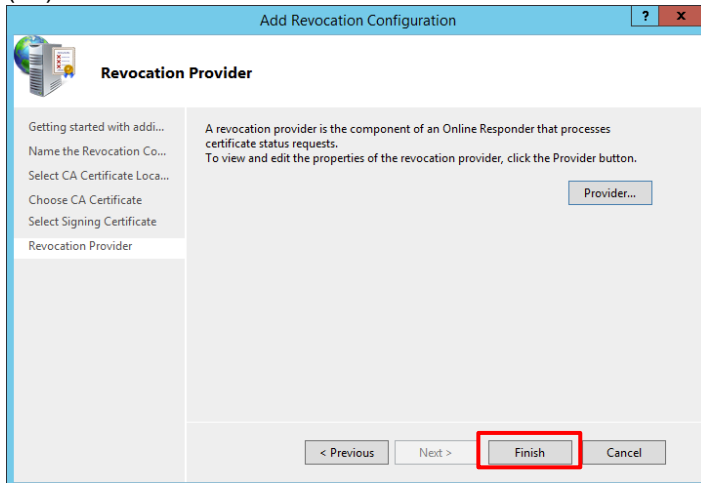
(8) 「Provider」をクリックします。



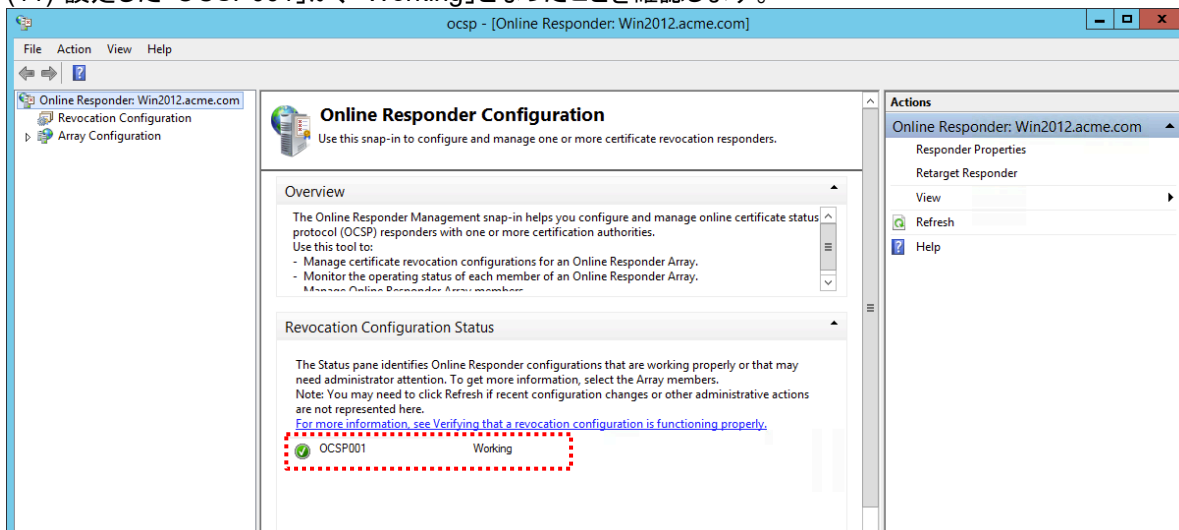
- (9) 検証用に、「Refresh CRLs based on their validity periods」のチェックを外して、最短の5分に変更し、「OK」をクリックします。(デフォルトでは、証明書を失効しても2日間程度反映されないため。)



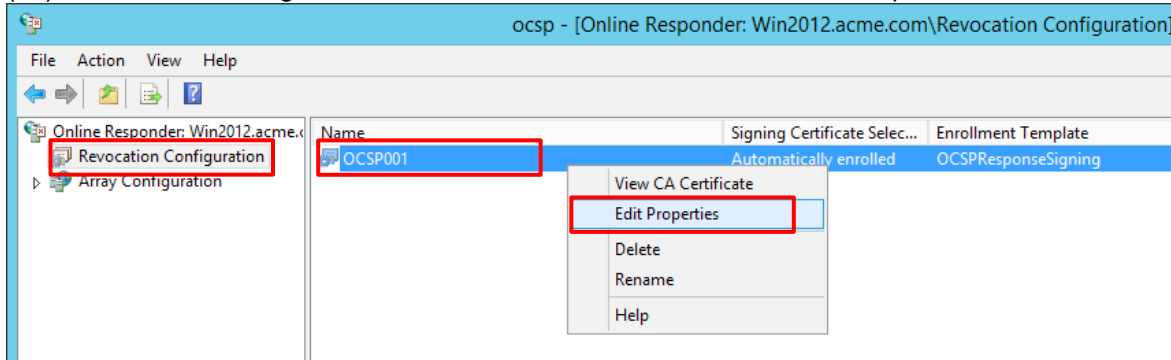
- (10) 「Finish」をクリックします。



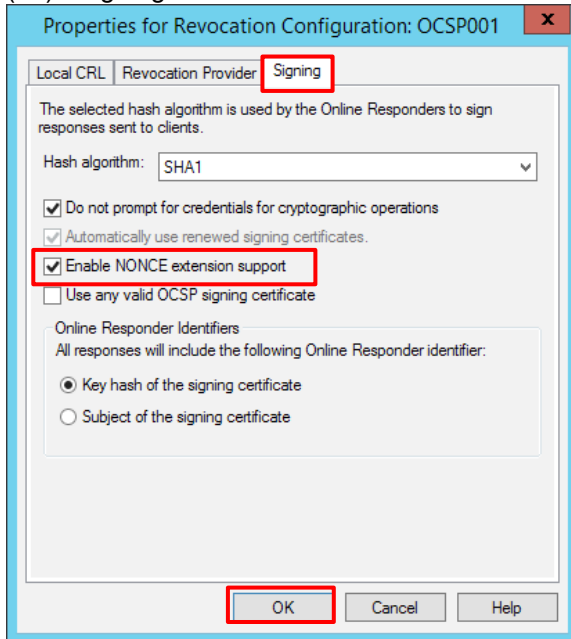
- (11) 設定した「OCSP001」が、「Working」となったことを確認します。



(12) 「Revocation Configuration」 → 「OCSP001」を右クリック → 「Edit Properties」を選択します。



(13) 「Signing」タブ → 「Enable NONCE extension support」にチェックを入れ、「OK」をクリックします。



8.4.4. 証明書プロファイルの OCSP 設定

PA Firewall の証明書プロファイルを設定変更して、OCSP による失効管理ができるようにします。

- (1) 「Device」タブ→「証明書の管理」の下の「証明書プロファイル」で表示された、設定済みの「WIN2012-CA-Profile」をクリックします。
- (2) a)「CRL の使用」のチェックを外し、「OCSP の使用」にチェックを入れます。
b)「WIN2012_SCEP」をクリックして表示された画面で、
c)「デフォルト OCSP URL」に「http://win2012.acme.com/ocsp」と入力し、d)「OK」をクリックします。

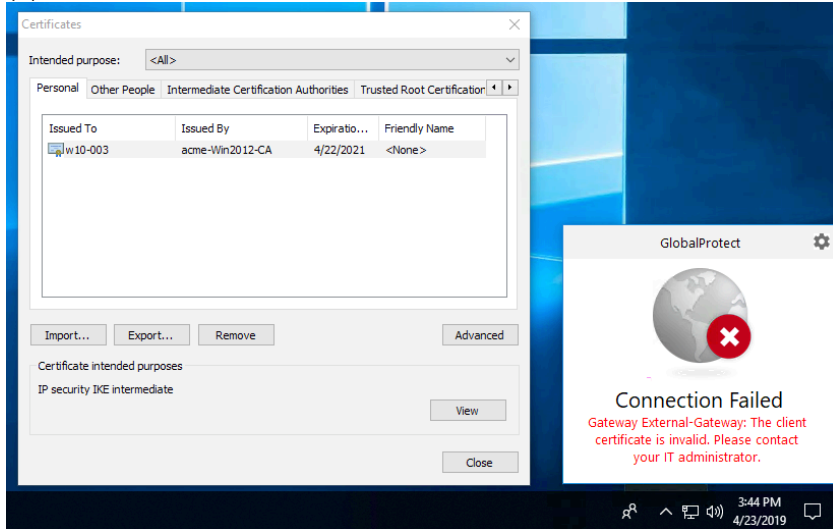


- (3) 「コミット」を実施します。

8.4.5. GP Agent からのアクセス

クライアント PC(w10-001~w10-003)の GP Agent からアクセスして、失効した w10-003 だけが接続できない状況を確認します。

- (1) w10-001 と w10-002 は接続できることを確認します。
- (2) CRL と同様に、W10-003 は失効しているのを、接続できないことを確認します。



8.4.6. PA Firewall の CLI コマンド

PA Firewall の CLI コマンドで、OCSP 取得状況を確認できます。

- (1) 取得した OCSP の状態確認

```
admin-admin@Azure-PA-VM> debug sslmgr view ocspl all
```

Current time is: Tue Apr 23 06:44:03 2019

Count	Serial Number (HEX)	Status	Next Update	Revocation Time
	Issuer Name Hash OCSP Responder URL			
[1]	1D0000000684A4703D8F85832C000000000006 9737e19d http://win2012.acme.com/ocsp	valid	Apr 24 18:35:48 2019 GMT	
[2]	1D0000000775C6FD389164B1BB000000000007 9737e19d http://win2012.acme.com/ocsp	valid	Apr 24 18:35:48 2019 GMT	
[3]	1D0000000849EDE4ABEB4CB8A4000000000008 9737e19d http://win2012.acme.com/ocsp	revoked	Apr 24 18:35:48 2019 GMT	Apr 23 06:25:00 2019 GMT

- (2) 取得した OCSP キャッシュの消去

CRL 同様に OCSP もキャッシュされます。
OCSP キャッシュを消去するには、以下 2 つのコマンドを実行する必要があります。

```
admin-admin@Azure-PA-VM> debug sslmgr delete ocspl all  
admin-admin@Azure-PA-VM> debug dataplane reset ssl-decrypt certificate-cache
```

Online Responder のキャッシュが最短でも 5 分なので、サーバー上でクライアント証明書を失効して、OCSP キャッシュを消去しても、その失効が反映されるには、最大 5 分待つ必要があります。

8.5. 新規ユーザーだけにクライアント証明書を配布する方法

ここまでの設定で、Active Directory に登録されている既存ユーザーへの SCEP によるクライアント証明書の配布が完了し、「ユーザー名&パスワード + クライアント認証(+失効管理)」という 2 要素認証が可能となりました。

次に発生する要件として、「既存ユーザーはこの 2 要素認証を維持しつつ、新入社員にだけクライアント証明書を配布したい」という状況が想定されます。

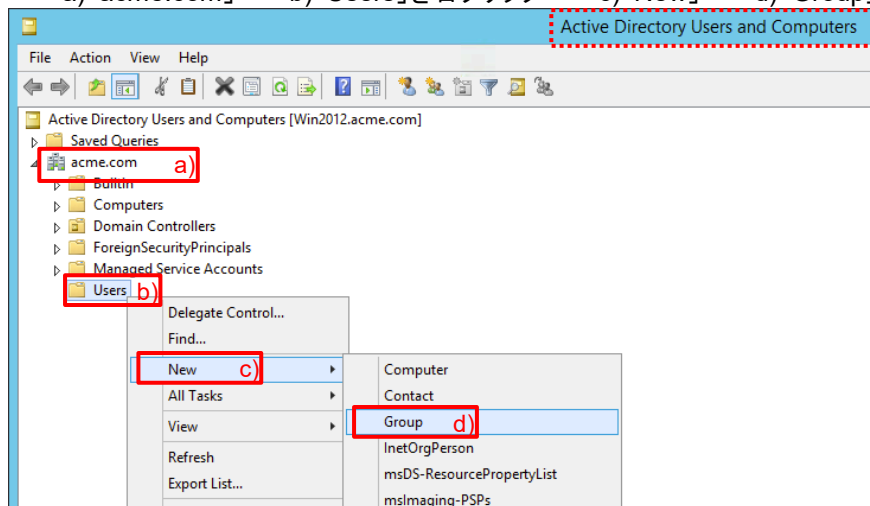
一つの案として、以下にその方法を記載します。

8.5.1. Active Directory に新グループを追加

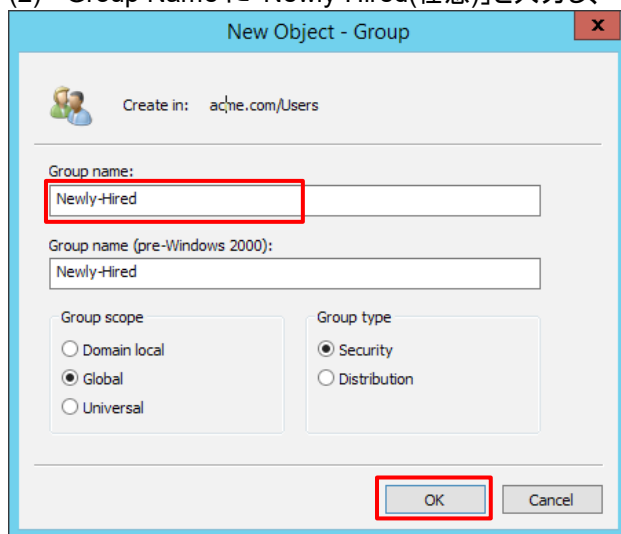
「新入社員を AD の User として登録する際に、新入社員用グループ:「Newly-Hired」を割り当てることで、そのグループだけにクライアント証明書を配布する」という設定方法を示します。

この設定方法を使えば、新入社員が入社したタイミングでは、AD の設定で、そのユーザーにグループを割り当てるだけでなく、GlobalProtect 設定を変更する必要はありません。

- (1) Win2012 の「Administrative Tools」 → 「Active Directory Users and Computers」を開きます。
 - a)「acme.com」 → b)「Users」を右クリック → c)「New」 → d)「Group」をクリックします。

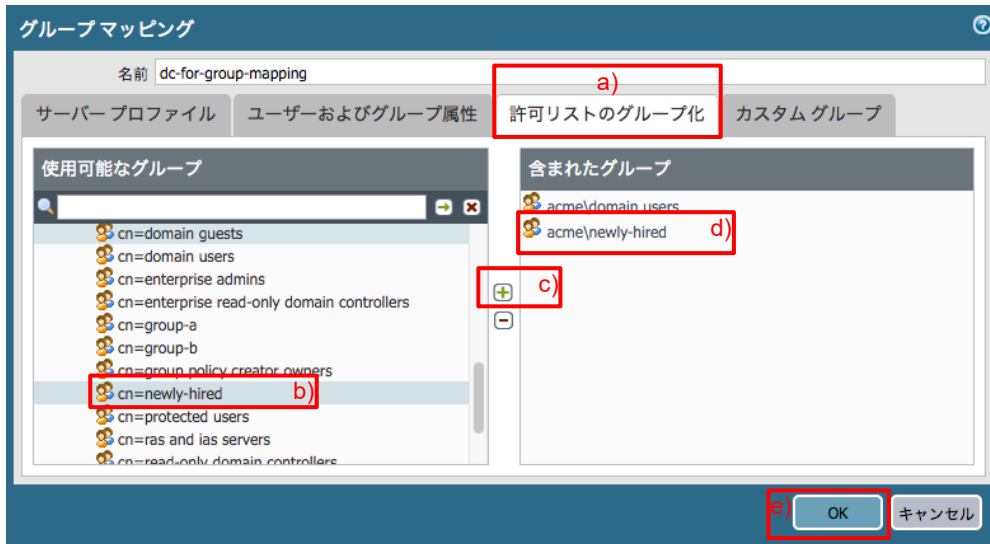


- (2) Group Name に「Newly-Hired(任意)」と入力し、「OK」をクリックします。



8.5.2. グループマッピングの追加

- (1) PA Firewall の「Device」タブ → 「ユーザーID」 → 「グループマッピング設定」タブで表示された、設定済みの「dc-for-group-mapping」をクリックします。
a)「許可リストのグループ化」 → 「DC=acme, DC=com」を展開 → 「cn=users」を展開し、b)「cn=newly-hired」を選択 → c) [+]をクリックして、d)の状態にします。e)「OK」をクリックします。



- (2) 「コミット」を実施します。

8.5.3. Portal の設定

Portal のエージェント設定を、Newly-Hired 用に追加します。

- (1) 「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → a)「エージェント」タブ → b)設定済みの「GP-Agent」の先頭にチェックを入れ、c)「コピー」をクリックします。



- (2) a)「認証」タブで、b)名前を「GP-Agent_for_NH(任意)」に変更します。
b)「SCEP」を選択して、d)設定済みの「WIN2012_SCEP」を選択します。

設定

認証 ユーザー/ユーザーグループ 内部 外部 アプリケーション データ収集

名前 GP-Agent_for_NH

クライアント証明書 SCEP WIN2012_SCEP

秘密鍵など、選択したクライアントの証明書は、クライアントマシンにインストールされます。

ユーザー認証情報の保存 Yes

認証オーバーライド

クッキーを生成して認証上書き

クッキーを受け入れて認証上書き

Cookie有効期間 Hours 24

クッキーの暗号化/復号化用の証明書 None

ダイナミックパスワード(2要素認証)を必要とするコンポーネント

ポータル 外部ゲートウェイ-マニュアルのみ

内部ゲートウェイ-全部 外部ゲートウェイ-自動検出

保存した認証情報を使用するのではなく、ユーザーを認証するには、ワンタイムパスワード(OTP)などのダイナミックパスワードを使用するオプションを選択してください。それにより、常に選択したオプションごとに新たな認証情報の入力を求めるメッセージが表示されます。

OK キャンセル

- (3) a)「ユーザー/ユーザーグループ」タブで、b)「ユーザー/ユーザーグループ」の下で「acme¥newly-hired」を選択します。c)「OK」をクリックします。

設定

認証 ユーザー/ユーザーグループ 内部 外部 アプリケーション データ収集

いずれか

OS

選択

ユーザー/ユーザーグループ

acme¥newly-hired

acme¥domain users

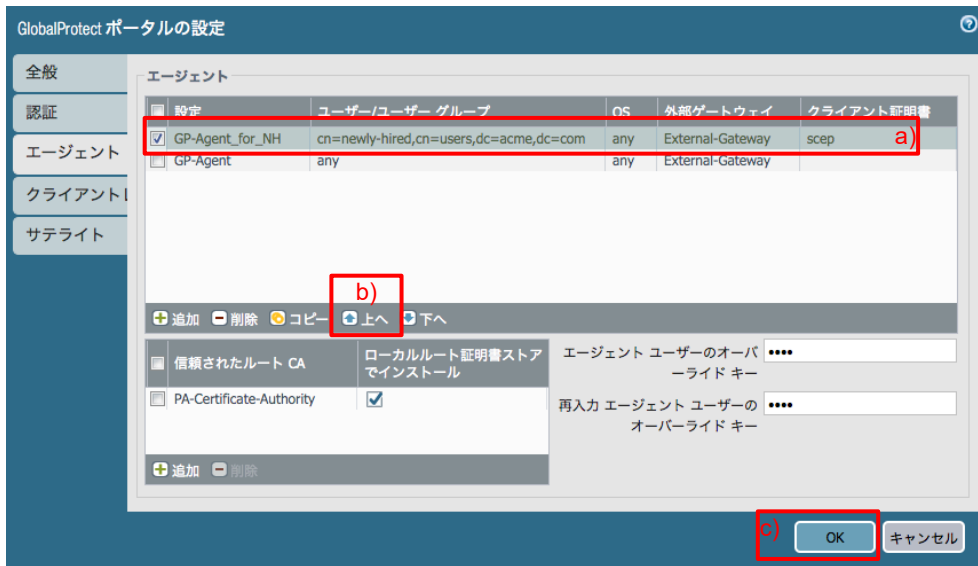
acme¥newly-hired

追加 削除

追加 削除

OK キャンセル

- (4) a)「GP-Agent_for_NH」の先頭にチェックを入れて、b)「上へ」をクリックして、上部へ移動します。
c)「OK」をクリックします。

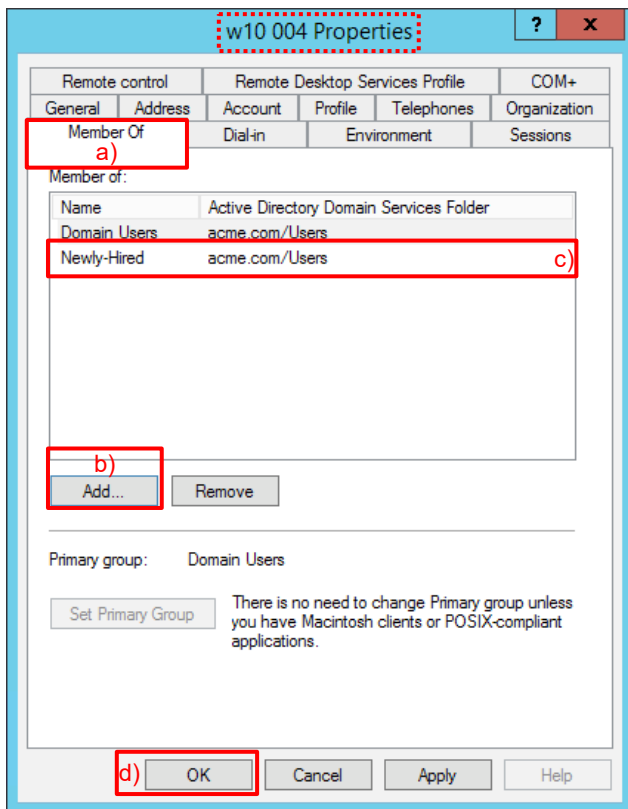


- (5) 「コミット」を実施します。

8.5.4. 新規ユーザーを「Newly-Hired」グループに入れる

w10-004 を新入社員と想定して、「Newly-Hired」グループのメンバーにします。

- (1) Win2012 の「Administrative Tools」 → 「Active Directory Users and Computers」を開きます。
「acme.com」 → 「Users」で、「w10 004」をクリックします。
- (2) a)「Member Of」タブで、b)「Add」をクリック → c)「Newly-Hired」を追加して、d)「OK」をクリックします。



8.5.5. GP Agent からのアクセス

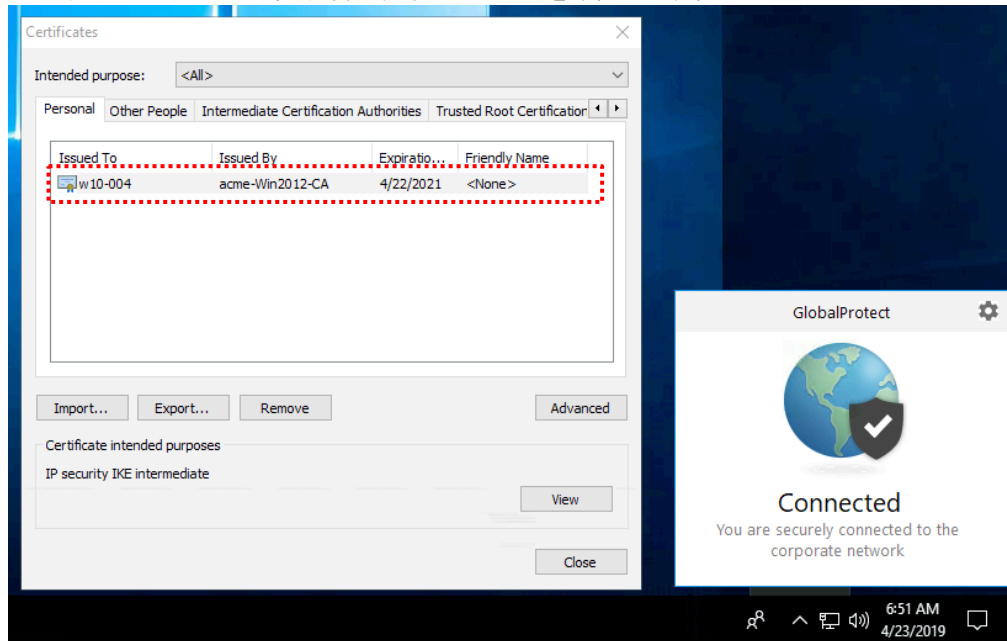
「Newly-Hired」グループだけにクライアント証明書が配布されることを確認します。

- (1) Active Directory の設定を即時反映させたい場合は、PA Firewall で下記のコマンドを実行します。
(先の設定で、グループマッピング設定を 60 秒に設定していれば、1 分で反映されます。)

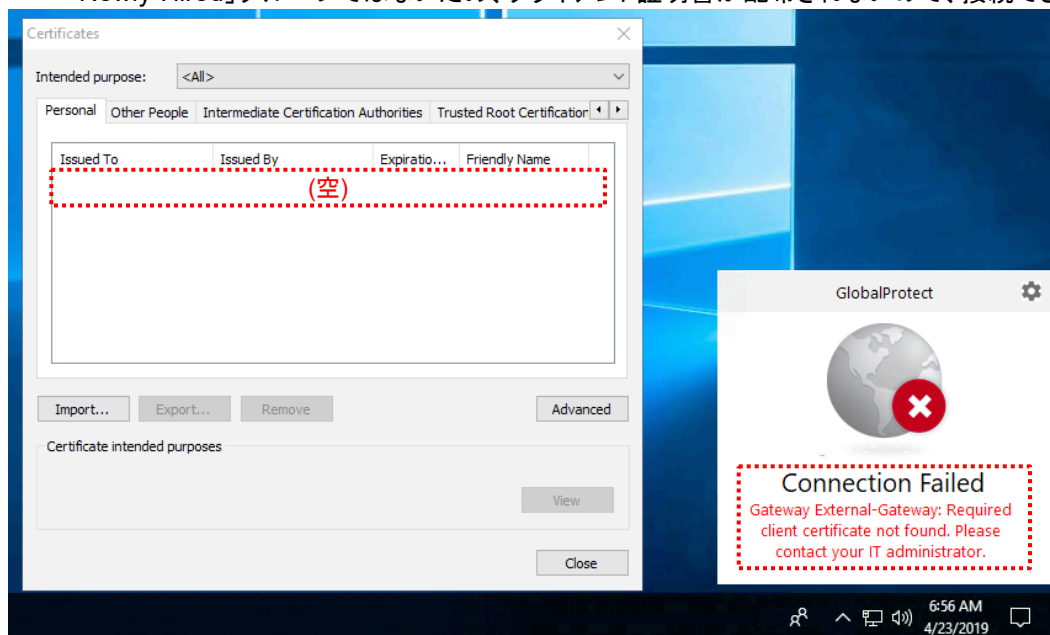
```
admin-admin@Azure-PA-VM> debug user-id refresh group-mapping all
```

```
group mapping 'dc-for-group-mapping' in vsys1 is marked for refresh.
```

- (2) w10-004 (Newly-Hired グループのメンバー) からアクセスします。
個別のクライアント証明書が発行されることを確認します。



- (3) w10-002 がクライアント証明書を保持している場合は削除します。
w10-002 からアクセスします。
「Newly-Hired」グループではないため、クライアント証明書が配布されないの、接続できません。



- (4) 新入社員(本ガイドでは w10-004)へのクライアント証明書配布完了を確認した後は、Active Directory で、w10-004 から「Newly-Hired」グループを削除する、という運用は必要です。

9. ワンタイムパスワード認証の設定

GlobalProtect は、ワンタイムパスワード(以降、OTP)を利用して、認証を強化したい、というニーズに対応することもできます。

本ガイドでは、比較的簡単にインストールできる、RADIUS プロトコルを使った OTP サーバー:RCDevs SA 提供の「WebADM Server Free Edition」を、ネットワーク構成図中の社内 LAN-B (オンプレミス側) に設置して、利用することになります。

9.1. Google Authenticator のインストール

OTP には「Google Authenticator」を使いますので、スマートデバイス(iOS または Android)にインストールします。

App Store (iOS) または Google Play (Android) からダウンロード&インストールできます。

9.2. OTP サーバーのインストールと設定

9.2.1. サーバーの初期設定

(1) 下記の RCDevs の Web サイト Link から、OTP サーバーの仮想マシンイメージをダウンロードします。

<https://www.rcdevs.com/downloads/VMWare+Appliances/>

VMWare Appliances	Version	Size	Date	Action
Virtual Appliance (OpenLDAP - CentOS 7) ★	1.6.9-3	732M	2019-02-12	Download
Virtual Appliance (OpenLDAP - CentOS 6) ★	1.6.9-3	447M	2019-02-12	Download

(2) 本ガイドでは、社内 LAN-B(サブネット:10.10.222.0/24)にこの仮想マシンを展開します。(RCDevs-VM.ovf ファイルを VMware 環境にインポートします。)

(3) 起動後、コンソール画面で、以下の通り設定します。

```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.5.1.el7.x86_64 on an x86_64

rcwm7 login: root (automatic login)
Last login: Mon Apr 29 23:52:15 on tty1
-bash: plymouth: command not found

-----
Welcome to RCDevs VMWare Appliance 1.6.9!
-----

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#? 5
Please select a country.
 1) Afghanistan      18) Israel           35) Palestine
 2) Armenia           19) Japan            36) Philippines
 3) Azerbaijan       20) Jordan           37) Qatar
 4) Bahrain           21) Kazakhstan      38) Russia
 5) Bangladesh       22) Korea (North)   39) Saudi Arabia
 6) Bhutan            23) Korea (South)   40) Singapore
 7) Brunei            24) Kuwait           41) Sri Lanka
 8) Cambodia          25) Kyrgyzstan      42) Syria
 9) China             26) Laos             43) Taiwan
10) Cyprus            27) Lebanon          44) Tajikistan
11) East Timor        28) Macau            45) Thailand
12) Georgia           29) Malaysia         46) Turkmenistan
13) Hong Kong         30) Mongolia         47) United Arab Emirates
14) India             31) Myanmar (Burma)  48) Uzbekistan
15) Indonesia         32) Nepal            49) Vietnam
16) Iran              33) Oman             50) Yemen
17) Iraq              34) Pakistan

#? 19

The following information has been given:

      Japan

Therefore TZ='Asia/Tokyo' will be used.
Local time is now:      Mon Apr  1 11:28:50 JST 2019.
Universal Time is now: Mon Apr  1 02:28:50 UTC 2019.

This VM is running with dynamic IP assignment (DHCP)
The current IP address is 10.10.222.105
Do you want to configure a static IP (y/n)? y
Please type the fixed IP address [10.10.222.105]: 10.10.222.201
Please type the network mask [255.255.255.0]: 変更なければ enter
255.255.255.0
Please type the gateway address [10.10.222.2]: 変更なければ enter
10.10.222.2
Please type your primary DNS server IP [8.8.8.8]: 10.9.2.5
Please type your secondary DNS server IP [1]: 8.8.8.8

Fixed IP address: 10.10.222.201
Network address: 10.10.222.0
Network mask: 255.255.255.0
Gateway IP address: 10.10.222.2
Primary DNS server: 10.9.2.5
Secondary DNS server: 8.8.8.8
Do you confirm (y/n): y
Writing /etc/sysconfig/network-scripts/ifcfg-ens32
Restarting network...

Setting up WebADM server...
Choose a directory template:
 1) Default configuration (RCDevs Directory)
 2) Other generic LDAP server (Novell eDirectory, Oracle, OpenLDAP)
 3) Active Directory without schema extension
Choose a template number [1]: 3
Please type the name/ip of the LDAP server [localhost]: 10.9.2.5
Please type the port for LDAP [389]: 変更なければ enter
389
Checking port...Ok
Please choose the encryption ([TLS/SSL/NONE]?NONE
Please type domain FQDN (i.e. dc=lab,dc=local) []: dc=acme,dc=com
Please type a user with read/write access to LDAP [cn=Administrator,cn=Users,dc=acme,dc=com]: cn=admin-admin,cn=Users,dc=acme,dc=com
Please type the user password: ADの管理者パスワードを入力
Testing user access...Ok
Please type the WebADM container [cn=WebADM,dc=acme,dc=com]: enter
```

～中略～ (以降、設定はありません。)

```
Starting services...
[ 229.572422] radiusd[5900]: Checking system architecture... Ok
[ 229.595906] ldproxy[5903]: Checking system architecture... Ok
[ 229.646188] ldproxy[5903]: Checking server configuration... Ok
[ 229.785020] webadm[5899]: Checking libudev dependency... Ok
[ 229.785722] radiusd[5900]: Checking server configuration... Ok
[ 229.831741] webadm[5899]: Checking system architecture... Ok
[ 230.507604] webadm[5899]: Checking server configurations... Ok
[ 230.608983] webadm[5899]: No Enterprise license found (using bundled Freeware license)
[ 230.609777] webadm[5899]: Please contact sales@rcdevs.com for commercial information
[ 230.672981] ldproxy[5903]: Starting OpenOTP LDAP Bridge... Ok
[ 230.802854] radiusd[5900]: Starting OpenOTP RADIUS Bridge... Ok
[ 231.636911] webadm[5899]: Starting WebADM Session server... Ok
[ 231.652652] webadm[5899]: Starting WebADM PKI server... Ok
[ 232.662158] webadm[5899]: Starting WebADM Watchd server... Ok
[ 232.731937] webadm[5899]: Starting WebADM HTTP server... Ok
[ 233.742084] webadm[5899]: Checking server connections. Please wait...
[ 233.818891] webadm[5899]: Connected LDAP server: LDAP Server 1 (10.9.2.5)
[ 233.819714] webadm[5899]: Connected SQL server: SQL Server (127.0.0.1)
[ 233.820472] webadm[5899]: Connected PKI server: PKI Server (127.0.0.1)
[ 233.821099] webadm[5899]: Connected Session server: Session Server (::1)
[ 234.015738] webadm[5899]: Checking LDAP proxy user access... Ok
[ 234.024853] webadm[5899]: Checking SQL database access... Ok
[ 234.037733] webadm[5899]: Checking PKI service access... Ok
Created symlink from /etc/systemd/system/multi-user.target.wants/radiusd.service to /usr/lib/systemd/system/radiusd.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/ldproxy.service to /usr/lib/systemd/system/ldproxy.service.
Ok

You can connect your server via SSH with 'ssh root@10.10.222.201'.
SSH root password is 'password'.

You can login RCDevs WebADM Admin Portal at 'https://10.10.222.201'.
WebADM login user DN is 'cn=admin-admin,cn=users,dc=acme,dc=com'.

WARNING: This appliance is configured with permissive firewall,
dummy certificates, default passwords for services and root access.
You MUST re-configure your appliance before any production use!

Press any key to finish!
-bash-4.2#
```

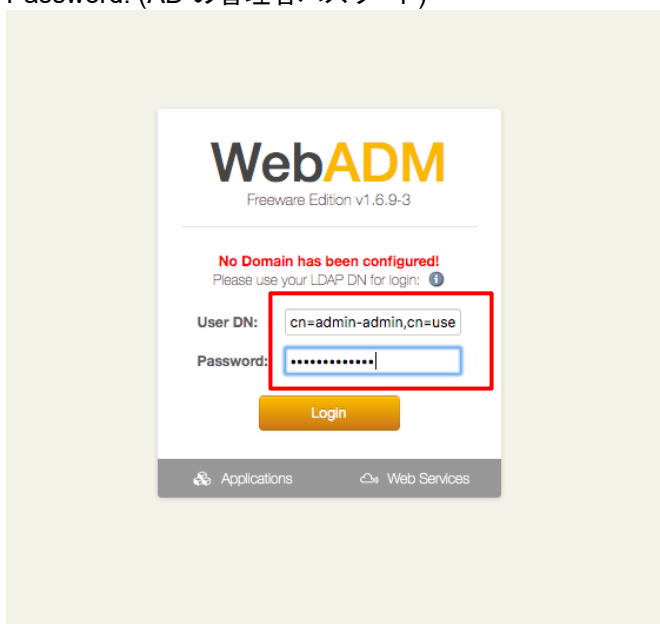
これで、設定が完了します。

9.2.2. WebADM の設定

9.2.2.1. WebADM の初期設定

- (1) <https://10.10.222.201> へ、到達可能な PC からアクセスします。
- (2) WebADM に、以下の値を使ってログインします。

User DN: cn=admin-admin,cn=users,dc=acme,dc=com
Password: (AD の管理者パスワード)



- (3) ログイン直後の画面です。
画面下方にある「Create default containers and objects」をクリックします。

LDAP Server 1 (Active Directory)

- DC=acme (12)
- CN=Builtin
- CN=Computers
- CN=ForeignSecurityPrincip...
- CN=Infrastructure
- CN=LostAndFound
- CN=Managed Service Accoun...
- CN=NTDS Quotas
- CN=Program Data
- CN=System
- CN=TPM Devices
- CN=Users (28)
- CN=Allowed RODC Password....
- CN=Cert Publishers
- CN=Cloneable Domain Contr...
- CN=Denied RODC Password R...
- CN=DnsAdmins
- CN=DnsUpdateProxy
- CN=Domain Admins

WebADM Freeware Edition v1.6.9-3
Copyright © 2010-2019 RCDevs SA, All Rights Reserved

Home Admin Create Search Import Databases Statistics Applications About Logout

WebADM Setup

Your WebADM installation is not completely configured!
Please run the following setup actions to finish configuring WebADM.

Checking LDAP schema
Reading schema objectclasses... Ok
Reading schema attributes... Ok
Checking account objectclass... Ok
Checking group objectclass... Ok
Checking config objectclass... Ok
Checking data attribute... Ok
Checking settings attribute... Ok
Checking type attribute... Ok

Checking WebADM super admins
Checking super admin 'cn=admin-admin'... Ok
Checking super admin 'cn=Domain Admins'... Ok

Checking LDAP permissions
Tree root: DC=acme,DC=com (Microsoft)
Checking proxy user permissions... Ok

Checking default LDAP objects
Checking adminroles container... Missing
Checking optionsets container... Missing
Checking webapps container... Missing
Checking webservs container... Missing
Checking mountpoints container... Missing
Checking domains container... Missing
Checking clients container... Missing

Create default containers and objects

You must logout when setup is completed.

～中略～

- (4) 「OK」をクリックします。

LDAP Server 1 (Active Directory)

- DC=acme (13)
- CN=Builtin
- CN=Computers
- CN=ForeignSecurityPrincip...
- CN=Infrastructure
- CN=LostAndFound
- CN=Managed Service Accoun...
- CN=NTDS Quotas
- CN=Program Data
- CN=System
- CN=TPM Devices
- CN=Users (28)
- CN=Allowed RODC Password....
- CN=Cert Publishers
- CN=Cloneable Domain Contr...

WebADM Freeware Edition v1.6.9-3
Copyright © 2010-2019 RCDevs SA, All Rights Reserved

Home Admin Create Search Import Databases Statistics Applications About Logout

Containers Setup

Creating WebADM Domains container cn=Domains,cn=WebADM,dc=acme,dc=com... Success
Creating Domain for cn=users,dc=acme,dc=com... Success
Creating WebADM OptionSets container cn=OptionSets,cn=WebADM,dc=acme,dc=com... Success
Creating OptionSet for cn=users,dc=acme,dc=com... Success
Creating WebADM AdminRoles container cn=AdminRoles,cn=WebADM,dc=acme,dc=com... Success
Creating WebADM WebApps container cn=WebApps,cn=WebADM,dc=acme,dc=com... Success
Creating WebADM WebSrvs container cn=WebSrvs,cn=WebADM,dc=acme,dc=com... Success
Creating WebADM Clients container cn=Clients,cn=WebADM,dc=acme,dc=com... Success
Creating WebADM MountPoints container cn=MountPoints,cn=WebADM,dc=acme,dc=com... Success

Ok

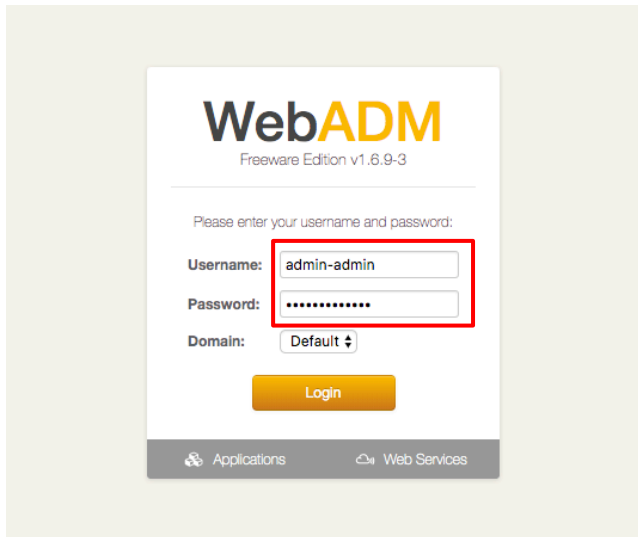
- (5) 「logout」をクリックして、一旦 logout します。

- CN=Group Policy Creator O...
- CN=Guest
- CN=Protected Users
- CN=RAS and IAS Servers
- CN=Read-only Domain Contr...
- CN=Schema Admins

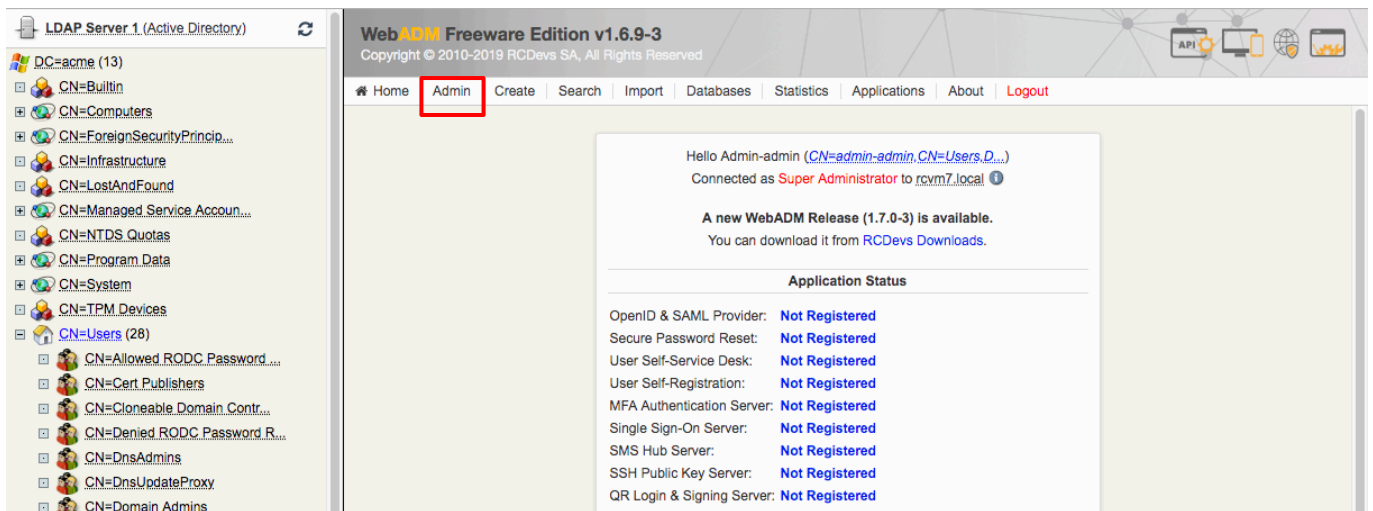
Checking mountpoints container... Ok
Checking domains container... Ok
Checking clients container... Ok

You must logout when setup is completed.

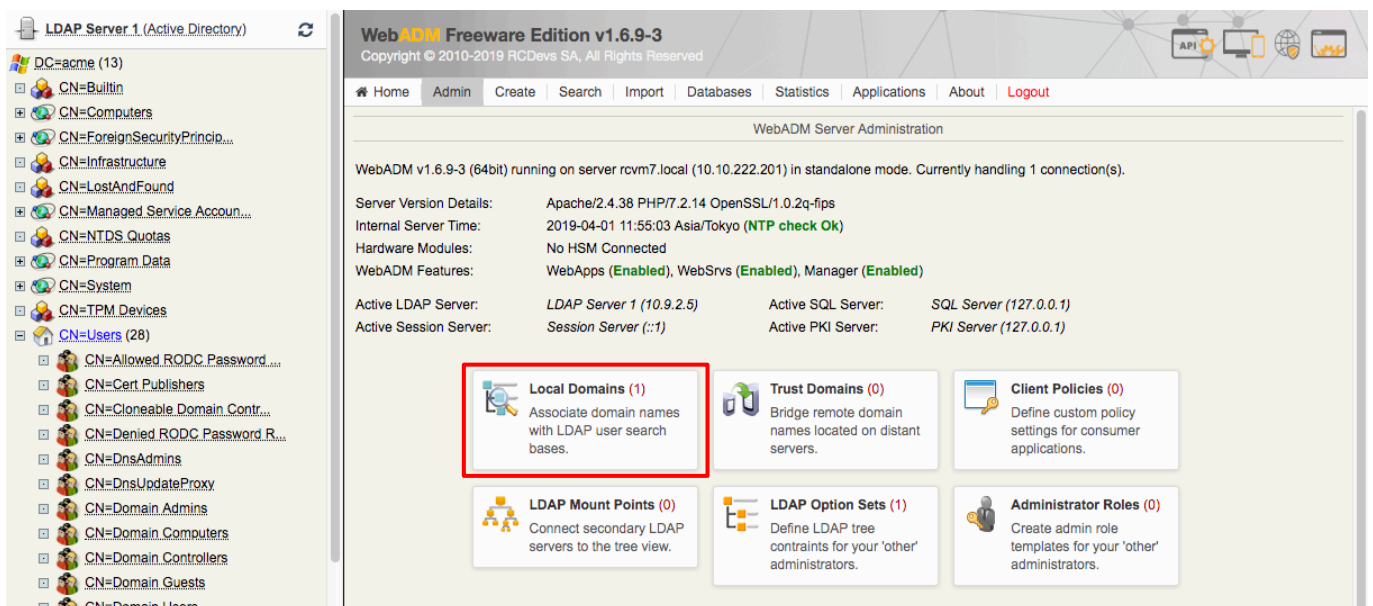
(6) 今度は、AD の管理者 Username と Password でログインします。



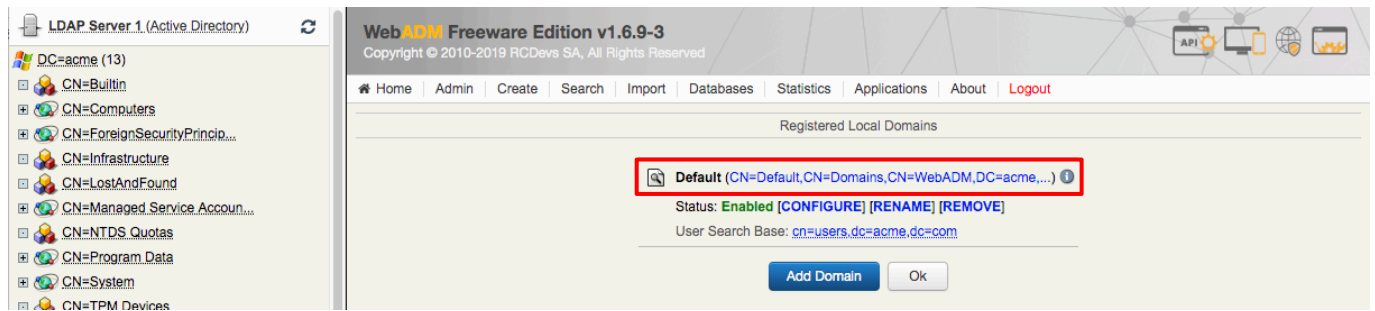
(7) 「Admin」タブをクリックします。



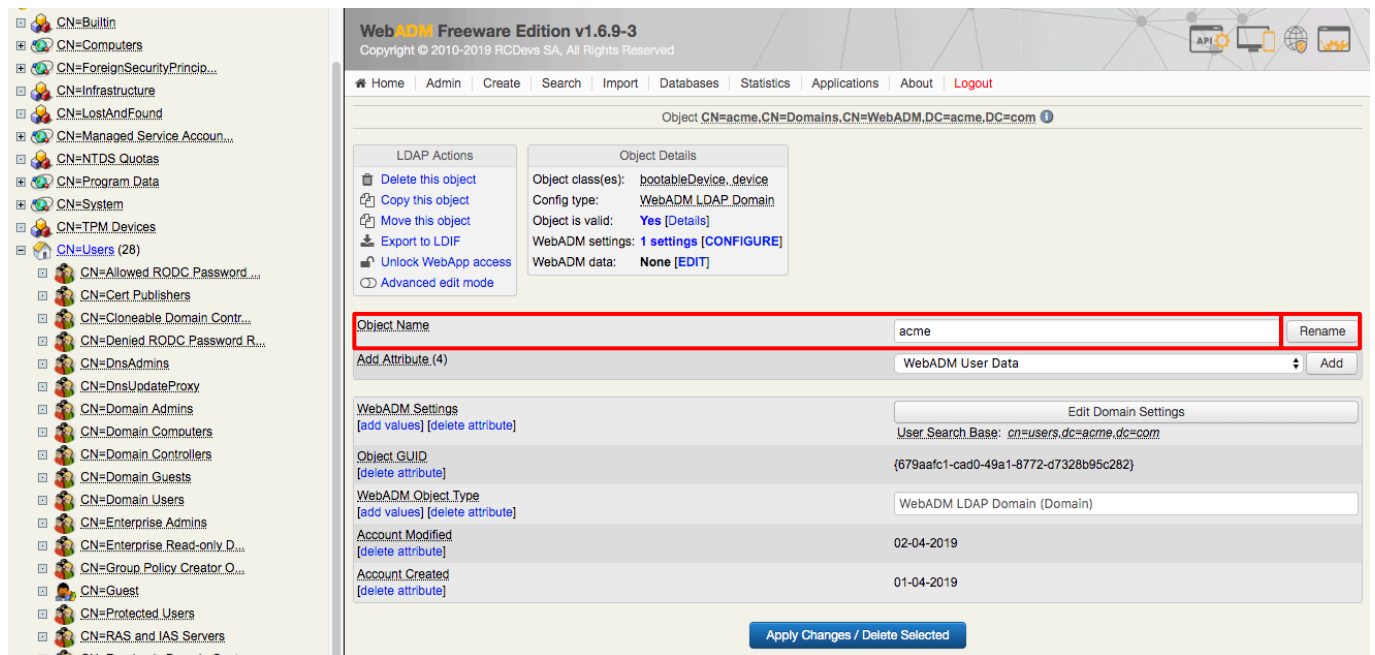
(8) Local Domains をクリックします。



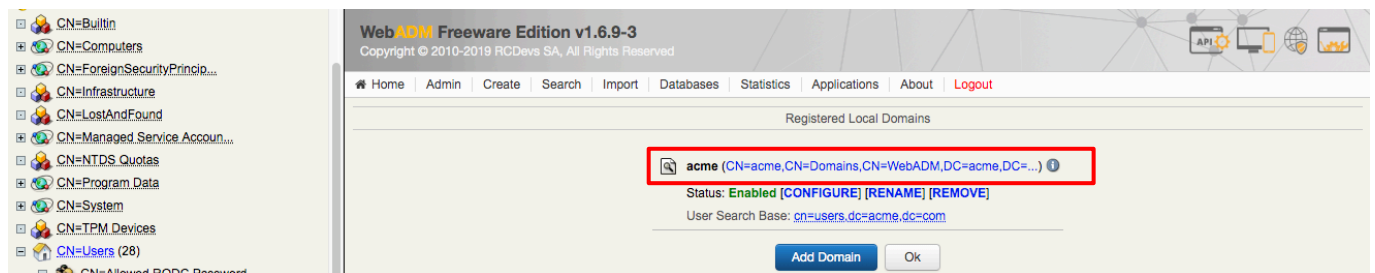
(9) 「CN=Default, CN=Domains～」をクリックします。



(10) Object Name に「acme」と入力して「Rename」をクリックします。



(11) Admin タブをクリックして、以下の状態(先頭が CN=acme)に変化したことを確認します。



(12) 「Applications」タブをクリックします。

「MFA Authentication Server (OpenOTP)の下 → 「Status: Not Registered」の右横の「REGISTER」をクリックします。

The screenshot shows the WebADM Freeware Edition v1.6.9-3 interface. The left sidebar displays a directory tree for 'LDAP Server 1 (Active Directory)' with 'CN=Users (28)' selected. The main content area shows the 'Applications' tab with a list of registered applications and services. The 'MFA Authentication Server (OpenOTP) v1.4.2-2 (Commercial)' service is highlighted. Its status is 'Not Registered' and the 'REGISTER' button is highlighted with a red box. The service details include: Multi-factor authentication service supporting OATH, HOTP/TOTP/OCRA, FIDO, YubiKey, SMS OTP and Mail OTP. Latest Version: 1.4.3-2 (DOWNLOAD). Service URL (SSL): https://10.10.222.201:8443/openotp/. Service URL (STD): http://10.10.222.201:8080/openotp/. Mobile Endpoint: https://10.10.222.201/ws/openotp/. U2F Facet Endpoint: https://10.10.222.201/ws/appid/. SOAP WSDL File: openotp.wsdl.

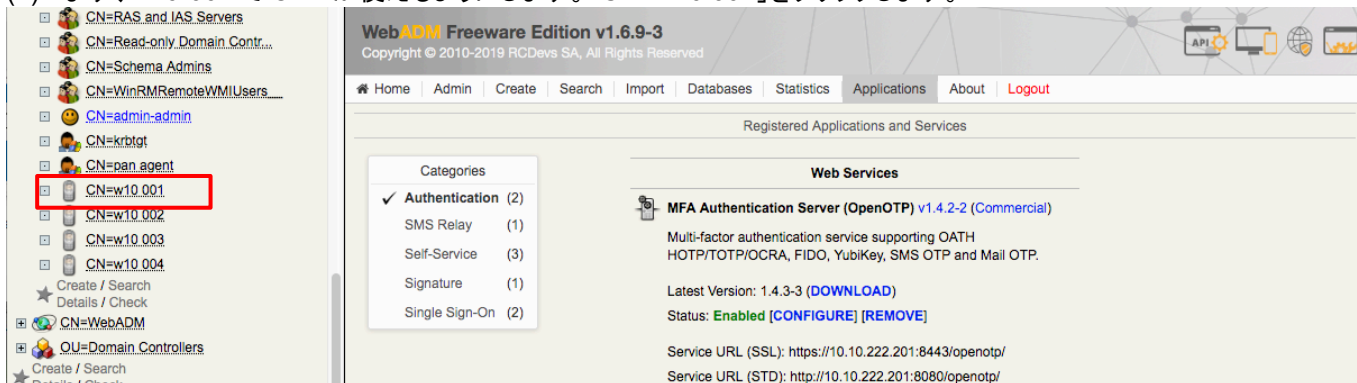
(13) 「Status: Enabled」に変わります。

The screenshot shows the WebADM Freeware Edition v1.6.9-3 interface. The left sidebar displays a directory tree for 'LDAP Server 1 (Active Directory)' with 'CN=Users (30)' selected. The main content area shows the 'Applications' tab with a list of registered applications and services. The 'MFA Authentication Server (OpenOTP) v1.4.2-2 (Commercial)' service is highlighted. Its status is now 'Enabled' and the 'CONFIGURE' button is highlighted with a red box. The service details include: Multi-factor authentication service supporting OATH, HOTP/TOTP/OCRA, FIDO, YubiKey, SMS OTP and Mail OTP. Latest Version: 1.4.3-3 (DOWNLOAD). Service URL (SSL): https://10.10.222.201:8443/openotp/. Service URL (STD): http://10.10.222.201:8080/openotp/.

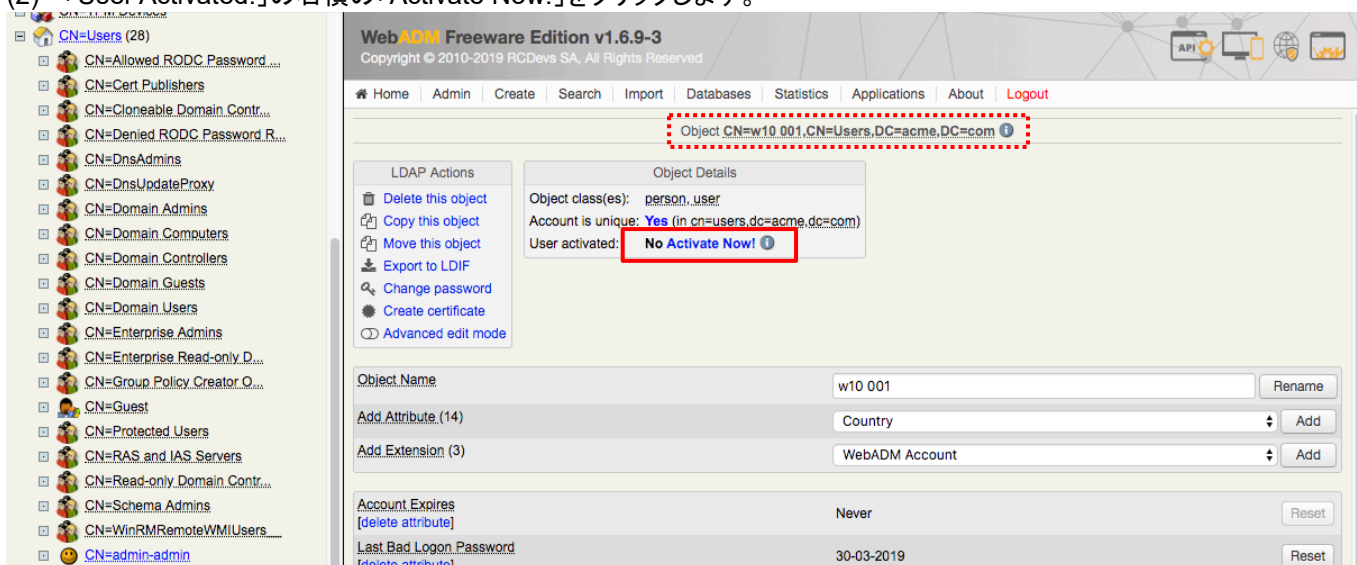
9.2.2.2. OTP の有効化

ユーザー毎に OTP 登録を行って、OTP 認証ができる状態にします。

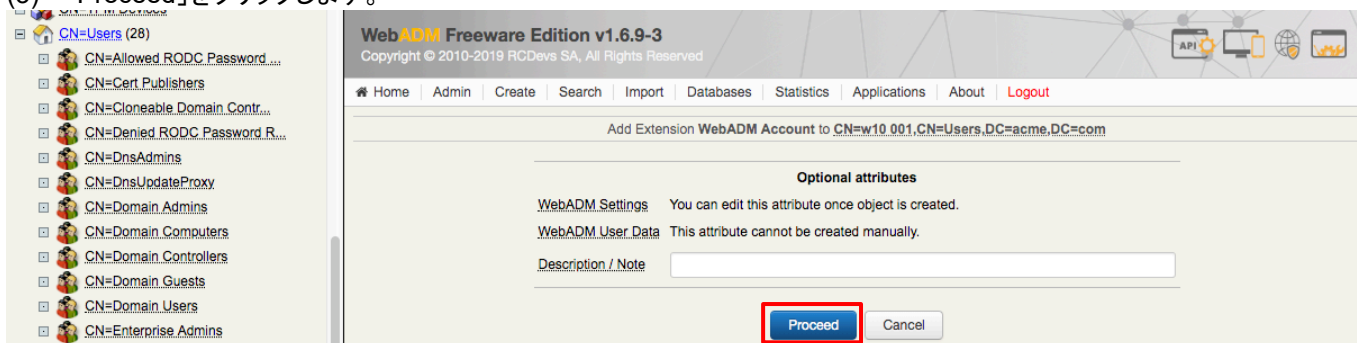
(1) まず、w10-001 で OTP が使えるようにします。「CN=w10 001」をクリックします。



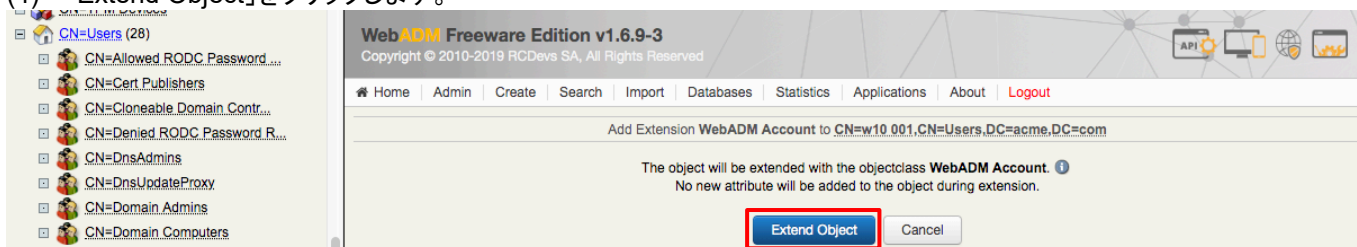
(2) 「User Activated:」の右横の「Activate Now!」をクリックします。



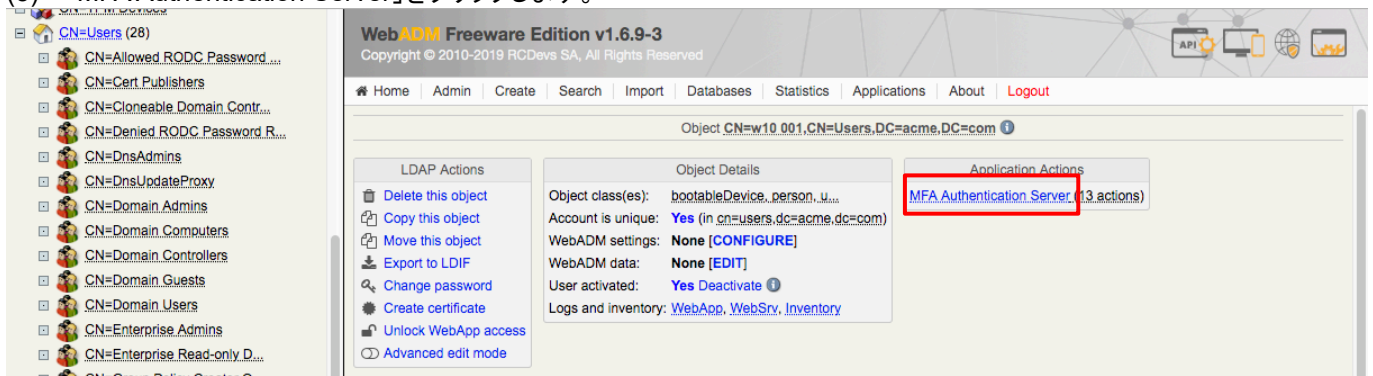
(3) 「Proceed」をクリックします。



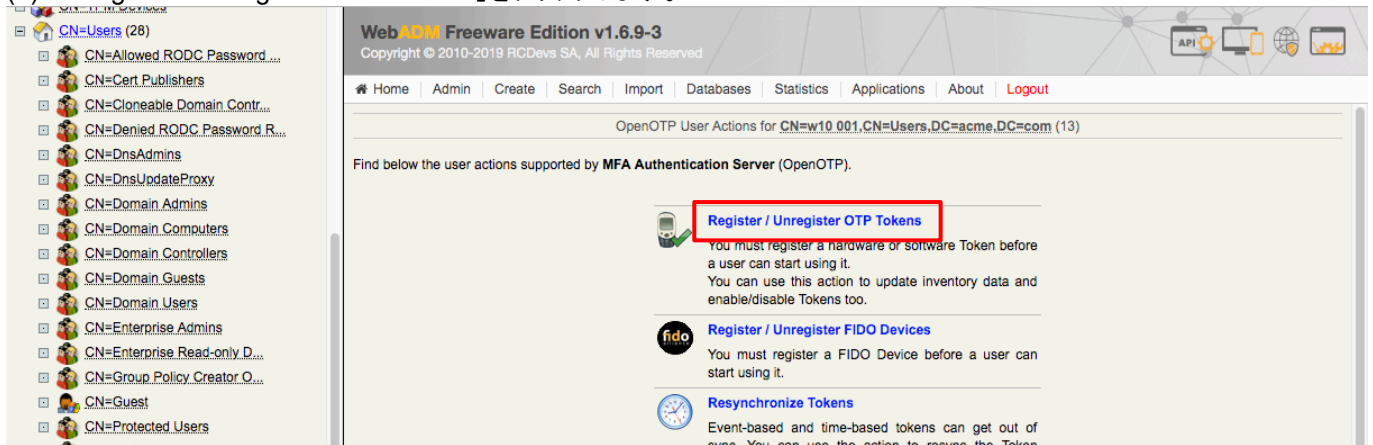
(4) 「Extend Object」をクリックします。



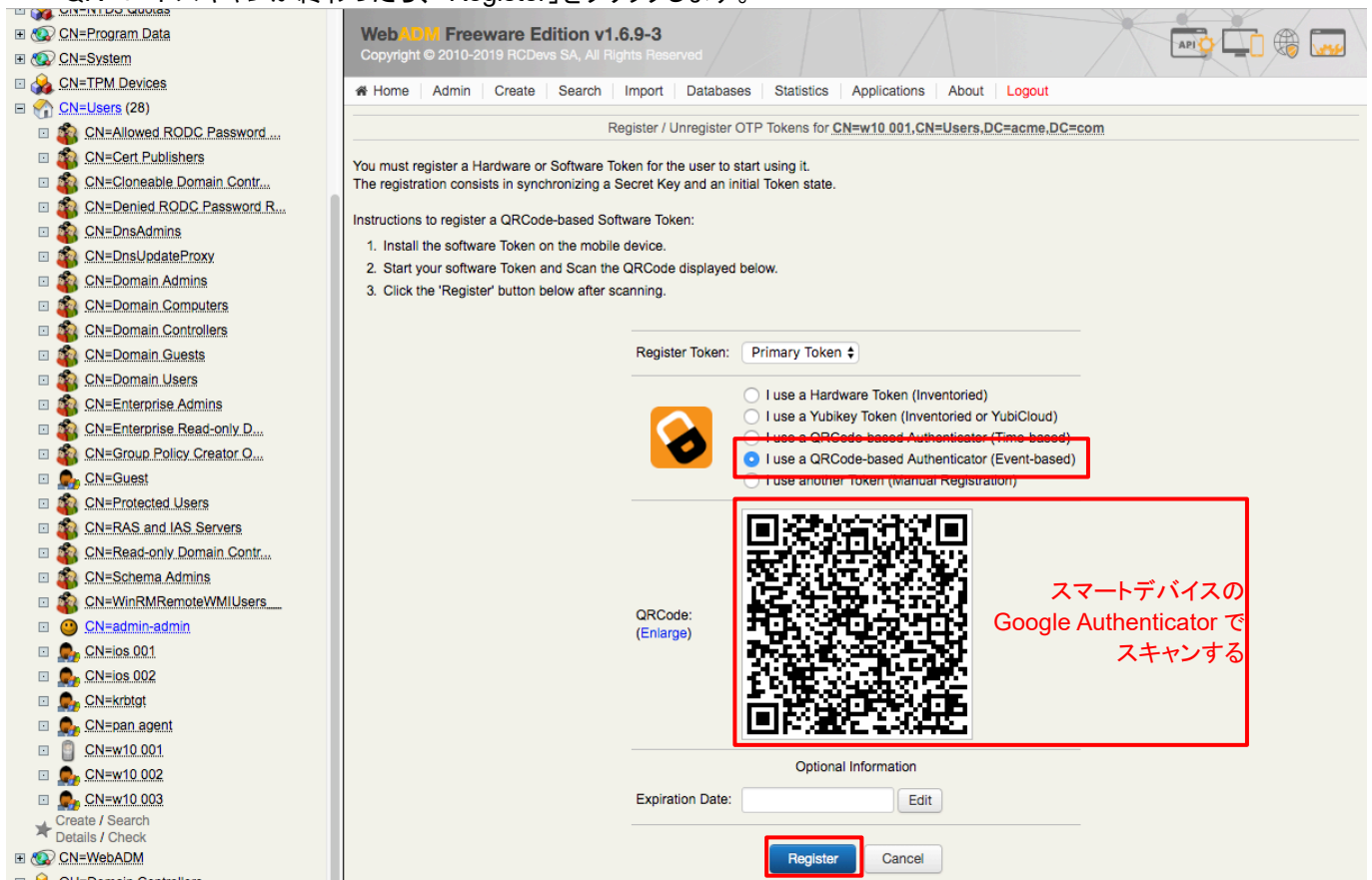
(5) 「MFA Authentication Server」をクリックします。



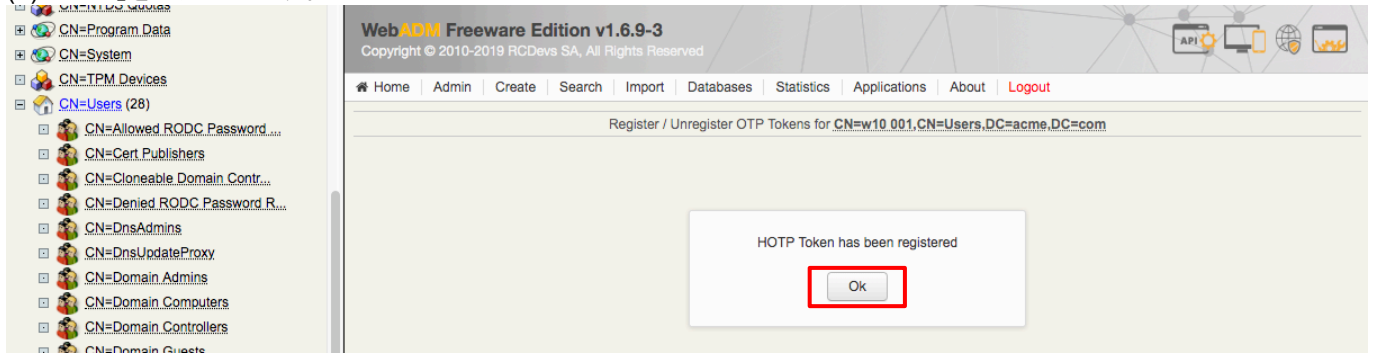
(6) 「Register / Unregister OTP Tokens」をクリックします。



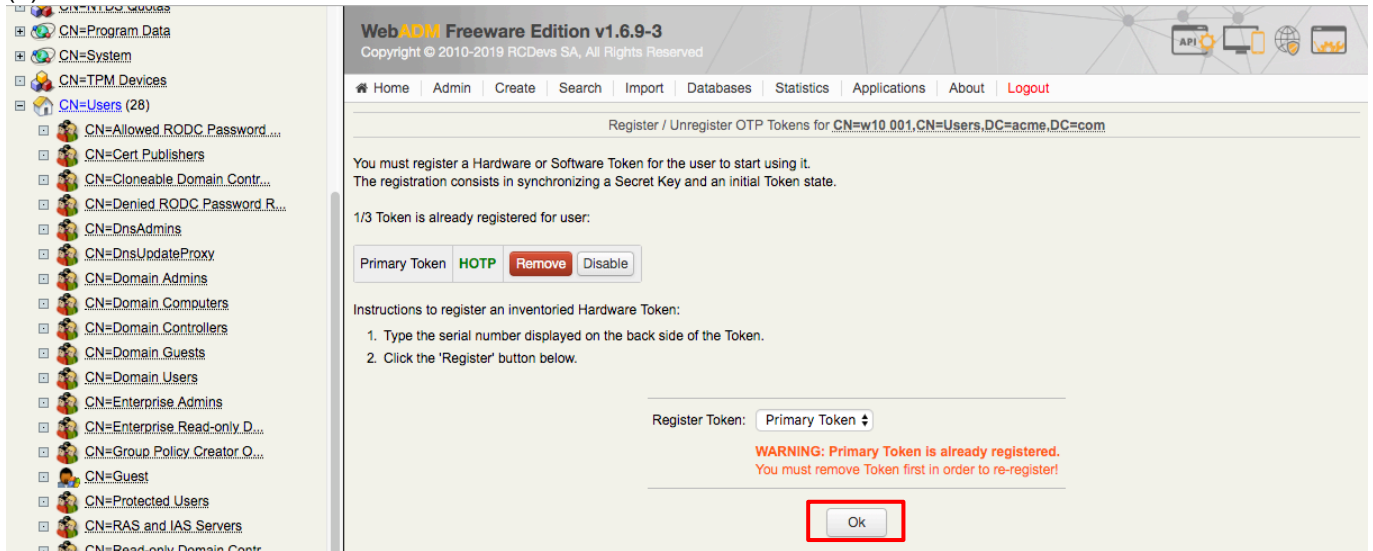
(7) 「I use a QRCode-based Authenticator (Event-based)」を選択します。
表示された QR コードを、スマートデバイスの Google Authenticator でスキャンします。
([例: iOS の場合] 上段の[+]をクリックして、下段に表示された「バーコードをスキャン」をクリックします。)
QR コードスキャンが終わったら、「Register」をクリックします。



(8) 「OK」をクリックします。



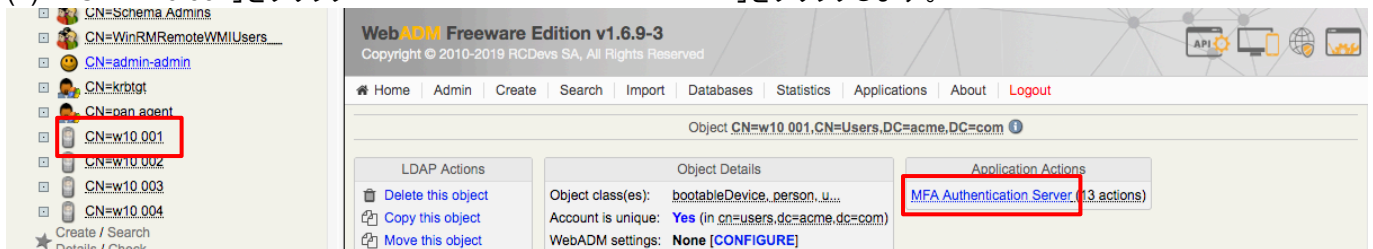
(9) 「OK」をクリックします。



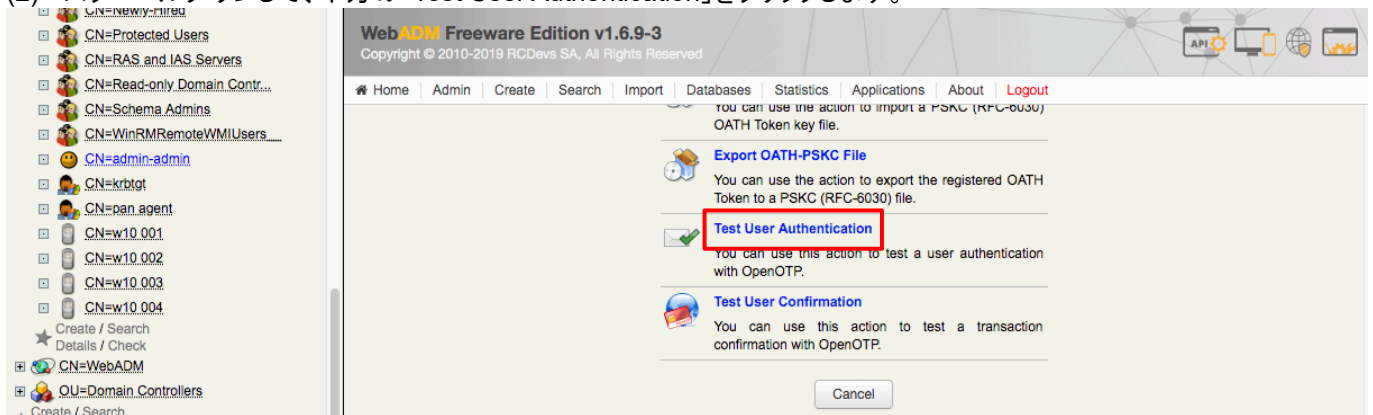
9.2.2.3. OTP の動作確認


Google Authenticator との連携が正しく動作するかをテストします。

(1) 「CN=w10.001」をクリック → 「MFA Authentication Server」をクリックします。



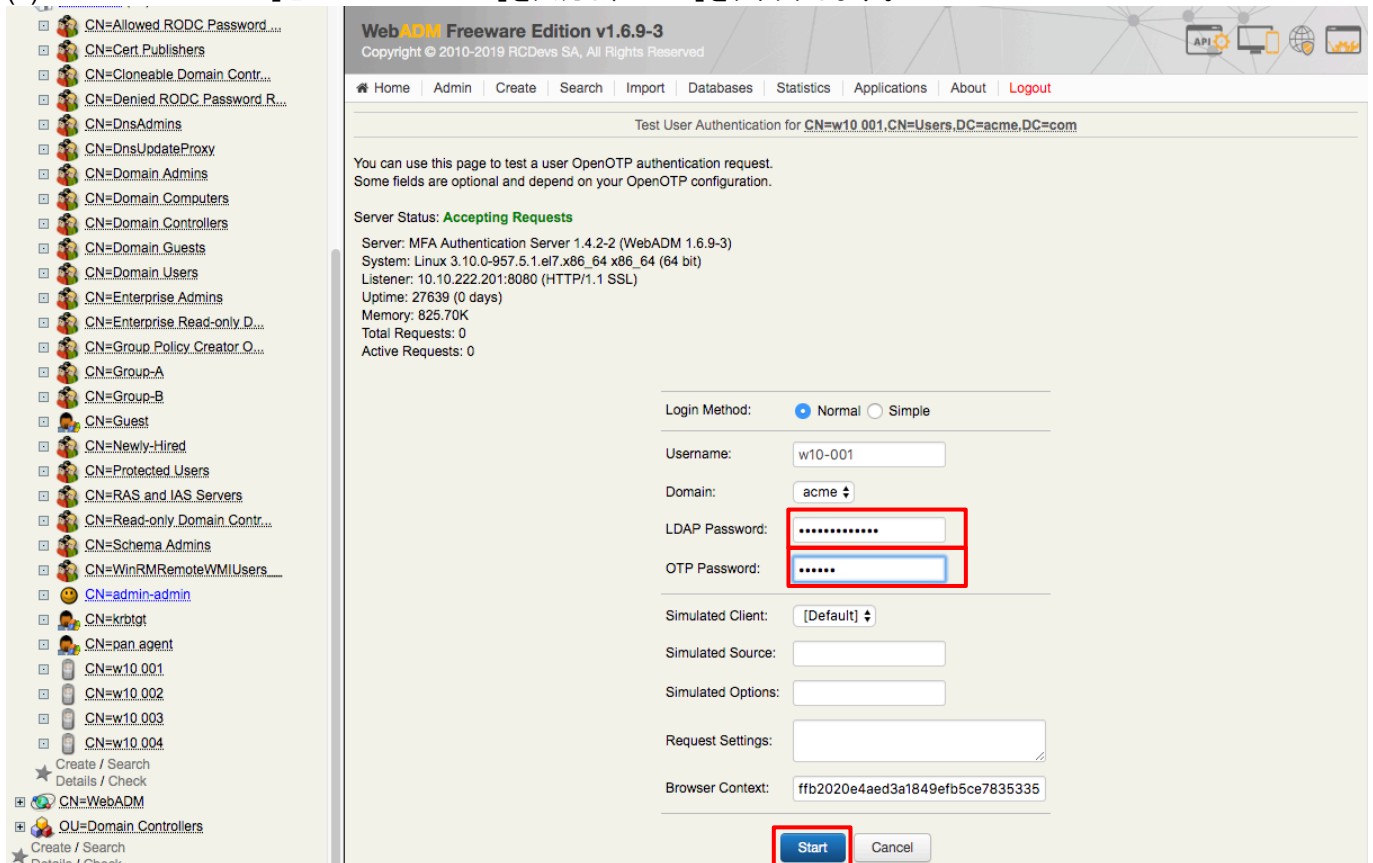
(2) スクロールダウンして、下方の「Test User Authentication」をクリックします。



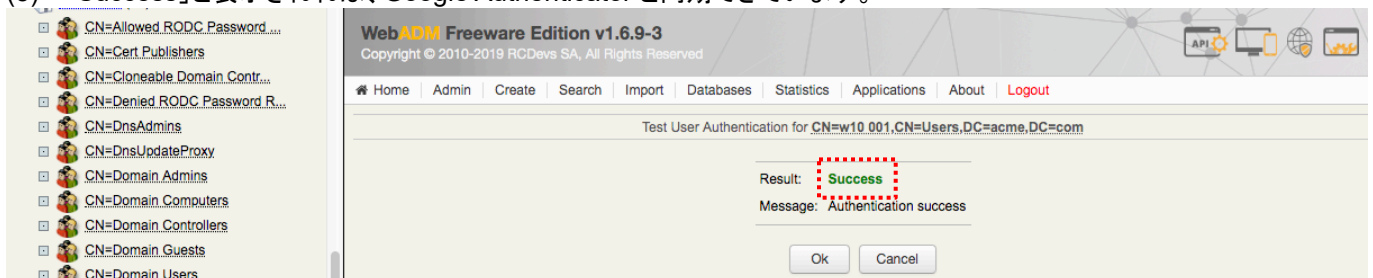
(3) スマートデバイス(例:iOS)の Google Authenticator を開き、 をクリックして表示された数字が OTP です。



(4) 「LDAP Password」と「OTP Password」を入力し、「Start」をクリックします。



(5) 「Success」と表示されれば、Google Authenticator と同期できています。



(6) 既述の「OTP の有効化」を繰り返して、他ユーザー(w10-002~w10-004)も OTP が使えるようにします。(Google Authenticator は、一つのアプリで複数のユーザーを登録できます。)

9.3. RADIUS 認証の設定

OTP サーバー:「WebADM Server Free Edition」は RADIUS なので、PA Firewall で、RADIUS 認証に関わる設定を行います。

9.3.1. サービスルートの変更

OTP サーバー(RADIUS サーバー)は、Trust ゾーン側に設置されているので、サービスルートを変更します。

- (1) a)「Device」 → b)「セットアップ」 → c)「サービス」 → d)「サービスルートの設定」で表示された画面で、e)のように、Radius の送信元インターフェイスおよび送信元アドレスを eth1/2 に変更します。
f)「OK」をクリックします。

The screenshot shows the Palo Alto Networks configuration interface. The 'Device' tab is selected at the top. In the left sidebar, 'セットアップ' (Setup) is highlighted. The main area shows the 'サービス' (Services) configuration page. The 'サービス機能' (Service Features) section has 'サービスルートの設定' (Service Route Configuration) selected. A modal window titled 'サービスルートの設定' (Service Route Configuration) is open, showing a table of services and their configurations. The 'Radius' service is selected, and its '送信元インターフェイス' (Source Interface) is set to 'ethernet1/2' and '送信元アドレス' (Source Address) is set to '10.9.2.4/24'. The 'OK' button is highlighted at the bottom of the modal.

サービス	送信元インターフェイス	送信元アドレス
<input type="checkbox"/> Mira	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Netflow	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> NTP	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Palo Alto Networks サービス	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Panorama	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> プロキシ	デフォルトを使用	デフォルトを使用
<input checked="" type="checkbox"/> Radius	ethernet1/2	10.9.2.4/24
<input type="checkbox"/> SCEP	ethernet1/2	10.9.2.4/24
<input type="checkbox"/> SNMP トラップ	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Syslog	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Tacplus	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> UID Agent	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> URL Updates	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> VM モニター	デフォルトを使用	デフォルトを使用
<input type="checkbox"/> Wildfire Private	デフォルトを使用	デフォルトを使用

- (2) 「コミット」を実施します。

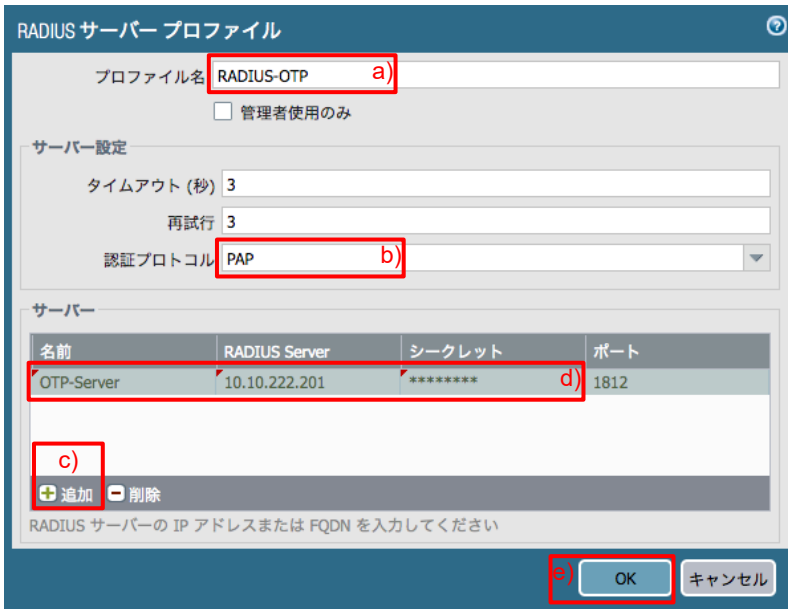
9.3.2. RADIUS サーバープロファイルの設定

RADIUS サーバーとの接続用パラメーターを指定する、サーバープロファイル設定を行います。

(1) a)「Device」タブ → b)「RADIUS」 → c)「追加」をクリックします。



(2) a) プロファイル名に「RADIUS-OTP(任意)」と入力します。
b) 認証プロトコルで「PAP」を選択します。
c) 「追加」をクリックします。
d) 名前に「OTP-Server(任意)」、RADIUS Server に「10.10.222.201」、シークレットに「testing123」と入力します。



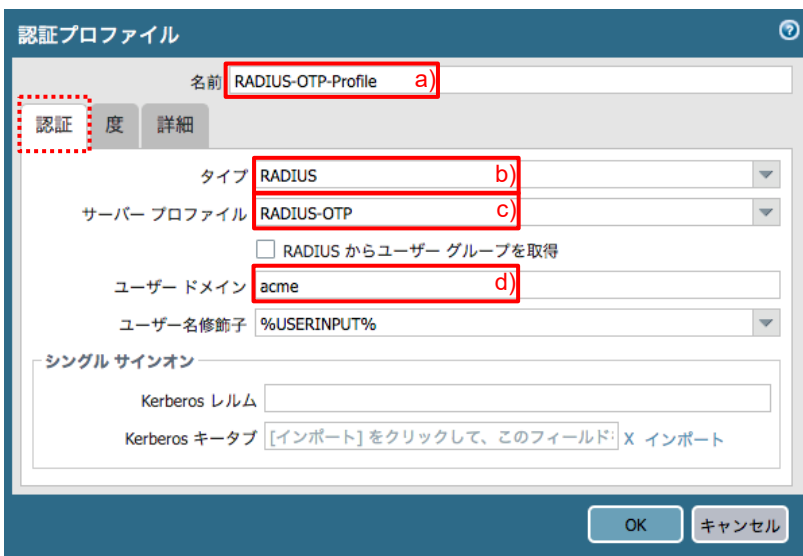
9.3.3. 認証プロファイルの設定

認証プロファイルを設定して、GlobalProtect Portal および Gateway が、OTP サーバー(=RADIUS サーバー)をユーザー認証サーバーとして利用できるようにします。

(1) a)「Device」 → b)「認証プロファイル」 → c)「追加」をクリックします。



(2) a)名前に「Auth-Profile01(任意)」を入力します。
「認証」タブで、
b)タイプは「RADIUS」を選択します。
c)サーバープロファイルは設定済みの「RADIUS-OTP」を選択します。
d)ドメインに「acme」と入力します。



- (3) a)「詳細」タブ → 許可リストの b)「追加」をクリックします。
c)グループマッピングの「許可リストのグループ化」で指定したグループ「domain users」を選択します。
d)「OK」をクリックします。



9.3.4. External Gateway の認証設定の変更

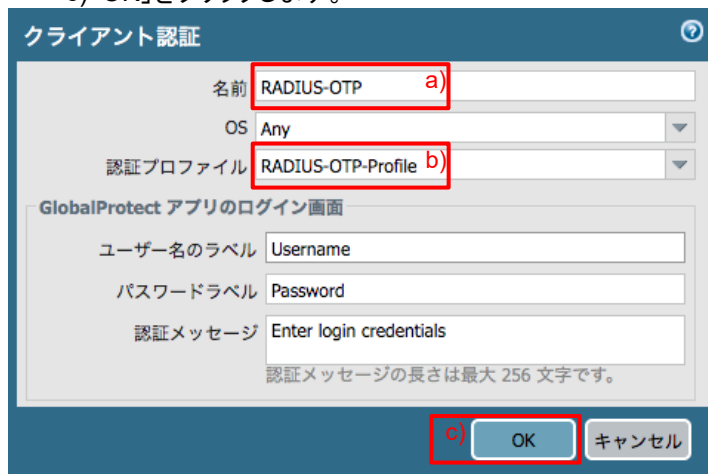
インターネットからのリモートアクセス VPN の場合だけ、ワンタイムパスワード認証を強制し、社内 LAN では、Active Directory 認証のまま利用する、という形態を想定します。

よって、Portal および Internal Gateway に変更は加えず、External Gateway のみ設定変更します。

- (1) 「Network」タブ → GlobalProtect の下の「ゲートウェイ」 → 設定済みの「External-Gateway」をクリックします。
 - a)「認証」タブ → b)設定済みの「ADAuth」をクリックします。



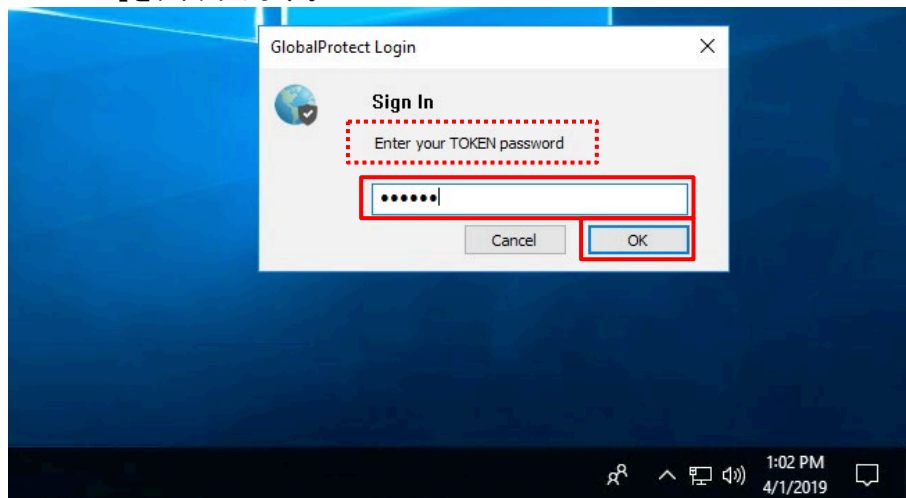
- (2) a)名前に「RADIUS-OTP(任意)」と入力し、b)認証プロファイルは設定済みの「RADIUS-OTP-Profile」を選択します。
 - a)「OK」をクリックします。



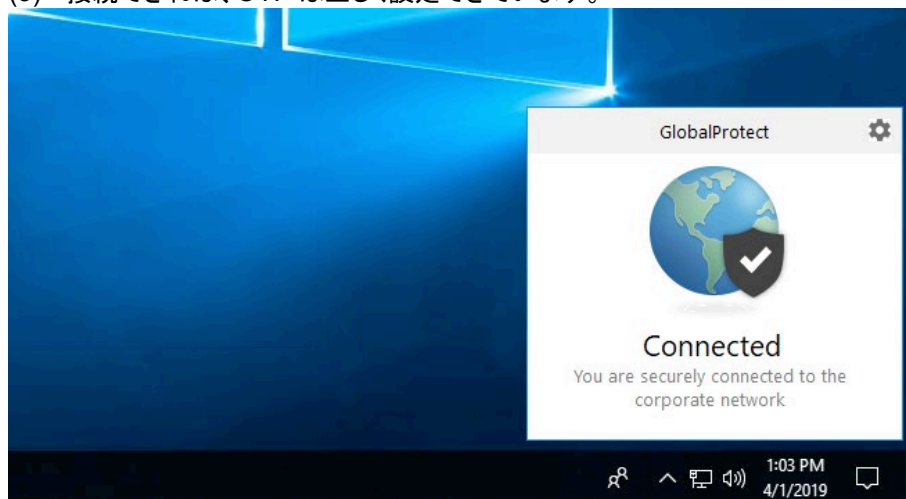
- (3) 「コミット」を実施します。

9.4. GP Agent からのアクセス

- (1) OTP 登録したユーザー名を持つクライアント PC から GP Agent で再アクセスします。
- (2) 以下のように、「Enter your TOKEN password」メッセージが出るので、Google Authenticator の OTP を入力し、「OK」をクリックします。



- (3) 接続できれば、OTP は正しく設定できています。



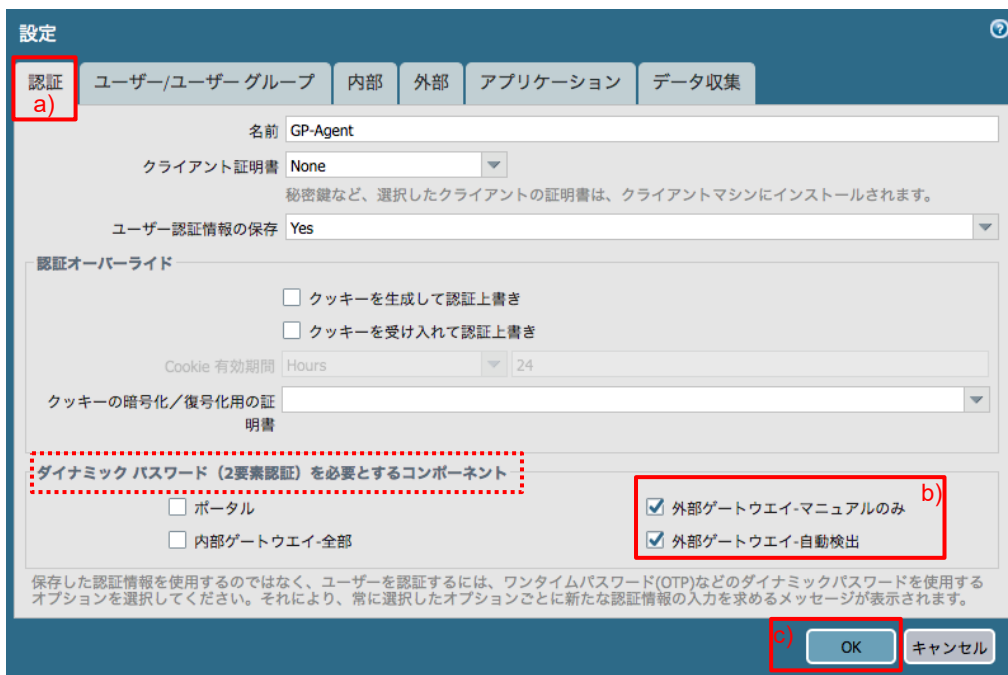
9.5. 外部からの接続はパスワードと OTP 両方の入力を強制する設定

例えば、以下のような要件があるとします。

- インターネットからの VPN 接続時の認証は、認証強化の目的で、OTP だけでなくパスワードも入力させたい。
- 逆に社内 LAN では、何も入力することなく、自動的に接続させたい。

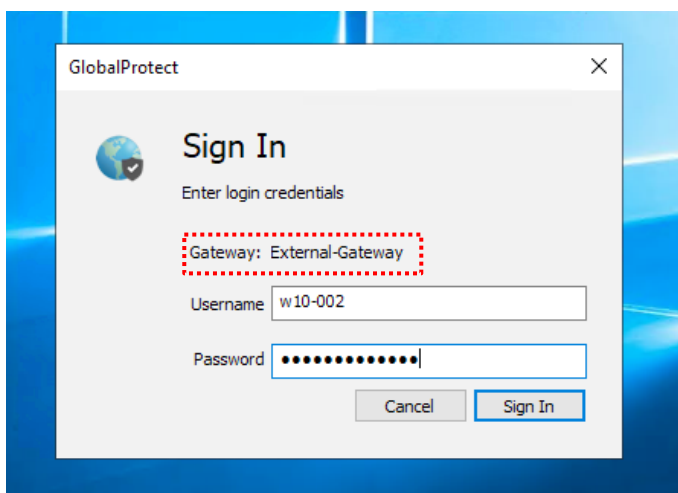
この要件は、Portal の設定で実現できます。

- (1) 「Network」タブ → GlobalProtect の下の「Portal」 → 設定済みの「Portal」をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブを開きます。
「ダイナミック パスワード (2 要素認証) を必要とするコンポーネント」の下の b)「外部ゲートウェイ」で始まる 2 つにチェックを入れます。c)「OK」をクリックします。



- (2) 「コミット」を実施します。

- (3) 外部のクライアント PC(例: w10-002)からアクセスすると、以下のように、External-Gateway が、パスワードの入力を求めてくるようになります。(この後、OTP(TOKEN)の入力を要求する画面に遷移します。)



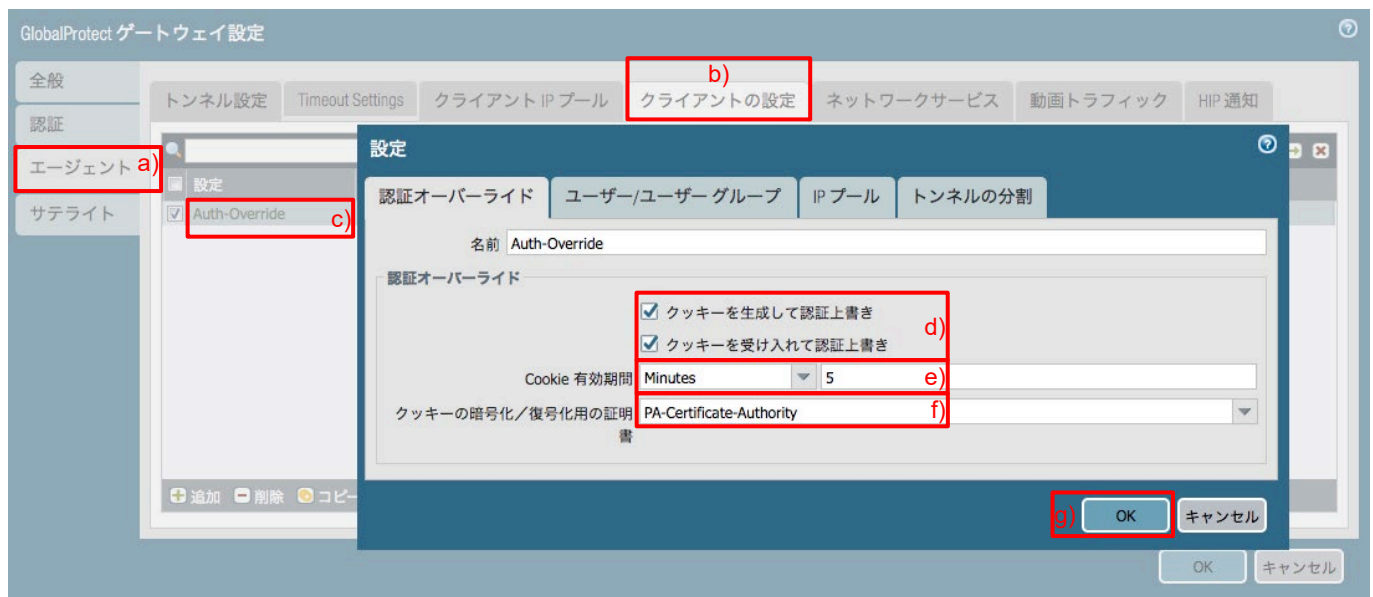
- (4) 内部のクライアント(例: w10-001)では、いままで通り、認証情報の入力を要求されることなく Internal-Gateway に接続できます。

9.6. VPN の再接続時に一定時間は OTP の再入力を必要としない設定

例えば、突然のクライアント PC の停止やサスペンドモードなどによって、一時的に VPN 接続が切断されて、再接続する場合に、その都度 OTP を入力するのは不便だと感じる場合があります。

それを回避するために、「一度 OTP 認証が成功したクライアント PC は、一定時間は再認証を必要としない」とする設定が可能です。

- (1) 「Network」タブ → GlobalProtect の下の「ゲートウェイ」 → 設定済みの「External-Gateway」をクリックします。
 - a) 「エージェント」タブ → b) 「クライアントの設定」タブ → c) 設定済みの「Auth-Override」をクリックします。
 - d) 「クッキーを生成して認証上書き」と「クッキーを受け入れて認証上書き」の両方にチェックを入れます。
 - e) Cookie 有効期間は、検証用に 5 分に設定します。
 - f) PA Firewall で生成した証明書の一つ(ここでは PA-Certificate-Authority)を選択します。
 - g) 「OK」をクリックします。



このことで、一度 External-Gateway で認証が成功すると、External-Gateway が GP Agent に対して 5 分間有効な Cookie を渡します。

5 分以内に再認証が行われた場合には、GP Agent はその Cookie を External-Gateway に渡すことで、認証を免除される、という仕組みです。

- (2) 認証が成功したクライアント PC から、5 分以内に再認証を実施します。
「パスワードの入力を要求されない」ことを確認します。
- (3) 認証が成功したクライアント PC から、5 分経過後に再認証を実施します。
「パスワードの入力を要求される」ことを確認します。

(実環境では 5 分は短すぎるので、デフォルトの 24 時間または適切と思われる時間を設定してください。)

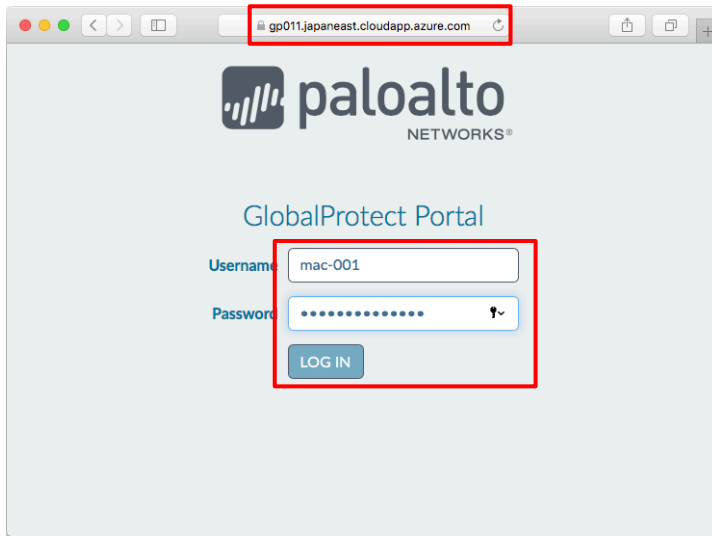
10. macOS からの接続

macOS の GP Agent から VPN 接続を行う場合のステップを記載します。
Windows との動作の差は、ほぼありません。

- ユーザー名: mac-001
- グループ: Domain Users, Newly-Hired (SCEP でのクライアント証明書配布用)
- WebADM で OTP 登録済み

10.1. GP Agent (v4.1.10) のダウンロードとインストール

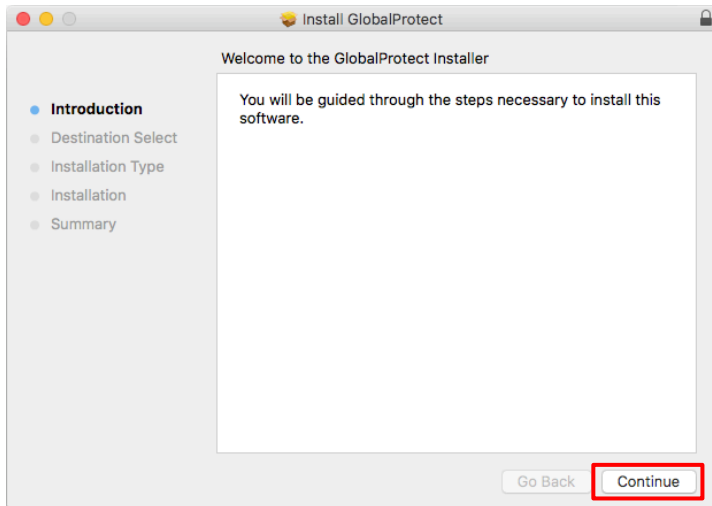
(1) Web ブラウザで GP Portal:「gp011.japaneast.cloudapp.azure.com」へ HTTPS でアクセスし、ログインします。



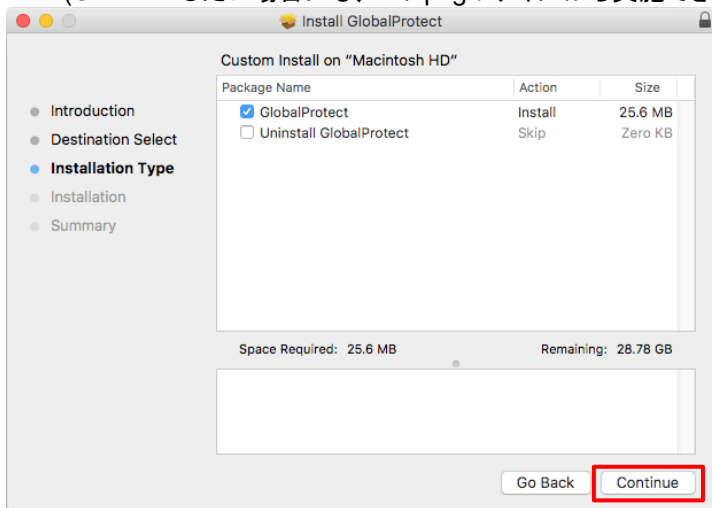
(2) Mac 用の GP Agent をクリックすると、ダウンロードが始まります。



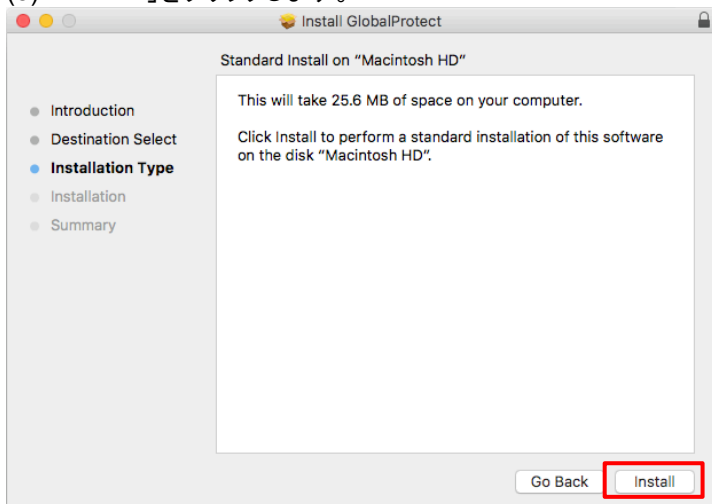
- (3) ダウンロードした GlobalProtect.pkg ファイルを展開すると、インストールが始まります。「Continue」をクリックします。



- (4) 「Continue」をクリックします。
(Uninstall したい場合にも、この pkg ファイルから実施できます。)



- (5) 「Install」をクリックします。



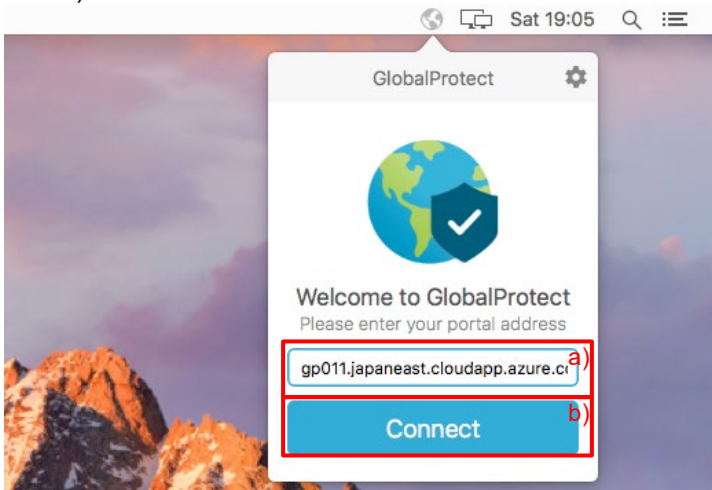
- (6) ここで、インストール権限を持つユーザーのパスワード入力を求められます。その後、インストールが開始されます。

10.2. Portal & Gateway へのアクセス

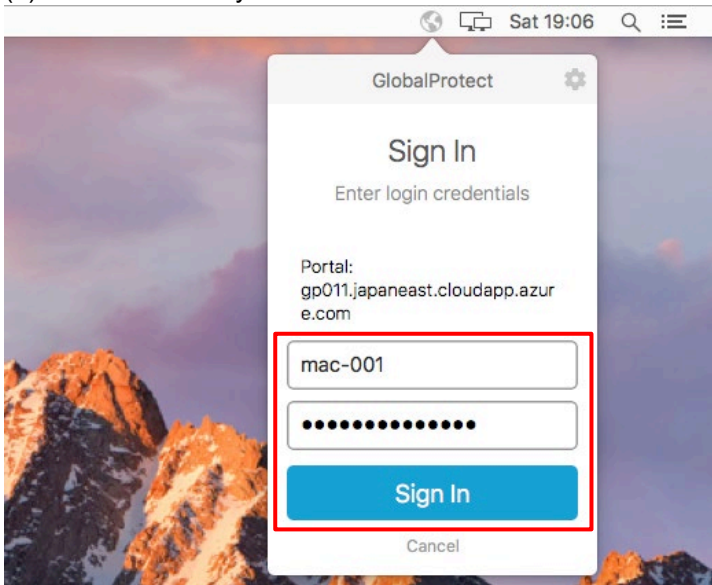
10.2.1. External Gateway へのログイン

インターネット上の macOS から接続する例です。

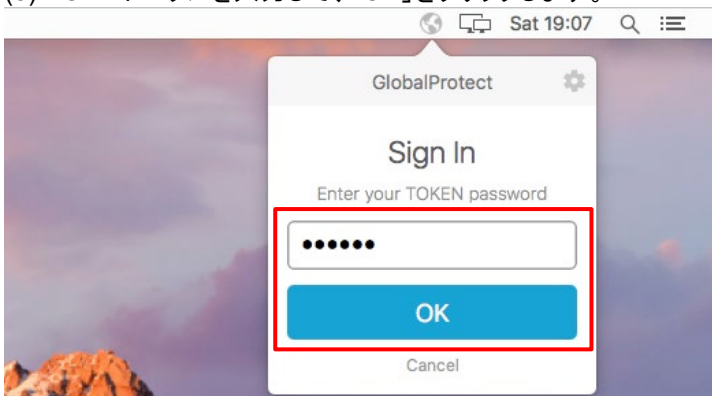
- (1) 表示された以下の GP Agent の画面で、a) Portal の FQDN:「gp011.japaneast.cloudapp.azure.com」を入力します。
b) 「Connect」をクリックします。



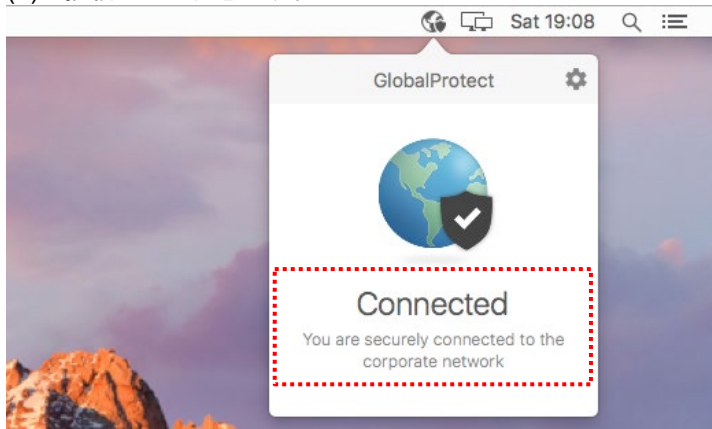
- (2) Active Directory に登録されているユーザー名とパスワードを入力し「Sign In」をクリックします。



- (3) OTP トークンを入力して、「OK」をクリックします。



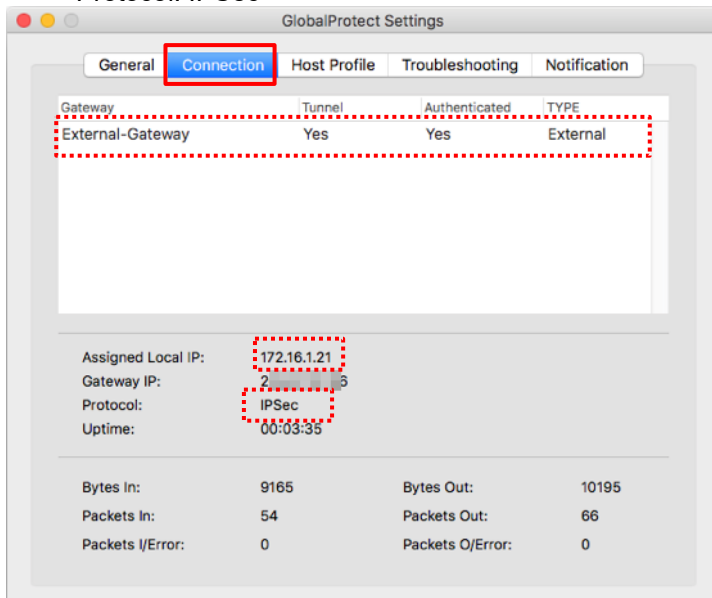
(4) 接続された状態です。



(5) [確認のみ]GP Agent の右上にある  をクリックして、「Settings」を選択します。

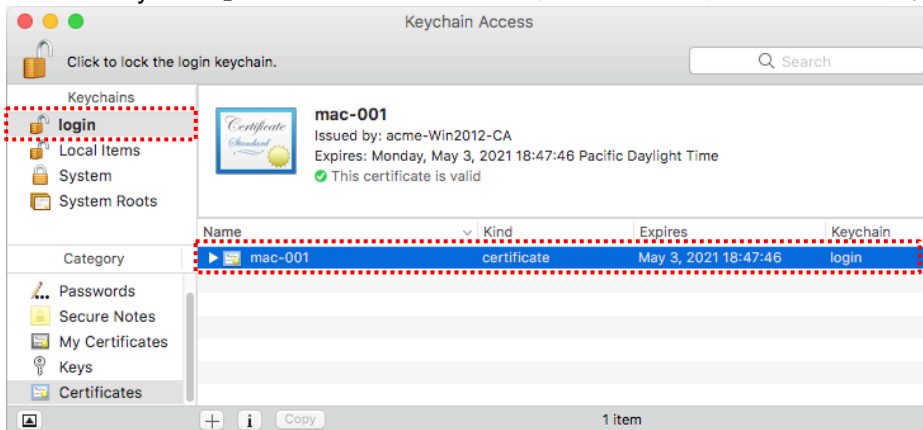
「Connection」タブをクリックして、以下の状態を確認します。

- External-Gateway で、Tunnel が Yes
- Assigned local IP: 172.16.1.x (Pool 設定した IP アドレス)
- Protocol: IPSec

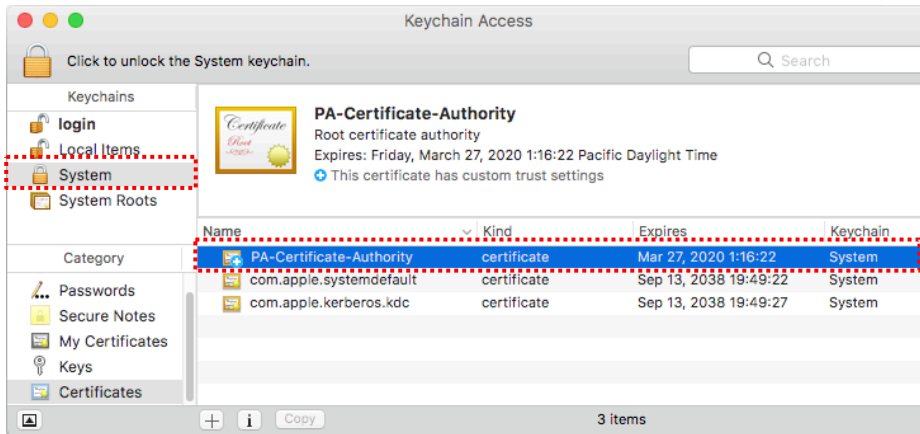


(6) macOS のキーチェーンアクセスを開きます。

「Newly-Hired」グループのメンバーなので、このユーザー個別のクライアント証明書が発行されています。



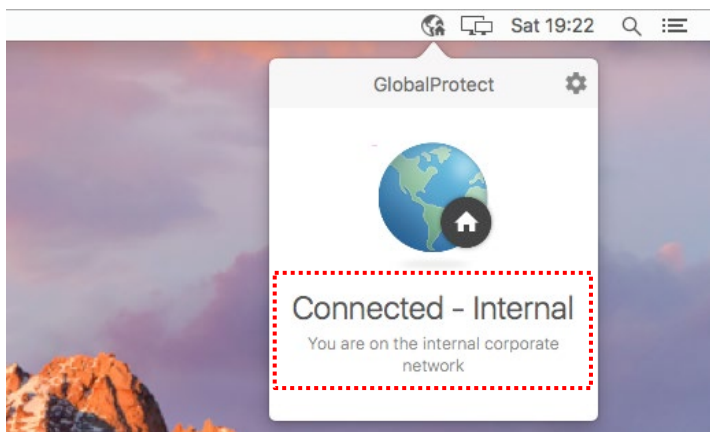
(7) Portal に設定したルート証明書も発行されています。



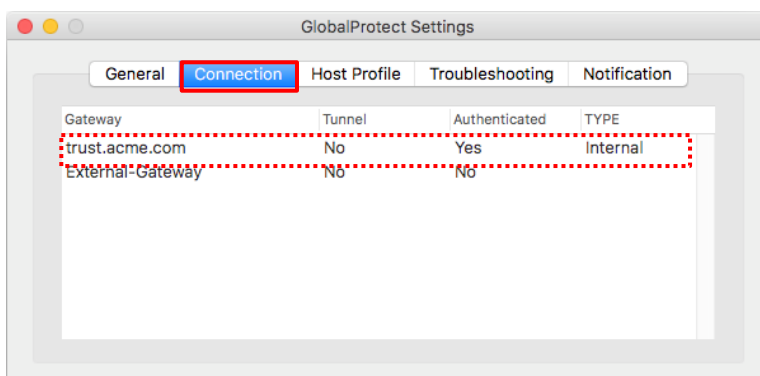
10.2.2. Internal Gateway へのログイン

社内 LAN の macOS から接続する例です。

(1) 最初に Portal へログインする際に、Username と Password を入力したので、社内 LAN での接続では、Username と Password を入力することなく、自動的に接続されます。



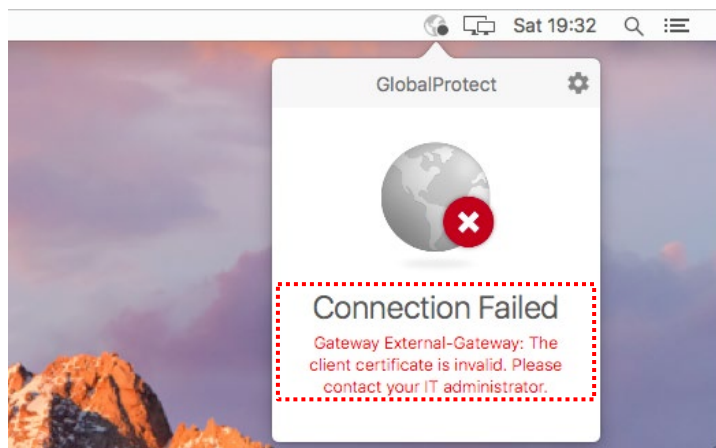
(2) 「Connection」タブをクリックして、Internal-Gateway である「trust.acme.com」の Authenticated が「Yes」であることを確認します。



10.3. クライアント証明書の失効

macOS のクライアント証明書を失効させた場合の挙動です。

- (1) ユーザー:mac-001 を「Newly-Hired」グループから外し、ADCS でクライアント証明書を失効させます。
- (2) GP Agent から再接続すると、接続に失敗し、クライアント証明書が無効であることを示すメッセージが出力されます。



※ macOS の場合、クライアント証明書を削除して、認証が拒否される動作を確認するのが難しいです。
macOS の場合、キーチェーンアクセスからクライアント証明書を削除しても、GP Agent (v4.1.10) が、自身のキャッシュからクライアント証明書を復活させる動作となることを確認しました。
(削除前のシリアル番号と、削除後に復活するクライアント証明書のシリアル番号が同じになっているはずです。)

この点は、Windows GP agent とは異なる点です。

11. User-ID でアクセス制御

ここまでの GlobalProtect 設定によって、外部からはもちろんのこと、内部でもユーザー識別が行われる状態になっています。

ここでは、このユーザー識別された情報を使って、アクセス制御する方法を記載します。

11.1. ユーザー名でアクセス制御

個々のユーザー単位で、セキュリティポリシーによるアクセス制御を行う例です。

以下の要件を想定します。

- VPN 接続した全クライアント PC から内部 DNS への到達は、主に PA Firewall 経由でのインターネット接続に必要である。
- 一方で、一部の VPN 接続ユーザーのみ、内部サーバーへ接続させたい。
(あるユーザーを急遽一時的に通過させる必要が出てきた場合、など)

(1) VPN から内部 DNS へ到達するためのセキュリティポリシーを追加します。

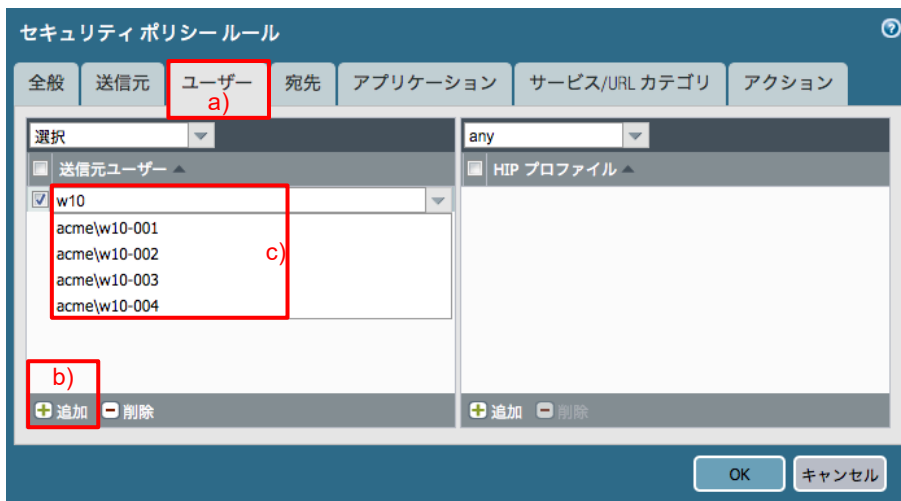
「Policies」タブ → 「セキュリティ」で表示されたセキュリティポリシーに、「VPN-to-Trust-DNS」の行を「VPN-to-Trust」の上に追加します。

名前	タグ	タイプ	送信元					宛先		アプリケーション	サービス	アクション
			ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス				
1 outbound	none	universal	Corp-VPN Trust	any	any	any	Untrust	any	any	any	許可	
2 VPN-to-Trust-DNS	none	universal	Corp-VPN Trust	any	any	any	Trust	any	dns	application-default	許可	
3 VPN-to-Trust	none	universal	Corp-VPN Trust	any	any	any	Trust	any	any	any	許可	
4 RDP	none	universal	Untrust JP	any	any	any	Trust	any	ms-rdp	any	許可	
5 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	許可	
6 interzone-default	none	interzone	any	any	any	any	any	any	any	any	拒否	

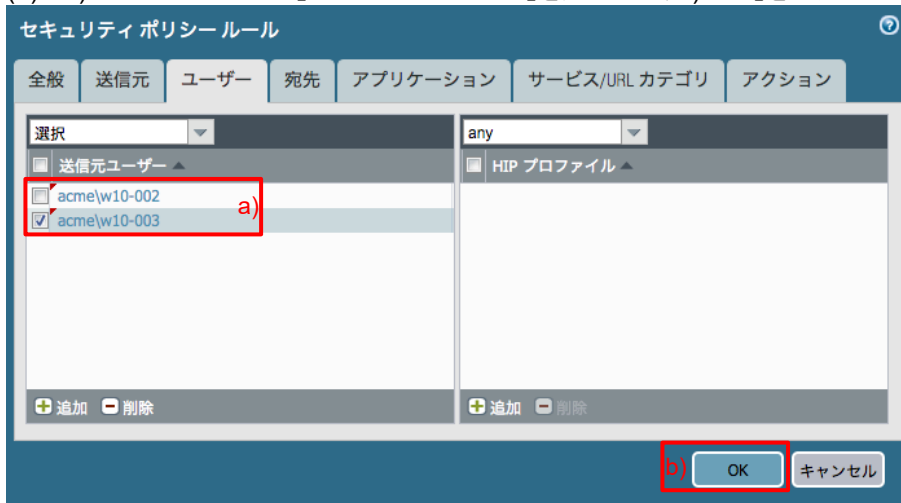
(2) 「VPN-to-Trust」ポリシーへ、「w10-002」と「w10-003」だけ、内部サーバーに到達させる設定を行います。

「VPN-to-Trust」をクリックします。

a)「ユーザー」タブ → b)「追加」をクリック → c)「送信元ユーザー」で、例えば「w10」と入力すると、その文字を持つユーザーの一覧が表示されます。



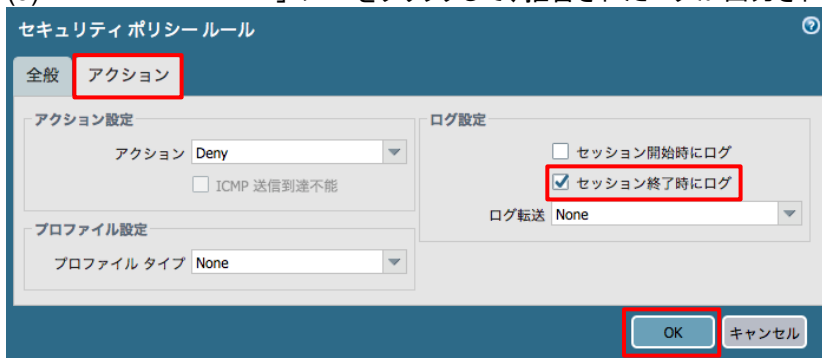
(3) a) 「acme¥w10-002」と「acme¥w10-003」を追加して、b)「OK」をクリックします。



(4) 「VPN-to-Trust」のセキュリティポリシーの「ユーザー」列に2つのユーザーが追加された状態です。

名前	タグ	タイプ	ゾーン	送信元			宛先		アプリケーション	サービス	アクション	
				アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス				
1	outbound	none	universal	Corp-VPN Trust	any	any	any	Untrust	any	any	許可	
2	VPN-to-Trust-DNS	none	universal	Corp-VPN	any	any	any	Trust	any	dns	application-default	許可
3	VPN-to-Trust	none	universal	Corp-VPN	any	acme¥w10-002 acme¥w10-003	any	Trust	any	any	any	許可
5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	許可
6	interzone-default	none	interzone	any	any	any	any	any	any	any	any	拒否

(5) 「interzone-default」の をクリックして、拒否されたログが出力されるようにしておきます。



(6) 「コミット」を実施します。

(7) 外部の w10-002, w10-003 は Win2012 の IIS 「<http://win2012.acme.com>」に到達できませんが、w10-004 は到達できないことを確認します。
(Web ブラウザのキャッシュが表示される場合があるので、ブラウザのリロードボタンで確認してください。)

(8) 「Monitor」タブ → 「トラフィック」で、w10-002, w10-003 は allow、w10-004 は deny であることを確認します。

	受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	宛先ポート	IP プロトコル	アプリケーション	アクション	ルール	セッション終了理由
	04/29 20:00:00	drop	Corp-VPN	Trust	172.16.1.8	acme¥w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/29 19:59:59	drop	Corp-VPN	Trust	172.16.1.8	acme¥w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/29 19:59:59	drop	Corp-VPN	Trust	172.16.1.8	acme¥w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/29 19:59:54	drop	Corp-VPN	Trust	172.16.1.8	acme¥w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/29 19:59:54	drop	Corp-VPN	Trust	172.16.1.8	acme¥w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/29 19:59:54	drop	Corp-VPN	Trust	172.16.1.8	acme¥w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/29 19:59:51	drop	Corp-VPN	Trust	172.16.1.8	acme¥w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/29 19:59:51	drop	Corp-VPN	Trust	172.16.1.8	acme¥w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/29 19:59:51	drop	Corp-VPN	Trust	172.16.1.8	acme¥w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/29 19:59:51	drop	Corp-VPN	Trust	172.16.1.8	acme¥w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/29 19:59:27	end	Corp-VPN	Trust	172.16.1.12	acme¥w10-002	10.9.2.5	80	tcp	web-browsing	allow	VPN-to-Trust	tcp-rst-from-server
	04/29 19:59:22	end	Corp-VPN	Trust	172.16.1.6	acme¥w10-003	10.9.2.5	80	tcp	web-browsing	allow	VPN-to-Trust	tcp-rst-from-server

11.2. グループでアクセス制御

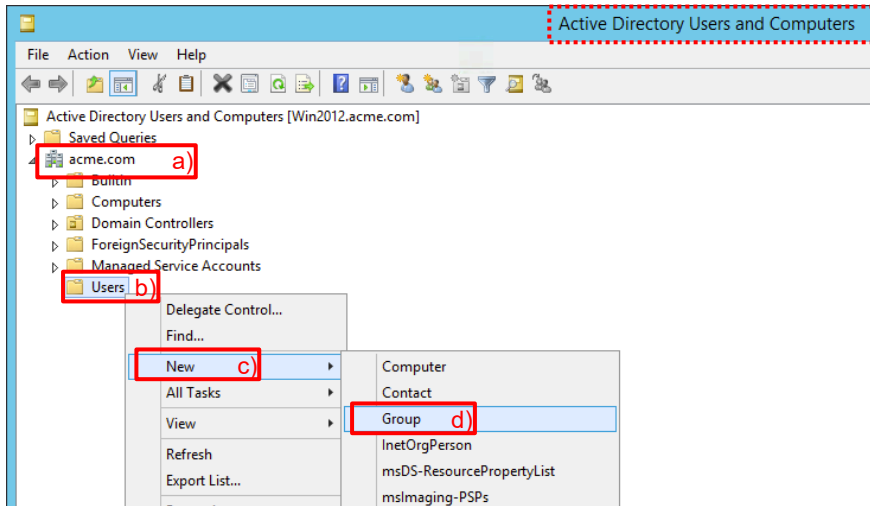
ユーザ名ではなく、グループ名でのアクセス制御も可能です。

こちらの方が、最初に PA Firewall を設定しておけば、あとは Active Directory 側の設定変更で制御できるので、使い勝手は良いと思います。

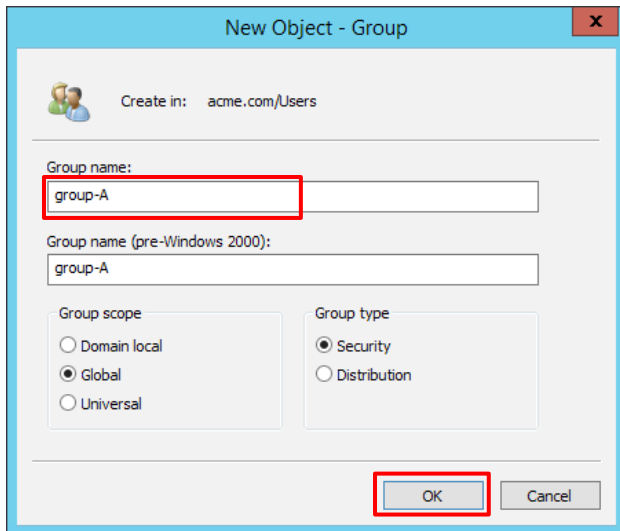
11.2.1. Active Directory の設定

(1) Win2012 の「Administrative Tools」 → 「Active Directory Users and Computers」を開きます。

a)「acme.com」 → b)「Users」を右クリック → c)「New」 → d)「Group」をクリックします。

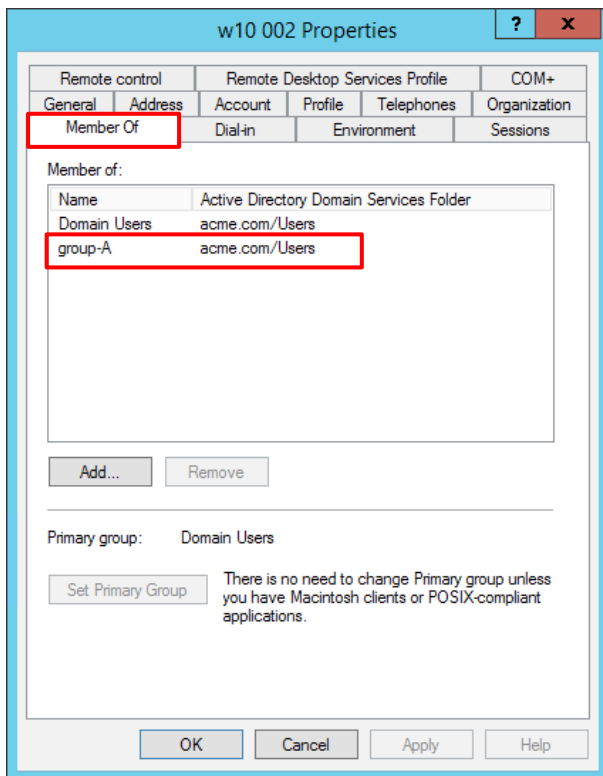


(2) Group Name に「group-A(任意)」と入力し、「OK」をクリックします。



(3) 同様に、「group-B(任意)」も設定します。

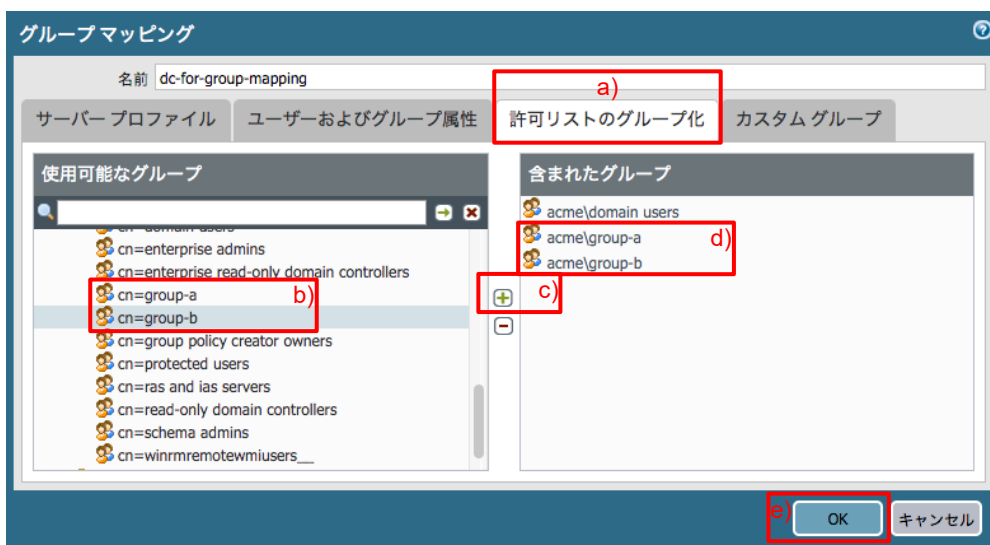
- (4) ユーザーをグループのメンバーにします。グループ割り当ては以下とします。
 group-A: w10-001, w10-002
 group-B: w10-003, w10-004



11.2.2. PA Firewall の設定

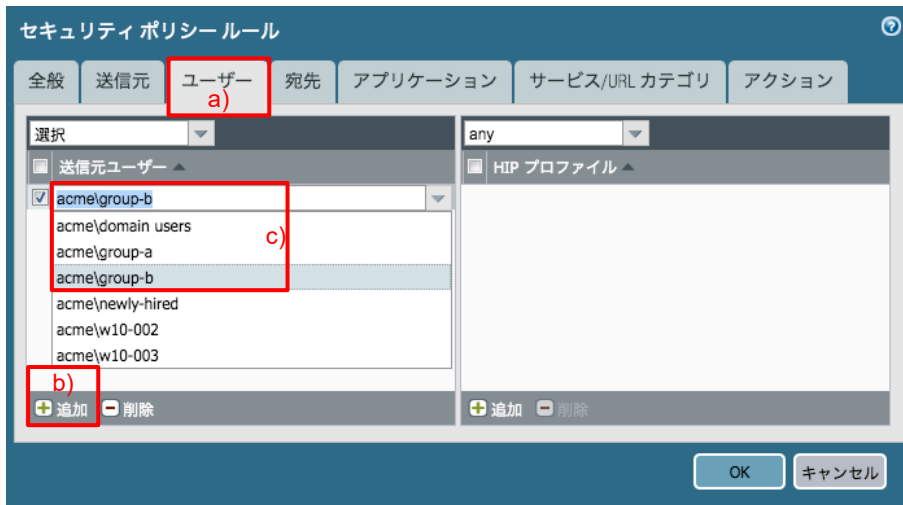
グループマッピングで、「group-A」と「group-B」を追加します。

- (1) PA Firewall の「Device」タブ → 「ユーザーID」 → 「グループマッピング設定」タブで表示された、設定済みの「dc-for-group-mapping」をクリックします。
 a) 「許可リストのグループ化」 → 「DC=acme, DC=com」を展開 → 「cn=users」を展開し、b) 「cn=group-a」を選択 → c) 「+」をクリック、同様に「cn=group-b」も追加して、d) の状態にします。e) 「OK」をクリックします。



- (2) 「コミット」を実施します。

- (3) 「VPN-to-Trust」ポリシーへ、「group-B」だけ、内部サーバーに到達させる設定を行います。
「VPN-to-Trust」をクリックします。
a)「ユーザー」タブ → b)「追加」をクリック → c)「送信元ユーザー」で「acme\group-b」のみを追加します。
(前項で設定したユーザーは削除してください。)



- (4) 「VPN-to-Trust」のセキュリティポリシーの「ユーザー」列に「group-b」だけが追加された状態です。

名前	タグ	タイプ	送信元				宛先		アプリケーション	サービス	アクション
			ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス			
1 outbound	none	universal	Corp-VPN Trust	any	any	any	Untrust	any	any	any	許可
2 VPN-to-Trust-DNS	none	universal	Corp-VPN	any	any	any	Trust	any	dns	application-default	許可
3 VPN-to-Trust	none	universal	Corp-VPN	any	acme\group-b	any	Trust	any	any	any	許可
5 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	許可
6 interzone-default	none	interzone	any	any	any	any	any	any	any	any	拒否

- (5) 「コミット」を実施します。
- (6) 外部の w10-002~w10-004 のクライアント PC から、Win2012 の IIS 「<http://win2012.acme.com>」にアクセスします。
「group-B」である外部の w10-003, w10-004 は到達できますが、「group-A」の w10-002 は到達できないことを確認します。(Web ブラウザのキャッシュが表示される場合があるので、ブラウザのリロードボタンで確認してください。)
- (7) 「Monitor」タブ → 「トラフィック」で、w10-003, w10-004 は allow、w10-002 は deny であることを確認します。

	受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	宛先ポート	IP プロトコル	アプリケーション	アクション	ルール	セッション終了理由
	04/30 12:05:47	end	Corp-VPN	Trust	172.16.1.6	acme\w10-003	10.9.2.5	80	tcp	web-browsing	allow	VPN-to-Trust	tcp-fin
	04/30 12:05:45	end	Corp-VPN	Trust	172.16.1.8	acme\w10-004	10.9.2.5	80	tcp	web-browsing	allow	VPN-to-Trust	tcp-fin
	04/30 12:05:32	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/30 12:05:32	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/30 12:05:32	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny

- 本ガイドでは、社内 LAN に接続された「group-A」の w10-001 は、Win2012 と同一サブネットに設置しているので、「<http://win2012.acme.com>」にアクセス可能ですが、例えば Win2012 を DMZ ゾーンに設置した場合に、同様の制御を行えば、社内 LAN からの接続においても、ユーザー名またはグループ名によるアクセス制御が可能です。

12. Host Information Profile で制御

Host Information Profile (以降、HIP) を設定することで、端末が持つセキュリティ情報でアクセス制御を行うことができます。一般的に「検疫」と言われる機能です。

例えば、端末の以下のような状態に応じてアクセス制御が可能です。

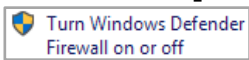
- アンチウイルスソフトウェアがインストールされているか
- パーソナルファイアウォールが動作しているか
- ハードディスクが暗号化されているか

本ガイドでは、比較的簡単に試すことができる、「パーソナルファイアウォールが動作している端末だけ、社内サーバーへアクセスさせる」という設定を行います。

12.1. HIP 検証用の事前設定

w10-002 の Windows10 で、Windows 標準のパーソナルファイアウォールを停止します。

「Control Panel」 → 「System and Security」 → 「Windows Defender Firewall」で表示された画面左側の、



をクリックして、パーソナルファイアウォールを停止します。

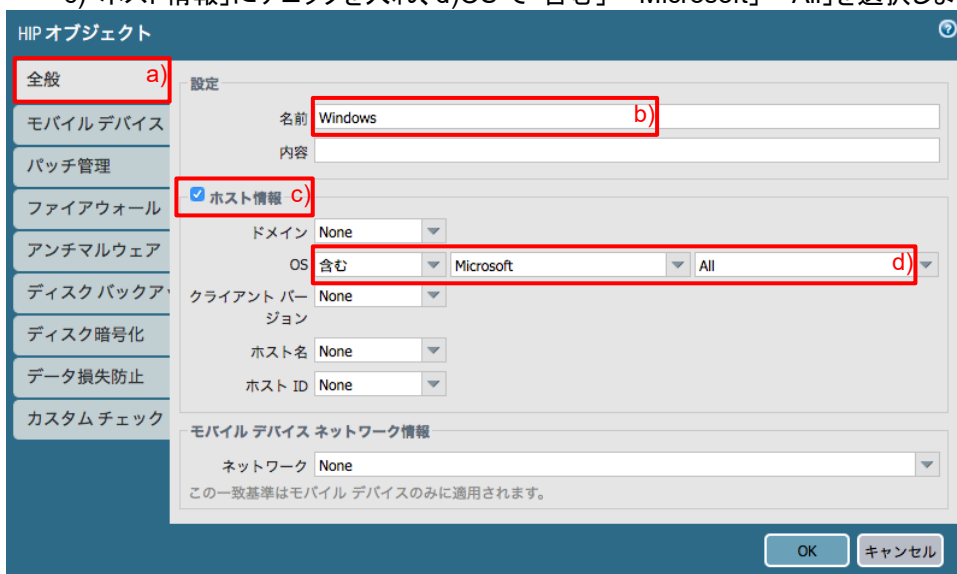
12.2. HIP オブジェクトと HIP プロファイルの設定

(1) a)「Objects」 → b)「HIP オブジェクト」 → c)「追加」 をクリックします。

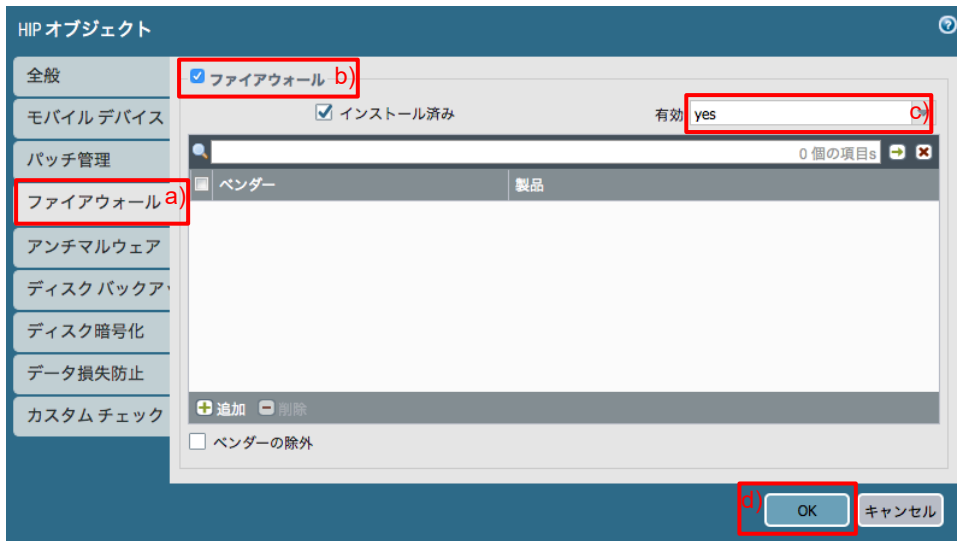


(2) a)「全般」タブで、b)名前に「Windows(任意)」と入力します。

c)「ホスト情報」にチェックを入れ、d)OS で「含む」「Microsoft」「All」を選択します。



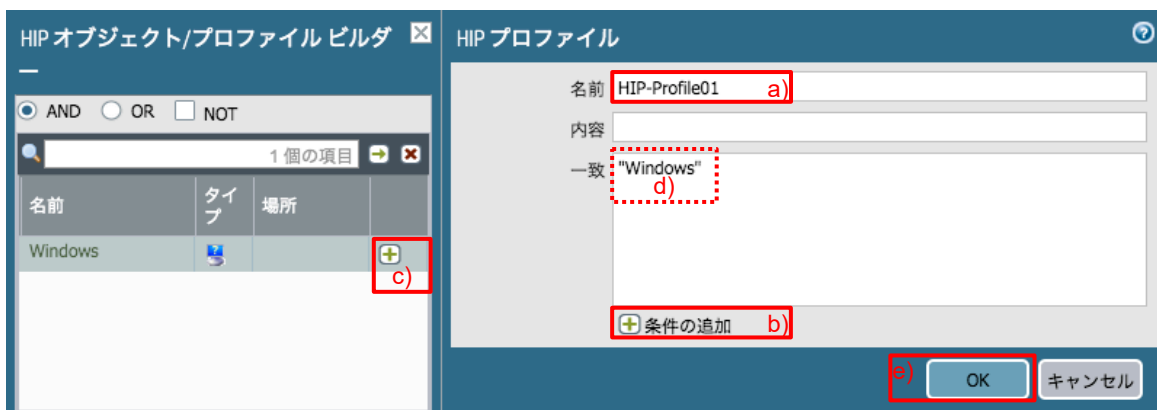
- (3) a)「ファイアウォール」タブで、b)「ファイアウォール」にチェックを入れます。
c)有効で「yes」を選択し、d)「OK」をクリックします。



- (4) a)「Objects」 → b)「HIP プロファイル」 → c)「追加」 をクリックします。



- (5) a)名前に「HIP-Profile01(任意)」と入力します。
b) 「+」条件の追加をクリックして表示された左側のウィンドウの c)「+」 をクリックすると、d)「一致」に「Windows」が加えられます。e)「OK」をクリックします。



- (6) 「コミット」を実施します。

12.3. HIP マッチログの確認

- (1) a)「Monitor」タブ → b)「HIP マッチ」で表示されたログで、c)送信元ユーザー列が「acme¥w10-002」であるログの先頭にある🔍をクリックします。

受信日時	送信元 IPv4	送信元 IPv6	送信元ユーザー	マシン名	オペレーティング システム	HIP	HIP タイプ
04/30 14:49:26	10.9.2.6		acme¥w10-001	WIN10-001	Windows	HIP-Profile01	profile
04/30 14:49:26	10.9.2.6		acme¥w10-001	WIN10-001	Windows	Windows	object
04/30 14:49:06	172.16.1.8		acme¥w10-004	WIN10-004	Windows	HIP-Profile01	profile
04/30 14:49:06	172.16.1.8		acme¥w10-004	WIN10-004	Windows	Windows	object
04/30 14:48:51	172.16.1.6		acme¥w10-003	W10-003	Windows	HIP-Profile01	profile
04/30 14:48:51	172.16.1.6		acme¥w10-003	W10-003	Windows	Windows	object
04/30 14:48:24	172.16.1.12		acme¥w10-002	WIN10-002	Windows	HIP-Profile01	profile
04/30 14:48:24	172.16.1.12		acme¥w10-002	WIN10-002	Windows	Windows	object

- (2) w10-002 が持つ HIP の情報の一覧が表示されます。
Windows Firewall が停止していることを検出しています。

ソフトウェア	ベンダー	バージョン	エンジン	バージョン	定義バージョン	日付	リアルタイム保護	最終スキャン
Windows Defender	Microsoft Corporation	4.18.1807.18075.1.1.15900.4	1.293.496.0	4/30/2019	✓	n/a		

ソフトウェア	ベンダー	バージョン	最終バックアップ
Windows Backup and Restore	Microsoft Corporation	10.0.17763.1	n/a
Windows File History	Microsoft Corporation	10.0.17763.1	n/a

ソフトウェア	ベンダー	バージョン
BitLocker Drive Encryption	Microsoft Corporation	10.0.17763.1

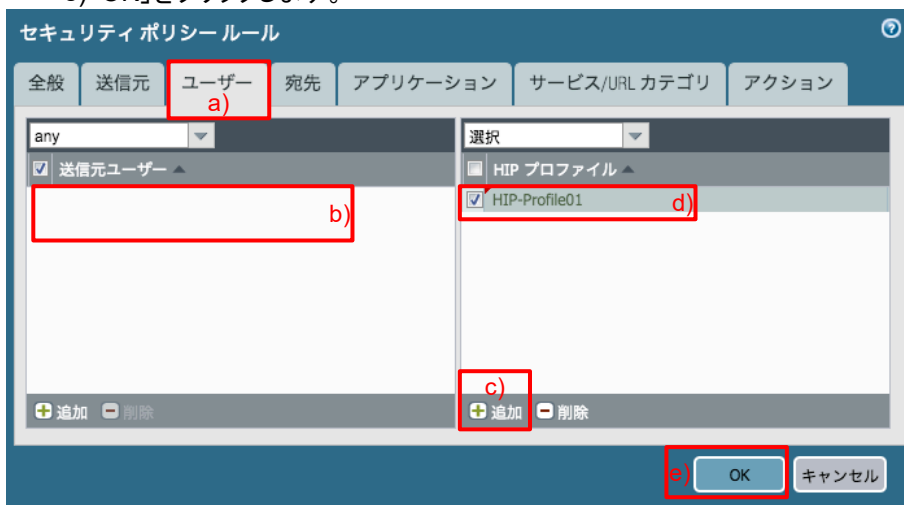
ソフトウェア	ベンダー	バージョン	有効
Windows Firewall	Microsoft Corporation	10.0.17763.1	✗

ソフトウェア	ベンダー	バージョン	有効
Windows Update Agent	Microsoft Corporation	10.0.17763.1	✓

タイトル	KB	項目 ID	重大度
2019-02 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows 10 Version 1809 for x64 (KB4486553)	4486553		✗
Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.293.501.0)	2267602		✗

12.4. セキュリティポリシーの設定

- (1) 「Policies」タブ → 「セキュリティ」で表示されたセキュリティーポリシーの「VPN-to-Trust」をクリックします。
 - a)「ユーザー」タブで、b)「送信元ユーザー」は(残って入れば)全て削除します。
 - c)「追加」をクリックして、d)設定済みの「HIP-Profile01」を選択します。
 - e)「OK」をクリックします。



- (2) 「VPN-to-Trust」の HIP プロファイル列に、「HIP-Profile01」が適用された状態です。

名前	タグ	タイプ	送信元					宛先		アプリケーション	サービス	アクション
			ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス				
1 outbound	none	universal	Corp-VPN	any	any	any	Untrust	any	any	any	許可	
2 VPN-to-Trust-DNS	none	universal	Corp-VPN	any	any	any	Trust	any	dns	application-default	許可	
3 VPN-to-Trust	none	universal	Corp-VPN	any	any	HIP-Profile01	Trust	any	any	any	許可	
5 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	許可	
6 interzone-default	none	interzone	any	any	any	any	any	any	any	any	拒否	

- (3) 「コミット」を実施します。

12.5. 動作確認

- (1) 外部の w10-002~w10-004 のクライアント PC から、Win2012 の IIS 「<http://win2012.acme.com>」にアクセスします。

w10-003 と w10-004 は到達できますが、Windows Firewall が停止している w10-002 は到達できないことを確認します。(Web ブラウザのキャッシュが表示される場合があるので、ブラウザのリロードボタンで確認してください。)

- (2) 「Monitor」タブ → 「トラフィック」で、w10-003, w10-004 は allow、w10-002 は deny であることを確認します。

	受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	宛先ポート	IP プロトコル	アプリケーション	アクション	ルール	セッション終了理由
	04/30 15:37:49	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/30 15:37:49	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/30 15:37:49	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/30 15:37:46	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/30 15:37:46	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/30 15:37:46	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
	04/30 15:37:21	end	Corp-VPN	Trust	172.16.1.6	acme\w10-003	10.9.2.5	80	tcp	web-browsing	allow	VPN-to-Trust	tcp-fin
	04/30 15:37:19	end	Corp-VPN	Trust	172.16.1.8	acme\w10-004	10.9.2.5	80	tcp	web-browsing	allow	VPN-to-Trust	tcp-fin

12.6. [参考]各種端末のHIP

参考までに、その他の OS の HIP 情報を記載しておきます。

12.6.1. macOS

ログ詳細			
生成済みレポート	05/04/2019 19:06:36		
ユーザー情報	User: mac-001	IP アドレス: 172.16.1.21	
ホスト情報	マシン名: Takuya's Mac	ドメイン:	
OS	Apple Mac OS X 10.12.6	ホスト ID: 00:0c:29:7f:b4:2d	
クライアント バージョン	4.1.10-4		
ネットワーク情報	インターフェイス	MAC アドレス	IP アドレス
	en0	00:0c:29:7f:b4:2d	192.168.55.146 fe80::1c1f:40ec:22de:750c
アンチマルウェア			
ソフトウェア	ベンダー	バージョン	最終スキャン
Gatekeeper	Apple Inc.	10.12.6	n/a
Disk Backup			
ソフトウェア	ベンダー	バージョン	最終バックアップ
Time Machine	Apple Inc.	1.3	n/a
Disk Encryption			
ソフトウェア	ベンダー	バージョン	
FileVault	Apple Inc.	10.12.6	
ドライブ	状態		
Macintosh HD	unencrypted		
Firewall			
ソフトウェア	ベンダー	バージョン	有効
Mac OS X Builtin Firewall	Apple Inc.	10.12.6	✗
Patch Management			
ソフトウェア	ベンダー	バージョン	有効
Software Update	Apple Inc.	2.2.1	✓
未定義パッチ			
タイトル	KB 項目 ID	重大度	
データ損失防止			
ソフトウェア	ベンダー	バージョン	有効
カスタム チェック			
レジストリ キー			
プロセス			
プロパティ リスト ファイル			

12.6.2. iOS

ログ詳細			
生成済みレポート	04/02/2019 14:27:46		
ユーザー情報	User: ios-001	IP アドレス: 172.16.1.8	
ホスト情報	マシン名: の iPhone	ドメイン:	
OS	Apple iOS 12.2	ホスト ID: 7E0182036A74E0D0F2308B439F3C492	
クライアント バージョン	5.0.4-19		
WiFi SSID	インターフェイス	MAC アドレス	IP アドレス
	pdp_ip0		10.56.137.49 fe80::1826:7796:89f2:c163 2001:268:942a:44a:14a8:918e:8e6d:43cc 2001:268:942a:44a:f44a:71c:f26:54e2
	pdp_ip1		fe80::1087:3994:90:2e 2001:268:b74c:488a:8ae:f9a:8be:ea42 2001:268:b74c:488a:4c81:5edd:3a2:6968
ネットワーク情報	インターフェイス	MAC アドレス	IP アドレス
	en0	02:00:00:00:00:00	fe80::1c35:448a:d942 10.137.120.72
	en1	02:00:00:00:00:00	
	awd0	02:00:00:00:00:00	fe80::983b:7796:5789
	utun1		fe80::115f:e143:15a5
	utun3		fe80::dd0c:39:61ac
	ipsec0		fe80::6e4d:f:897c
	ipsec1		2001:268:b74c:488a:8ae:f9a:8be:ea42 fe80::6e4d:f:897c
	utun2		2001:268:b74c:488a:8ae:f9a:8be:ea42 172.16.1.8
モバイル デバイス			
デバイス状態			
最終チェックイン日時	登録日時	場所	
		, @	
タ			
グ			
デバイスの準拠性			
管理対象 root 化/jailbreak ディスク暗号化が設定されていません パスコードが設定されていません マルウェアあり			
デバイス情報			
デバイス モデル	電話番号	シリアル番号	
IMEI	ICCID	UDID	
		7E0182036A74E0D0F2308B439F3C492	
カスタム チェック			
レジストリ キー			
プロセス			
プロパティ リスト ファイル			

12.6.3. Android

ログ詳細 🔍 🗨️ 🗑️

生成済みレポート	05/02/2019 14:11:21		
ユーザー情報	User: ard-001	IP アドレス: 172.16.1.15	
ホスト情報	マシン名: KYT31-293c715391	ドメイン:	
OS	Google Android 5.1	ホスト ID: 16184518278e32c	
クライアント バージョン	5.0.0-2		
WIFI SSID	66D0DCAD73C5026179F2DF027872892E		
ネットワーク情報	インターフェイス	MAC アドレス	IP アドレス
	wlan0	80:73:9F:AF:60:A9	192.168.0.14 240f:36:e868:1:8273:9fff:feaf:60a9 fe80::8273:9fff:feaf:60a9
	tun0		240f:36:e868:1:343e:7d40:ee63:67a3
	lo		172.16.1.15 ::1

モバイル デバイス

デバイス状態

最終チェックイン日時	登録日時	場所
		, @

タグ

デバイスの準拠性

管理対象	root 化/jailbreak	ディスク暗号化が設定されていません	パスワードが設定されていません	マルウェアあり
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

デバイス情報

デバイス モデル	電話番号	シリアル番号
IMEI	ICCID	UDID

カスタム チェック

レジストリ キー

プロセス

プロパティ リスト ファイル

12.6.4. Linux

ログ詳細 🔍 🗨️ 🗑️

生成済みレポート	03/01/2019 09:33:53		
ユーザー情報	User: ct7-001	IP アドレス: 10.10.2.10	
ホスト情報	マシン名: centos7	ドメイン:	
OS	Linux CentOS 7.6.1810 ホスト ID: CA4248C4-08D3-1147-9843-6EC0CDCD3FC1		
クライアント バージョン	5.0.0-79		
ネットワーク情報	インターフェイス	MAC アドレス	IP アドレス
	eth0	00:0D:3A:51:3B:A3	10.10.2.10 fe80::20d:3aff:fe51:3ba3

カスタム チェック

レジストリ キー

プロセス

プロパティ リスト ファイル

13. スマートデバイスからの接続

スマートフォンとタブレット PC をまとめて「スマートデバイス」と呼ぶことにします。

iOS で接続する場合を例として、スマートデバイスからの接続を確認します。

13.1. SCEP によるクライアント証明書のインポート

13.1.1. 課題

iOS や Android は基本的には、アプリケーションから OS の証明書ストア領域への直接のアクセスができないようになっています。

よって、iOS や Android の GP Agent アプリケーションが GP Portal から SCEP で受け取ったクライアント証明書は、そのアプリ内で一時的にキャッシュされるだけで、スマートデバイス OS の証明書ストアには保存されません。

また、iOS や Android の GP Agent アプリケーションが再度 GP Portal へ接続する際には、アプリ内のキャッシュフォルダを全てクリーンアップしてから接続する仕様になっています。

そのため、「SCEP 利用によるスマートデバイスへのクライアント証明書は、SCEP で配信し続ける」必要があるので、SCEP 利用の場合は事実上、ID&パスワード認証だけの場合と大差ないことになります。

以降、その挙動を確認します。

13.1.2. 正常な動作の確認

ここまでの設定では、ログインアカウントを「Newly-Hired」グループのメンバーにすることで、SCEP によるクライアント証明書の配布が可能になっていますので、アカウントをその状態にします。

- AD ユーザ名: ios-002
- AD グループ: Domain users (デフォルト)
Newly-Hired (SCEP でのクライアント証明書配布用)
- ワンタイムパスワード: WebADM へ登録済み

13.1.2.1. iOS の GP Agent のダウンロード&インストール

App Store へアクセスし、GP Agent をダウンロード&インストールします。



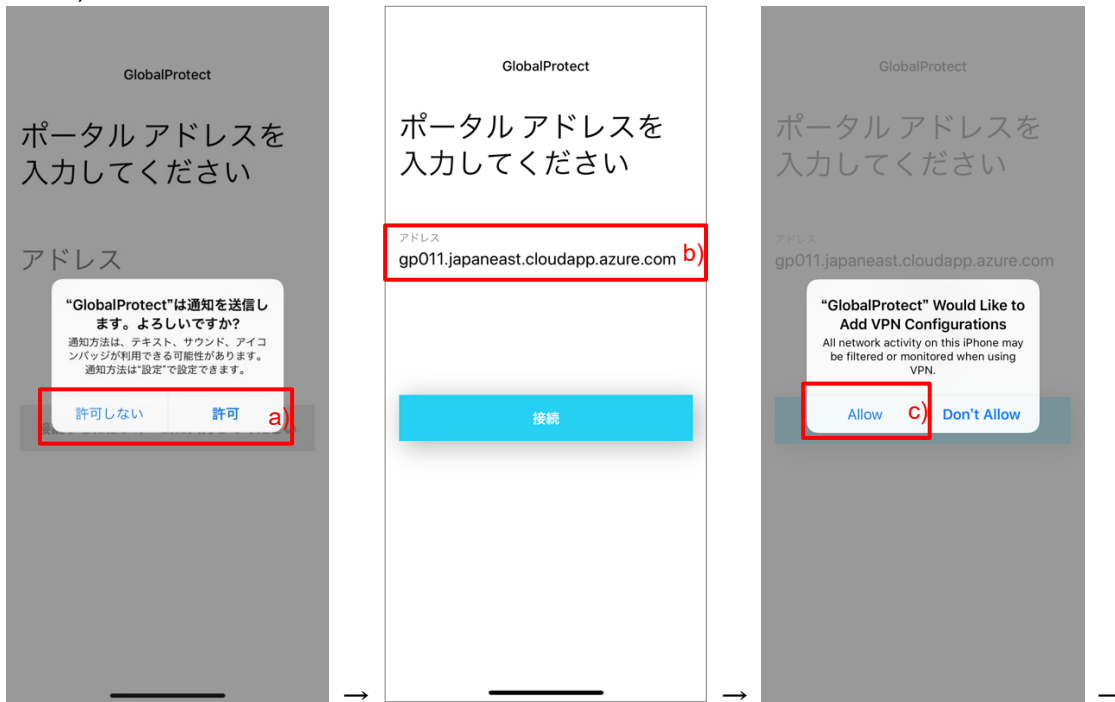
13.1.2.2. External-Gateway へのログイン

(1) 初期設定です。

a) 通知の許可はどちらでも構いません。

b) Portal の宛先:「gp011.japaneast.cloudapp.azure.com」を入力します。

c) iOS の VPN 設定を許可するかどうかを確認されますので、「Allow」をクリックします。



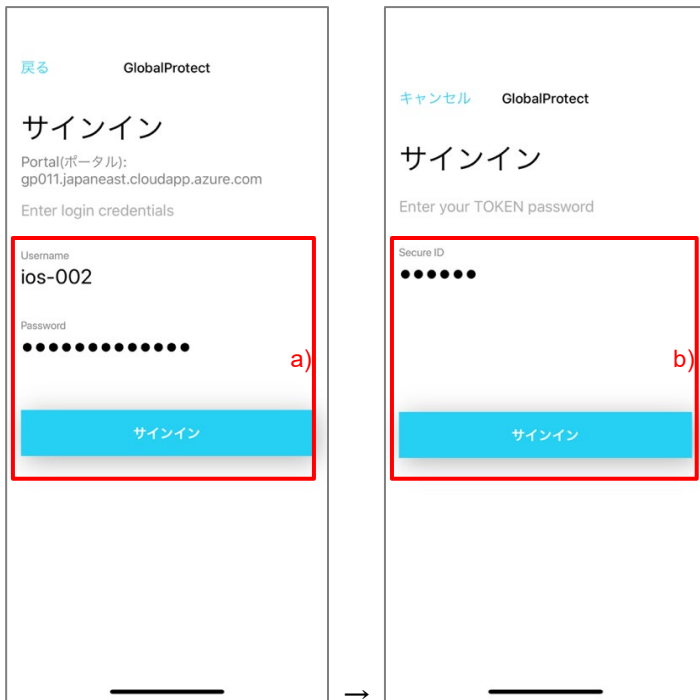
d) パスコードを入力します。

e) 独自サーバー証明書を利用しているので、最初だけは、証明書の警告がでますが「続行」をクリックします。



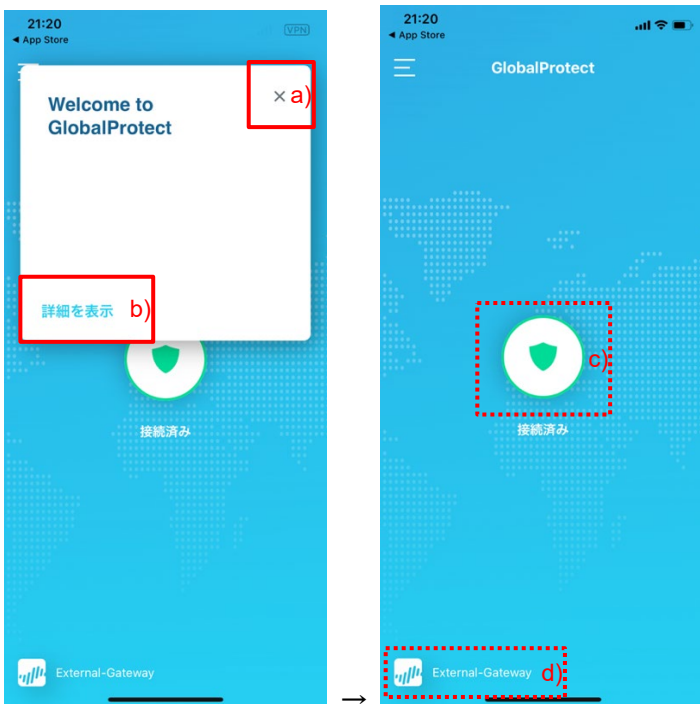
(2) サインインします。

- a) ユーザ名とパスワードを入力し、「サインイン」をクリックします。
- b) ワンタイムパスワードを入力し、「サインイン」をクリックします。



(3) 接続完了です。

- a) の×をクリックして消去するか、b)をクリックして「次回から表示しない」をチェックしてください。
- 外部からの接続が成功した場合には c)盾のマークが表示され、d)External-Gateway と表示されます。



13.1.2.3. [参考]Internal-Gateway へのログイン

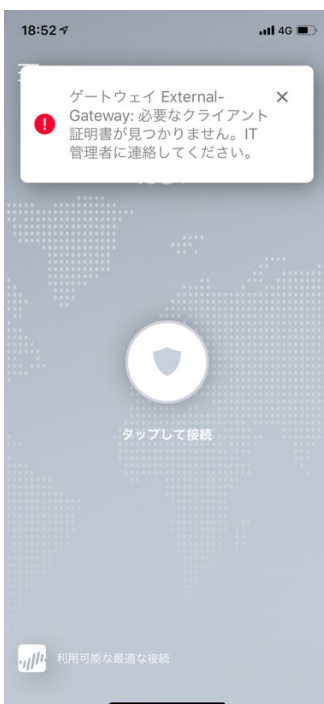
社内 LAN に接続した場合は、ここまでの Portal および Internal Gateway の設定のままであれば自動的に接続され、a)家のマークになり、b)Internal Network と表示されます。



13.1.3. SCEP を無効化した場合の動作の確認

ここまでの設定で、Gateway には証明書プロファイルを設定してクライアント証明書認証を行う状態にしているので、そこに接続できたということは、「iOS にも SCEP によるクライアント証明書の配布はできている」ということになります。

しかし、SCEP を無効にする=ログインアカウントを「Newly-Hired」グループから外すと、接続できなくなります。そのため、スマートデバイスの場合は、SCEP を無効にすることはできない=配信し続ける必要がある、ということです。



13.1.4. スマートデバイスだけに SCEP を常時有効にする

必要最低限の設定だけで、スマートデバイスだけに SCEP でクライアント証明書を配信し続ける方法を記載します。

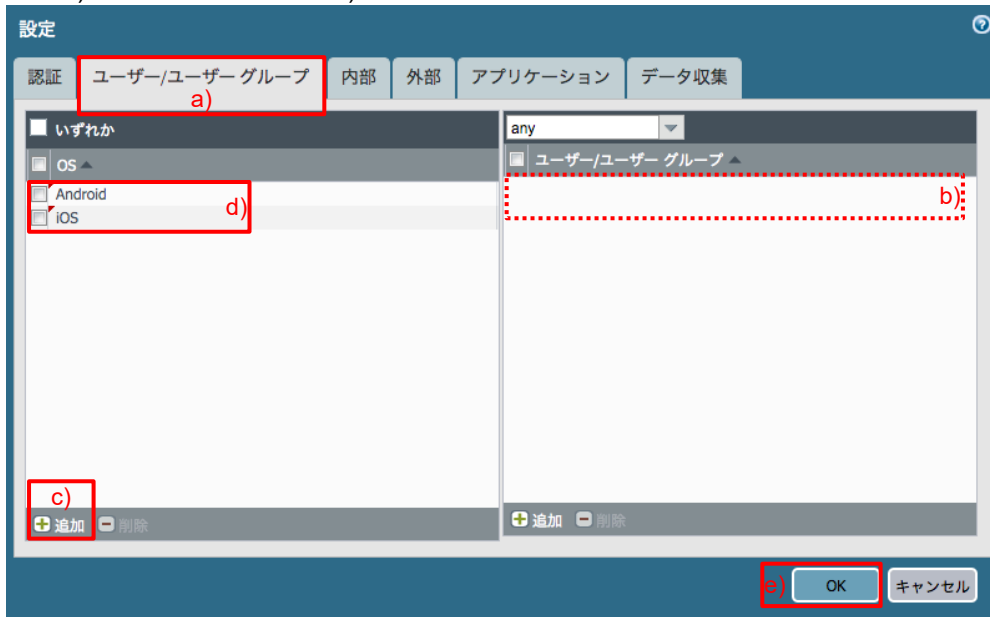
- (1) 「Network」タブ → GlobalProtect の下の「Portal」 → 設定済みの「Portal」をクリック → a)「エージェント」タブ → b)設定済みの「GP-Agent_for_NH」の先頭にチェックを入れ、c)「コピー」をクリックします。



- (2) 「認証」タブで、b)名前を「GP-Agent_for_SD(任意)」に変更します。



- (3) a)「ユーザー/ユーザーグループ」タブで、b) 「ユーザー/ユーザーグループ」を削除します。
c)「追加」をクリックして、d)「Android」と「iOS」を追加します。



- (4) 「GP-Agent_for_SD」の先頭にチェックを入れて、b)「上へ」をクリックして、先頭に移動します。



- (5) 「コミット」を実施します。

13.1.4.2. 接続確認

- (1) AD 上で、ユーザー:「ios-002」が、まだ「Newly-Hired」グループのメンバーの場合は、そのグループを削除します。
(2) ユーザー:「ios-002」で、iOS を使って接続できることを確認します。

13.2. 手動によるクライアント証明書のインポート

一般的に、クライアント証明書認証に期待する動作は以下 2 つです。

- クライアント証明書が失効した端末は接続できない
- クライアント証明書を持っていないデバイスは接続できない

SCEP 利用の場合は既述の通り、スマートデバイスだけでは Portal からクライアント証明書を配布し続ける必要があるの
で、期待する上記 2 つの効果が得られません。

よって上記 2 つの期待値を満たすには、スマートデバイスには SCEP は利用せず、手動でクライアント証明書をインポ
ートする方法を検討する必要があります。

iOS12 の GP Agent 5.0 以降でクライアント証明書を利用するには、「MDM」または「Apple Configurator 2」を使ってイン
ポートする必要があります。

(以下、参考 URL)

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000boSUCAY>

本ガイドでは、無償で使える「Apple Configurator 2」を使って、iOS へインポートするステップを示します。

13.2.1. Certification Authority Web Enrollment のインストール

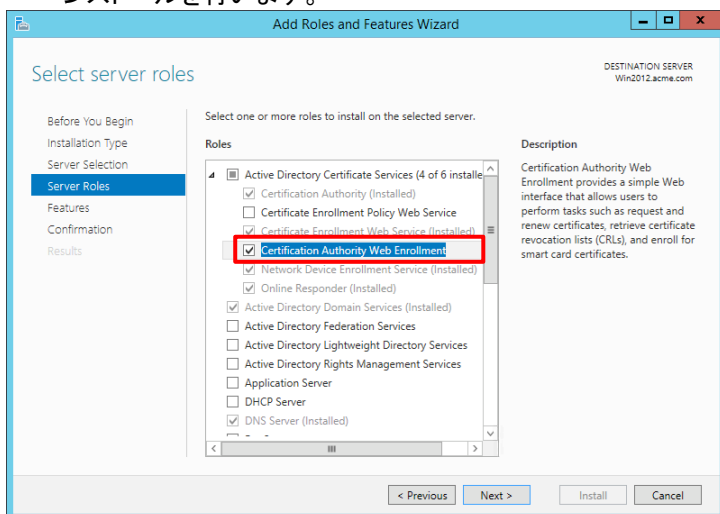
クライアント証明書と秘密鍵をセットで出力する PKCS#12 形式のクライアント証明書ファイルが生成できるようにするに
は、Win2012 の Certification Authority Web Enrollment を有効にする必要があります。

(本ガイドでは、既に CA のインストール時に同時にインストール済みですが、念のため、以下にステップを記載します。)

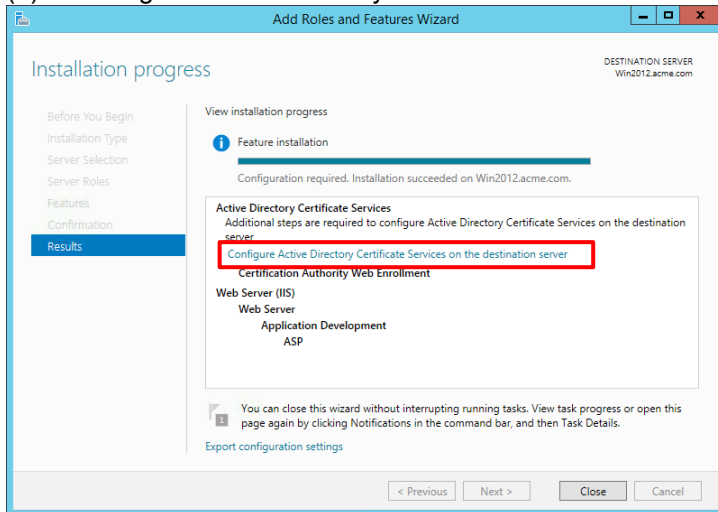
(1) Win2012 の Server Manager で、「Add roles and features」をクリックします。

(2) 以下の画面までは「Next」をクリックして進めます。

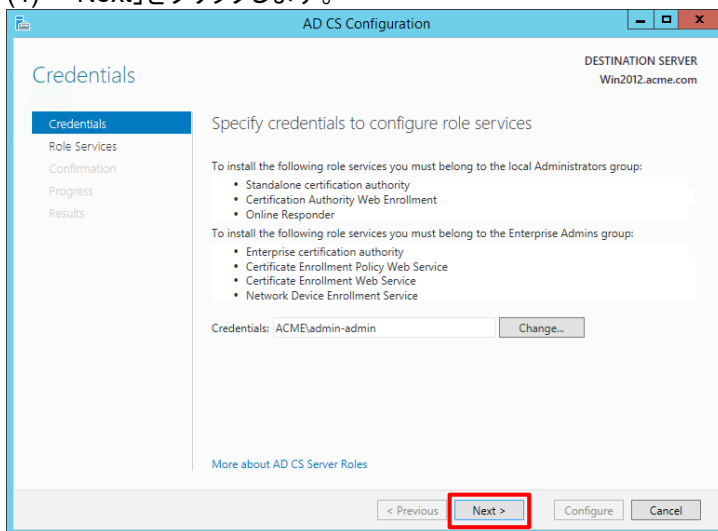
以下の画面で、「Active Directory Certificate Services」の下の「Certification Authority Web Enrollment」を選択してイ
ンストールを行います。



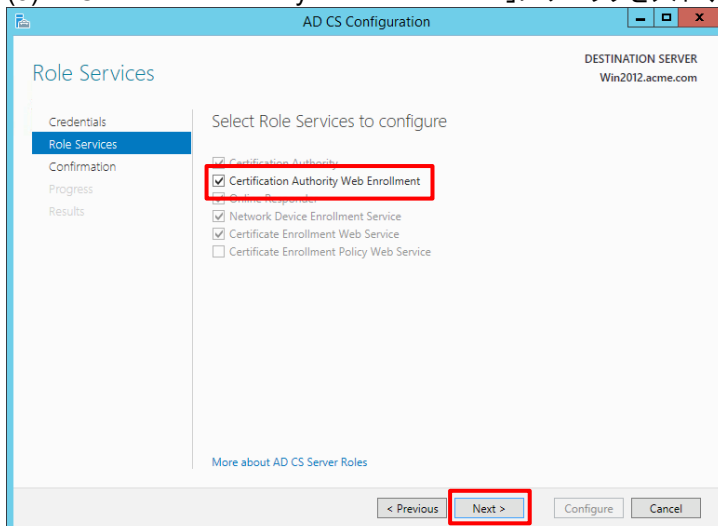
(3) 「Configure Active Directory Certificate Services on the destination server」をクリックします。



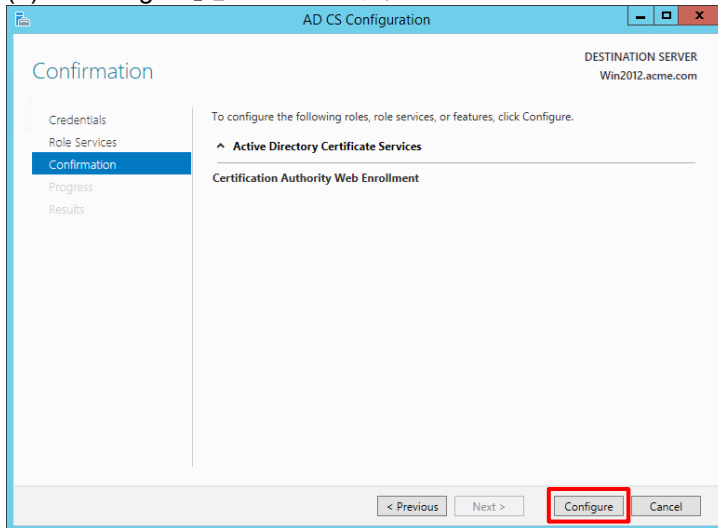
(4) 「Next」をクリックします。



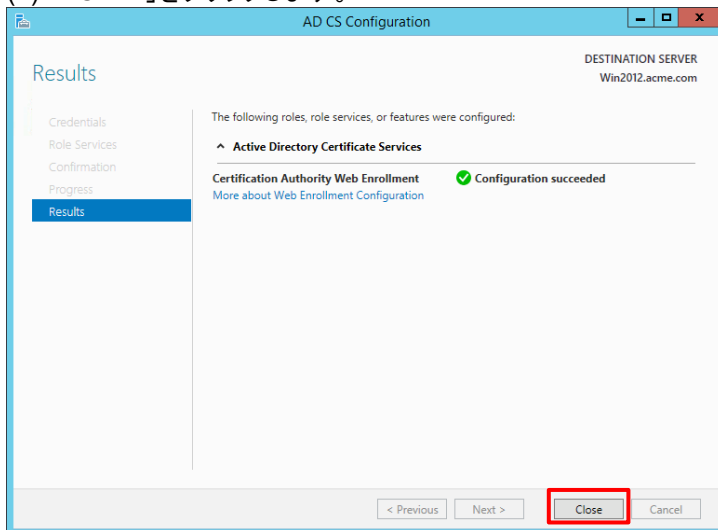
(5) 「Certificate Authority Web Enrollment」にチェックを入れ、「Next」をクリックします。



(6) 「Configure」をクリックします。

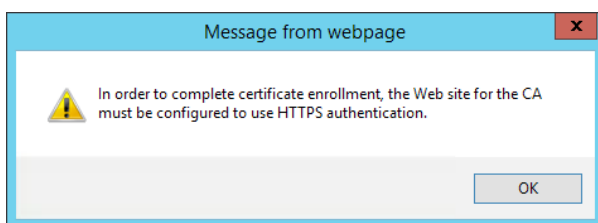


(7) 「Close」をクリックします。



13.2.2. [参考] クライアント証明書発行には IIS の HTTPS 化が必須

Win2012 の Web ブラウザ(IE)で、「http://win2012.acme.com/certsrv/」へアクセスして、クライアント証明書を生成したいユーザ名とパスワードを入力すると、生成ステップの途中まで進めますが、以下のように警告が出てそれ以上はすすめなくなります。



よって、IIS を HTTPS 対応にしなければなりません。

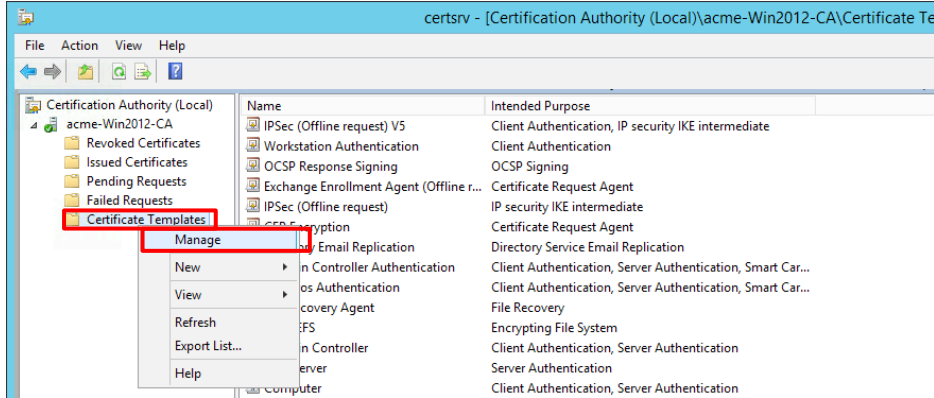
13.2.3. IIS の HTTPS 化

IIS を HTTPS 化しますが、「適当なサーバ証明書を割り当てて HTTPS 化すればよい」というものではなく、若干ステップが多めです。

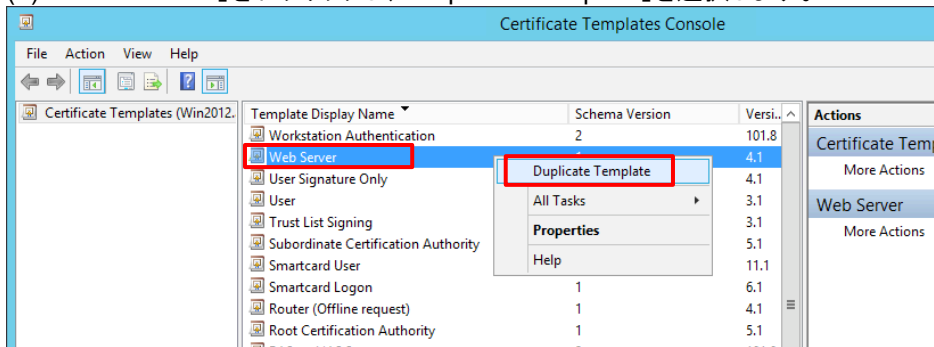
13.2.3.1. CA の設定

(1) Win2012 の Administration Tools から「Certification Authority」を開きます。

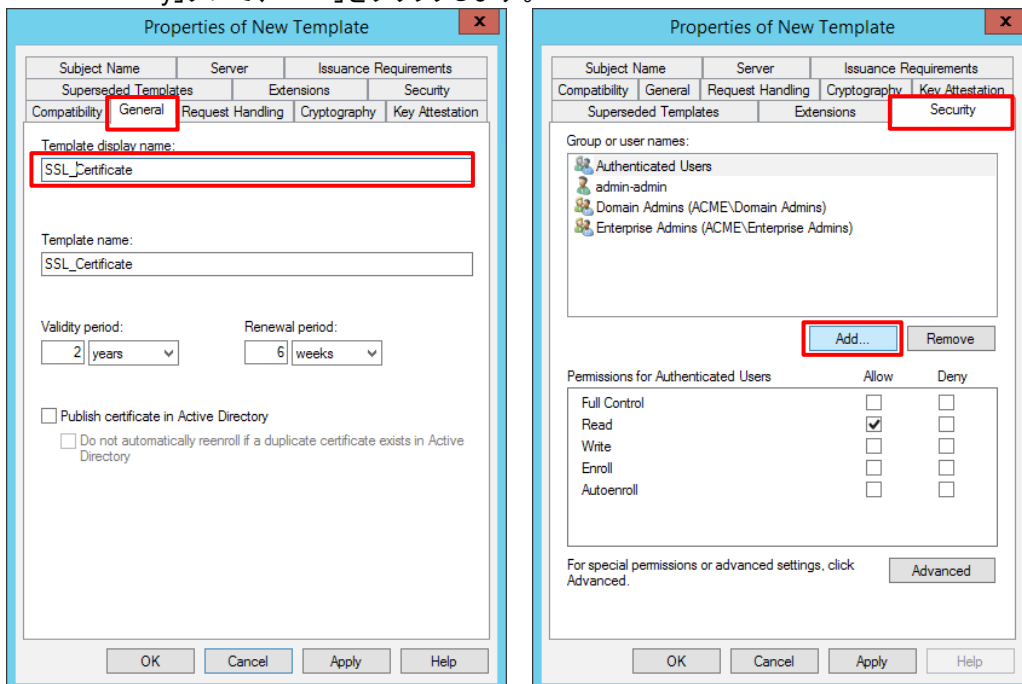
(2) 「acme-Win2012-CA」の下の「Certificate Templates」を右クリックし、「Manage」を選択します。



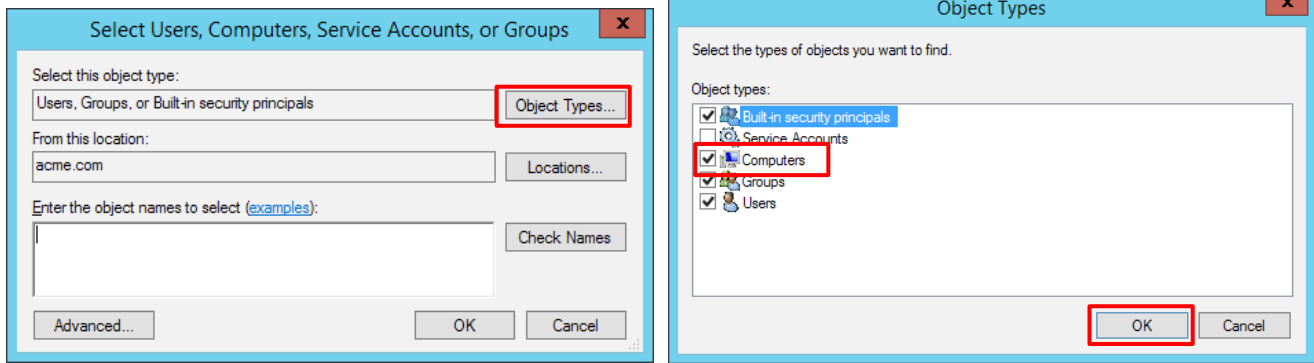
(3) 「Web Server」を右クリックし、「Duplicate Template」を選択します。



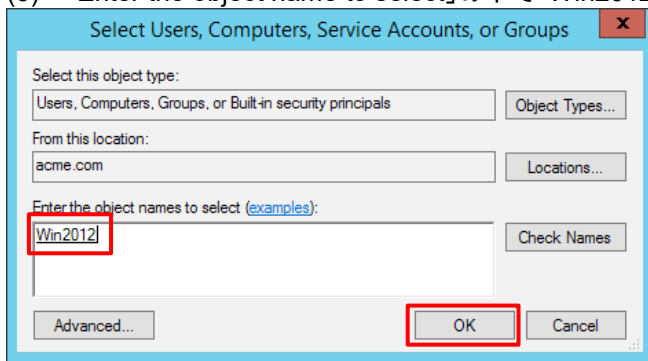
(4) 「General」タブで、「Template display name」に「SSL_Certificate(任意)」と入力します。
「Security」タブで、「Add」をクリックします。



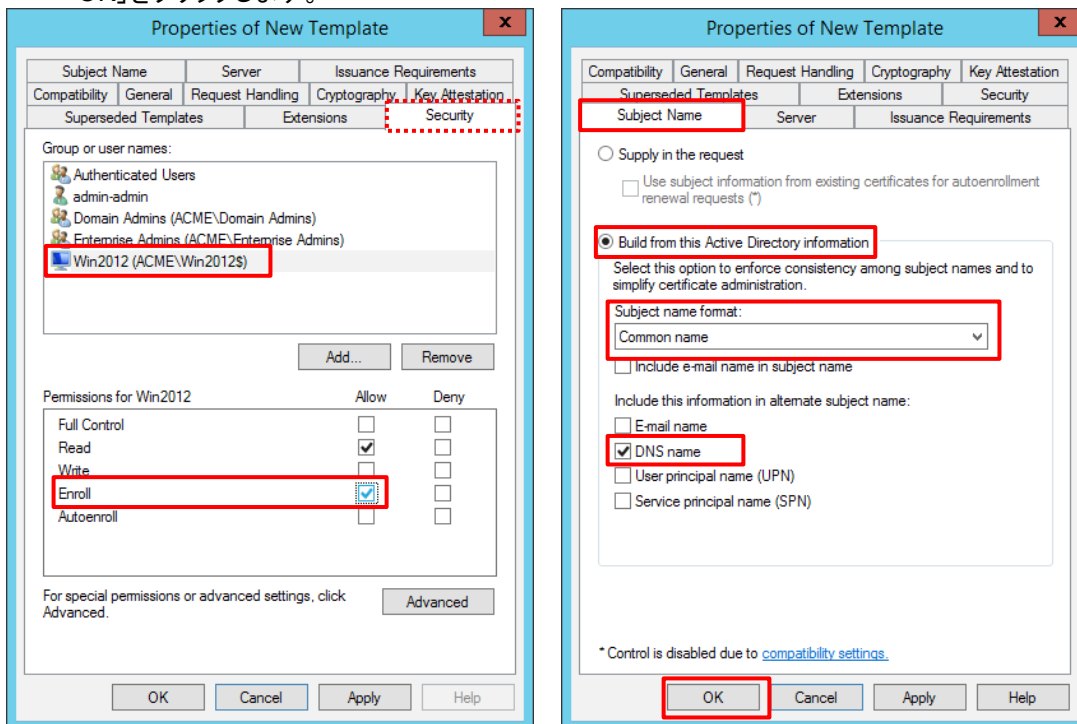
(5) 「Object Type」をクリックして、「Computers」にチェックを入れて「OK」をクリックします。



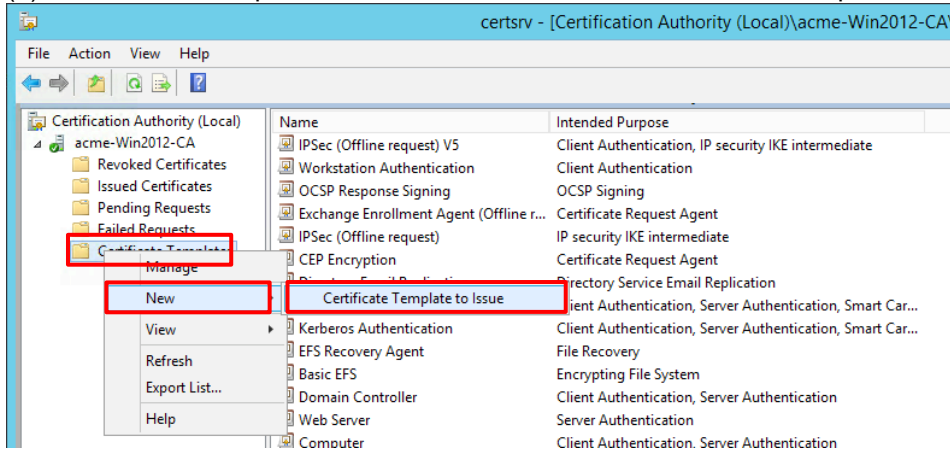
(6) 「Enter the object name to select」の下で「Win2012」を選択して、「OK」をクリックします。



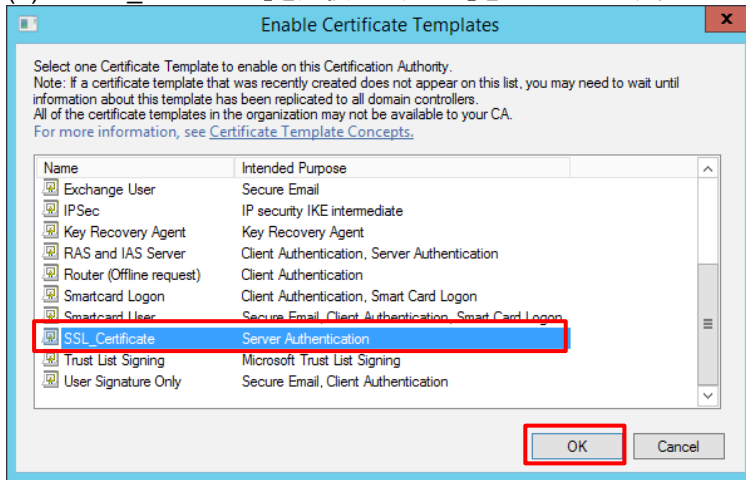
(7) 「Security」タブで、「Win2012」を選択し、「Enroll」にチェックを入れます。
 「Subject Name」タブで、「Build from this Active Directory information」を選択します。
 「Subject name format:」の下で「Common Name」を選択し、「DNS name」にチェックを入れます。
 「OK」をクリックします。



(8) 「Certificate Templates」を右クリックし、「New」 → 「Certificate Template to Issue」をクリックします。




(9) 「SSL_Certificate」を選択して、「OK」をクリックします。



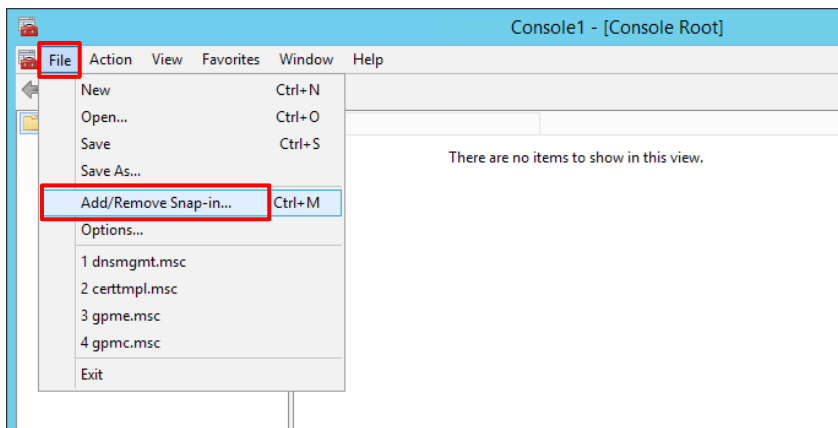
13.2.3.2. MMC からサーバ証明書を作成

MMC で、先ほど生成した Certificate Template を使って、IIS 用のサーバ証明書を作成します。

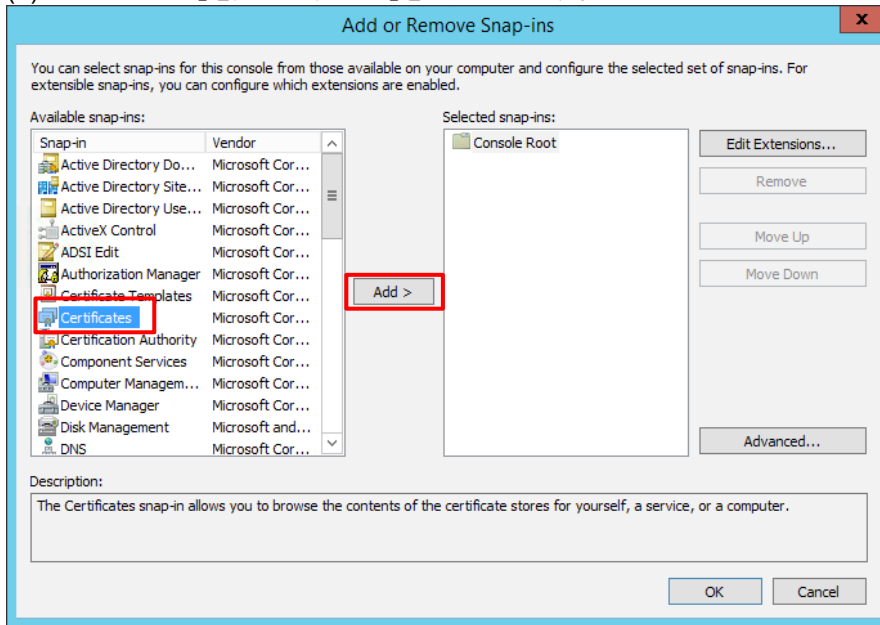
(1) Win2012 のデスクトップの左下にある  をクリックします。
表示された画面左上の検索で、「mmc.exe」と入力し、MMC を起動します。



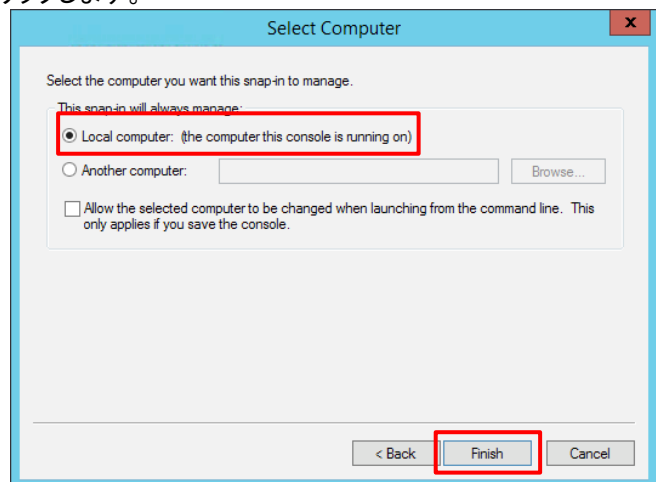
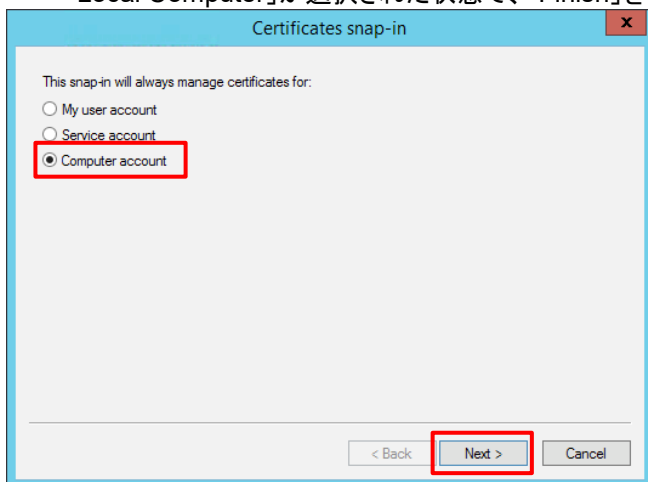
(2) MMC で「File」 → 「Add/Remove Snap-in...」をクリックします。



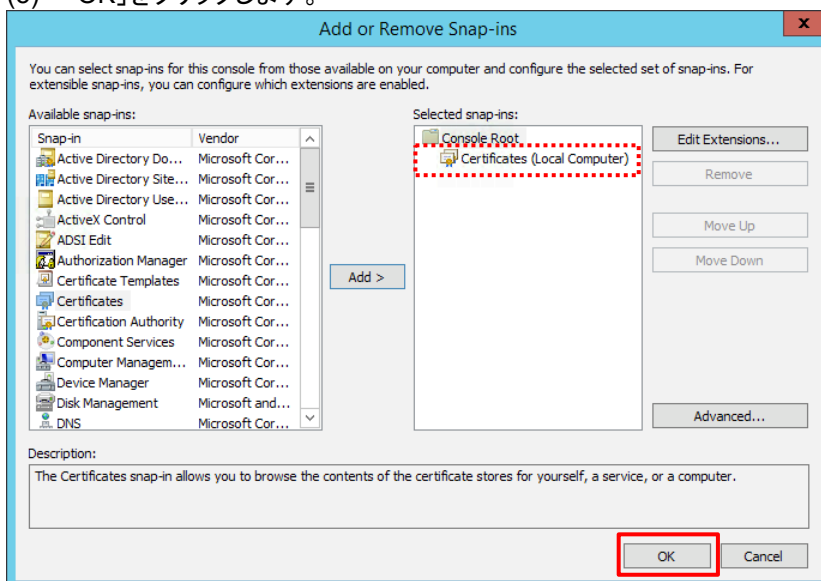
(3) 「Certificate」を選んで、「Add」をクリックします。



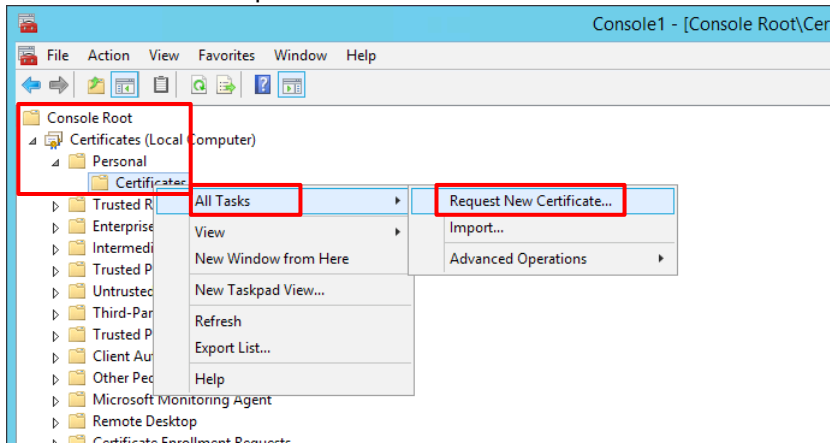
(4) 「Computer account」を選択して「Next」をクリックします。
「Local Computer」が選択された状態で、「Finish」をクリックします。



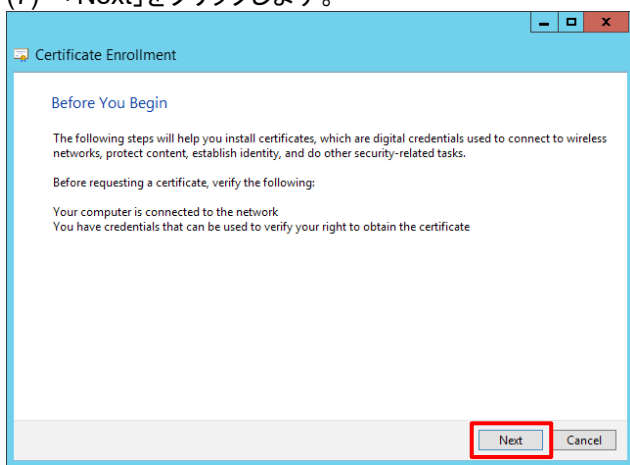
(5) 「OK」をクリックします。



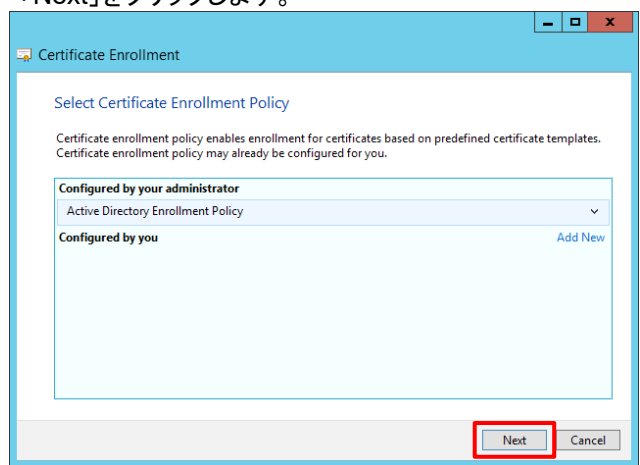
(6) 「Console Root」 → 「Certificates (Local Computer)」 → 「Personal」 → 「Certificates」を右クリック → 「All Tasks」 → 「Request New Certificate...」を選択します。



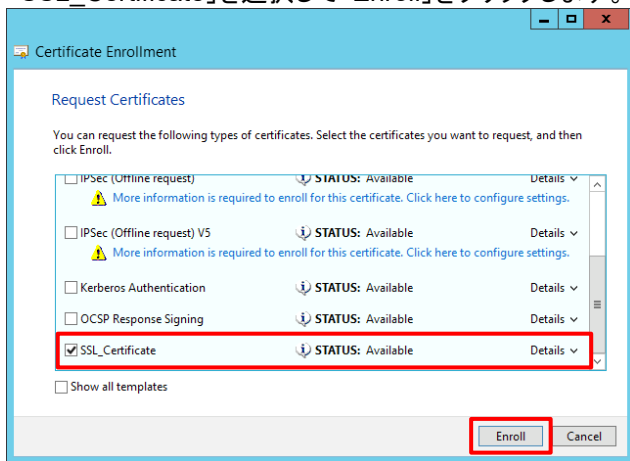
(7) 「Next」をクリックします。



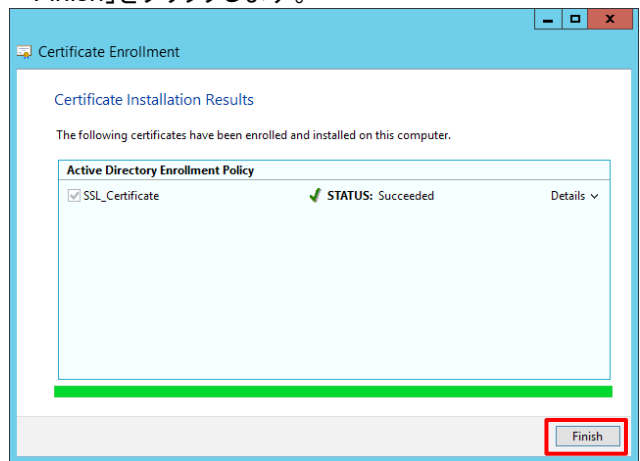
「Next」をクリックします。



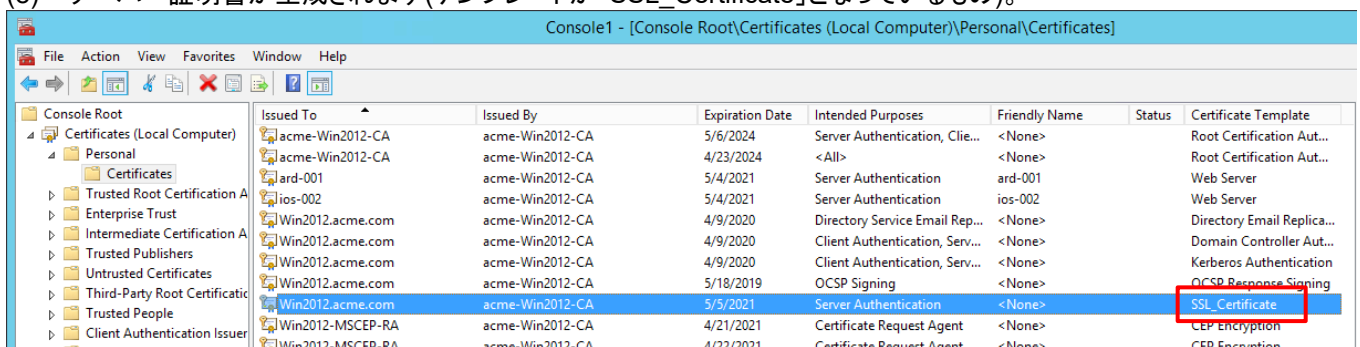
「SSL_Certificate」を選択して「Enroll」をクリックします。



「Finish」をクリックします。



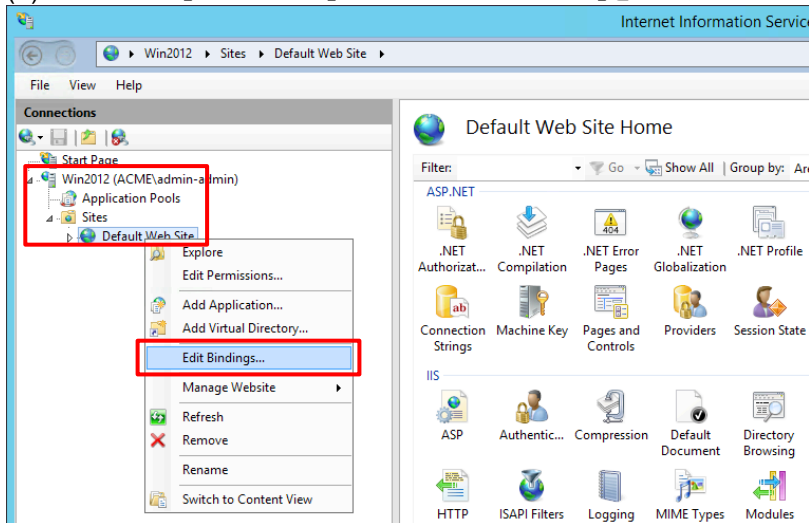
(8) サーバー証明書が生成されます(テンプレートが「SSL_Certificate」となっているもの)。



13.2.3.3. IIS の設定

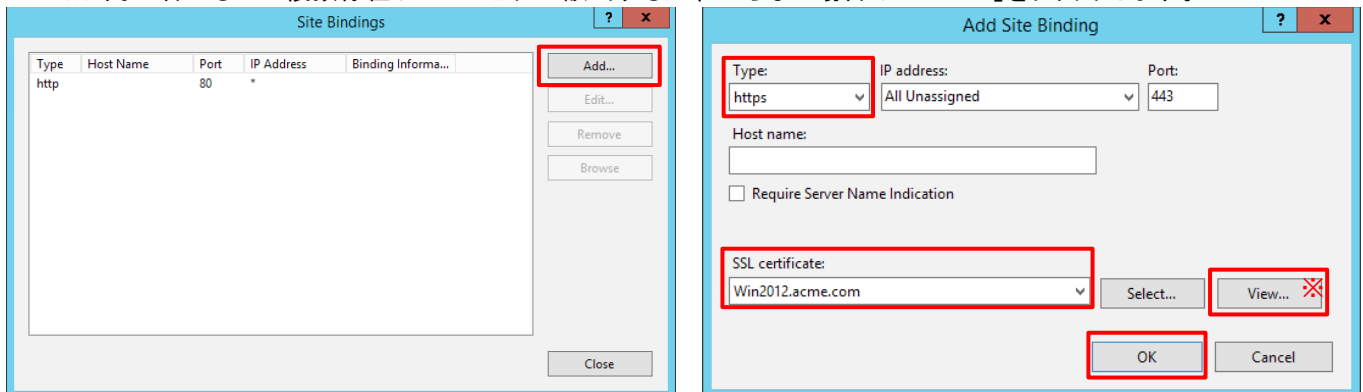
生成したサーバ証明書を、IIS に割り当てます。

- (1) Win2012 の Administration Tools から「Internet Information Service (IIS) Manager」を開きます。
- (2) 「Win2012」 → 「Sites」 → 「Default Web Site」を右クリック → 「Edit Bindings...」を選択します。

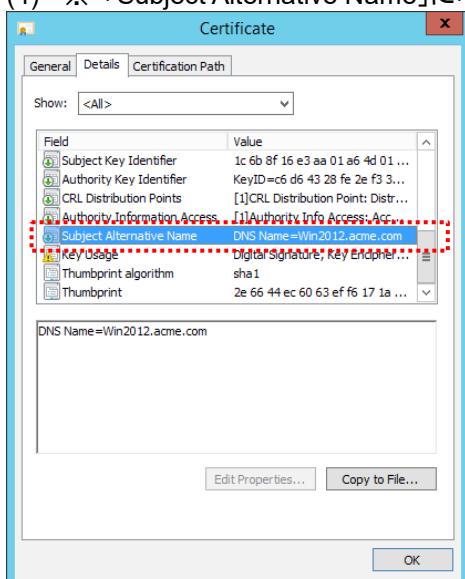


- (3) 「Add」をクリックします。「Type:」で https を選択し、「SSL certificate:」で、生成したサーバ証明書を選択し、「OK」をクリックします。

※ 同一名ものが複数存在してどれが該当するかわからない場合は「View...」をクリックします。



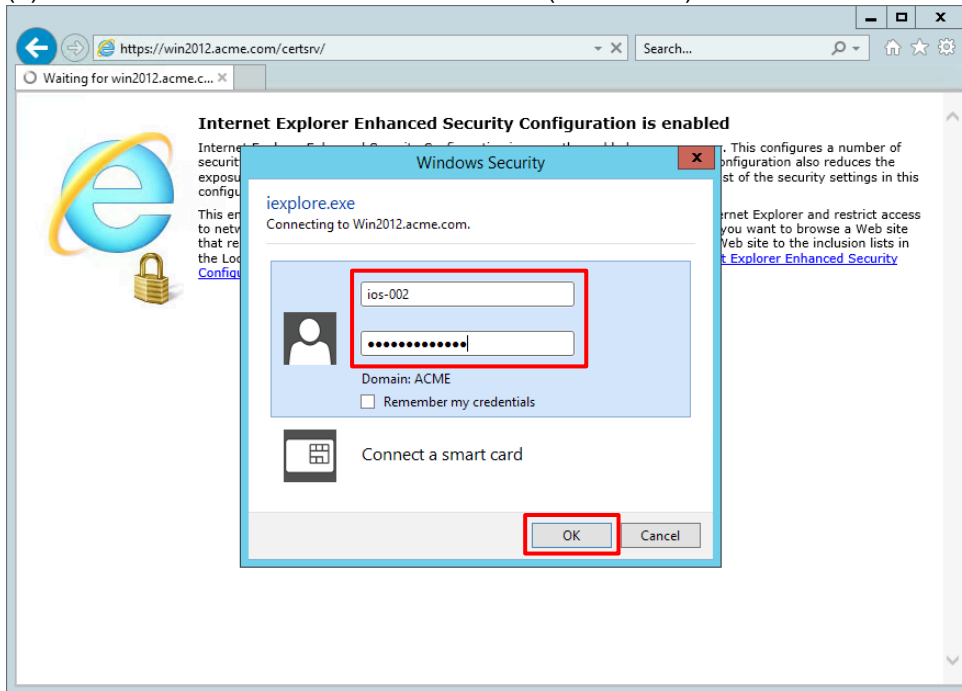
- (4) ※ 「Subject Alternative Name」に「DNS Name=Win2012.acme.com」と記載されたものが該当します。



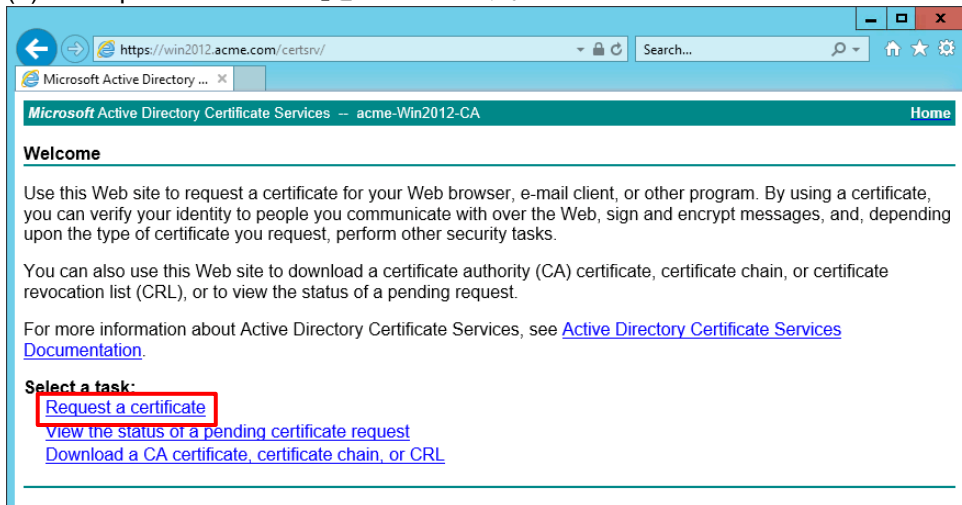
13.2.4. クライアント証明書の発行

(1) Win2012 の Web ブラウザ(IE)から、「https://win2012.acme.com/certsrv/」へアクセスします。

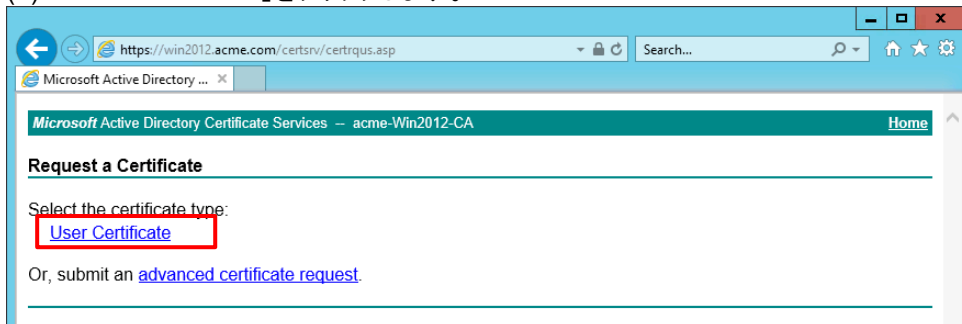
(2) クラクライアント証明書を生成したいユーザー(例: ios-002)でログインします。



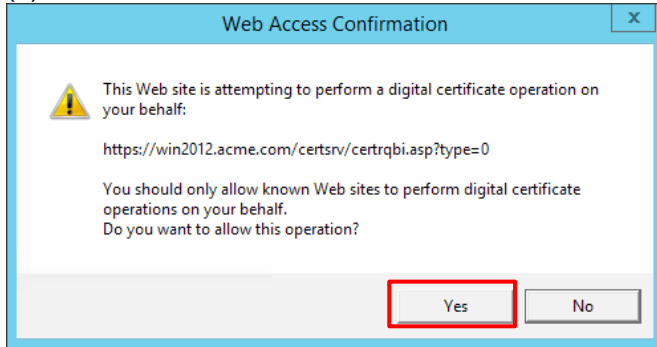
(3) 「Request a certificate」をクリックします。



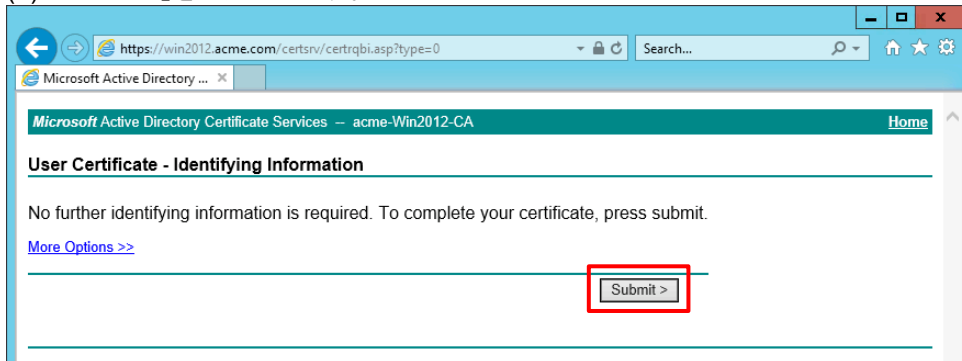
(4) 「User Certificate」をクリックします。



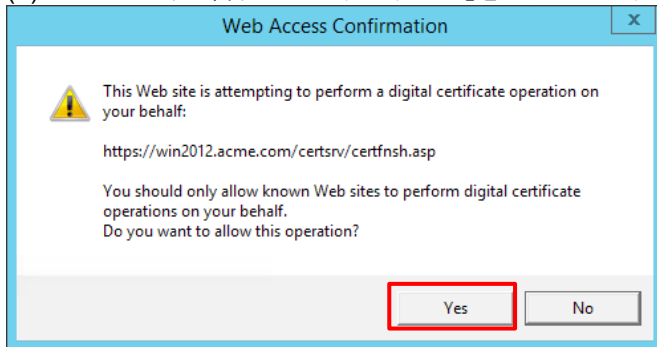
(5) 以下のような警告がでますが、「Yes」をクリックします。



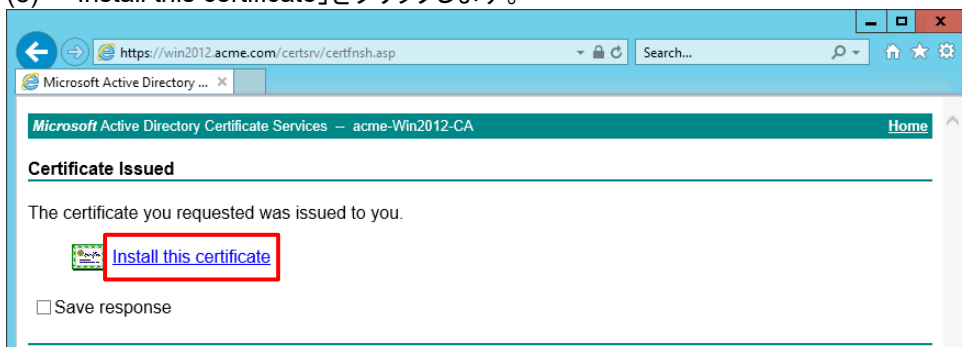
(6) 「Submit」をクリックします。




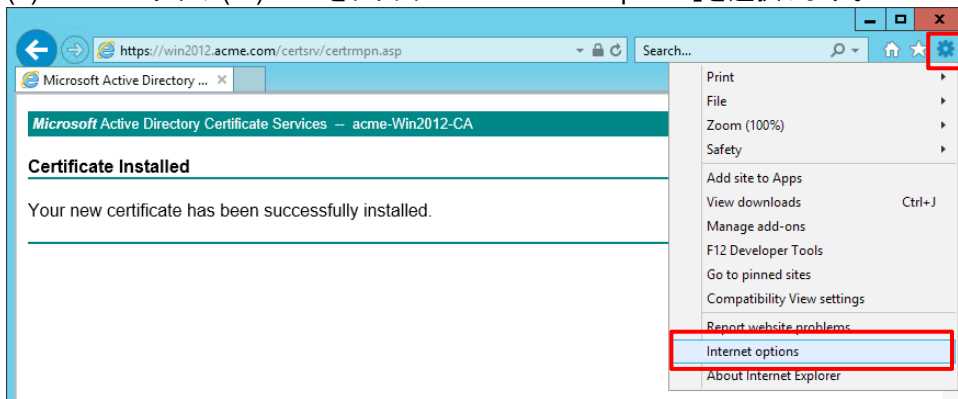
(7) 以下のような警告がでますが、「Yes」をクリックします。



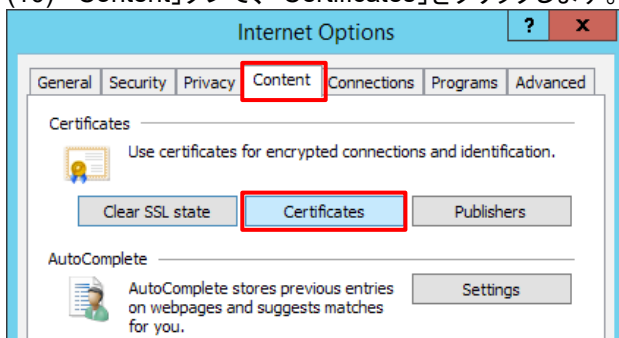
(8) 「Install this certificate」をクリックします。



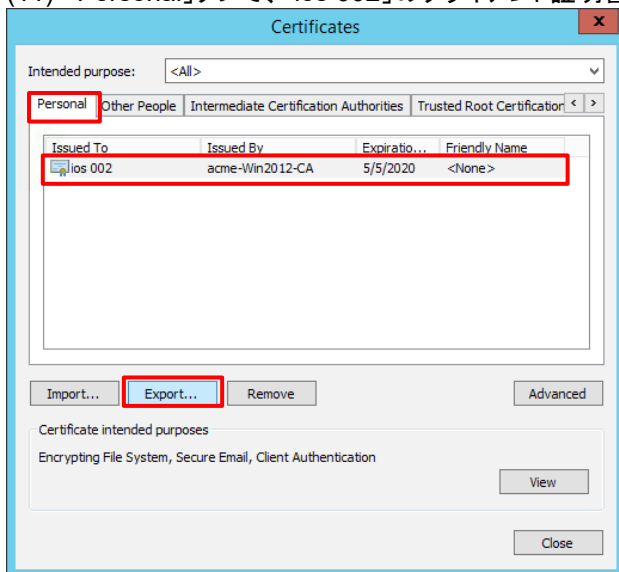
(9) Webブラウザ(IE)の  をクリック → 「Internet Options」を選択します。



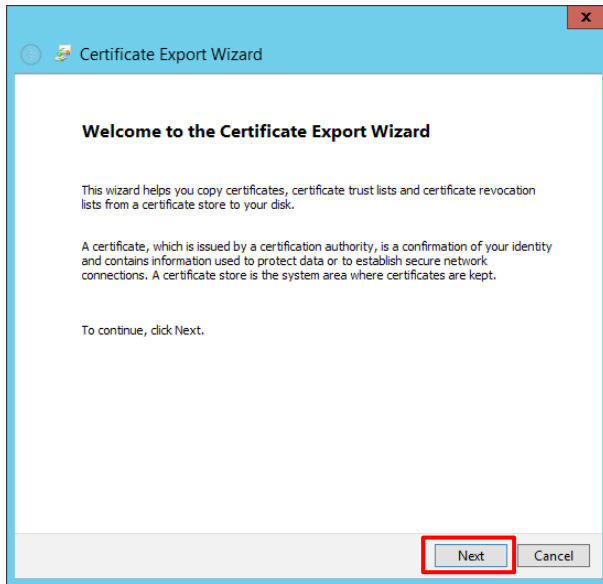
(10) 「Content」タブで、「Certificates」をクリックします。



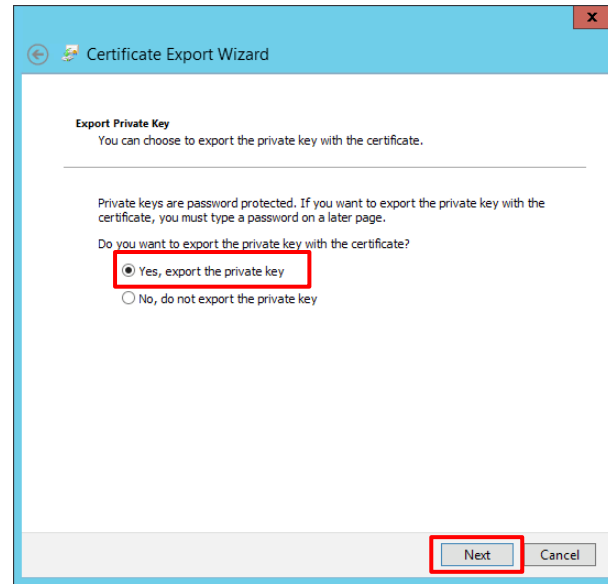
(11) 「Personal」タブで、「ios 002」のクライアント証明書を選択し、「Export」をクリックします。



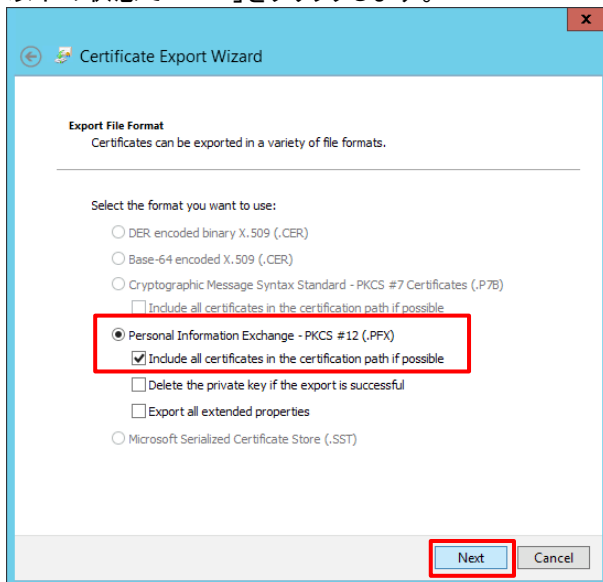
(12) 「Next」をクリックします。



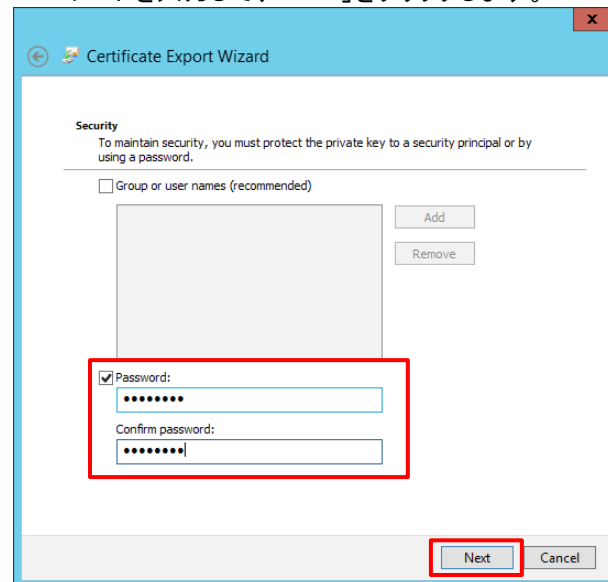
「Yes, export the private key」を選択して、「Next」をクリックします。



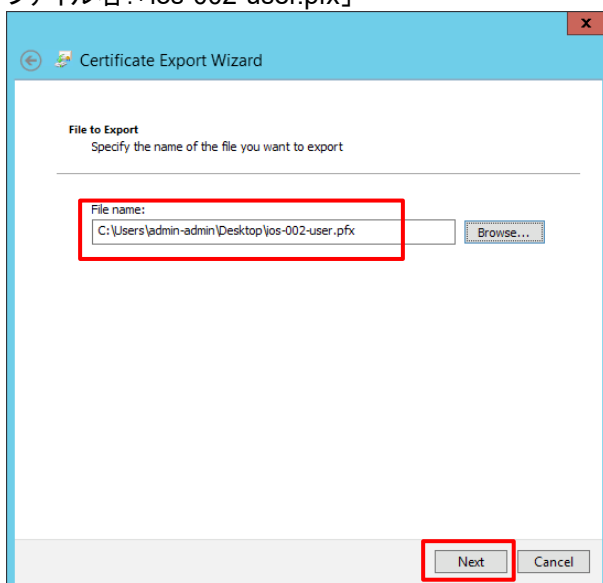
以下の状態で「Next」をクリックします。



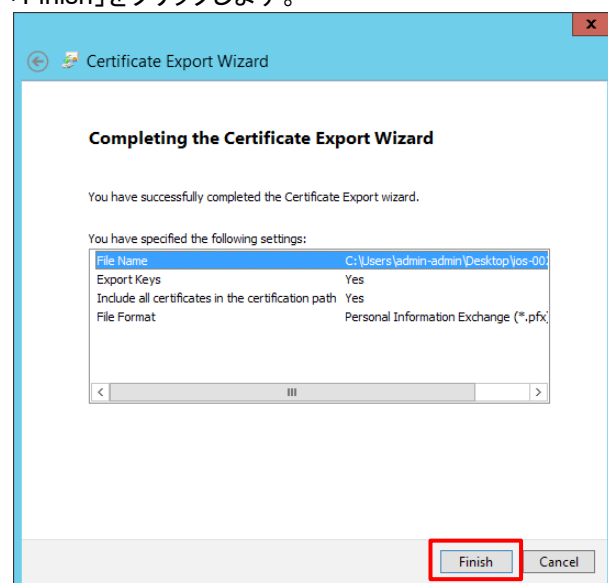
パスワードを入力して、「Next」をクリックします。



ファイル名を指定して、「Next」をクリックします。
ファイル名:「ios-002-user.pfx」



「Finish」をクリックします。



13.2.5. Apple Configurator 2 によるプロファイルの生成と iOS へのインポート

「Apple Configurator 2」を使って、生成したクライアント証明書を iOS へインポートします。

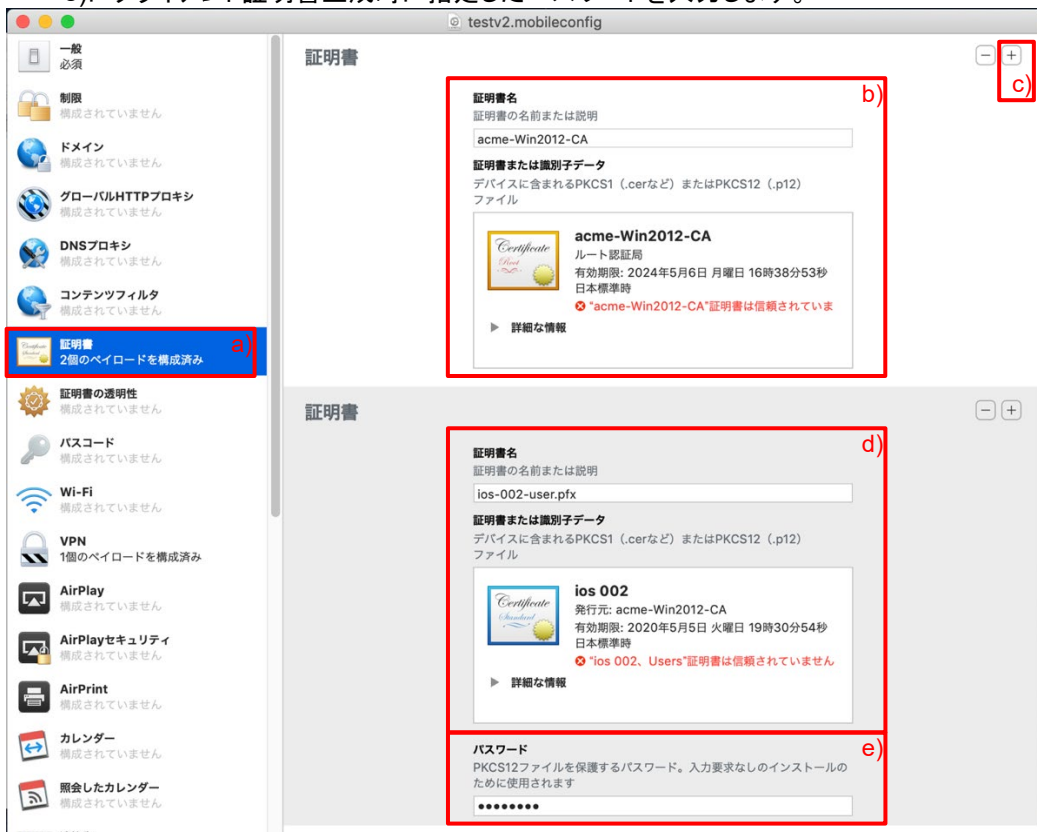
- (1) 本ソフトウェアは、macOS 10.14 Mojave にのみ対応していますので、その OS が稼働する Mac を準備します。
- (2) クライアント証明書「ios-002-user.pfx」と、ルート証明書「acme-Win2012-CA」をその Mac にコピーします。
- (3) macOS の App Store で本ソフトウェアを検索し、インストールし、起動します。
- (4) 「ファイル」 → 「新規プロファイル」をクリックします。



- (5) a) 「一般」で、名前(任意)を入力します。本ガイドでは「testv2」としています。



- (6) a) 「証明書」で「構成」ボタンを押して、c) Win2012 のルート証明書「acme-Win2012-CA」を指定します。
c) [+] をクリックし、d) クライアント証明書「ios-002-user.pfx」を追加します。
e) にクライアント証明書生成時に指定したパスワードを入力します。



- (7) a) 「VPN」で「構成」ボタンを押して、b)接続名に「GPsslvpn(任意)」と入力します。
- c) 接続のタイプで「カスタム SSL」を選択します。
- d) 識別子とサーバには「gp011.japaneast.cloudapp.azure.com」と入力します。
- e) アカウントには「ios-002」と入力します。
- f) ユーザ認証で「証明書」を選択して、g) 資格情報で「ios-002-user.pfx」を選択します。



(8) 「ファイル」 → 「保存」を選択して、任意の場所に、「testv2.mobileconfig」を保存します。

(9) iOS 端末を、macOS とライトニングケーブルで接続します。

(10) Apple Configurator 2 が iOS 端末を認識した状態で、「アクション」 → 「追加」 → 「プロファイル...」を選択して、「testv2.mobileconfig」ファイルを選択します。



(11) iOSを確認します。

a)「閉じる」をクリックして、「設定」Appを確認します。

b)「プロフィールがダウンロードされました」をクリックして表示された画面で、c)「インストール」をクリックします。



下記のような警告が出ますが、d)およびe)の「インストール」をクリックします。

e)「完了」をクリックします。

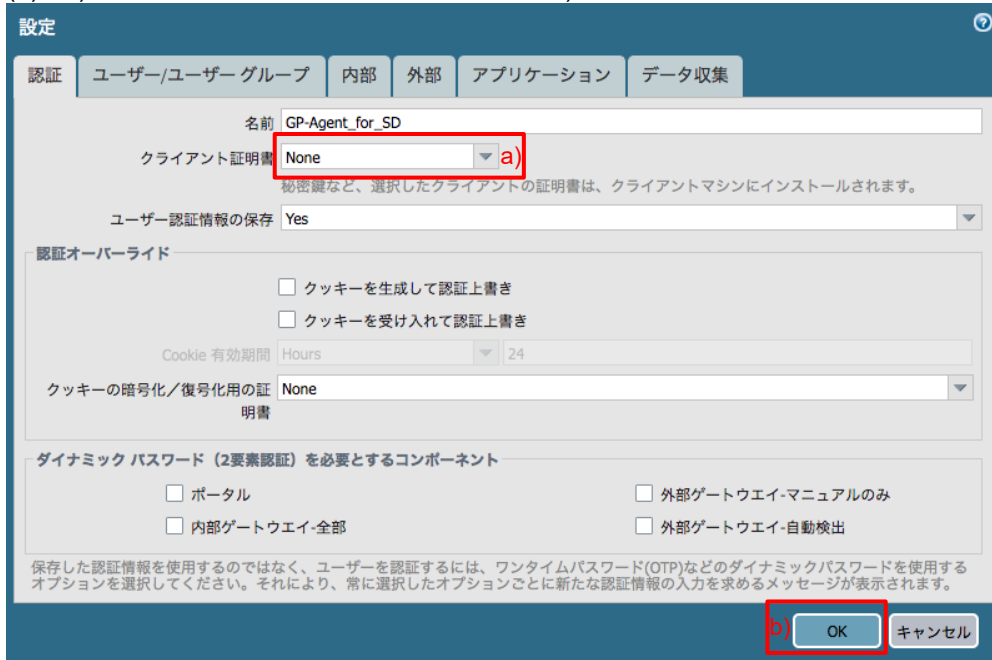
f)「未署名」の状態ですが、クライアント証明書認証としては問題ありません。



13.2.6. Portal の設定変更

SCEP 利用のステップで、スマートデバイスへはクライアント証明書を常時配布する設定にしているはずですので、それを停止します。

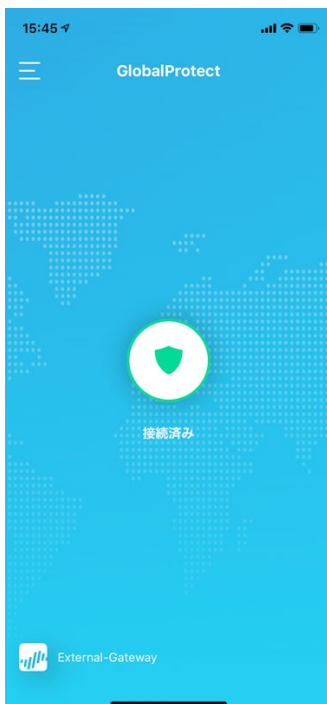
- (1) 「Network」タブ → GlobalProtect の下の「Portal」 → 設定済みの「Portal」をクリック → a)「エージェント」タブ → b)設定済みの「GP-Agent_for_SD」をクリックします。
- (2) a)クライアント証明書を「None」に設定して、b)「OK」をクリックします。



- (3) 「コミット」を実施します。

13.2.7. iOS からのアクセス

外部の iOS から接続できることを確認します。



以上で終了です。

14. おわりに

PA Firewall のアドオン機能である GlobalProtect の基本的な設定方法に関しては以上です。

パロアルトネットワークスでは、この他にも様々なセキュリティソリューションを展開しています。

- Cortex XDR
 - ネットワーク、エンドポイント、クラウドから集めたログデータを、総合的かつ多面的に判断して脅威を検知および対処する Detection & Response サービス
- Prisma Access
 - 遠隔拠点やモバイルユーザーの VPN アクセスを、エンタープライズレベルのセキュリティで提供するクラウド型 VPN サービス
- Prisma SaaS
 - SaaS セキュリティに特化した、Cloud Access Security Broker (CASB) サービス
- Prisma Public Cloud
 - パブリッククラウド環境で生じる新たなセキュリティ脅威を検出/排除し、コンプライアンス準拠を継続的にサポートするクラウドベースのセキュリティサービス

これらの強力なセキュリティソリューションによって、パロアルトネットワークスが、皆様のネットワークが抱える様々なセキュリティの課題を包括的に解決することができます。

これらの具体的な内容に関しては、弊社にお気軽にお問合せください。

また本ガイドに記載されていない PA シリーズの設定方法に関するより詳細が必要な場合は、各種 WEB サイトにてご確認いただくか、ご購入元にお問い合わせください。

<パロアルトネットワークス WEB サイトの紹介>

パロアルトネットワークス総合サイト

<https://www.paloaltonetworks.jp/>

ナレッジベース総合サイト(英語)

<https://support.paloaltonetworks.com/>

ライブコミュニティ(英語・一部日本語)

<https://live.paloaltonetworks.com/>

以上

パロアルトネットワークス株式会社

〒100-0010 東京都千代田区内幸町2丁目1-番 6 号 日比谷パークフロント 15 階

本資料はパロアルトネットワークスのエンジニアが特定のソフトウェアバージョンの動作仕様に基づいて作成した構築・設計を補助するための資料であり、メーカー公式資料とは異なります。資料の記載内容に誤りがあった際には指摘に基づいて修正を行いますが、内容についての責任は一切負いません。また、修正、変更、改訂は予告無く行われます。