BIG-IP APM
ネットワークアクセス
かんたんセットアップガイド(v11.4.1 対応)
初級編 & 中級編

F5 Networks Japan

V1.0

目次

1. はじめに

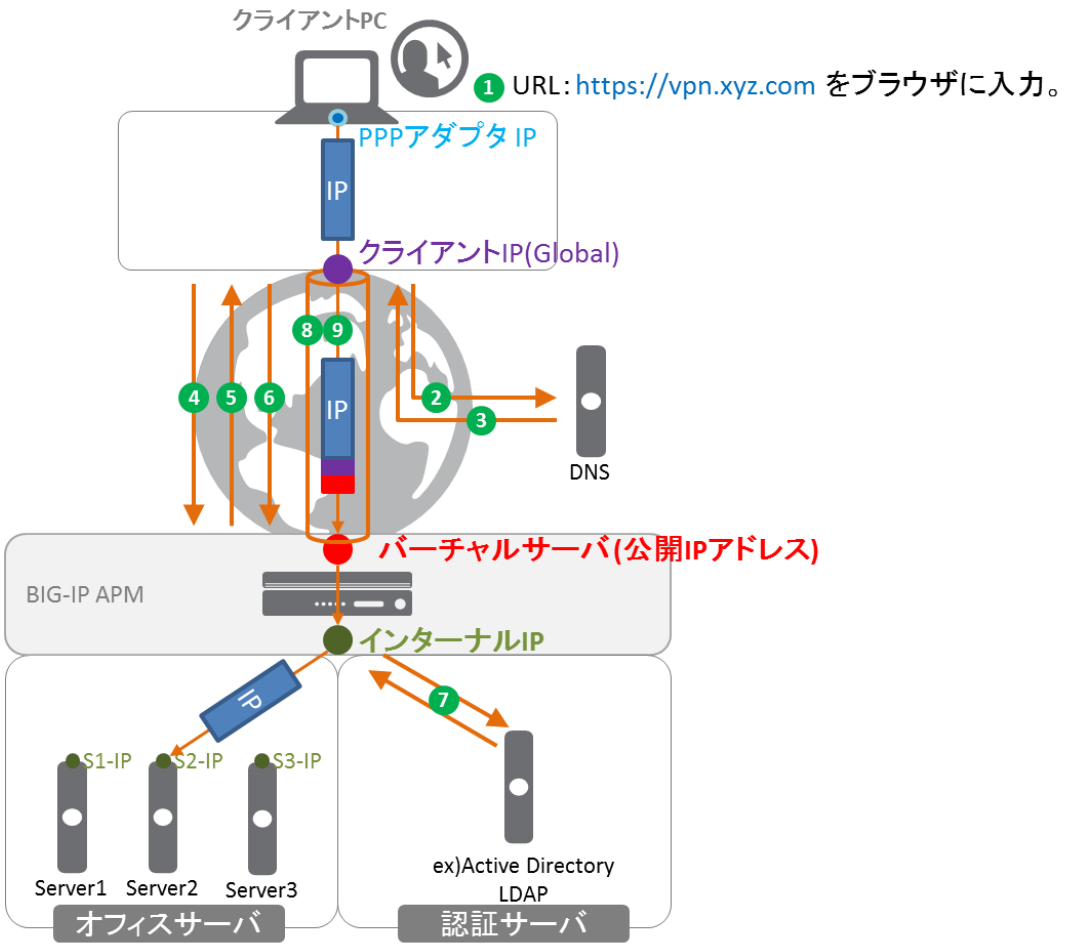
本セットアップガイドにて BIG-IP Access Policy Manager（以下、APM）のネットワークアクセスの設定方法についてご案内します。

BIG-IP APM は、SSL-VPN トンネルによるリモートアクセス(これをネットワークアクセスと呼びます)をはじめとして、高度な認証機能(例：クレデンシャルキャッシング方式シングルサインオン，SAML シングルサインオン等)も兼ね備えています。

本ガイドでは、BIG-IP APM をご購入いただいてすぐにネットワークアクセスを始められるように、必要となる典型的なセットアップ手法を、豊富なスクリーンショットを交えて解説します。

1.1. APM ネットワークアクセス動作概要

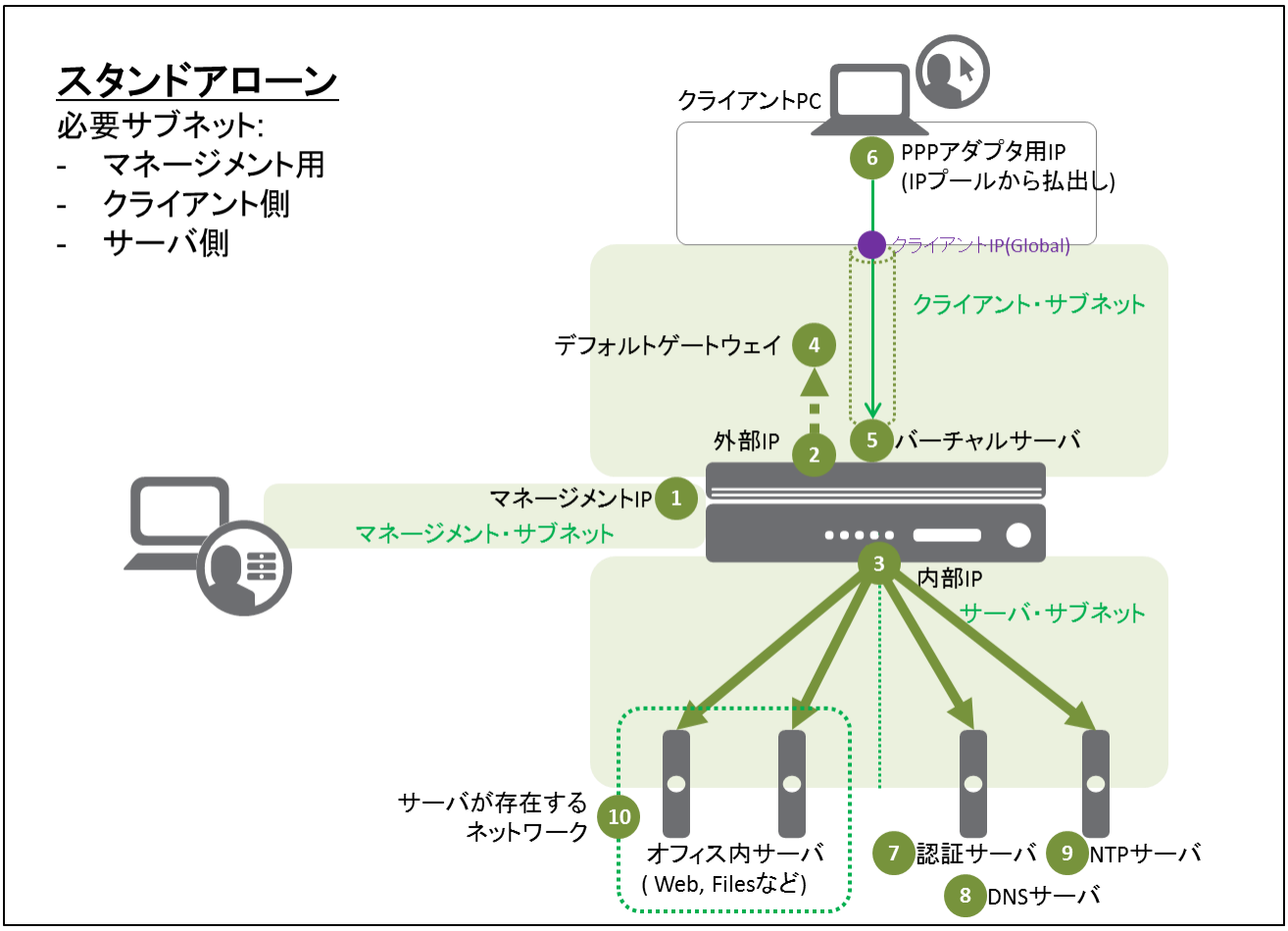
APM のネットワークアクセスは以下のような流れで動作します。



① クライアントが Web ブラウザに、URL：https://vpn.xyz.com を入力。
② クライアント PC は、vpn.xyz.com の IP アドレスを解決するために、DNS クエリを送信。
③ DNS サーバから vpn.xyz.com の IP アドレスを得る。
④ Web ブラウザは、その IP アドレス(バーチャルサーバ)宛に HTTPS リクエストを送信。
⑤ BIG-IP APM は、ログインページを表示。
⑥ クライアントは、ユーザ名とパスワードを入力。
⑦ BIG-IP APM は認証サーバに問合せを行い、認証が正しく行われたことのレスポンスを得る。
⑧ BIG-IP APM は、クライアント PC との間で SSL-VPN トンネルを確立する。このとき、クライアント PC の PPP アダプタには、事前に APM に設定された IP アドレスプールの中から一つ IP アドレスが払い出される。
(この後、クライアント PC は、PPP アダプタを使って、オフィスサーバ群へアクセスができるようになる。)
⑨ PPP アダプタから出た IP パケットは、インターネット上のグローバル IP アドレスでカプセル化(＝トンネル化)され、BIG-IP APM に到着。APM はそのカプセル化を解き、APM のルーティングテーブルに従って、そのカプセル化が解かれた IP パケットを送り出す。

2. スタンドアローン

2.1. スタンドアローンイメージ

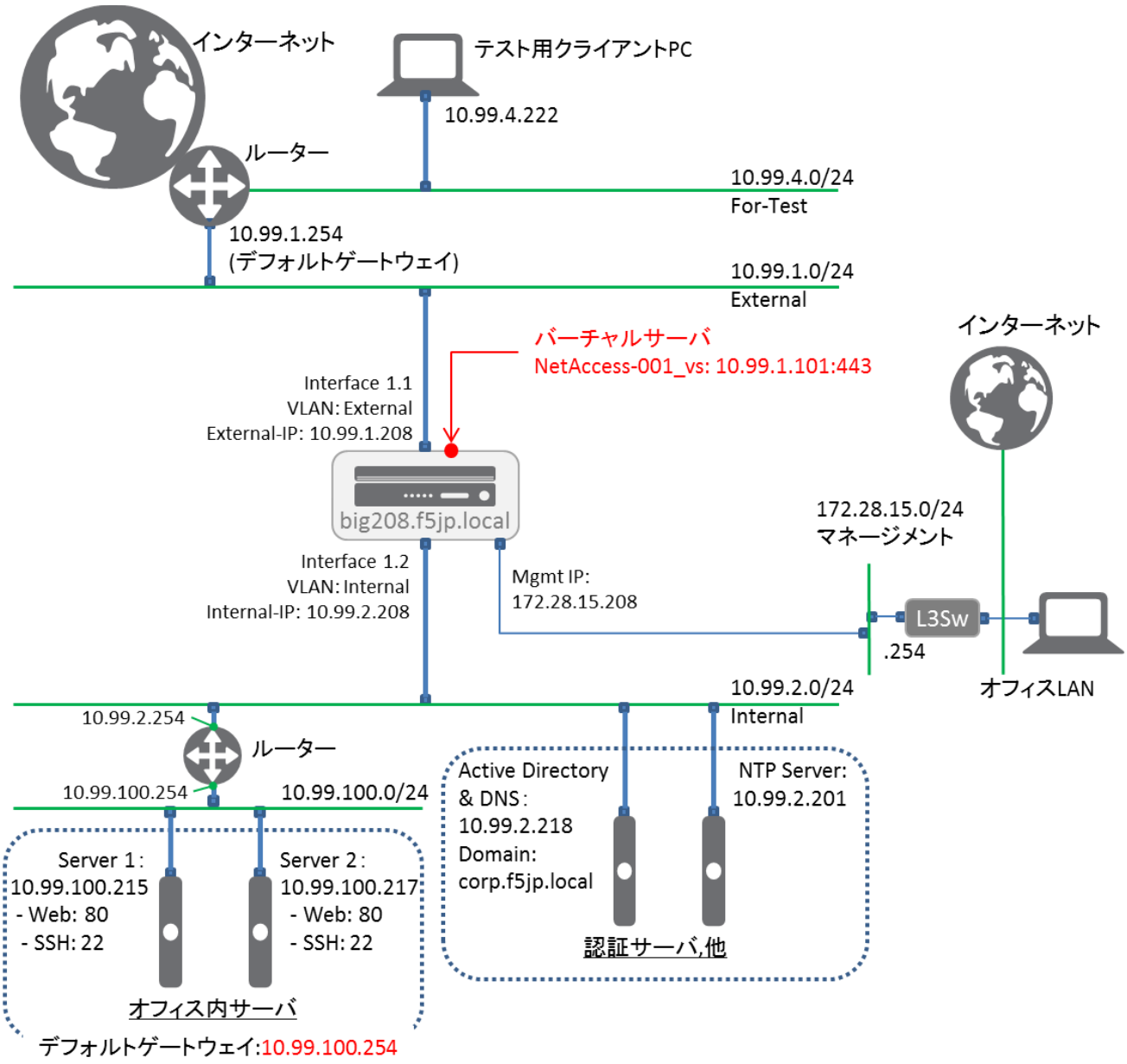


上図①～⑨の IP アドレスが必要になりますので、あらかじめご用意ください。
なお、①管理 IP は工場出荷時に 192.168.1.245/24 がプリセットされています。

	項目	名前(サンプル)	値
-	ホスト名	Big208.f5jp.local	
①	管理 IP	---	172.28.15.208/24
②	External インタフェース	external	10.99.1.208
③	Internal インタフェース	internal	10.99.2.208
④	デフォルトゲートウェイ	default-GW	10.99.1.254
⑤	バーチャルサーバアドレス	NetAccess-001_vs	10.99.1.101:443
⑥	PPP アダプタ用 IP アドレスプール	NetAccess-001_lp	10.99.99.11-20
⑦	認証サーバ (Active Directory)	NetAccess-001_aaa_srvr	10.99.2.218
⑧	DNS サーバ (Active Directory)	---	10.99.2.218
⑨	NTP サーバ	---	10.99.2.201
⑩	サーバが存在するネットワーク	---	10.99.100.0/24
	CLI パスワード (デフォルト)	---	ID/Password : root/default
	GUI パスワード (デフォルト)	---	ID/Password : admin/admin

2.2. スタンドアローンのネットワークサンプル

まずは、冗長化しない状態を想定して、1 台のみ設定していきます。



BIG-IP の APM リモートアクセス用 Virtual Server は 10.99.1.101:443 とします。

Active Directory のドメインは、「corp.f5jp.local」とします。
Active Directory には、以下 3 つのユーザが登録されています。

ユーザ名	パスワード	グループ
test1001	test1001	CorpA-Group
test1002	test1002	CorpB-Group
test1003	test1003	CorpC-Group

BIG-IP のデフォルトゲートウェイは、インターネット方向を想定したルーター：10.99.1.254 に設定します。

オフィス内サーバのデフォルトゲートウェイは、直上のルーター：10.99.100.254 に設定されているものとします。

動作確認は、テスト用に設置した PC(図中の「テスト用クライアント PC」)から行うこととします。

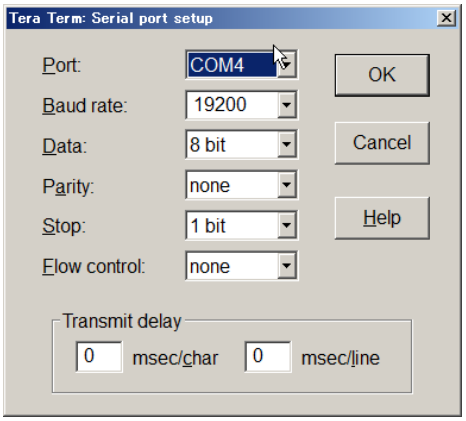
3. 初期設定

3.1. 管理ポートの IP アドレス設定

BIG-IP へ、専用コンソールケーブル(同梱)を使用し、Baud Rate 19,200 で接続します。

例：BIG-IP2000S

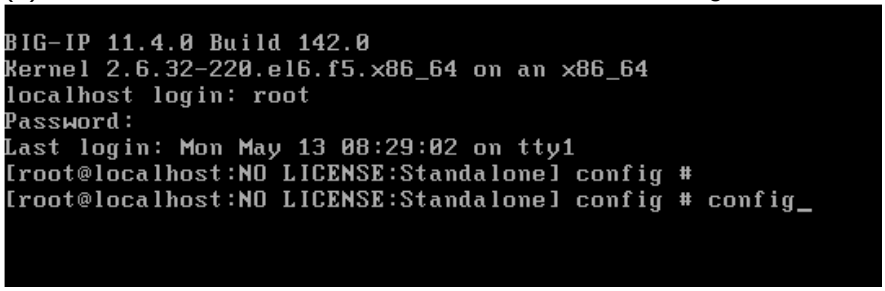
例：TeraTerm のシリアルポート設定



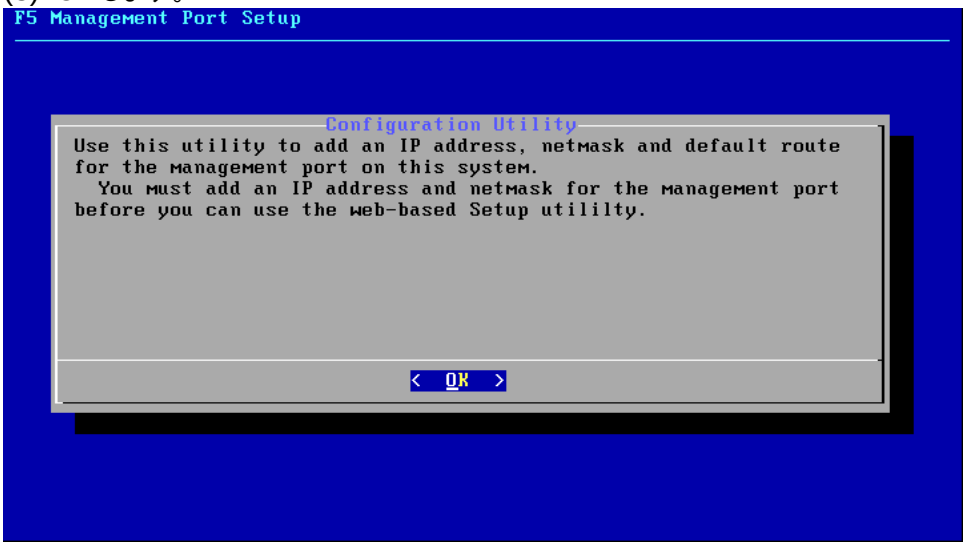
(1) デフォルトログインは、以下です。

ID: root
Password: default

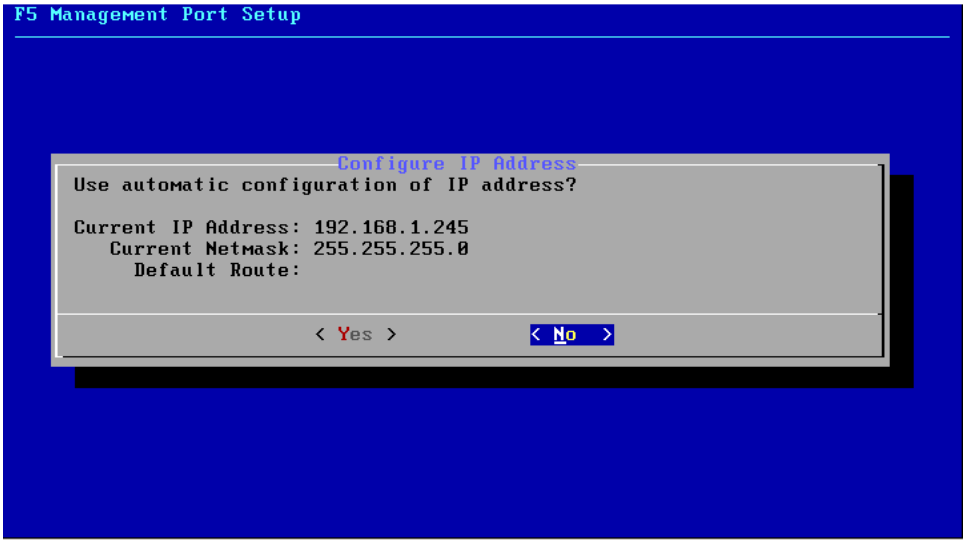
(2) 管理ポートの IP アドレスを設定するために、コマンド：config を入力し、Enter します。



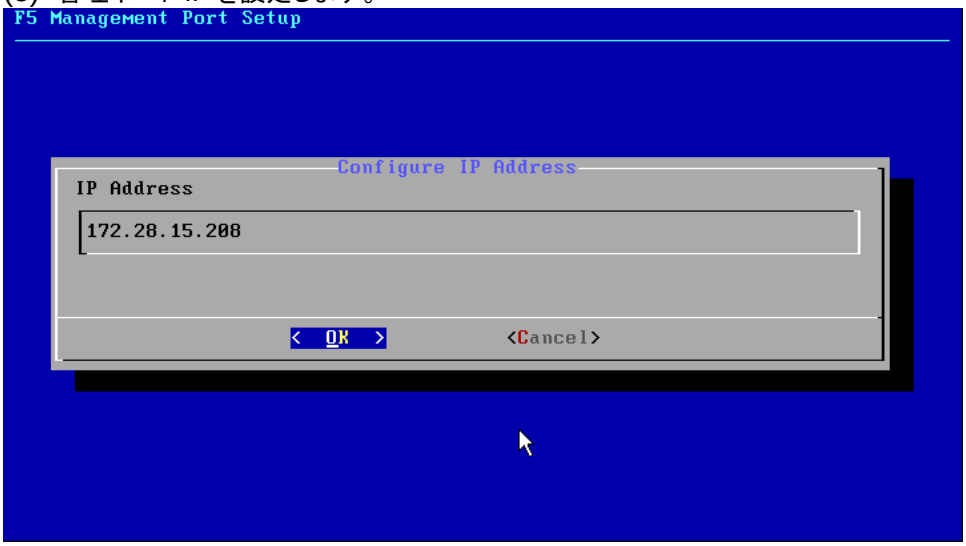
(3) OK します。



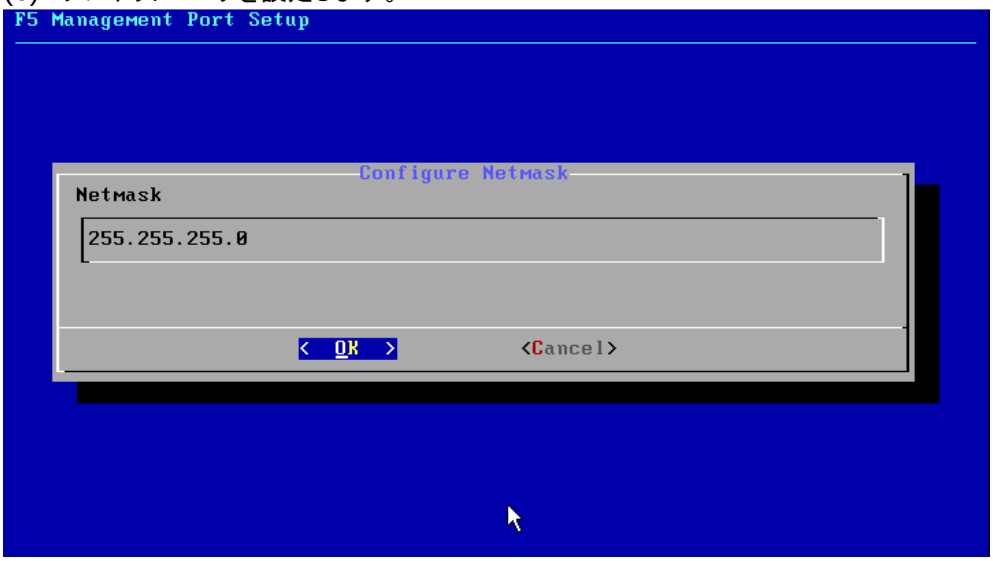
(4) DHCP を利用するかどうかを聞いてきますので、環境に合わせて設定します。
本環境では、DHCP は利用しないので、「No」を選択します。



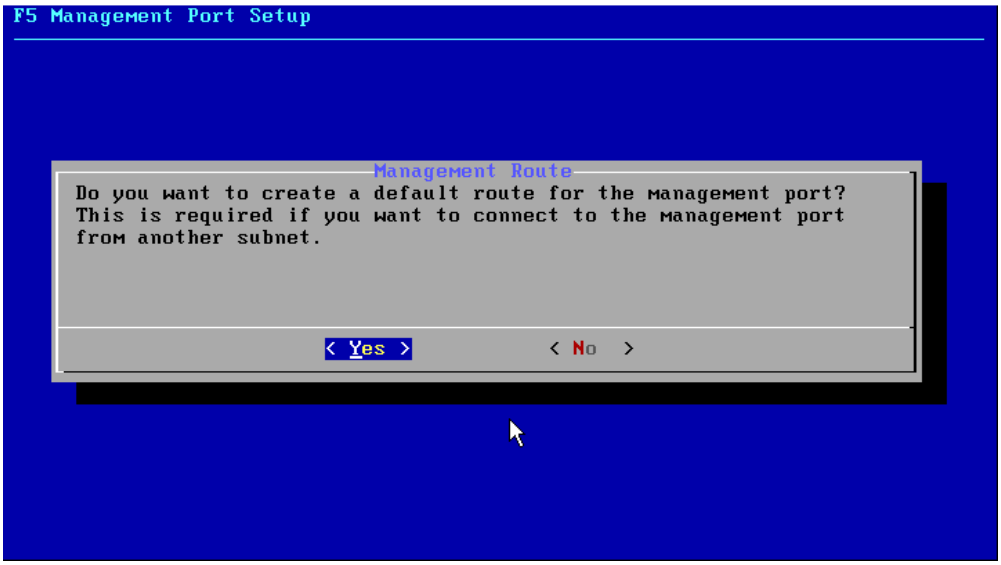
(5) 管理ポート IP を設定します。



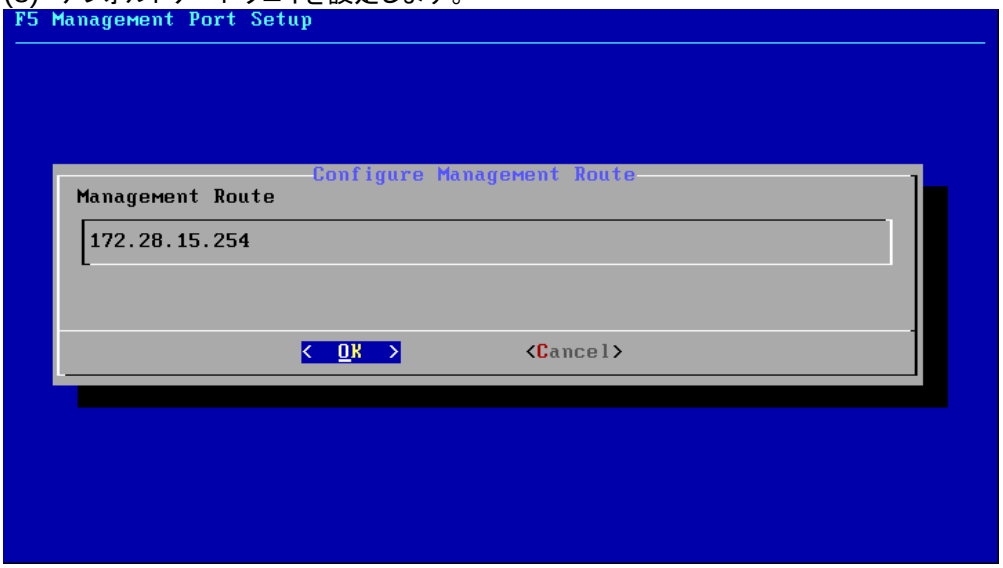
(6) サブネットマスクを設定します。



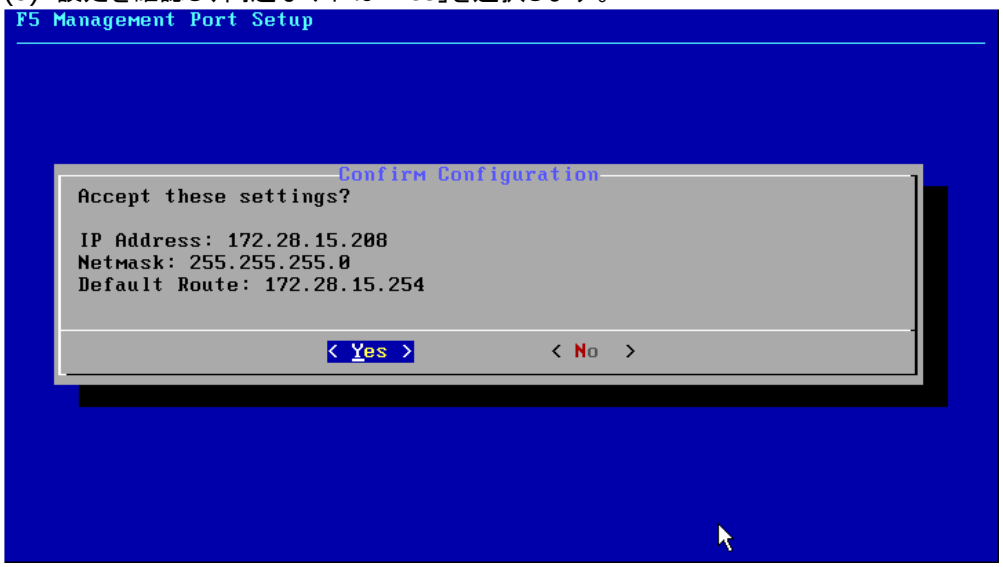
(7) デフォルトゲートウェイを設定するかどうかを聞いてきますので、環境に合わせて設定します。
本環境では必要なので、「Yes」を選択します。



(8) デフォルトゲートウェイを設定します。



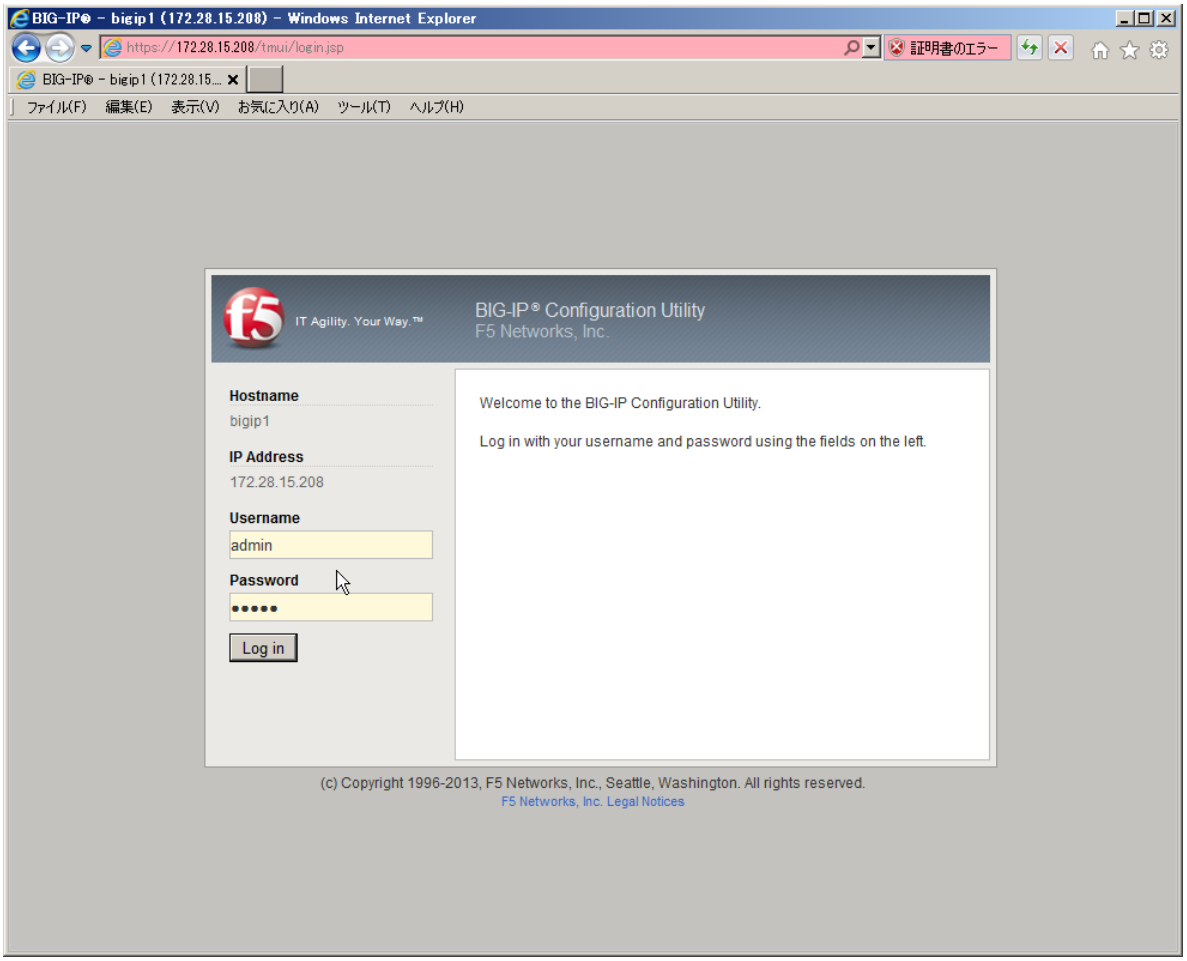
(9) 設定を確認し、問題なければ「Yes」を選択します。



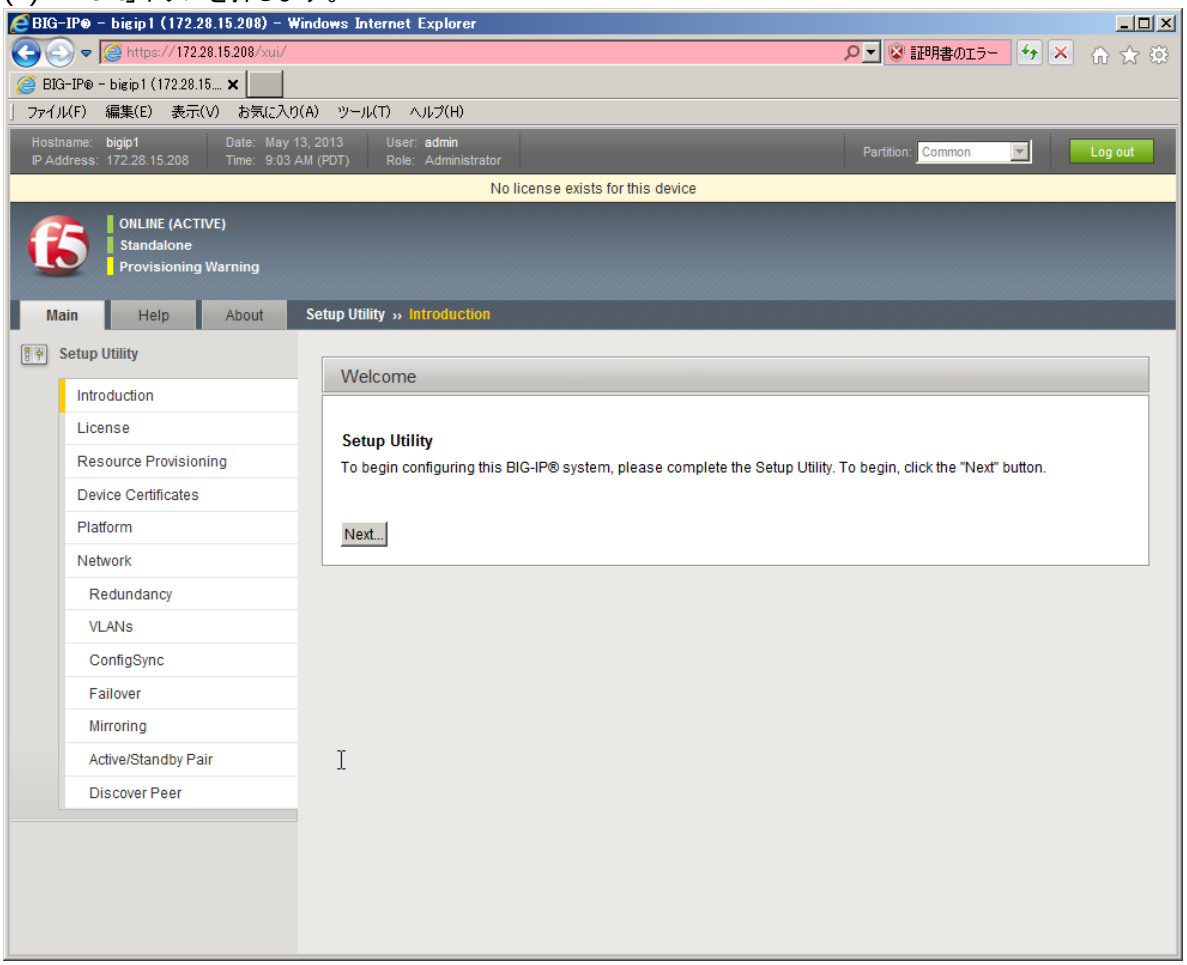
3.2. 管理ポートへの GUI アクセス→ライセンスの取得

管理用 PC から、設定した BIG-IP の管理 IP アドレスへ、HTTPS でアクセスします。
管理用 PC はライセンスアクティベーションの為、インターネットへ接続できる環境である必要があります。
デフォルトの証明書は、正式に取得した証明書ではないため、以下のような画面が現れますが、「続行する」を選択してください。

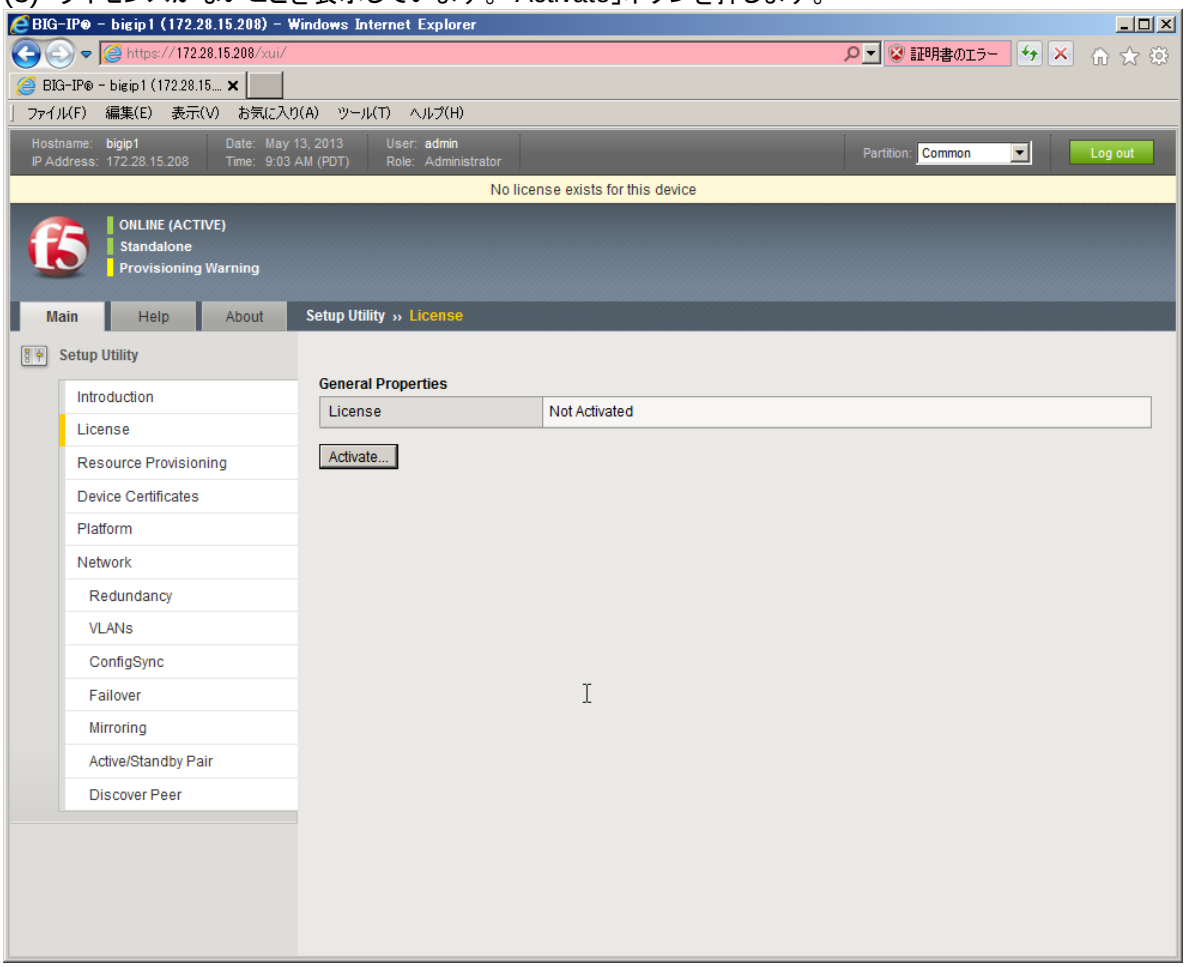
(1) ログイン画面が現れますので、以下のデフォルトの ID と Password でログインしてください。
ID：admin
Password：admin



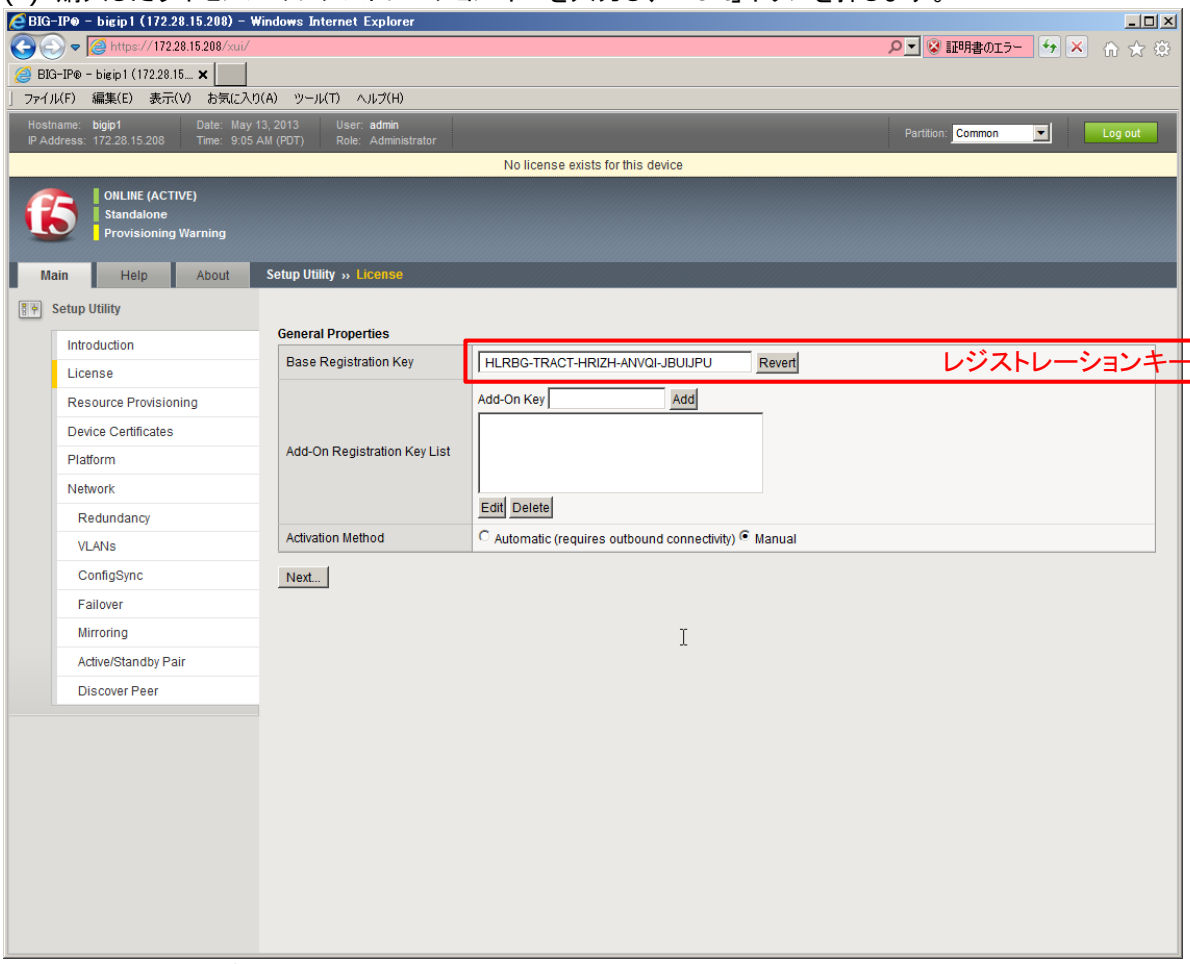
(2) 「Next」ボタンを押します。



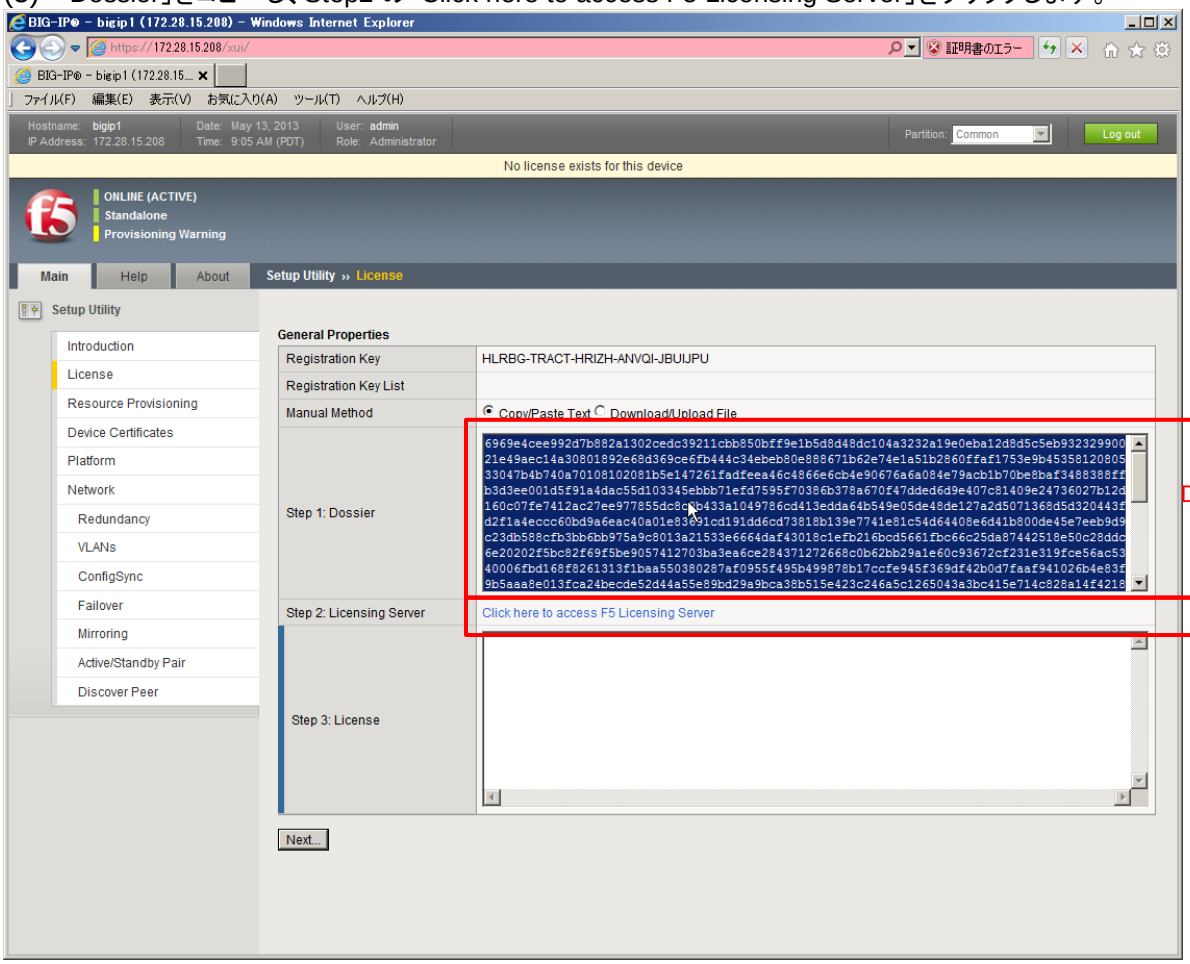
(3) ライセンスがないことを表示しています。「Activate」ボタンを押します。



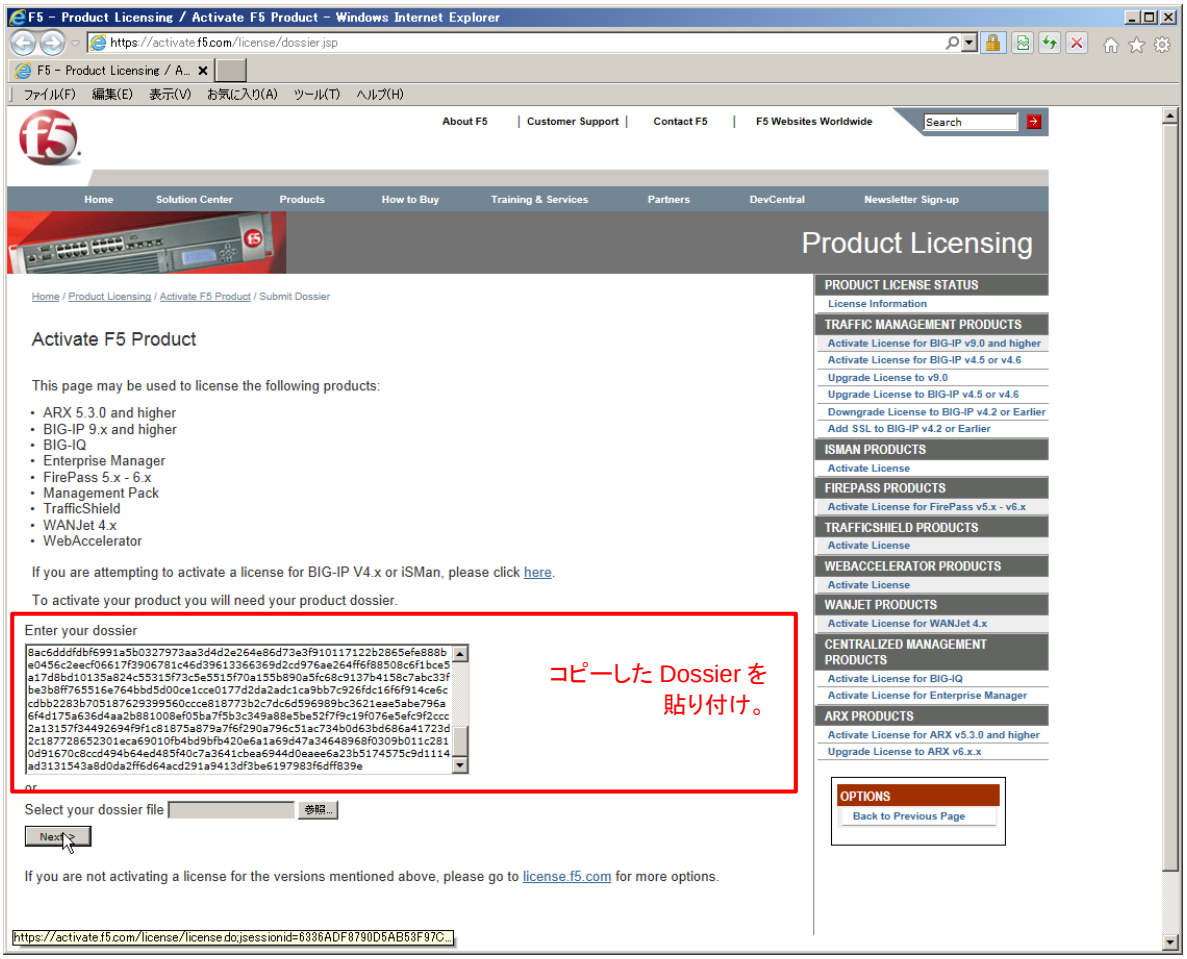
(4) 購入したライセンスのレジストレーションキーを入力し、「Next」ボタンを押します。



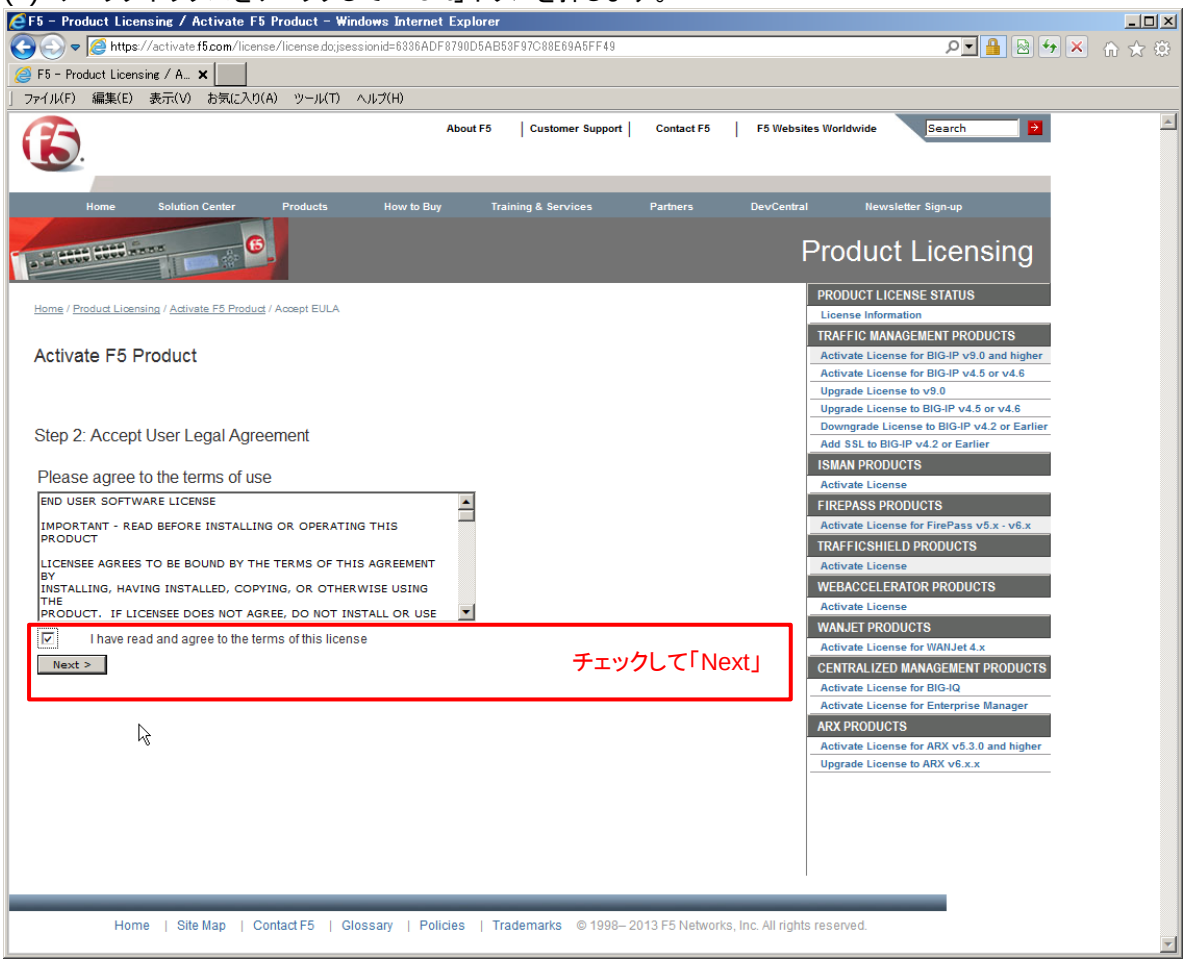
(5) 「Dossier」をコピーし、Step2 の「Click here to access F5 Licensing Server」をクリックします。



(6) ライセンス取得するための Web サイト：activate.f5.com へ飛びますので、「Enter your dossier」フィールドの中に、上記でコピーした Dossier を貼り付けます。「Next」ボタンを押します。

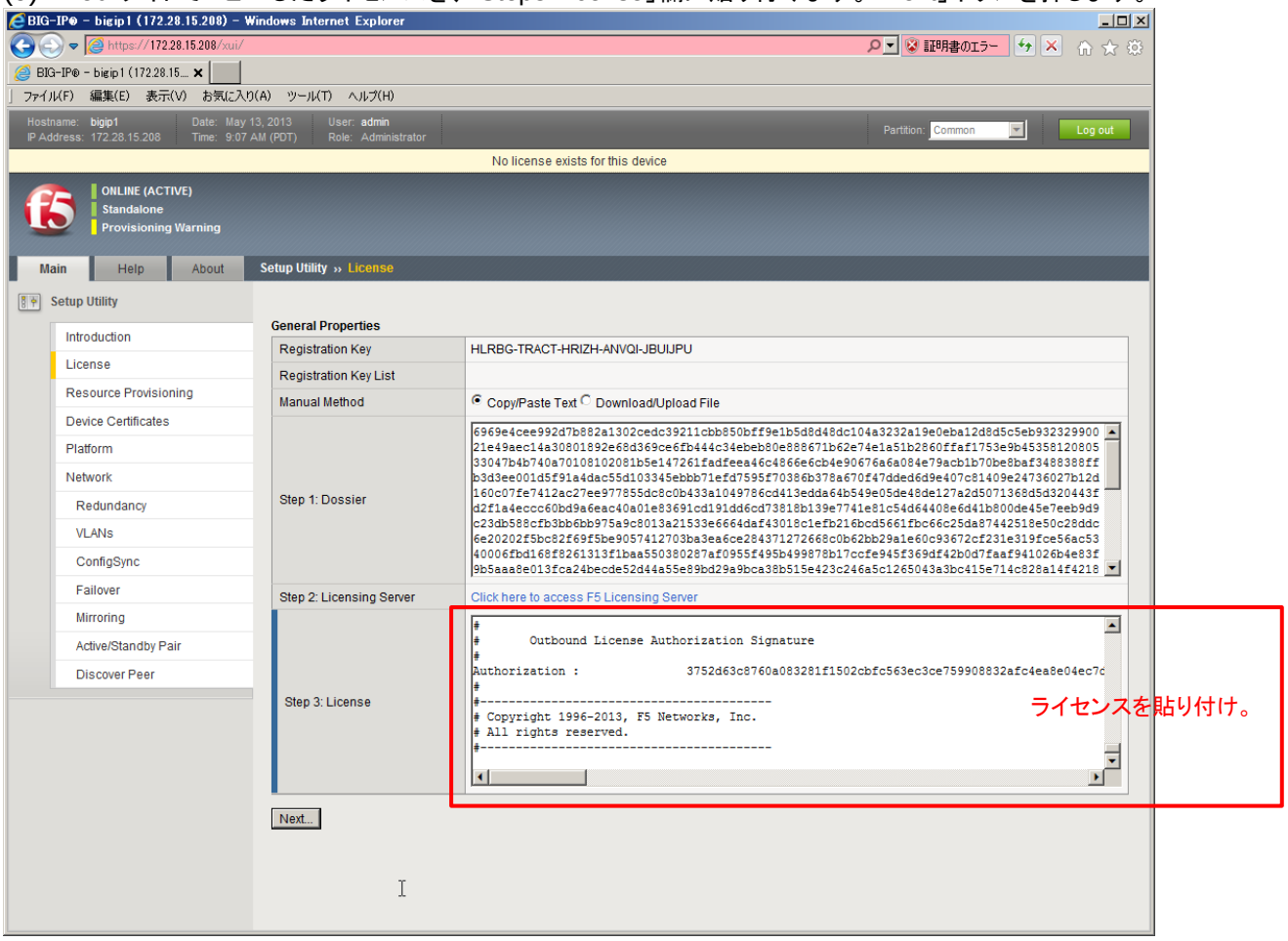


(7) チェックボックスをチェックして「Next」ボタンを押します。

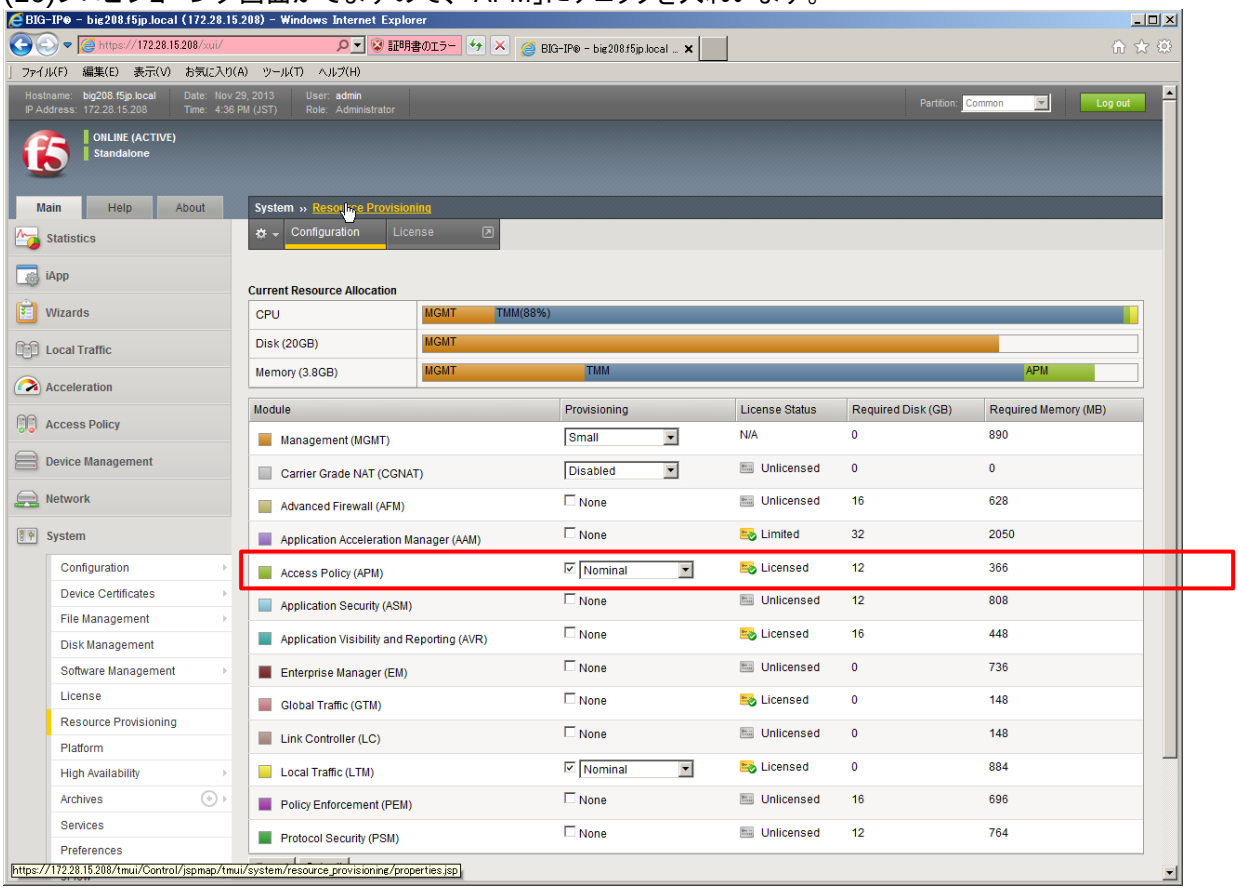


(8) ライセンスキーが表示されるので、全てをコピー(またはファイルをダウンロード)します。

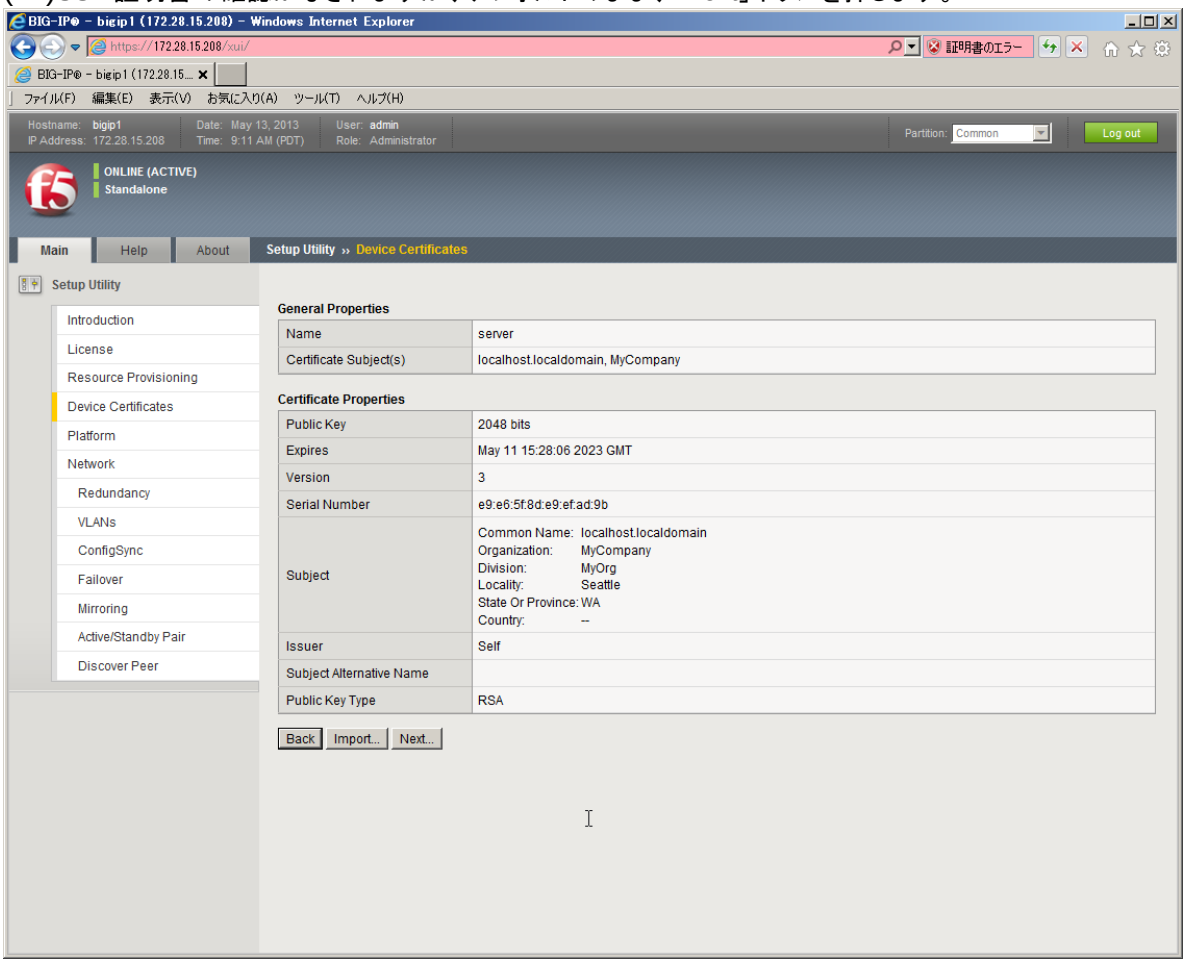
(9) Web サイトでコピーしたライセンスを、「Step3:License」欄に貼り付けます。「Next」ボタンを押します。



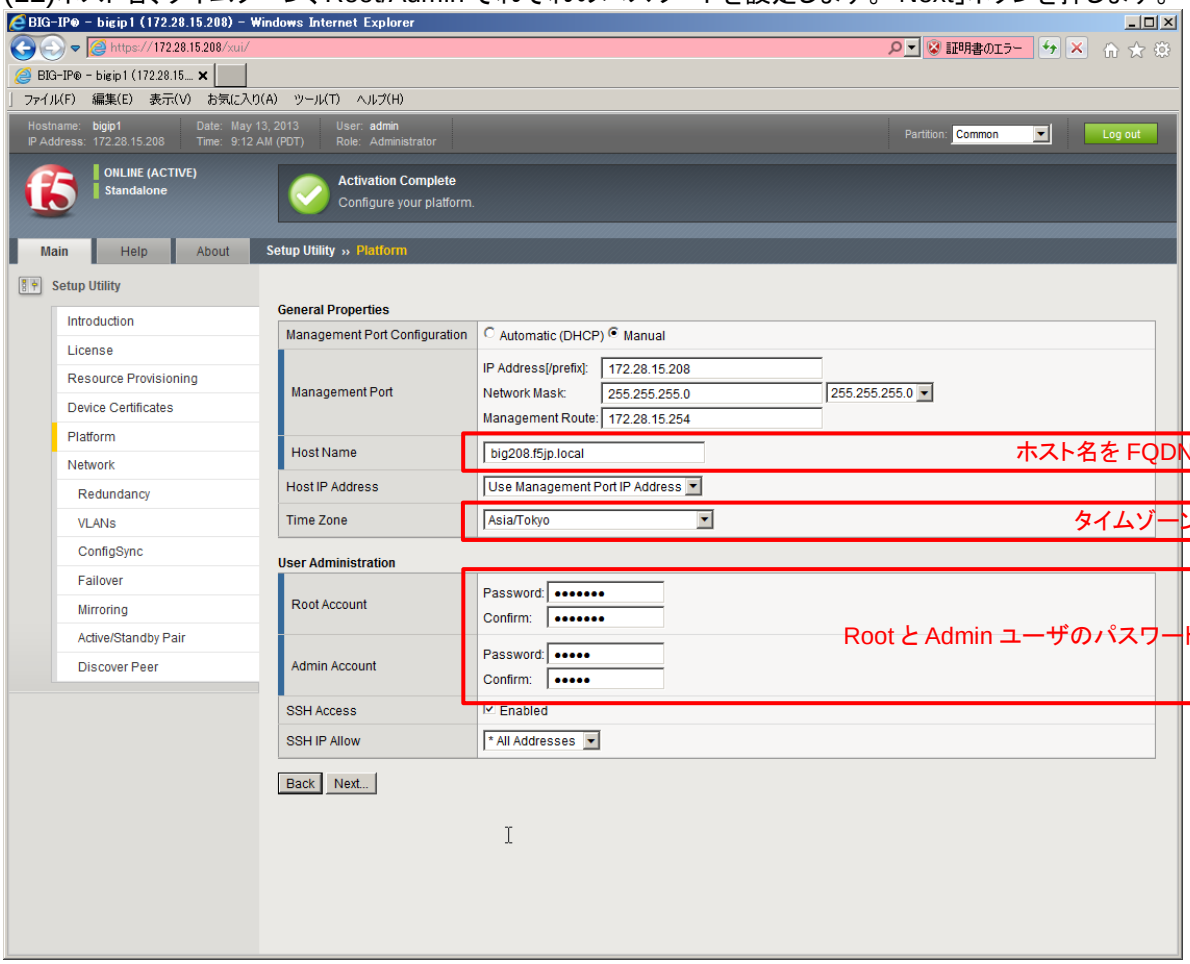
(10)プロビジョニング画面がでますので、「APM」にチェックを入れいます。



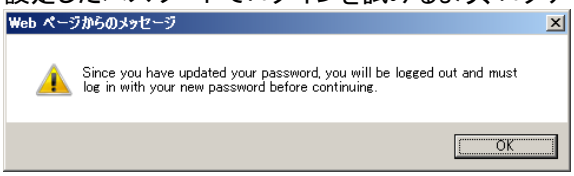
(11)SSL 証明書の確認がなされますが、デフォルトのまま、「Next」ボタンを押します。



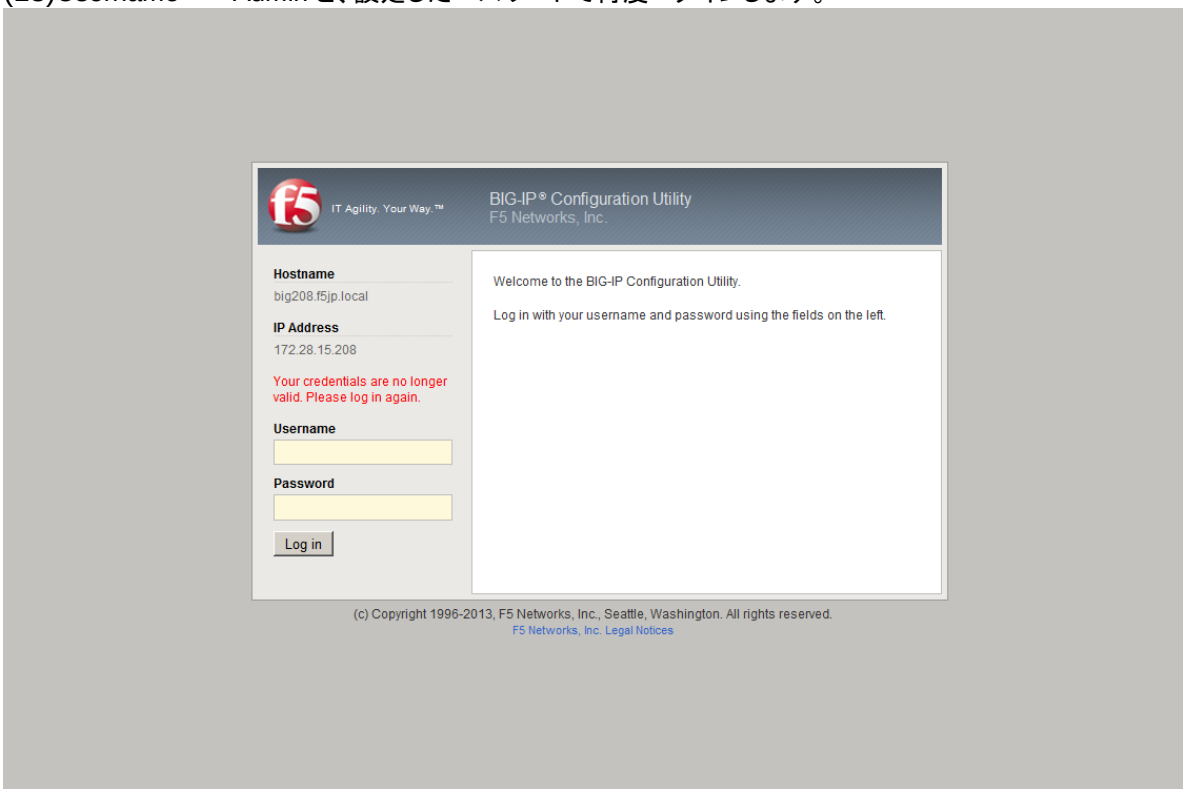
(12)ホスト名、タイムゾーン、Root/Admin それぞれのパスワードを設定します。「Next」ボタンを押します。



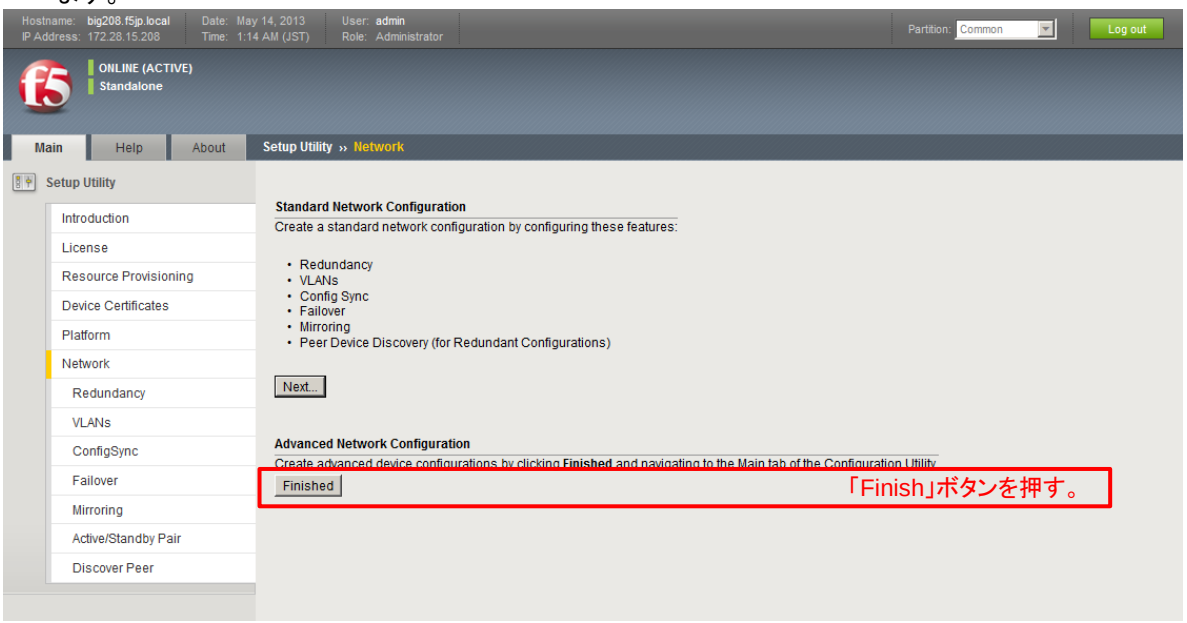
設定したパスワードでログインを試みるよう、ログアウト→ログインするように指示があります。「OK」ボタンを押します。



(13)Username ＝ Admin と、設定したパスワードで再度ログインします。



(14)この後、Standard Network Configuration の「Next」を押すことでウィザード形式にて冗長化も含めた設定が可能ですが、ここではスタンドアローン構成にするため、Advanced Network Configuration の「Finished」ボタンを押します。



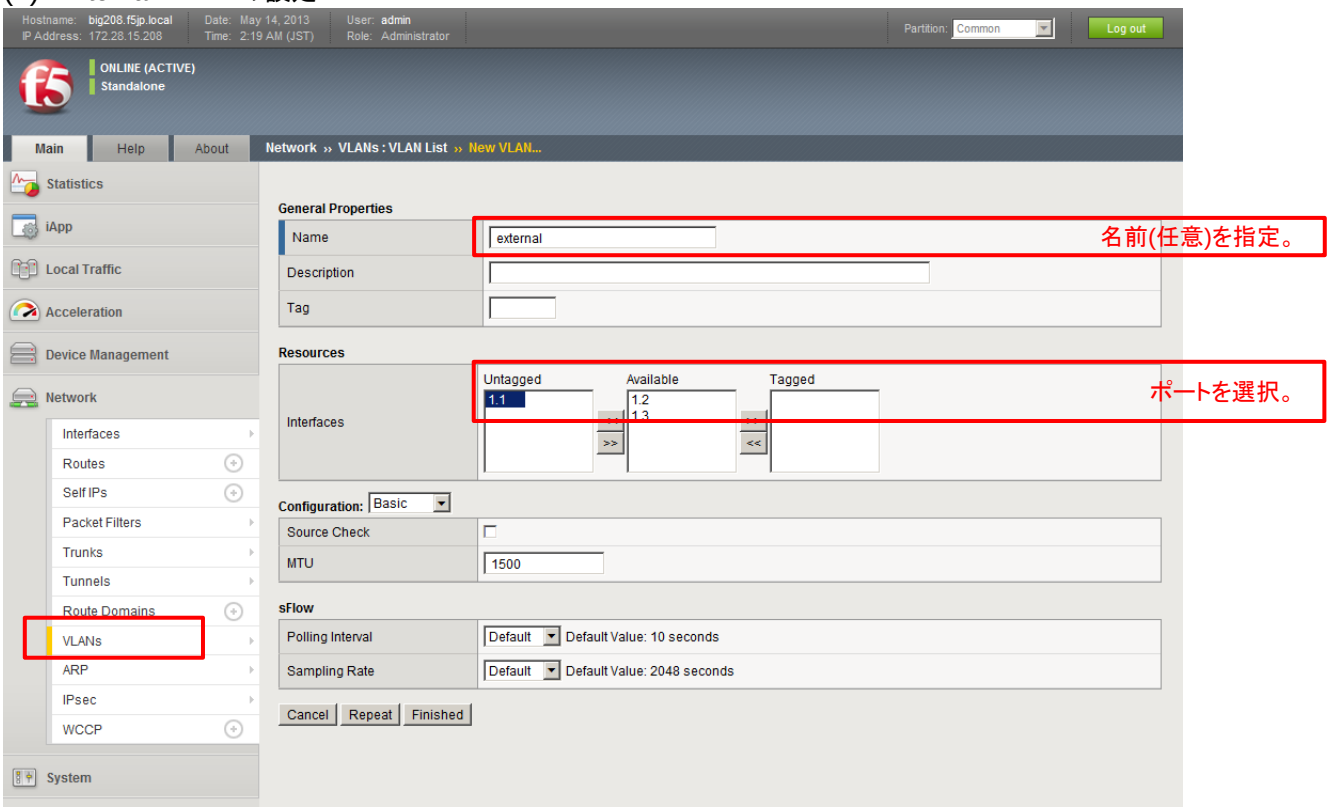
4. ネットワーク設定

VLAN や VLAN インタフェースへの IP 設定（Self-IP 設定）およびルーティング設定を行います。

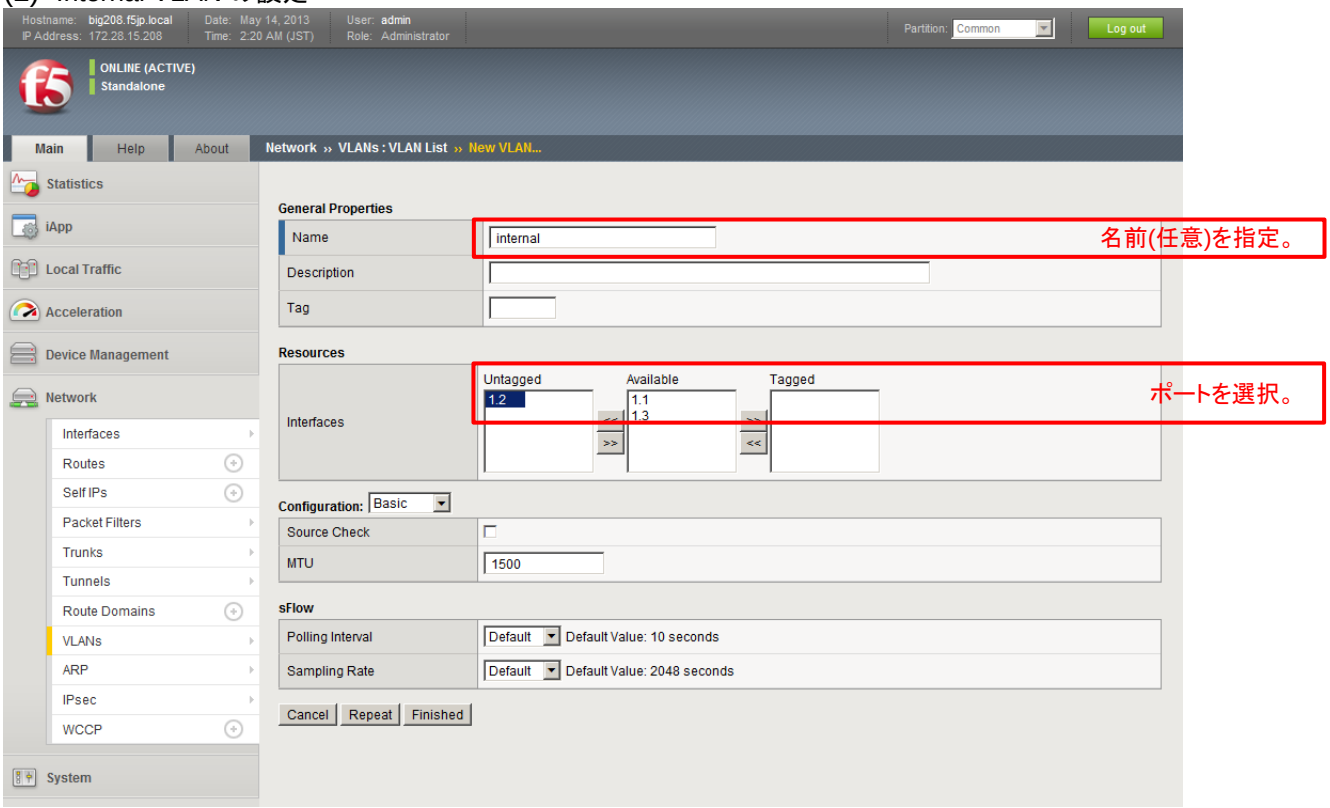
4.1. VLAN の作成

まず、VLAN を作成します。
「Main」メニュー → 「Network」 → 「VLAN」で表示された画面の右上にある「Create」ボタンを押します。

(1) External VLAN の設定



(2) Internal VLAN の設定

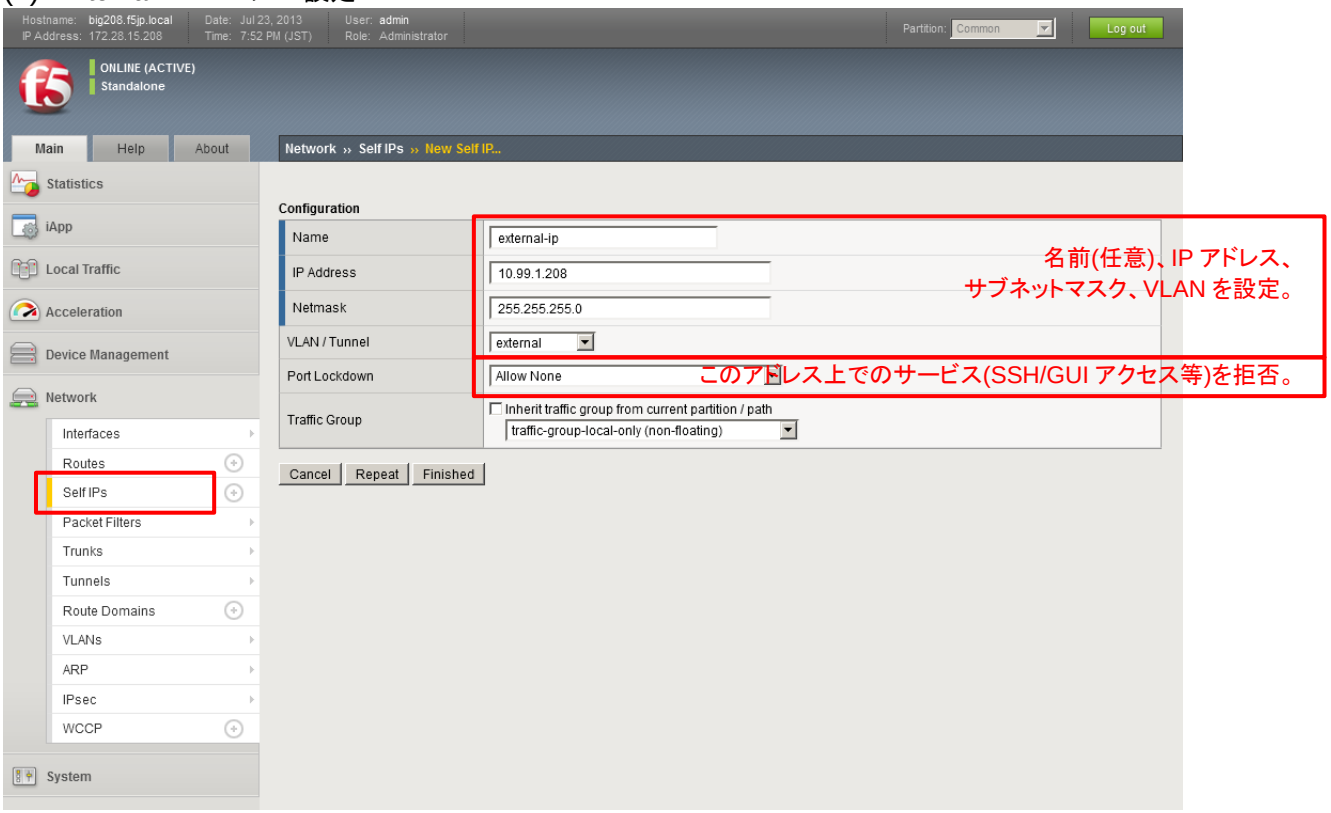


4.2. Self IP の設定

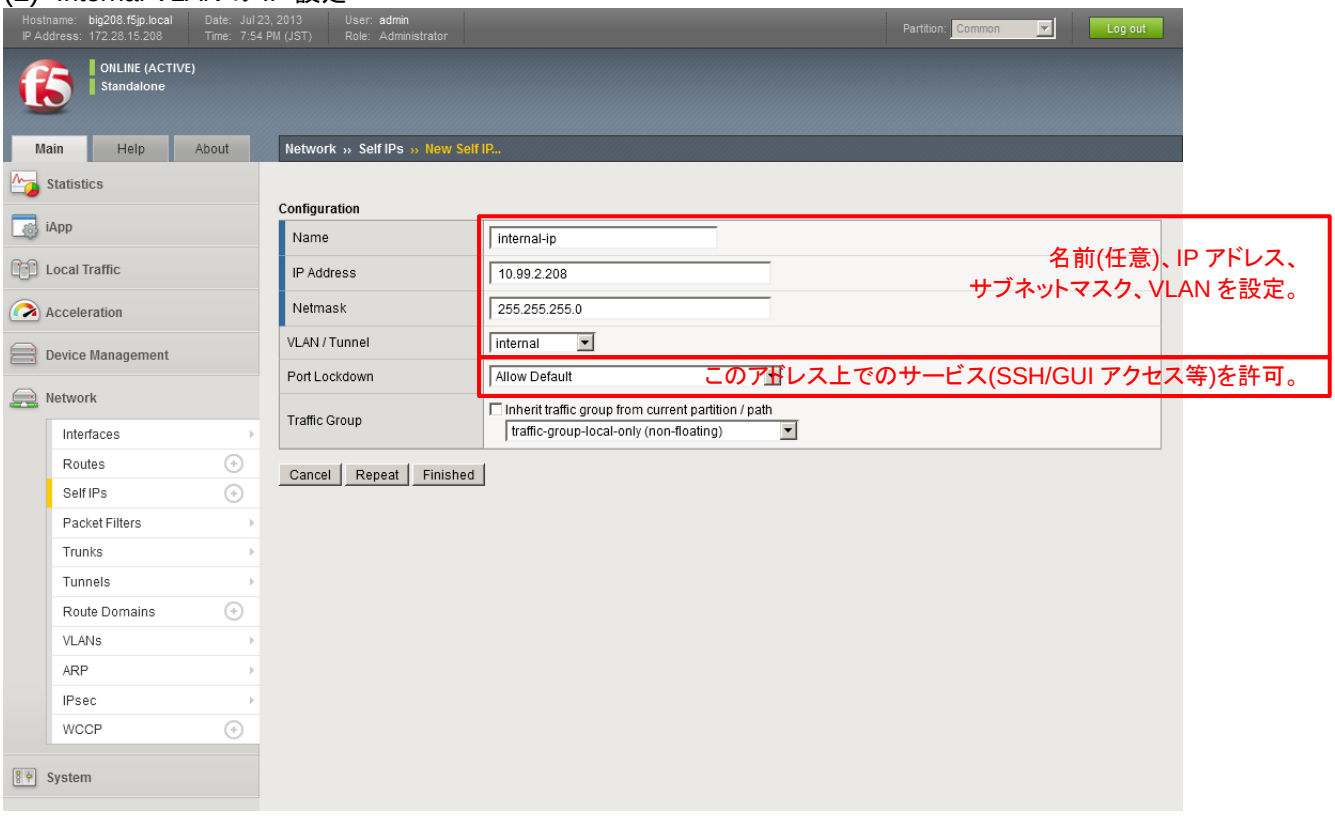
BIG-IP に設定した VLAN それぞれに対して、IP アドレスを設定していきます。
BIG-IP 自身に設定する IP アドレスを、Self IP と呼びます。

「Main」メニュー → 「Network」 → 「Self IPs」で表示された画面の右上にある「Create」ボタンを押します。

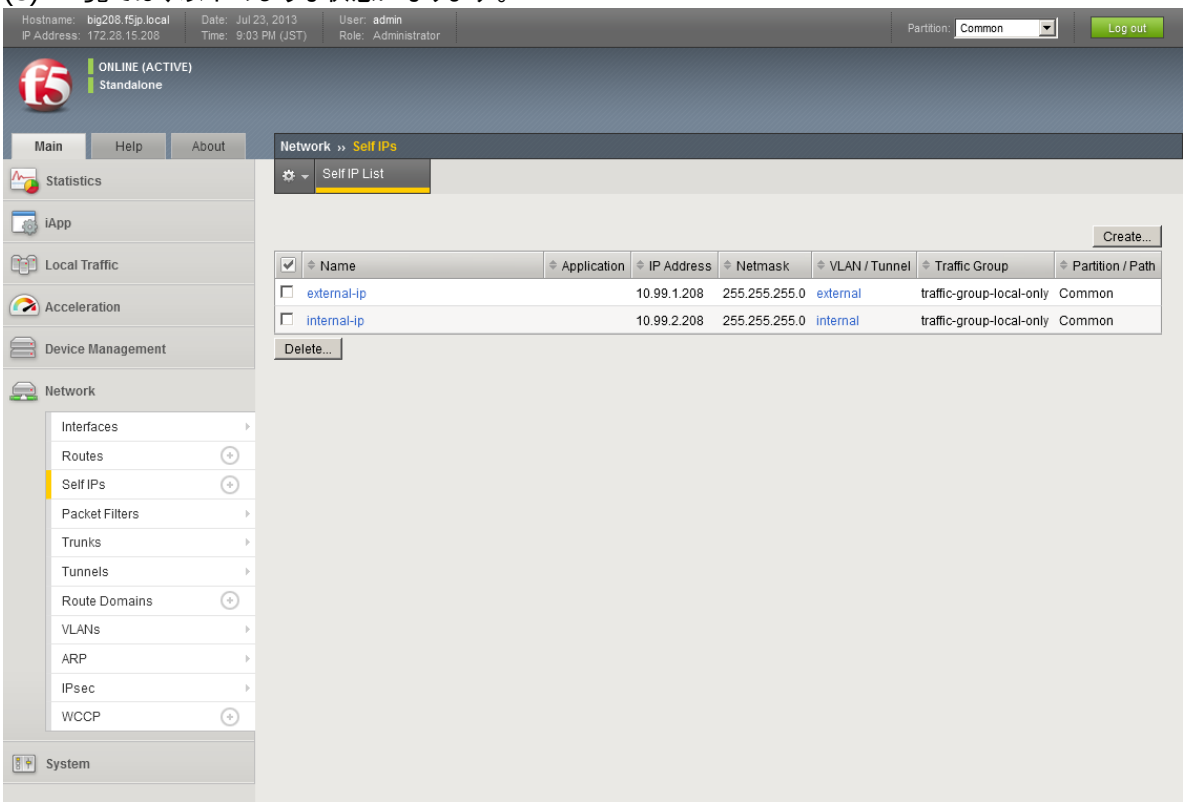
(1) External VLAN の IP 設定



(2) Internal VLAN の IP 設定



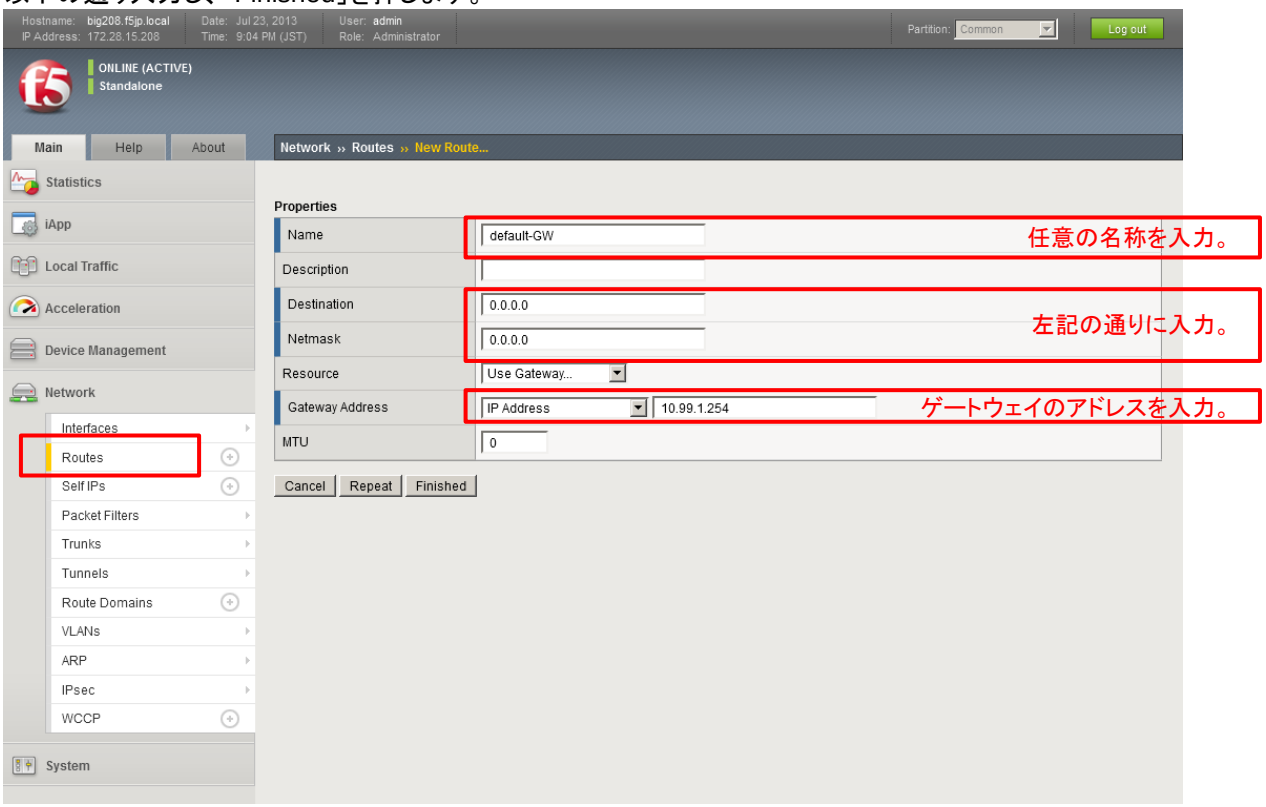
(3) 一覧では、以下のような状態になります。



4.3. ルーティングの設定

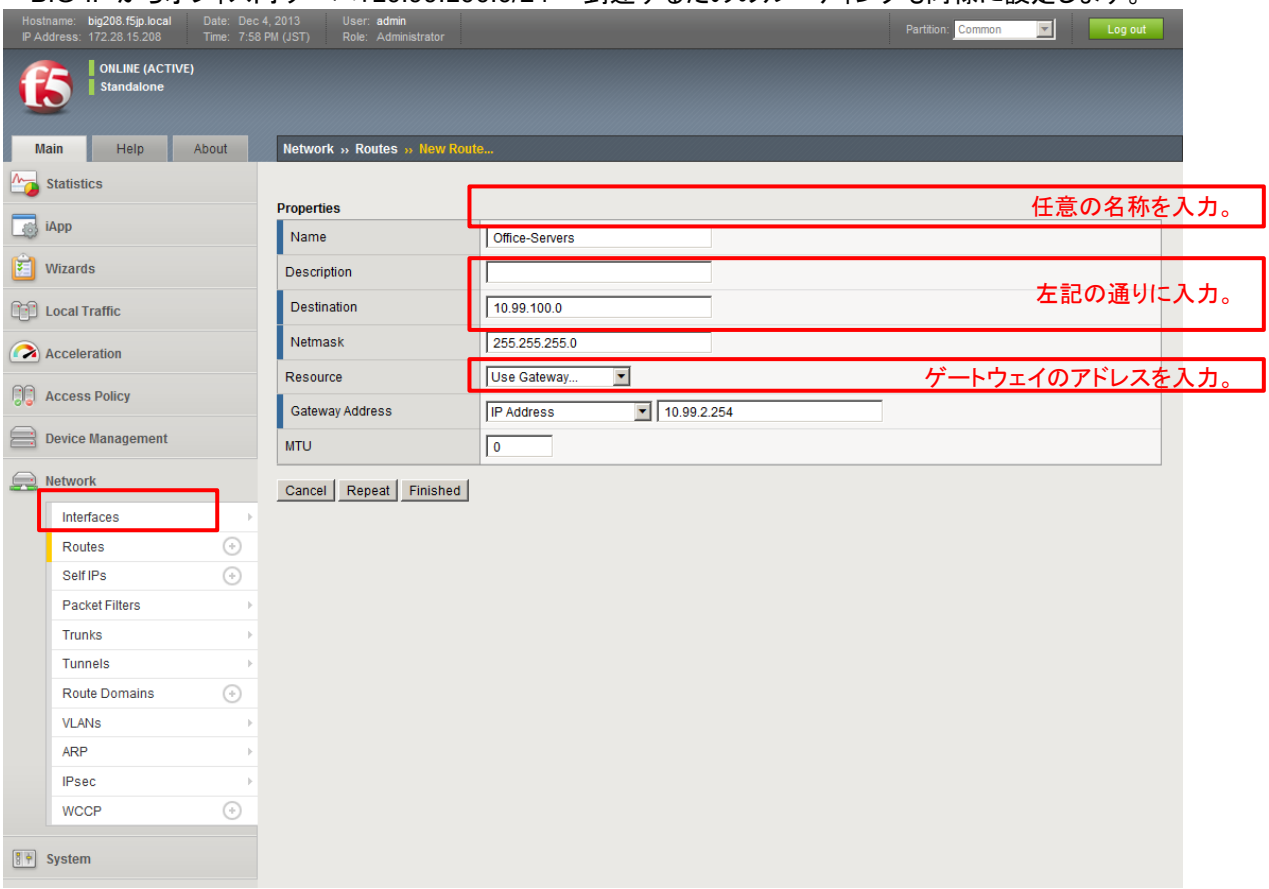
4.3.1. デフォルトゲートウェイの設定

「Main」メニュー → 「Network」 → 「Routes」で表示された画面の右上にある「Add」ボタンを押します。以下の通り入力し、「Finished」を押します。



4.3.2. オフィス内サーバへのルーティング設定

BIG-IP からオフィス内サーバ：10.99.100.0/24 へ到達するためのルーティングも同様に設定します。

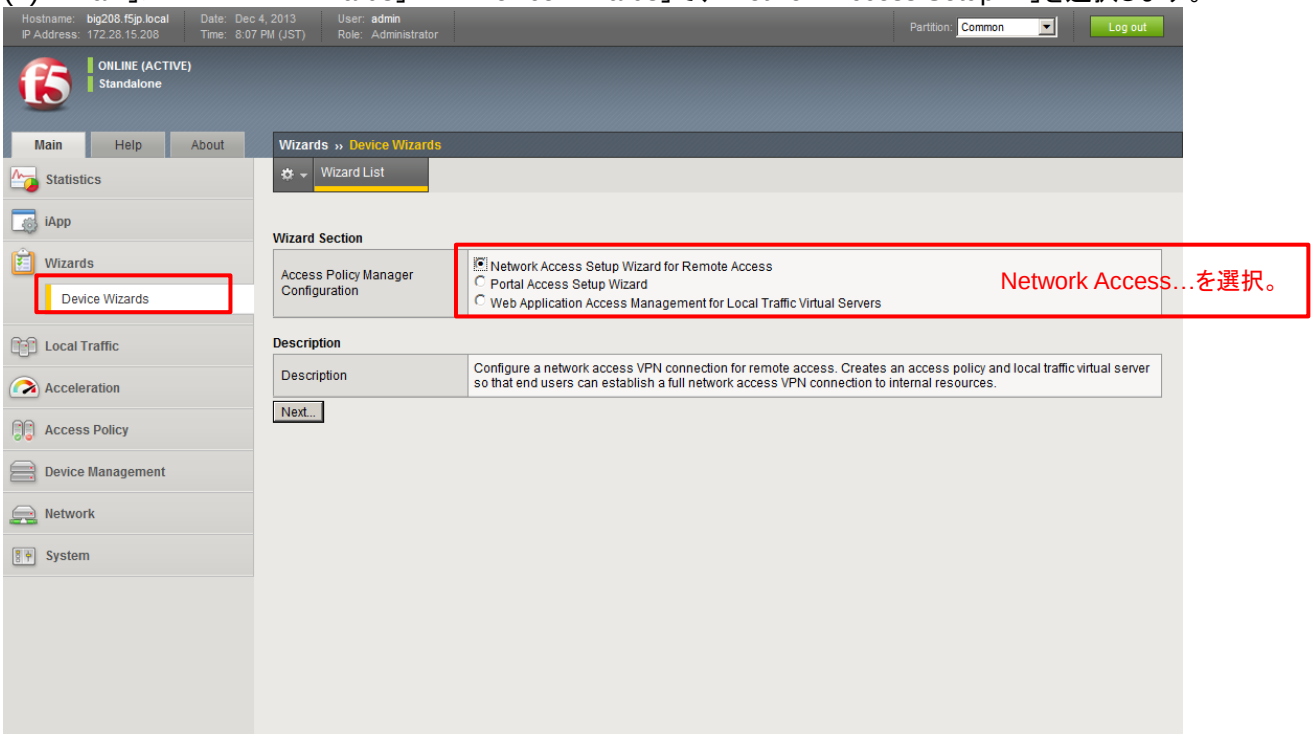


5. 初級編

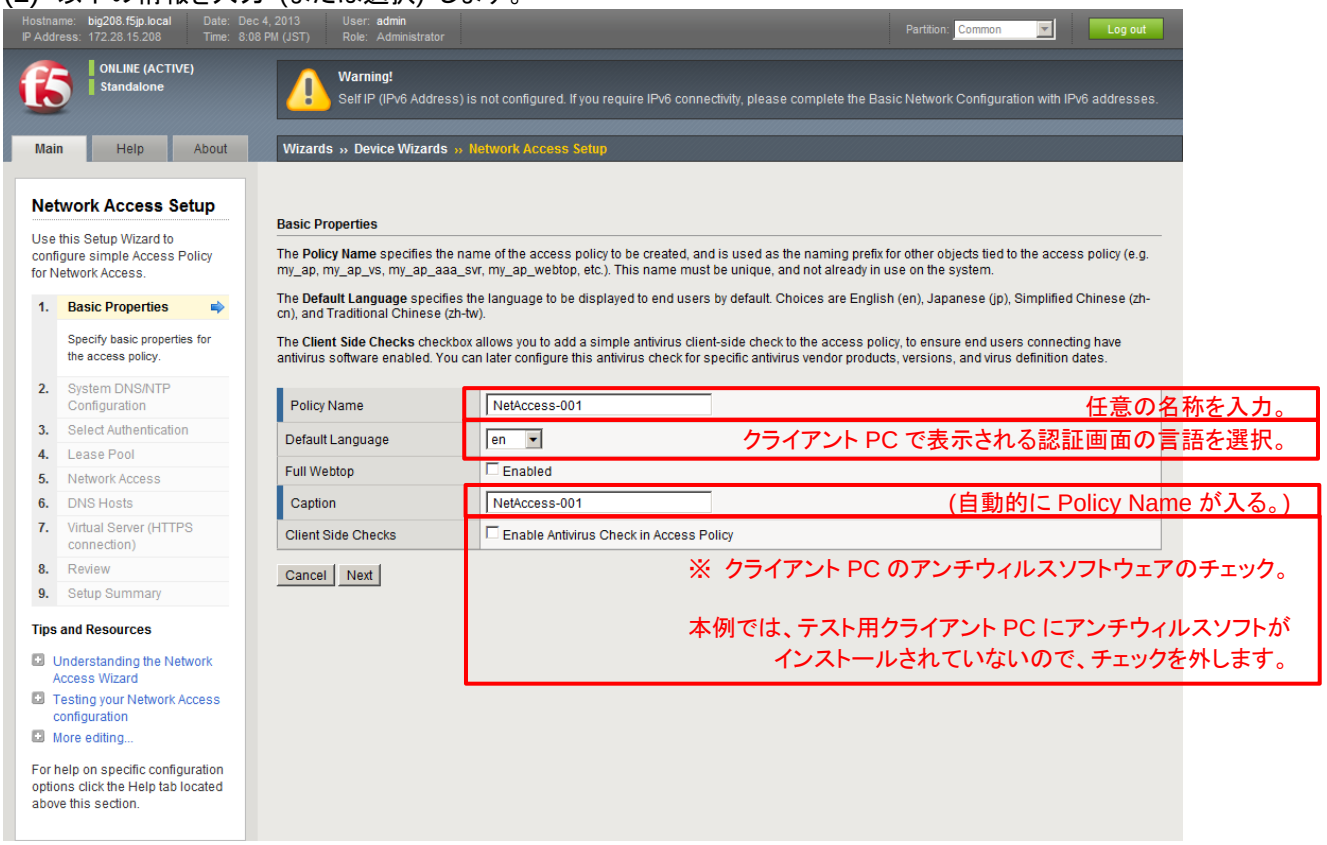
5.1. ウィザードを使って設定する方法

ウィザード(Wizards)を利用すると、ネットワークアクセス設定に必要な情報が一通りそろっていれば、簡単に 10 分程度で設定することができます。

(1)「Main」メニュー →「Wizards」→「Device Wizards」で、「Network Access Setup …」を選択します。

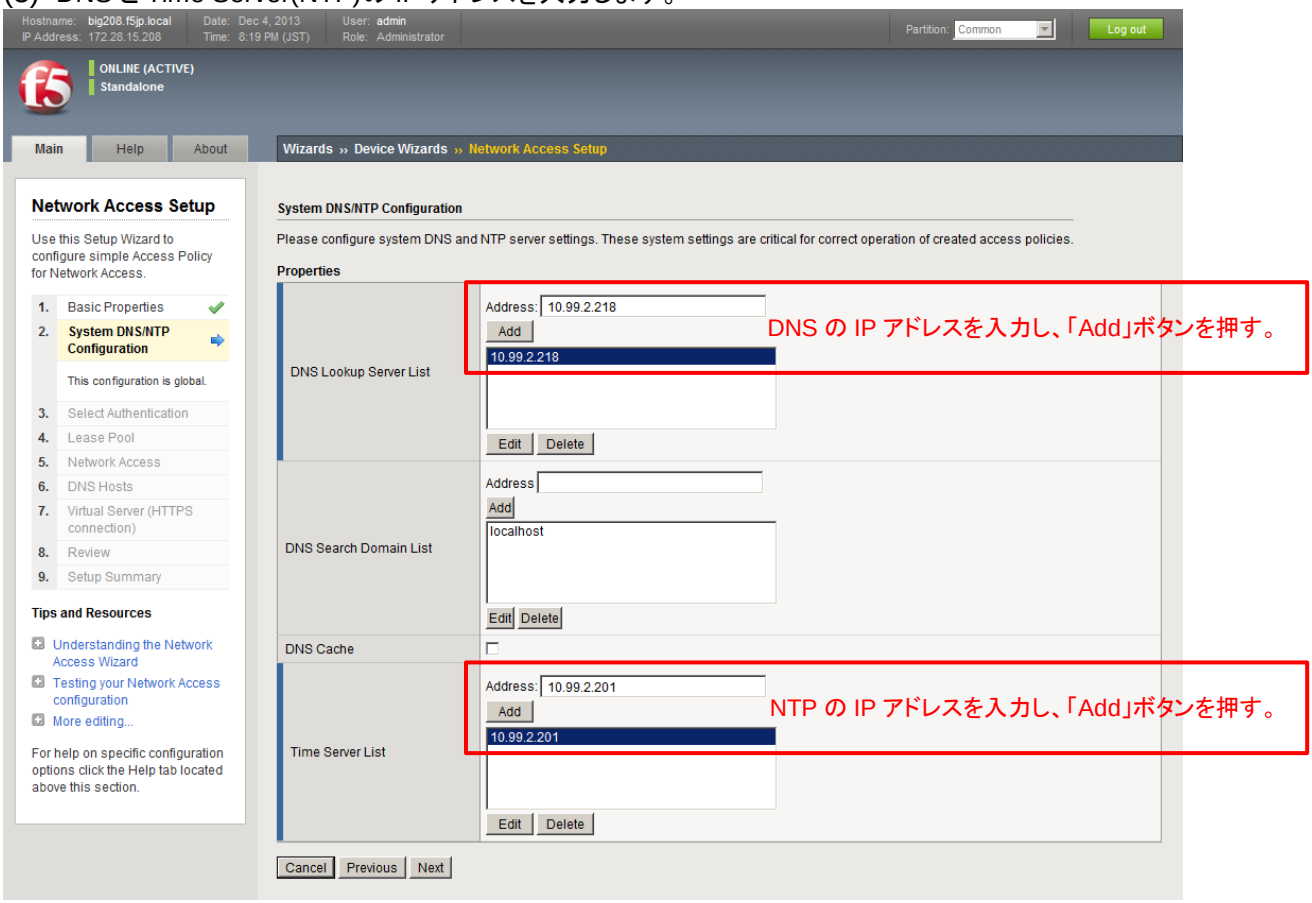


(2) 以下の情報を入力 (または選択) します。

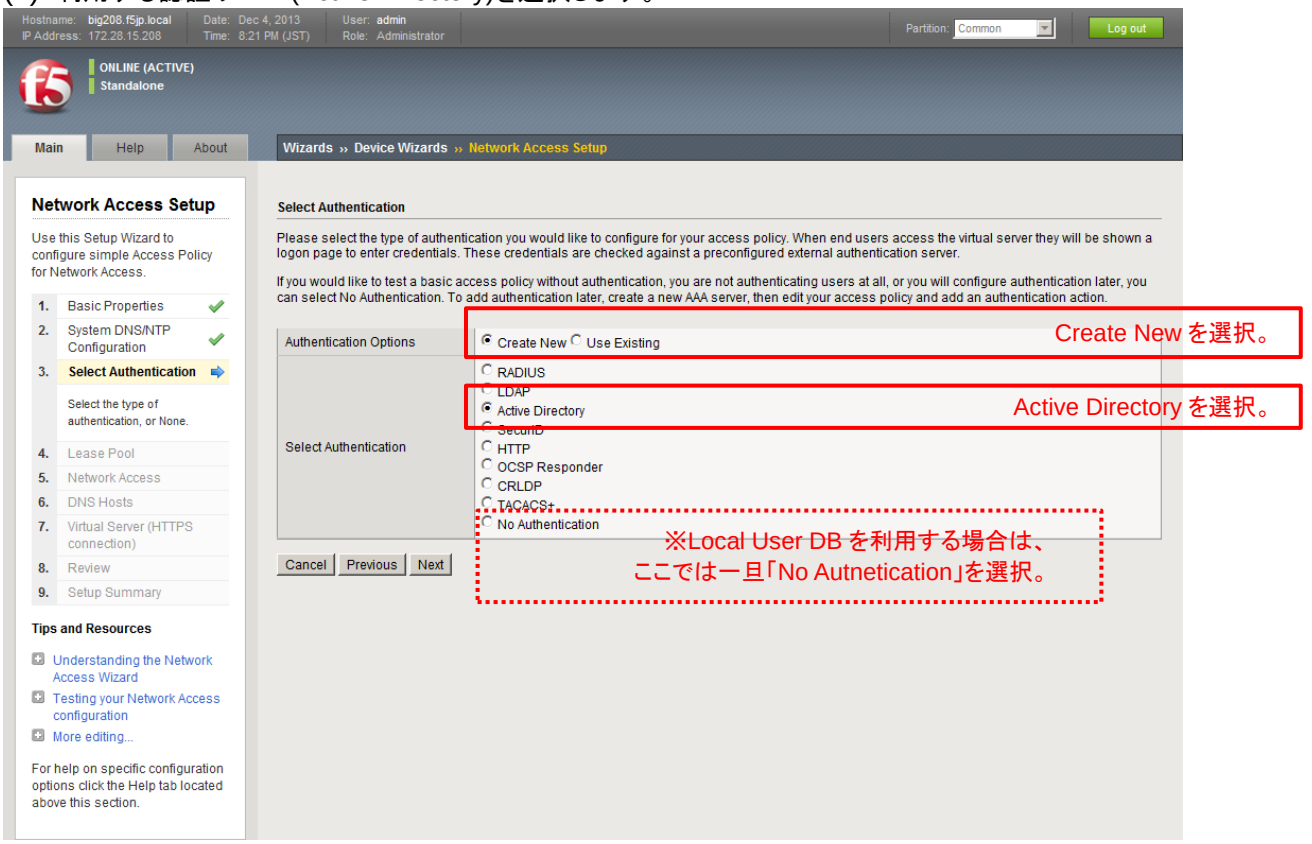


※このチェックボックスを有効にしておくことで、クライアント PC 内にインストールされているアンチウィルスソフトウェアのチェックが行われます。詳しくは、 [参考]アンチウィルスソフトウェアのチェックについて を参照ください。

(3) DNS と Time Server(NTP)の IP アドレスを入力します。

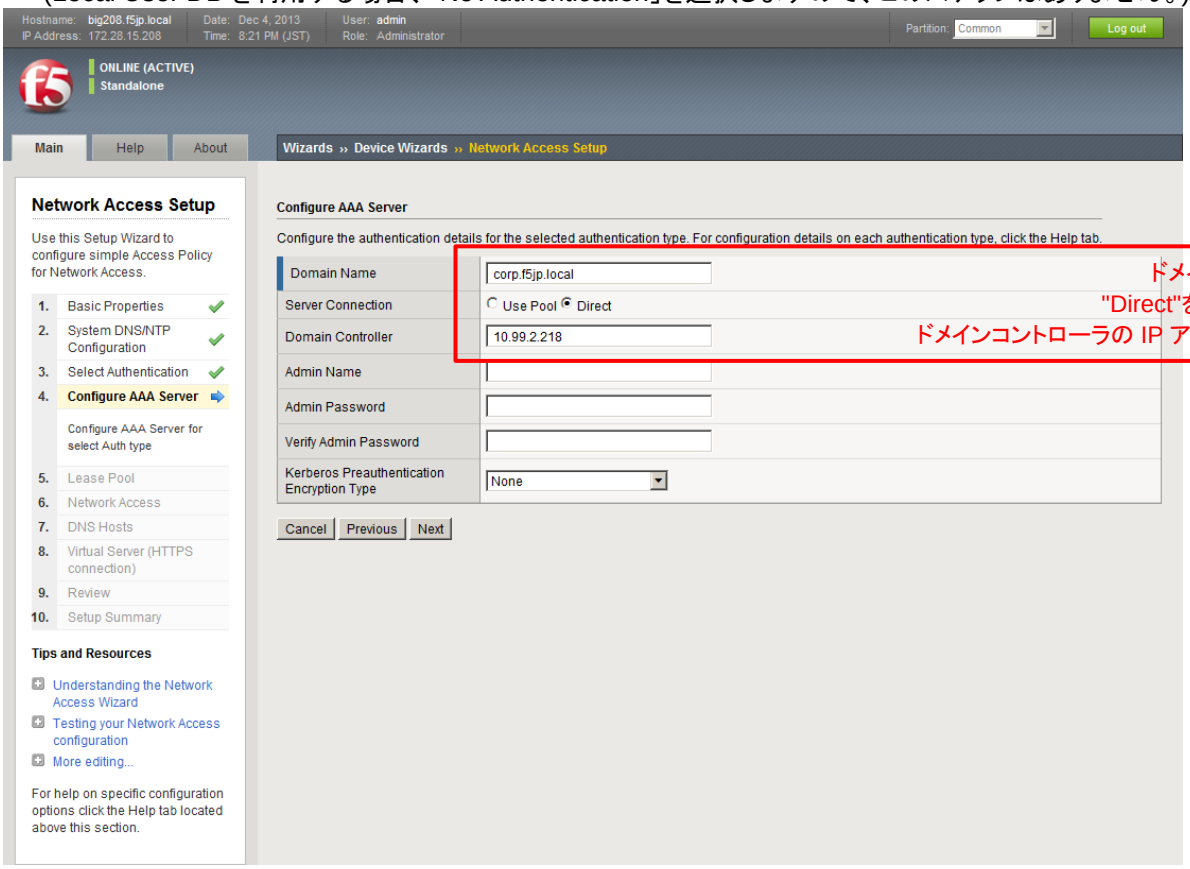


(4) 利用する認証サーバ(Active Directory)を選択します。



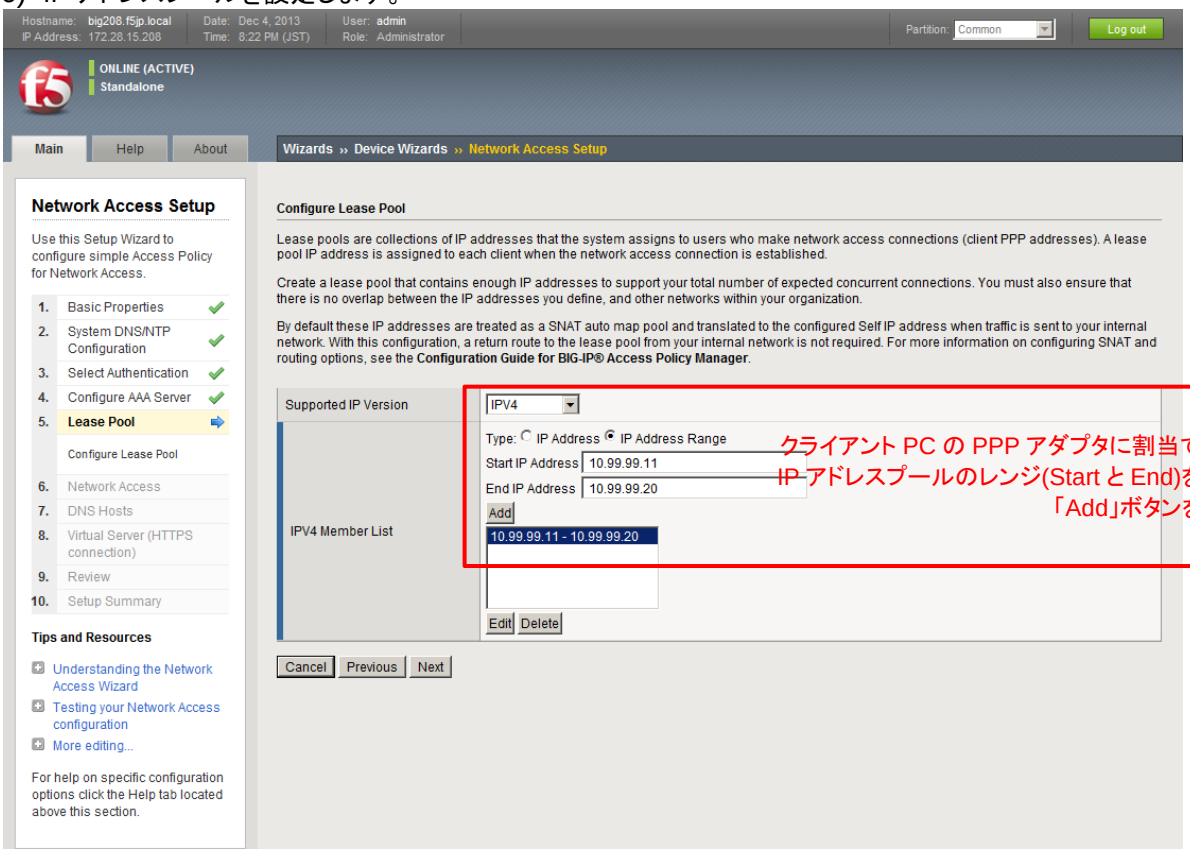
※Local User DB を使いたい場合、ウィザード形式には Local User DB を選択する項目が存在しない(V11.4.1)ので、ウィザード設定完了後に設定変更を行います。よって、ここでは一時的に「No Authentication」を選択します。

(5) Active Directory による認証に必要な情報を入力します。
(Local User DB を利用する場合、「No Authentication」を選択しますので、このステップはありません。)



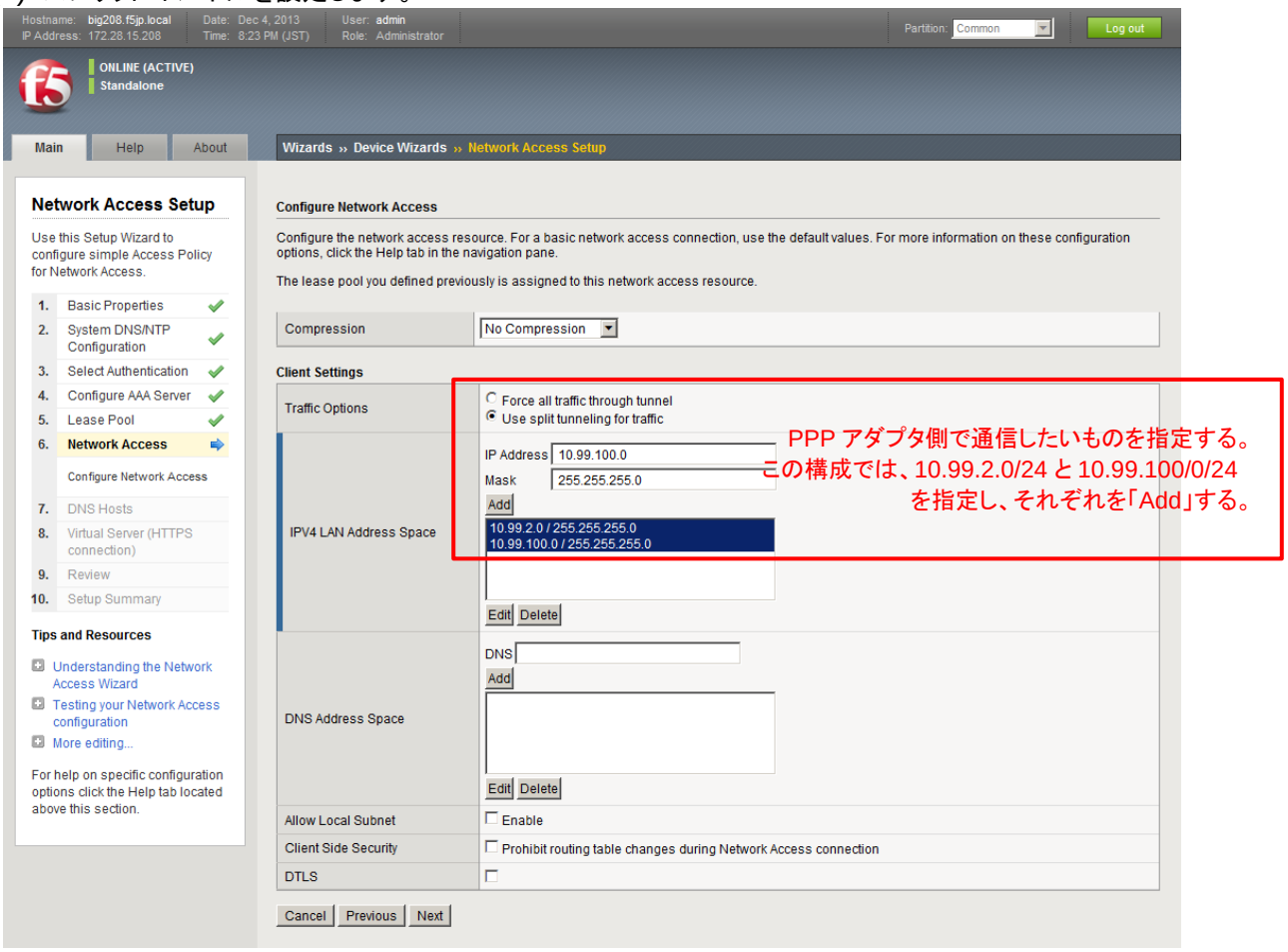
ドメイン名。
"Direct"を選択。
ドメインコントローラの IP アドレス。

(6) IP アドレスプールを設定します。



クライアント PC の PPP アダプタに割当てられる
IP アドレスプールのレンジ(Start と End)を入力。
「Add」ボタンを押す。

(7) スプリット・トンネルを設定します。

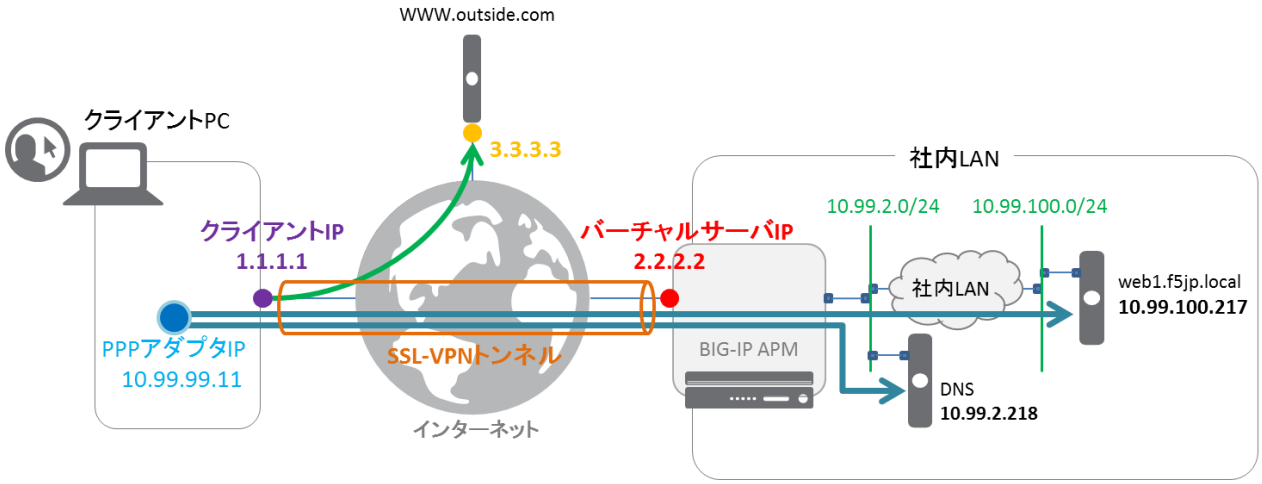


＜スプリット・トンネルとは＞

SSL-VPN トンネルを使う通信と、使わない通信を分けたいときにつかいます。

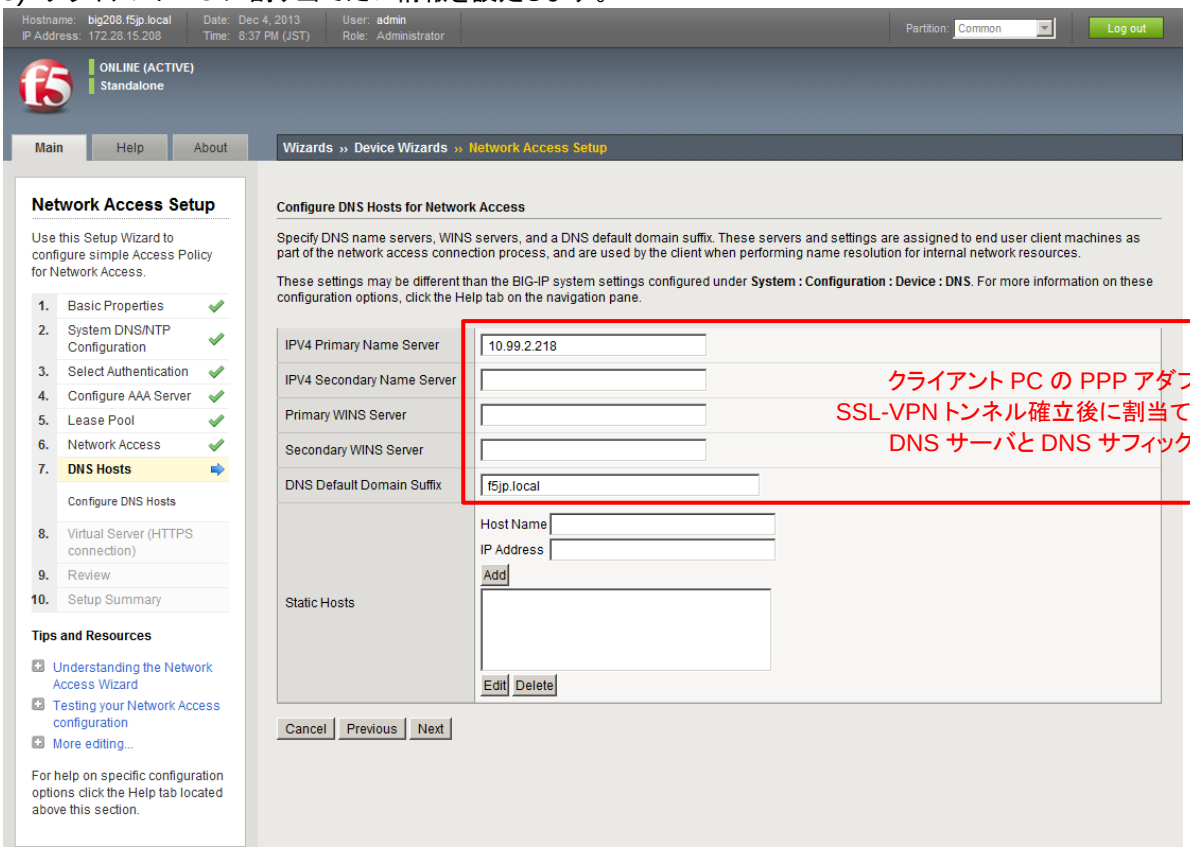
例えば、以下のような要件があったとします。
① 社内 LAN のサーバは、10.99.2.0/24 と 10.99.100.0/24 に設置されているので、それらは SSL-VPN トンネルを使いたい。
② しかし、同時にインターネットも使いたい。

このような要件を実現するのがスプリット・トンネルです。



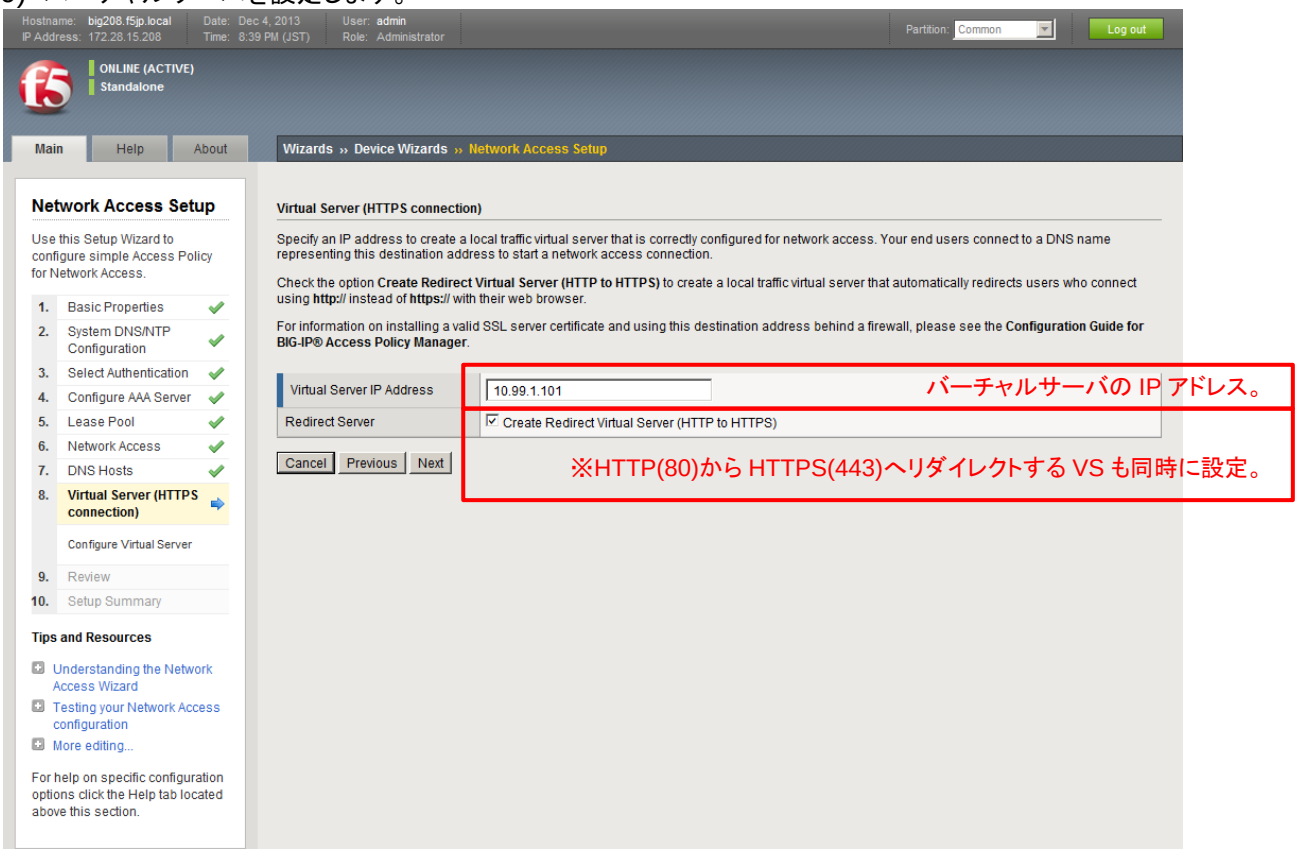
「Use split Tunnelling for Traffic」を選択し、トンネルに向かわせたいネットワーク帯(10.99.2.0/24, 10.99.100.0/24)を指定することで、そのネットワークだけは SSL-VPN トンネルを通り、それ以外は、クライアント IP(上図の 1.1.1.1)を使ってインターネット(上図 3.3.3.3 の web サーバへの通信)を使う、ということが可能になります。

(8) クライアント PC に割り当てたい情報を設定します。



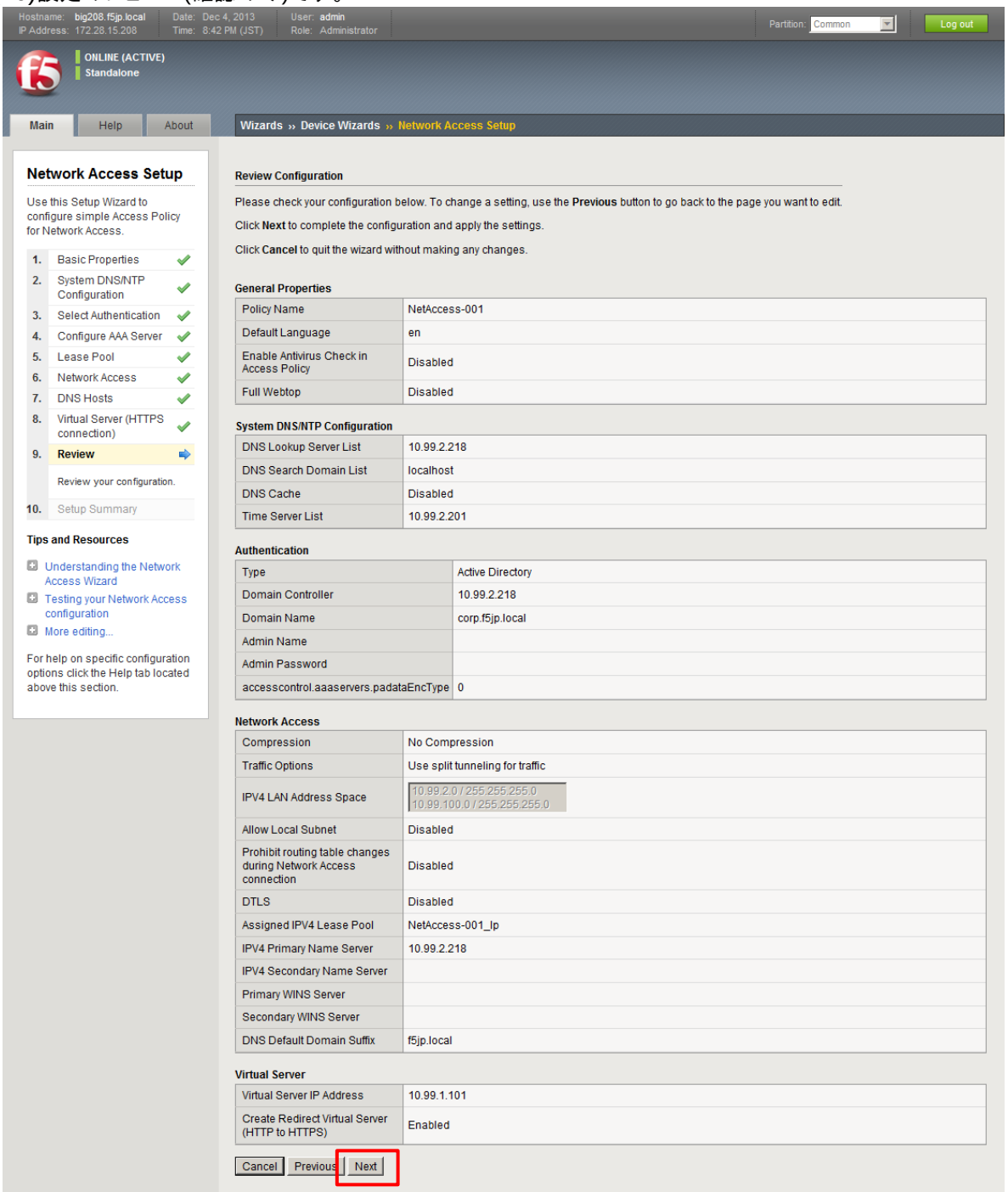
※ここに指定した DNS サフィックス宛の通信(f5jp.local)は、この DNS サーバを利用する、という設定です。

(9) バーチャルサーバを設定します。

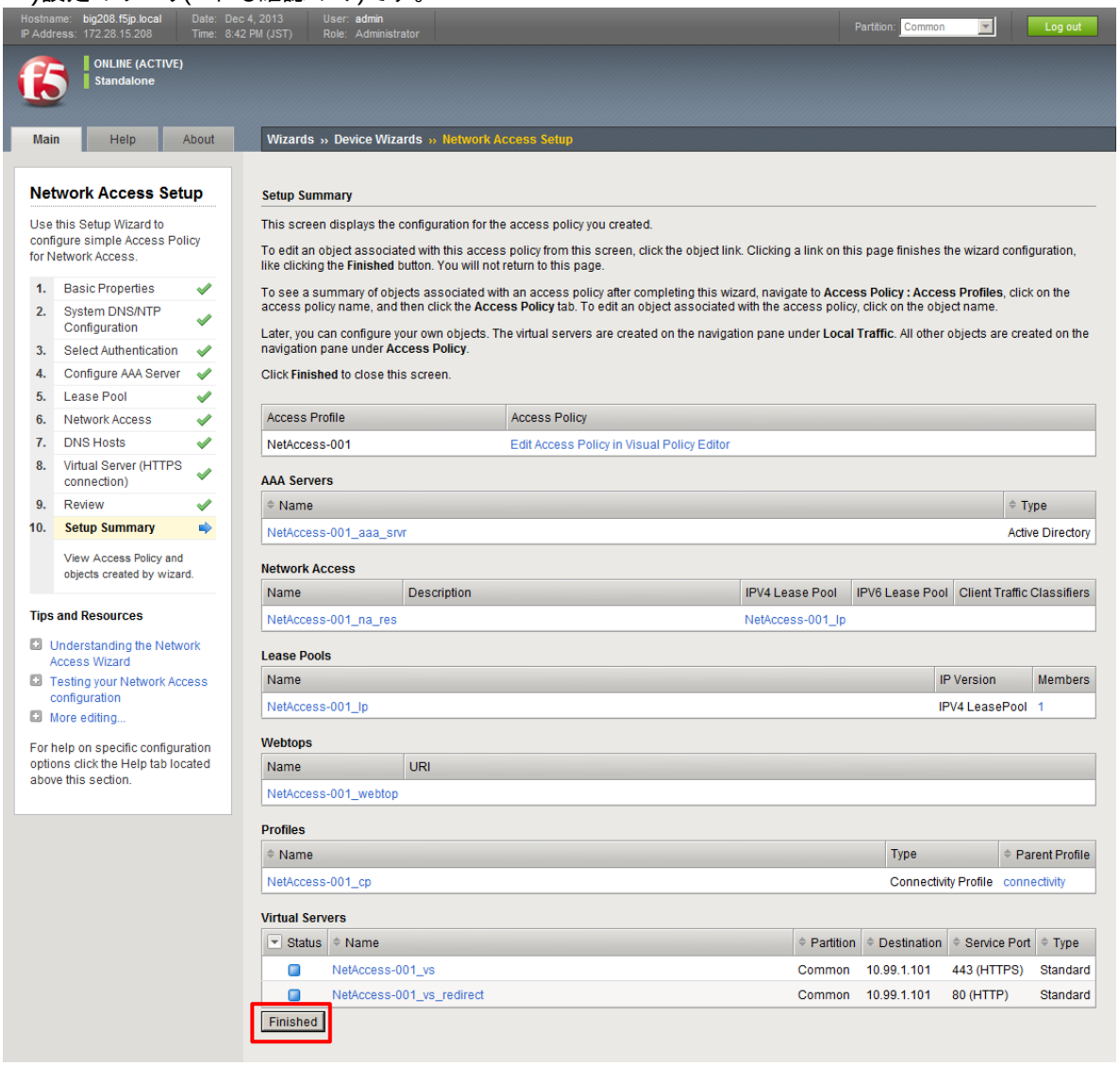


※このチェックボックスを有効にすることで、HTTP(80)で Virtual Server へアクセスしても、自動的に HTTPS(443)へリダイレクトする Virtual Server が生成されます。不要であれば、チェックを外してください。

(10)設定のレビュー(確認のみ)です。



(11)設定のサマリ(これも確認のみ)です。



以上でネットワークアクセス設定は完了です。

5.2. クライアントからのアクセス

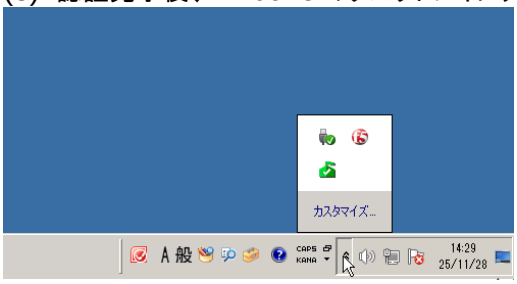
5.2.1. Windows の Web ブラウザからのアクセス

クライアント PC の Web ブラウザから、設定した Virtual Server へアクセスします。
Windows 7 + Internet Explorer を使った場合の例です。

(1) 初アクセス時には、SSL-VPN クライアント用の ActiveX コンポーネントをインストールする必要があります。
インストールするためには、Windows の管理者権限が必要です。

(2) 認証フォーム画面が現れますので Active Directory に登録されているユーザ名とパスワードを入力します。

(3) 認証完了後、Windows のタスクトレイに入ります。



5.2.2. Windows 用 Edge Client ソフトウェアからのアクセス

Windows クライアント用ソフトウェア：Edge Client を利用する手順を以下に示します。

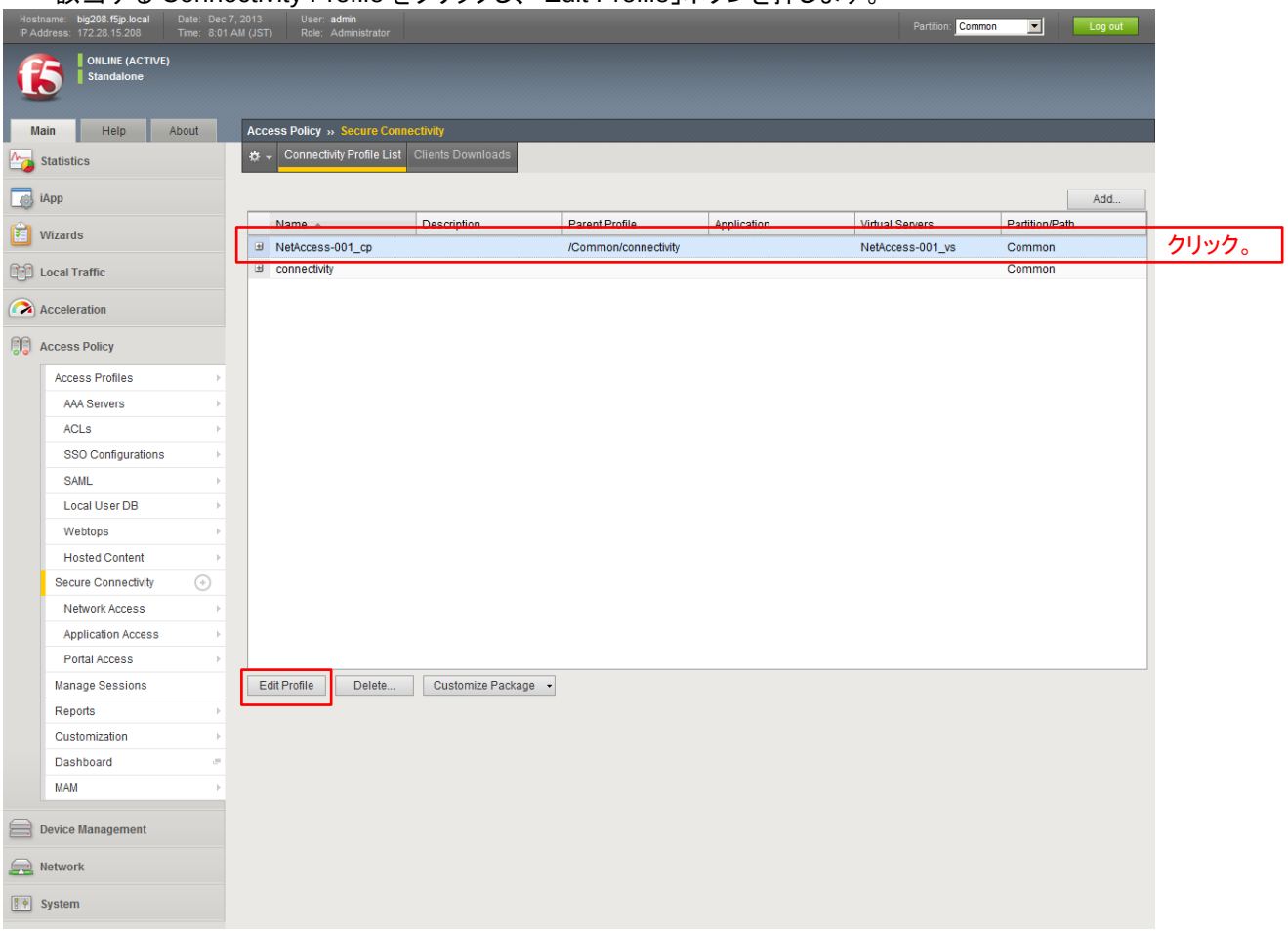
このソフトウェアは、BIG-IP APM からクライアント PC (Windows または Mac) へダウンロードして利用するソフトウェアです。

このソフトウェアは、プロトコルレベルで行っていることは Web ブラウザと同様ですが、Web ブラウザでは実現できない、いくつかの便利な機能を実装しています。

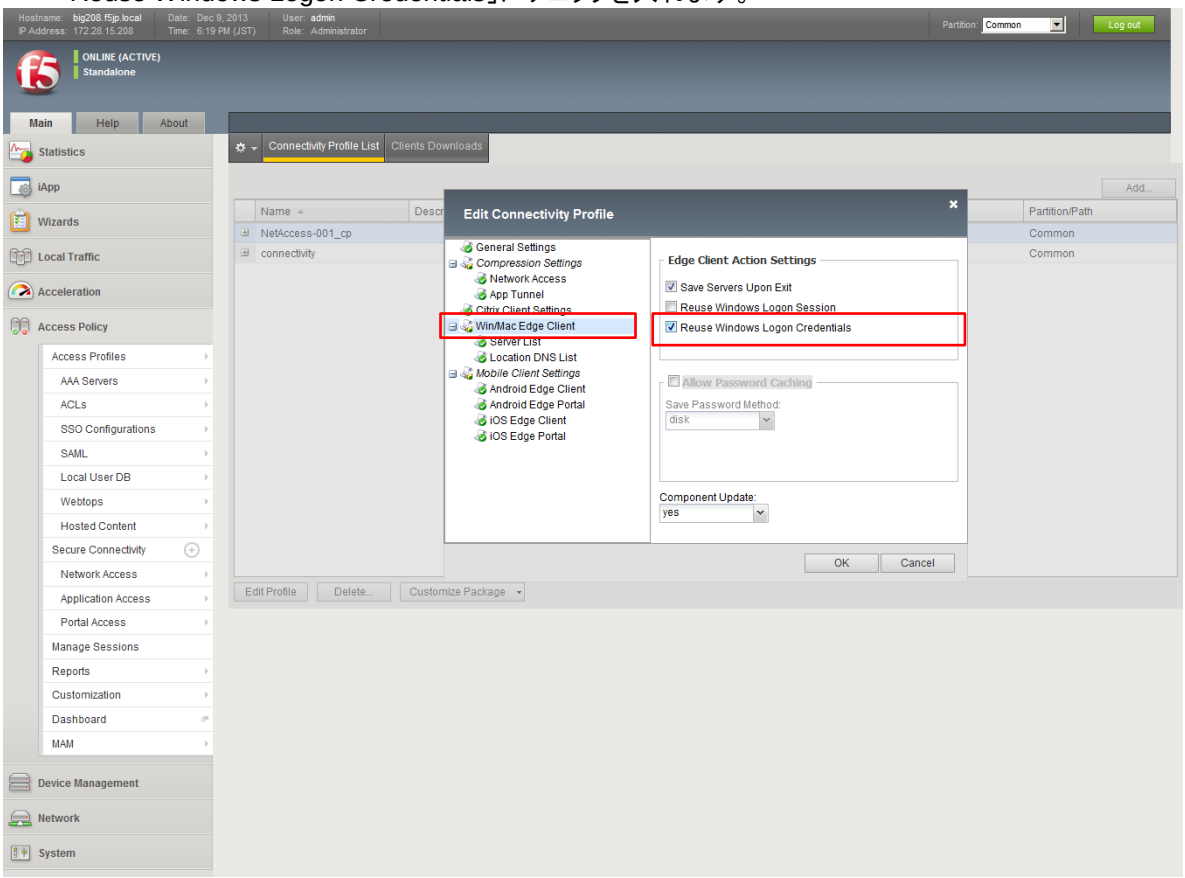
例えば、Windows へのログイン時に利用する ID と Password を使うように Edge Client に設定すると、BIG-IP APM へのログイン時には、ID/Password の入力を求められることなく、自動的に APM へ接続することが可能です。

サンプルとして、以下にその設定方法を示します。

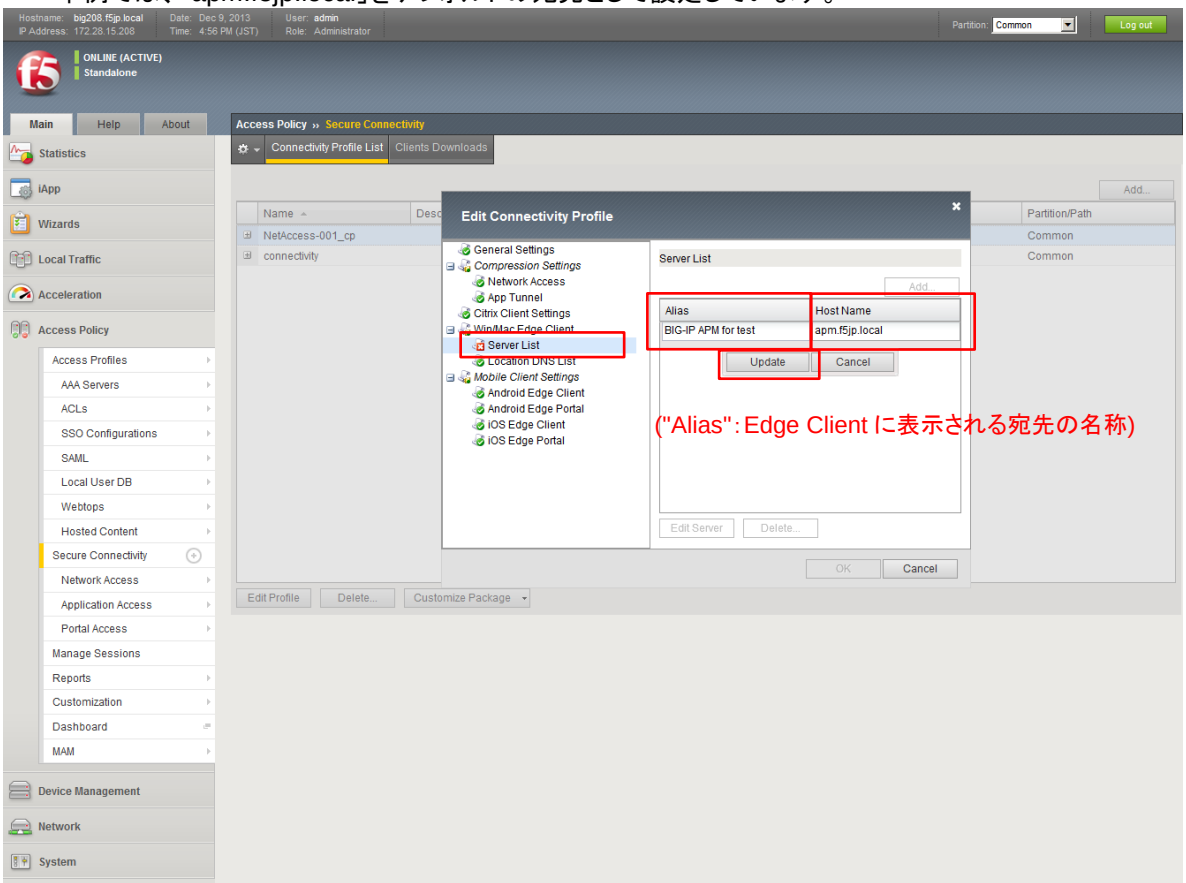
(1) 「Main」メニュー → 「Access Policy」 → 「Secure Connectivity」 で、以下の画面が表示されます。
該当する Connectivity Profile をクリックし、「Edit Profile」ボタンを押します。



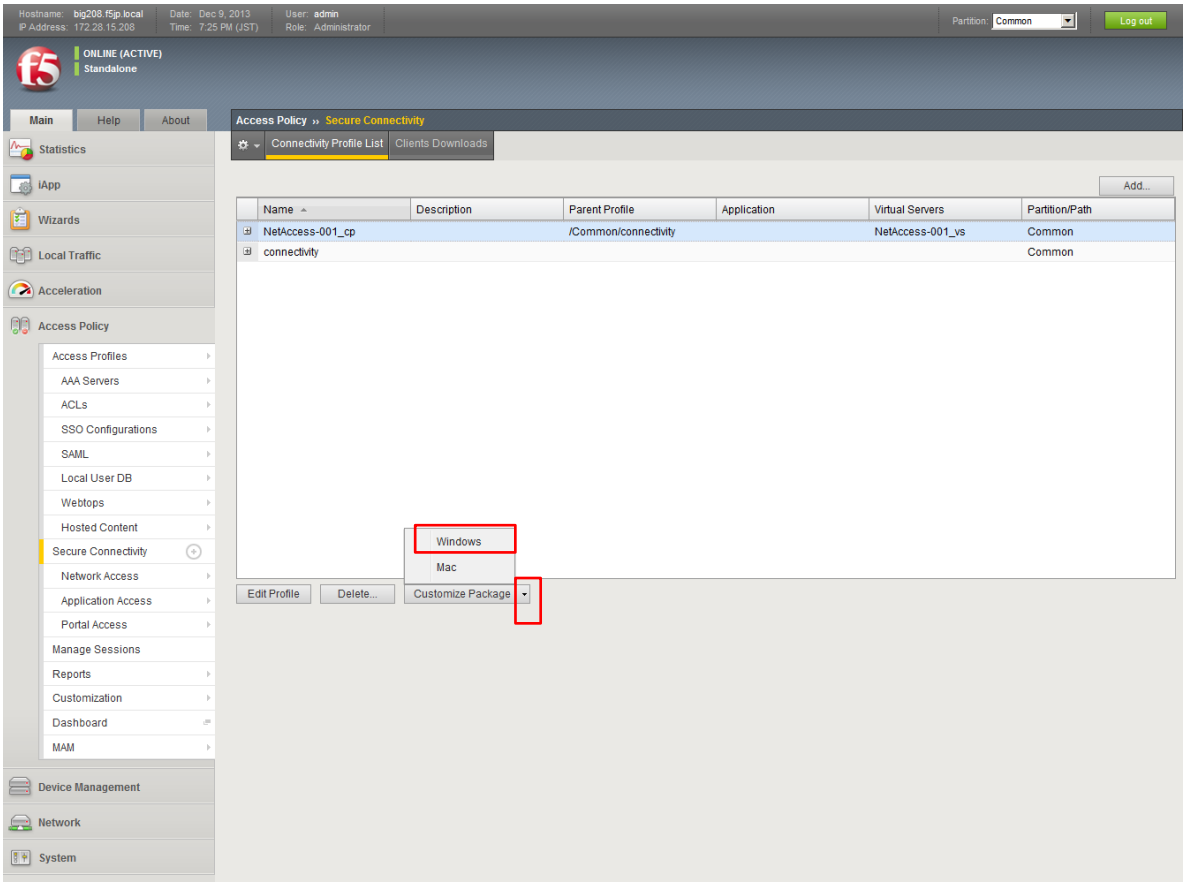
(2) 「Win/Mac Edge Client」をクリックすると、以下の画面が現れます。
「Reuse Windows Logon Credentials」にチェックを入れます。



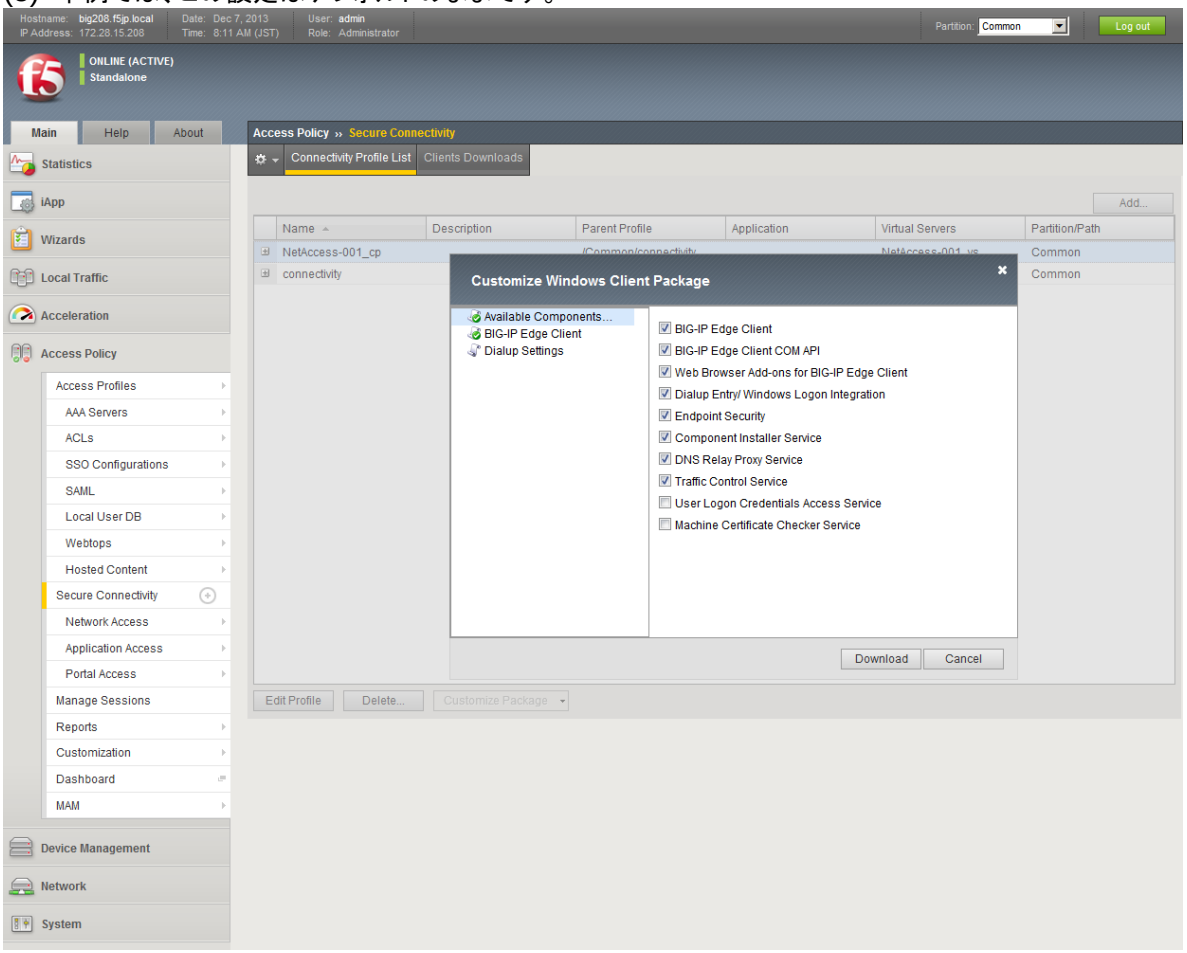
(3) Edge Client を使う際に、デフォルトの宛先を指定しておきます。
「Server List」をクリックすると、以下の画面が現れます。
本例では、「apm.f5jp.local」をデフォルトの宛先として設定しています。



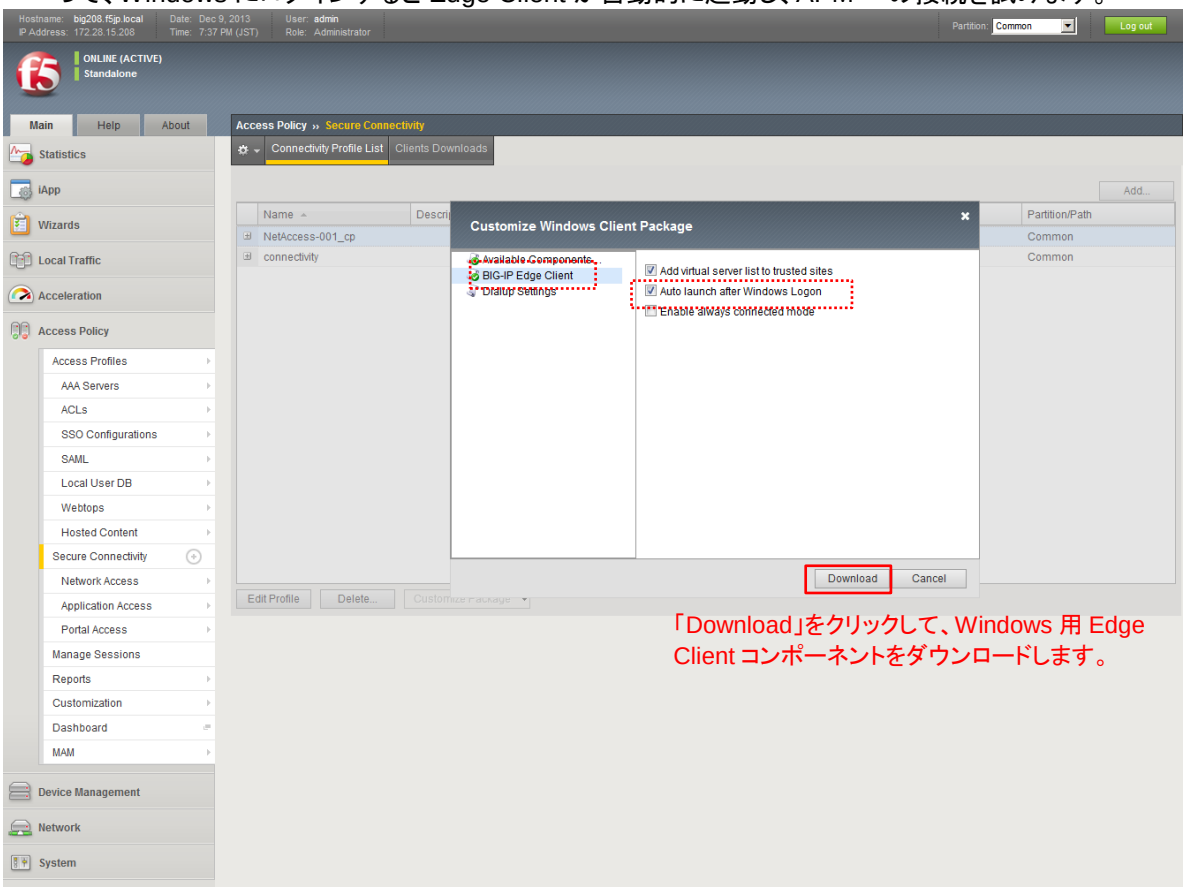
(4) 「Customize Package」横の▼をクリックすると、「Windows」用か「Mac」用かの選択が現れます。
ここでは、「Windows」を選択します。



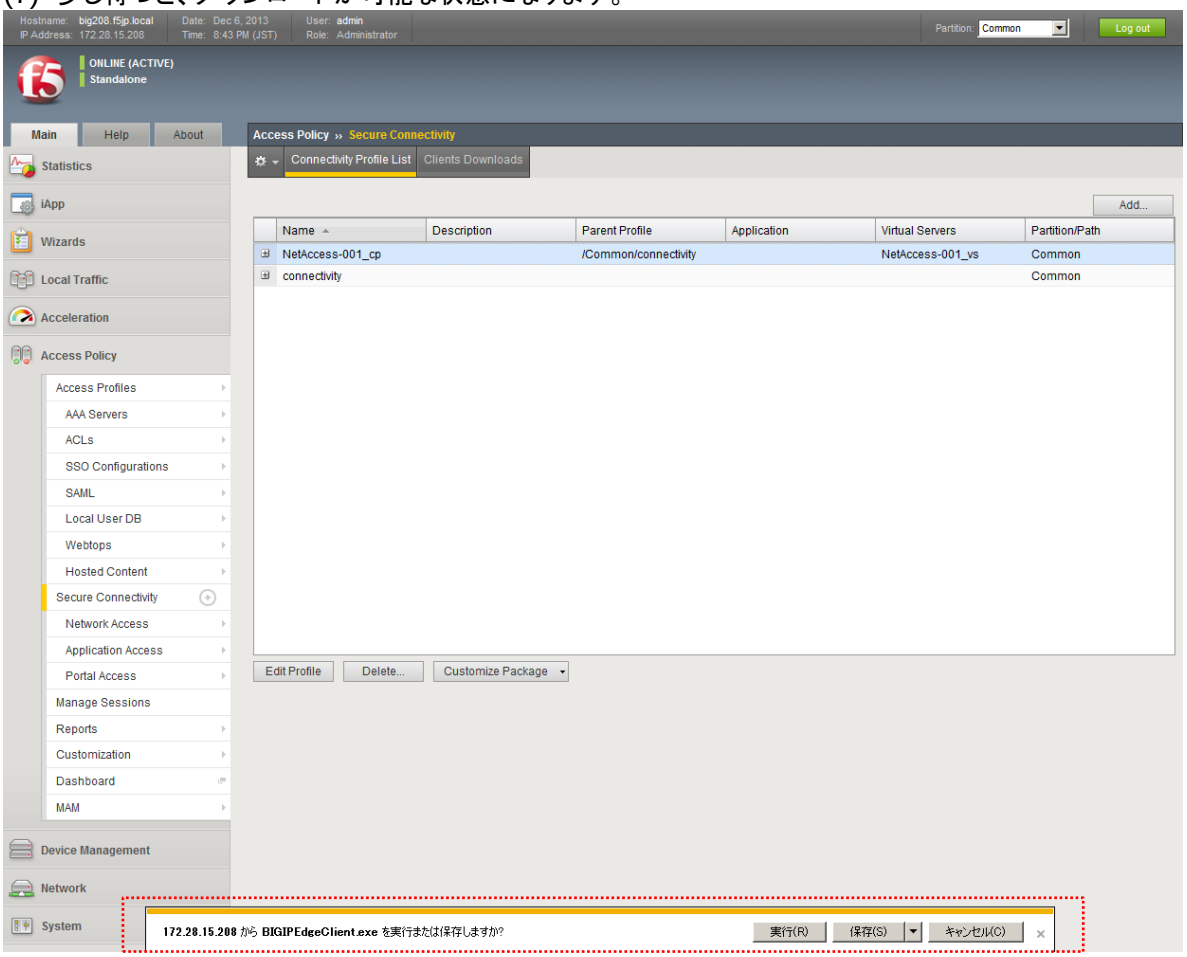
(5) 本例では、この設定はデフォルトのままです。



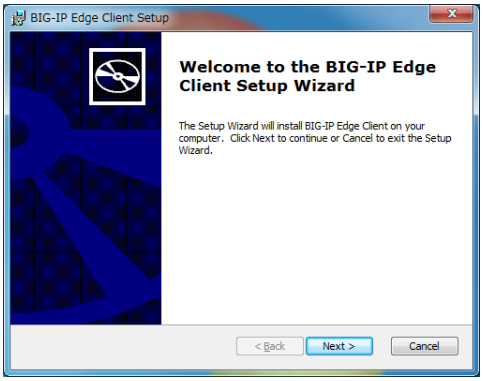
(6) 「BIG-IP Edge Client」をクリックします。
こちらの設定もデフォルトのままですが、「Auto launch after Windows Logon」に注目してください。この設定によって、Windows にログインすると Edge Client が自動的に起動し、APM への接続を試みます。

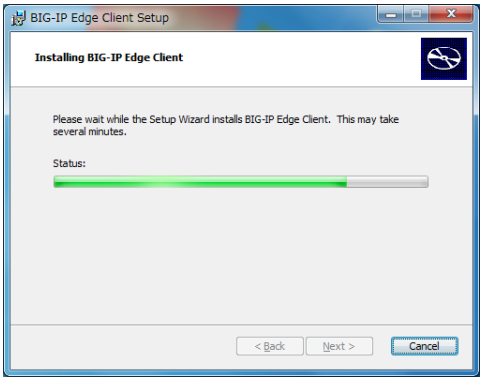


(7) 少し待つと、ダウンロードが可能な状態になります。

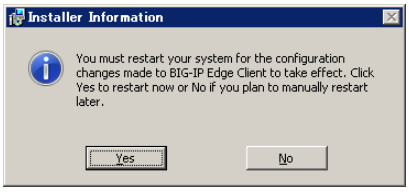


(8) ダウンロードしたコンポーネントをクライアント PC にコピーし、インストールを行います。

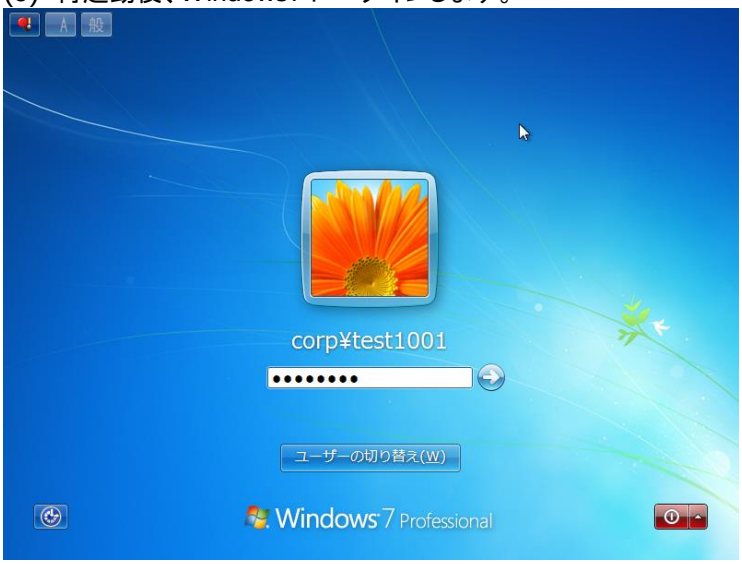




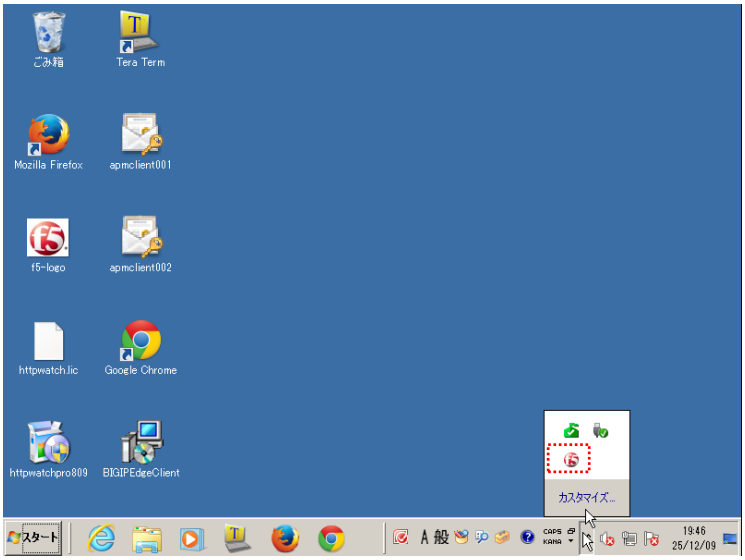
クライアント PC の再起動を要求されますので、「Yes」を選択して再起動してください。



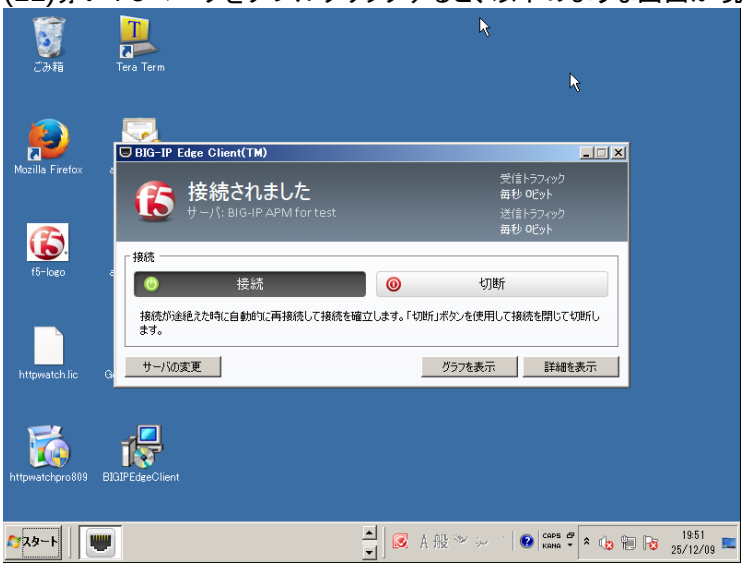
(9) 再起動後、Windows7 にログインします。



(10)Windows ログオン時の ID とパスワードを使って、自動的に APM への接続が行われます。
以下の状態は、接続完了後です。



(11)赤い F5 マークをダブルクリックすると、以下のような画面が現れます。接続されていることが分かります。



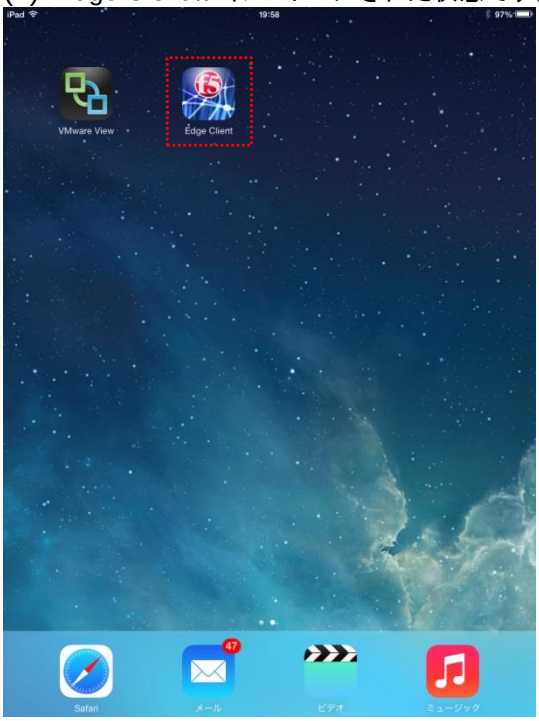
5.2.3. Apple iPad からのアクセス

BIG-IP APM へのネットワークアクセスは、Apple iPad や Google Android からの接続も可能です。

サンプルとして、Apple iPad からの接続方法を以下に示します。

(1) App Store から、「F5 BIG-IP Edge Client」をダウンロード＆インストールします。

(2) Edge Client がインストールされた状態です。



(3) 画面下の「設定」アイコンをクリックすると、以下の画面が現れます。
表示された画面の「接続先の追加」をクリックします。

(4) 以下の「設定」画面が現れます。必要項目を設定します。
入力が終わったら、右上「保存」ボタンを押します。

任意の名称を入力。

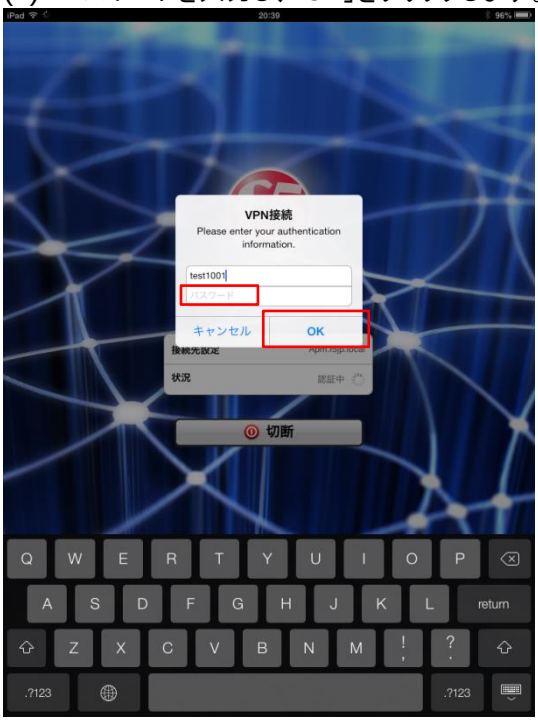
APM の VS(ホスト名 or IP アドレス)を入力。

ユーザ名の入力。

(5) 画面下の「接続」アイコンをクリックします。

(6) 「接続」ボタンを押します。

(7) パスワードを入力し、「OK」をクリックします。



(8) ネットワークアクセスの接続が成功した状態です。

以降、サファリブラウザなどから、社内サーバへのアクセスが可能となります。

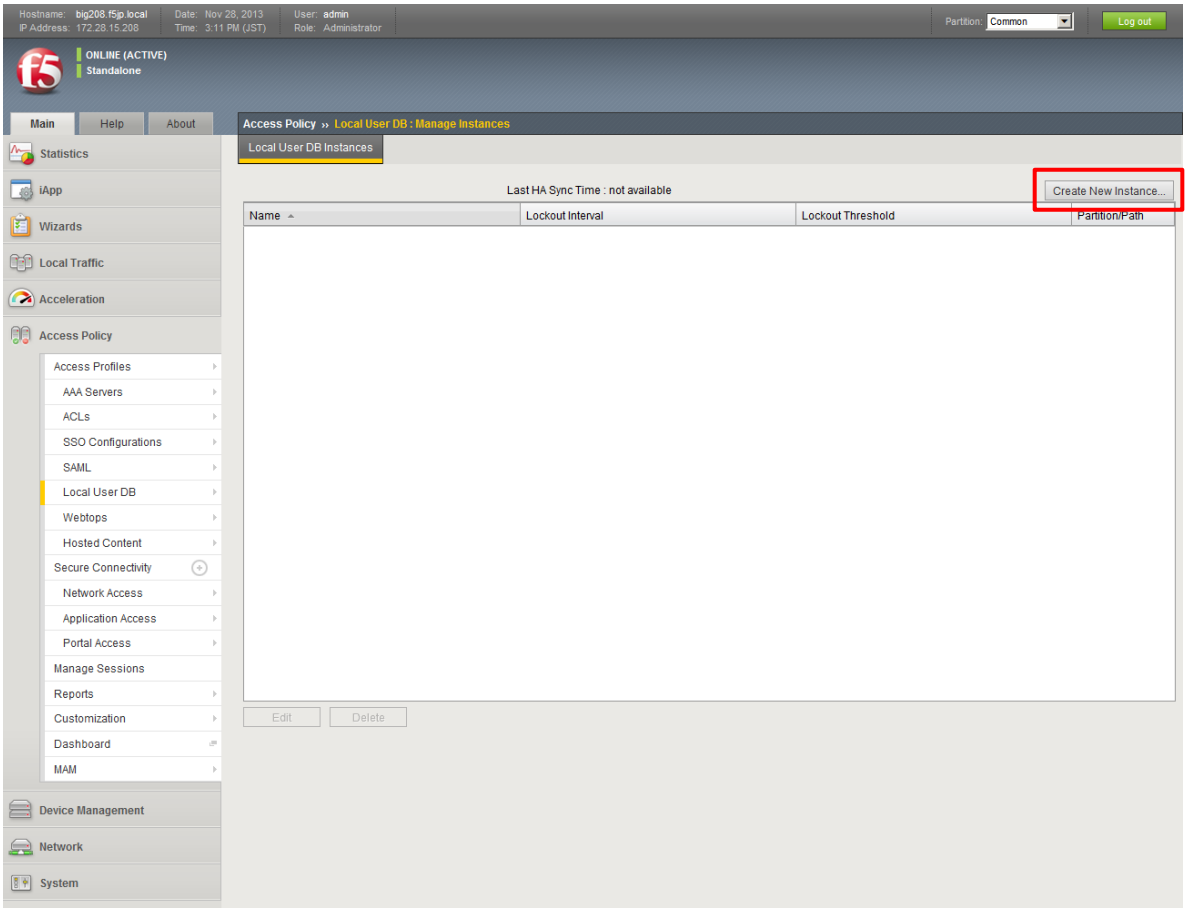
Google Android の場合もほぼ同様の手順でご利用頂けます。
Android 用 Edge Client は、Google Play からダウンロードしてください。

5.3. Local User DB による認証

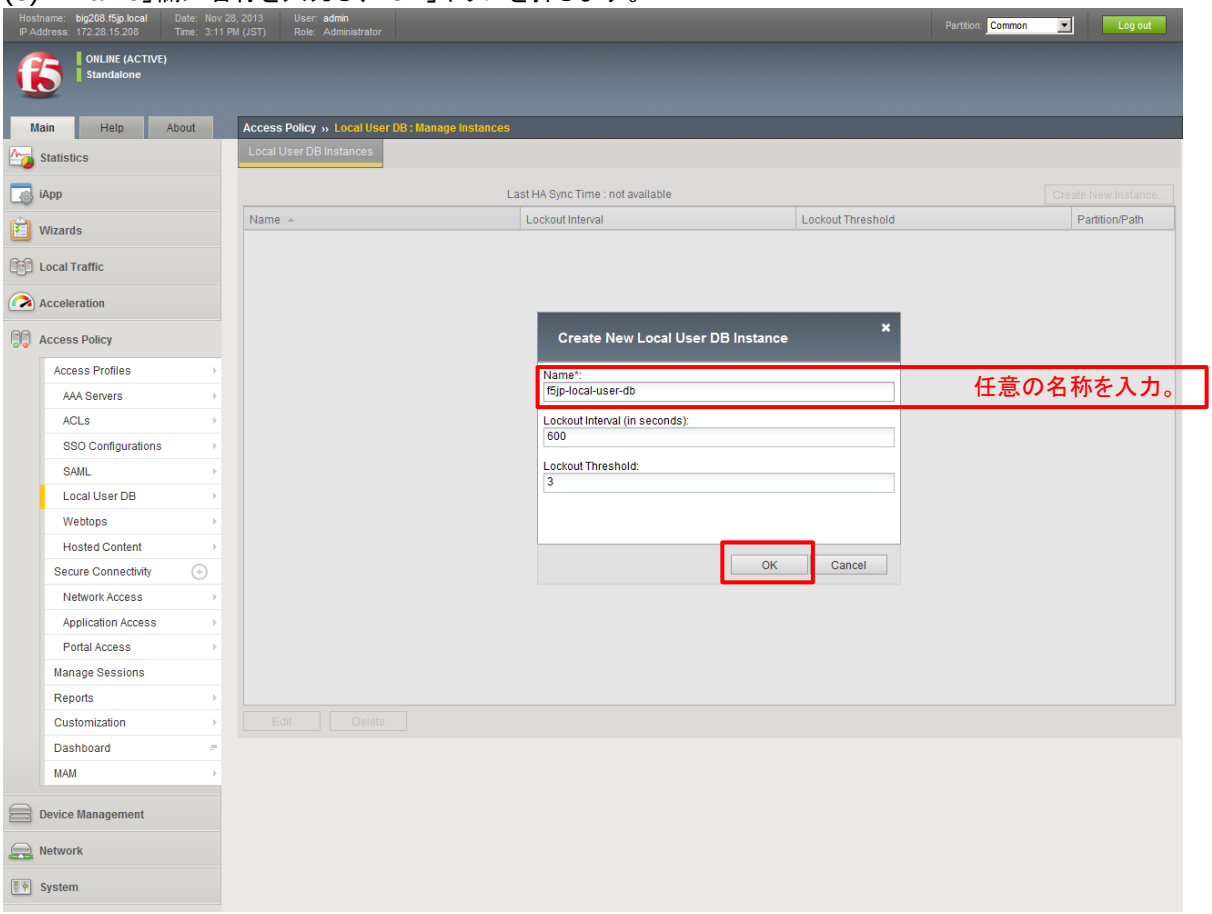
Active Directory のような認証サーバがない場合、APM が持つ Local User DB を利用する方法があります。しかし、ウィザード設定では、Local User DB が選択できません(V11.4.1)。
以下に、Local User DB を利用する方法を記載します。

(1) 既述のウィザード設定手順の中で、「Select Authentication」ページで「No Authentication」を選び、最後まで進みます。

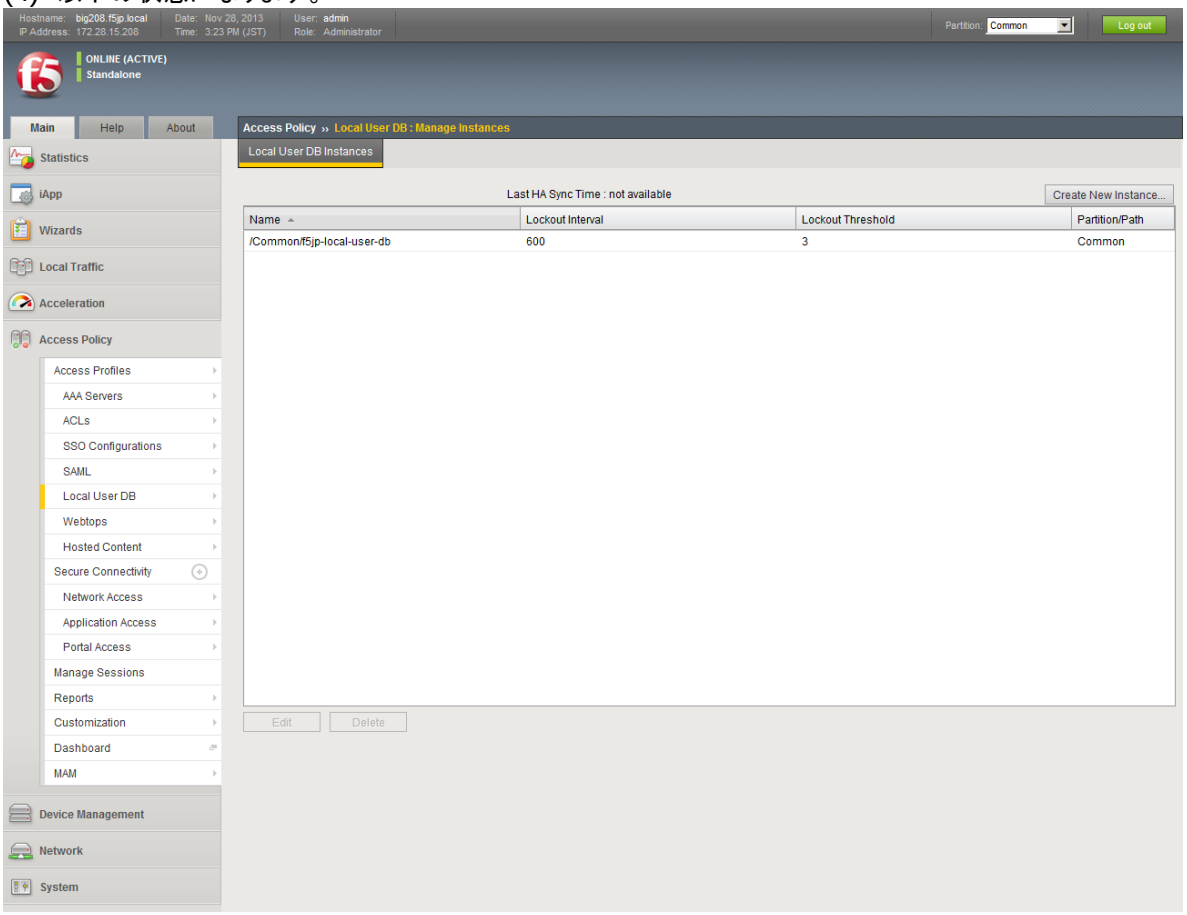
(2) Local User DB を設定します。
「Main」メニュー → 「Access Policy」 → 「Local User DB」 → 「Manage Instances」で以下の画面が現れます。
まずは Instance（User DB の名前のようなもの）を設定します。
「Create New Instance」ボタンを押します。



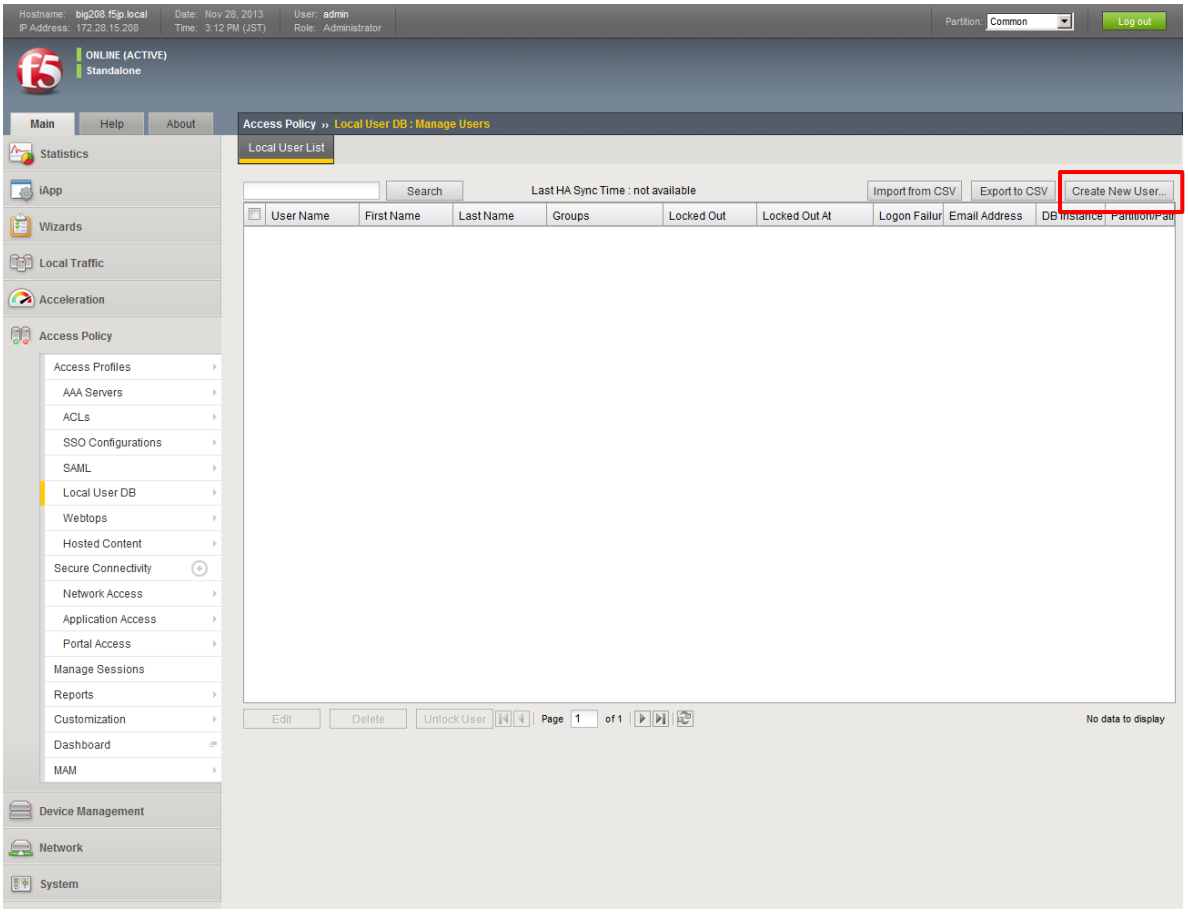
(3) 「Name」欄に名称を入力し、「OK」ボタンを押します。



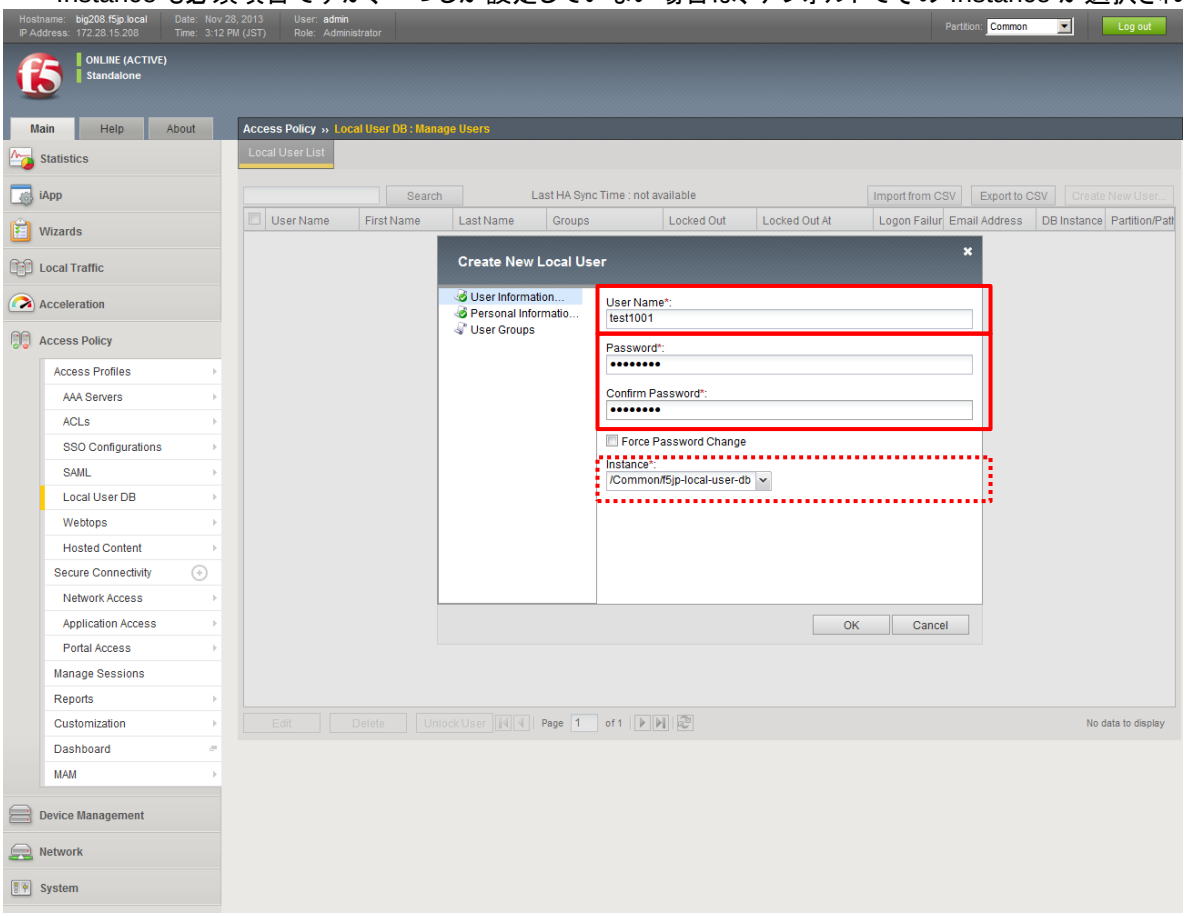
(4) 以下の状態になります。



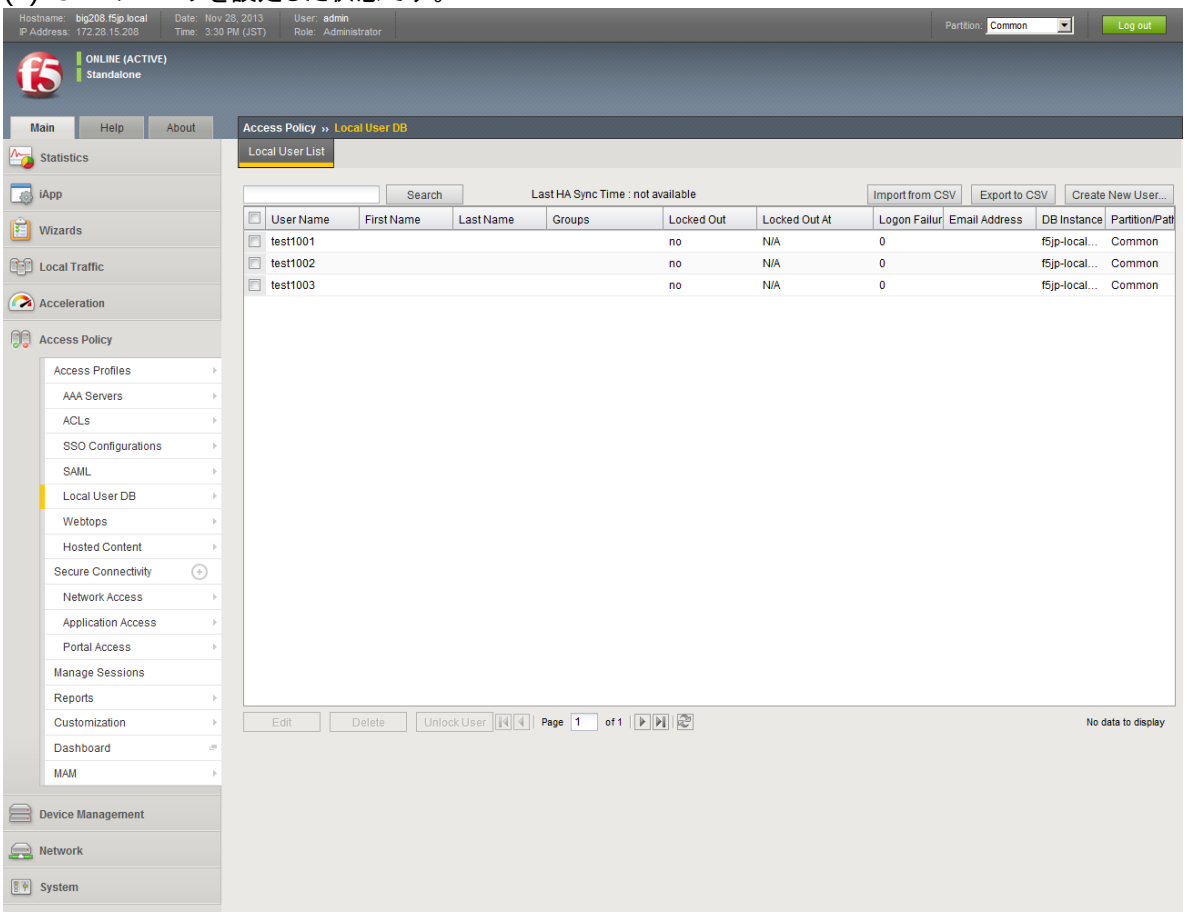
(5) 「Main」メニュー →「Access Policy」→「Local User DB」→「Manage Users」で、以下の画面が現れます。
「Create New User」ボタンを押します。



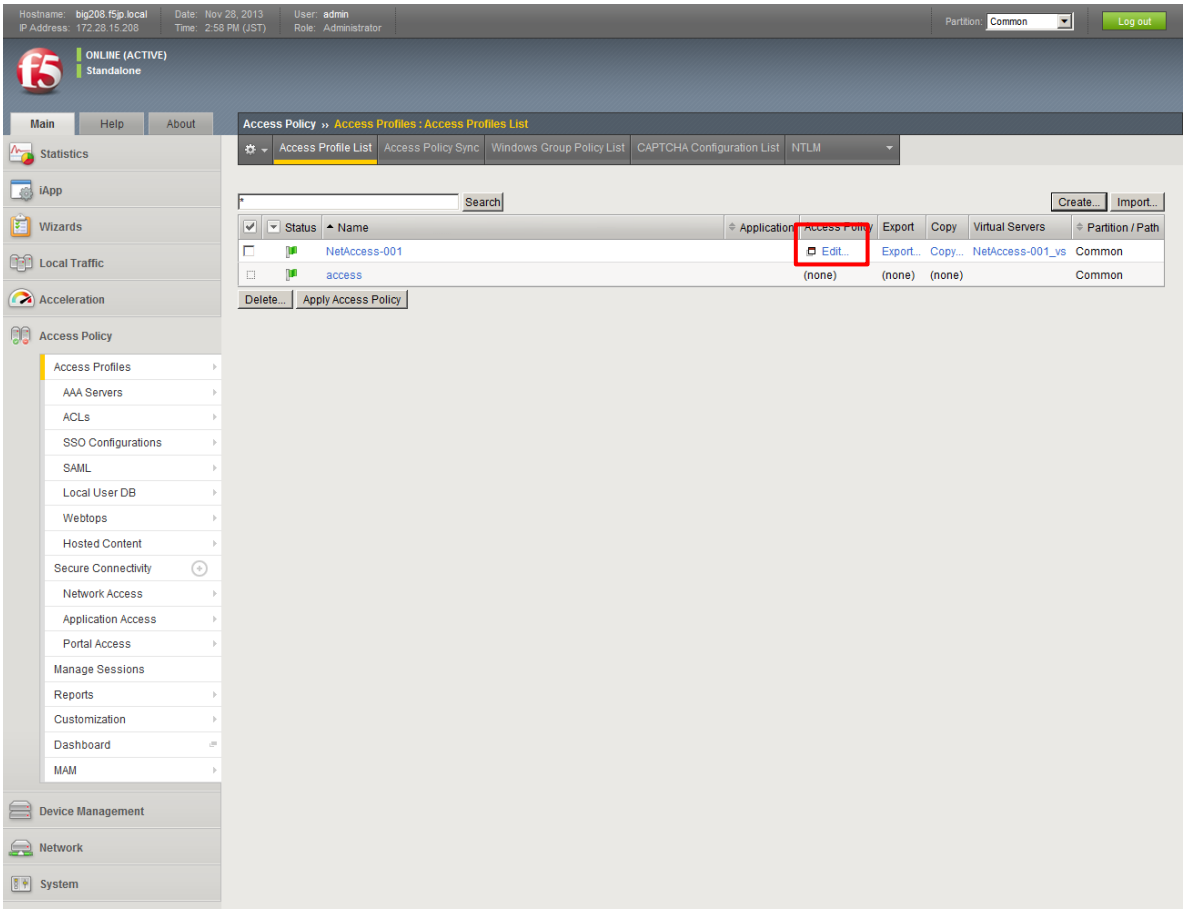
(6) Username, Password を入力します。「*」の部分が必須項目です。
Instance も必須項目ですが、一つしか設定していない場合は、デフォルトでその Instance が選択されています。



(7) 3 つのユーザを設定した状態です。



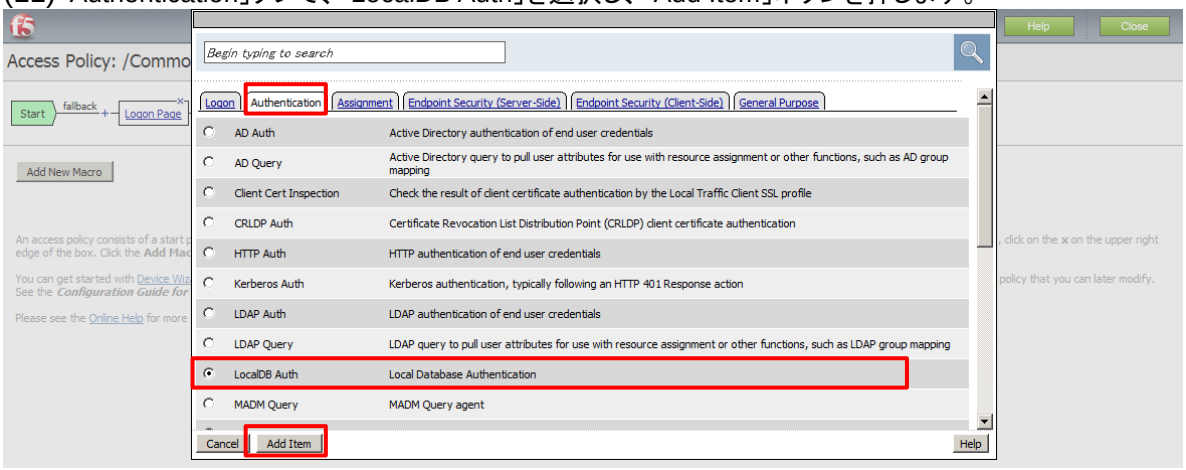
(8) 「Main」メニュー →「Access Policy」→「Access Profiles」で表示された、「NetAccess-001」の行にある「Edit」をクリックします。



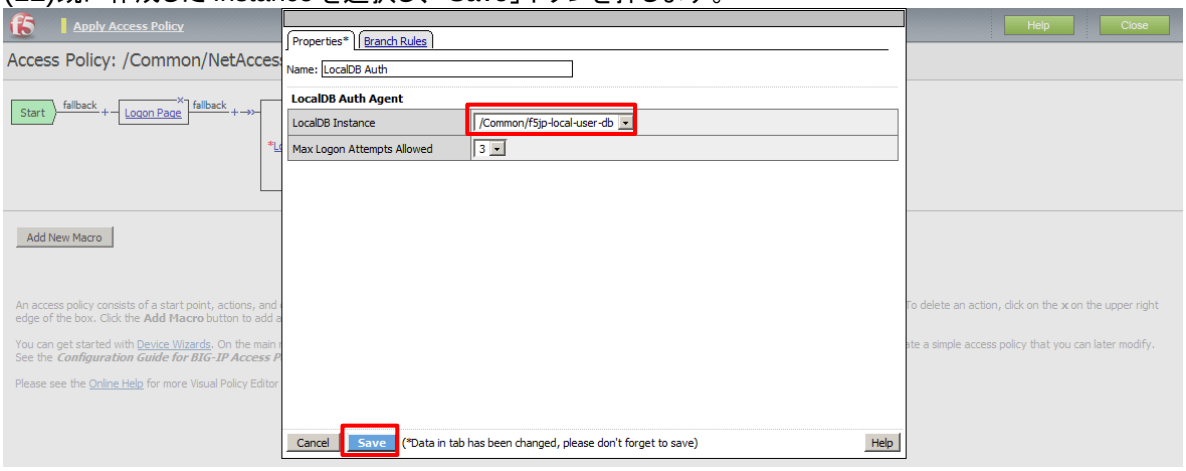
(9) 新しいウィンドウが開き、以下のような証明書に関わる警告画面が表示されますが、「このサイトの閲覧を続行する」を選択してください。

(10)「Logon Page」の後ろにある「+」ボタンをクリックします。

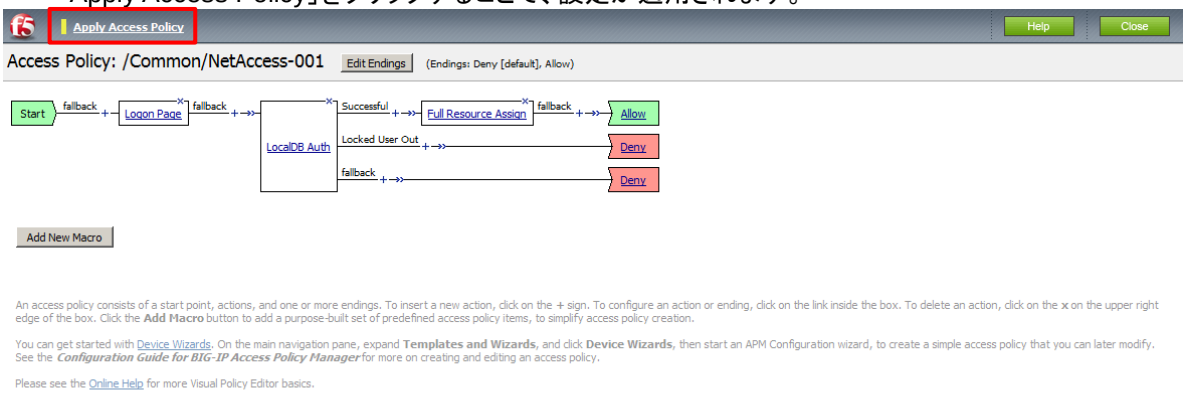
(11)「Authentication」タブで、「LocalDB Auth」を選択し、「Add Item」ボタンを押します。



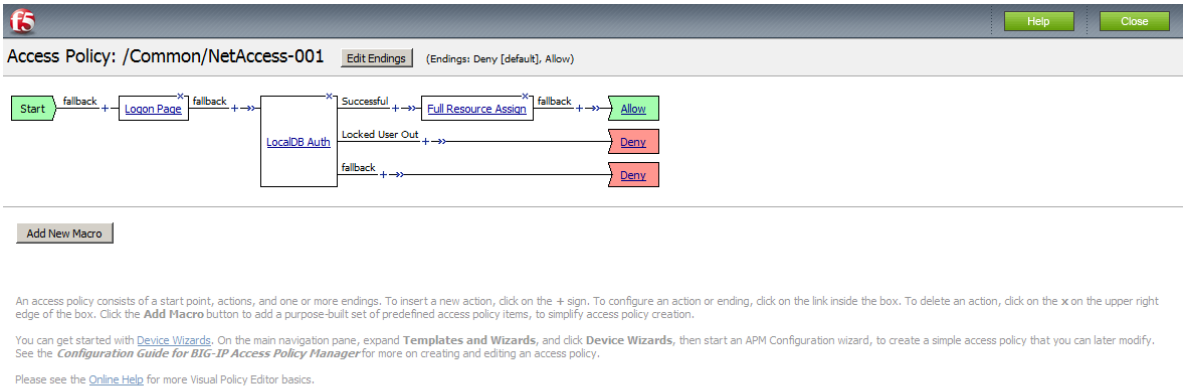
(12)既に作成した Instance を選択し、「Save」ボタンを押します。



(13)以下の状態になります。
　　この段階では、設定した内容が適用されていません。
　　「Apply Access Policy」をクリックすることで、設定が適用されます。



(14)「Apply Access Policy」の表示が消えます。
　　Local User DB 認証の設定はこれで完了です。



5.3.1.　クライアント PC からのアクセス

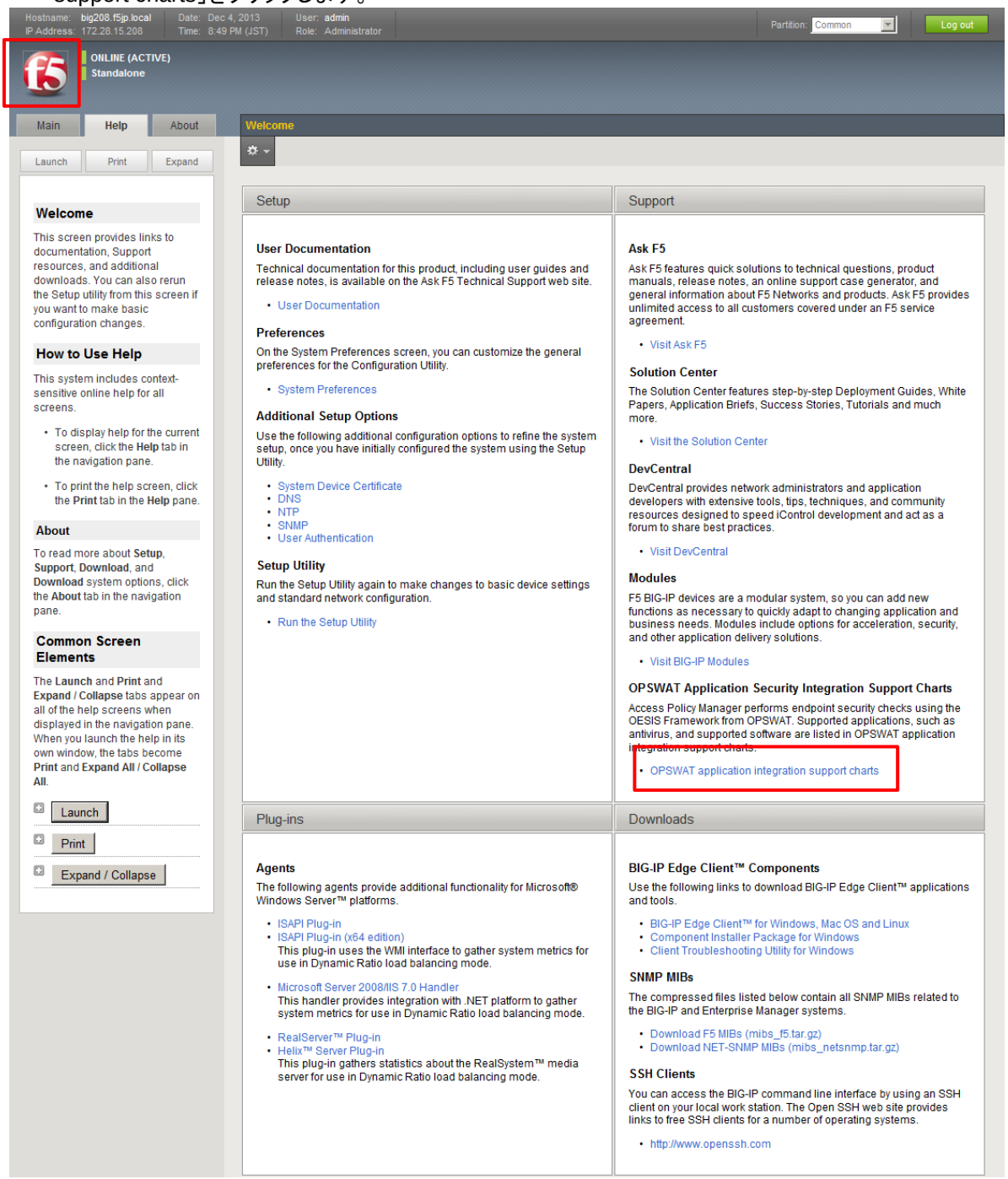
クライアント PC から、Local User DB に登録したユーザでアクセスできることを確認します。

5.4. ［参考］アンチウィルスソフトウェアのチェックについて

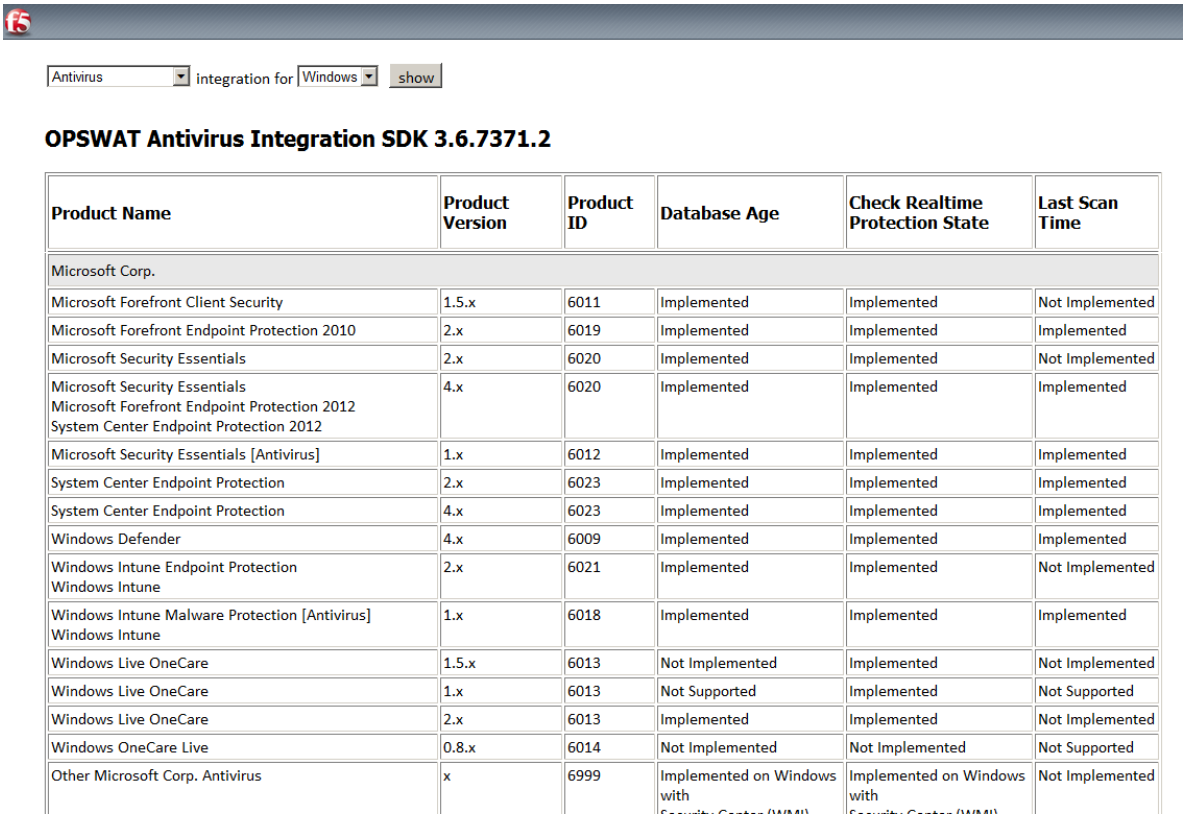
BIG-IP APM では、クライアント PC 上にインストールされているアンチウィルスソフトウェアをチェックすることもできます。

そのアンチウィルスソフトウェアの一覧は、以下の画面から確認できます。

(1) 左上の「f5」の赤いマークをクリックすると、以下の画面が現れますので、「OPSWAT application integration support charts」をクリックします。



(2) 以下のような、アンチウィルスソフトウェアの一覧が表示されます。
ウィザード設定で、アンチウィルスソフトウェアをチェックする設定を入れる(以下の"[参考]ウィザード画面の～"を参照ください)と、この一覧上のソフトウェアがクライアント PC にインストールされているかどうかのチェックが行われます。

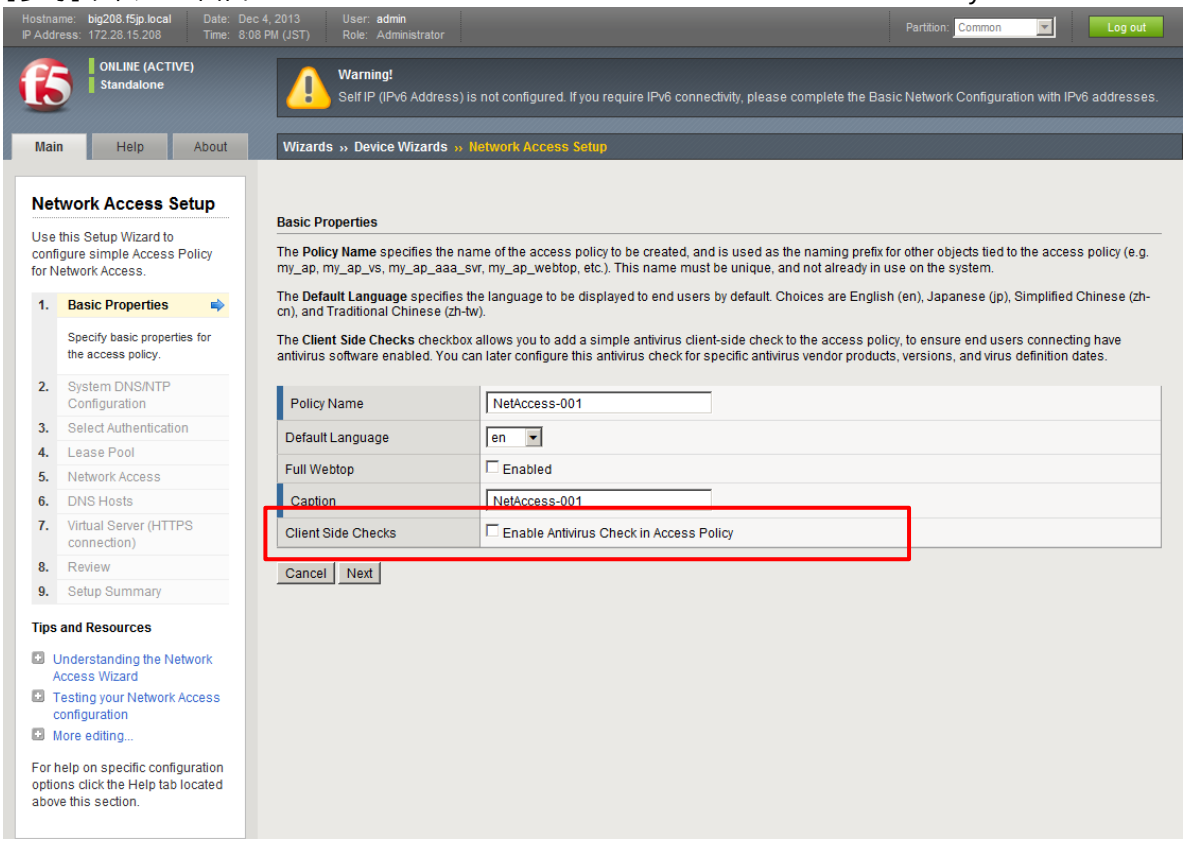


Antivirus integration for Windows show

OPSWAT Antivirus Integration SDK 3.6.7371.2

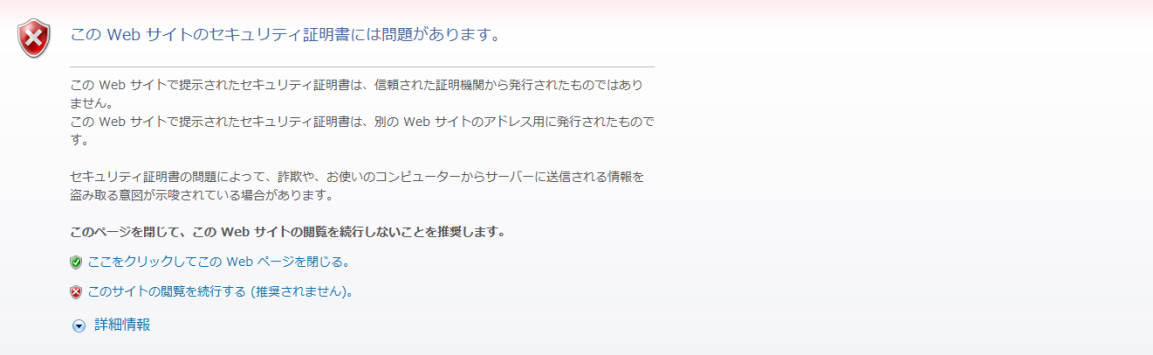
Product Name	Product Version	Product ID	Database Age	Check Realtime Protection State	Last Scan Time
Microsoft Corp.					
Microsoft Forefront Client Security	1.5.x	6011	Implemented	Implemented	Not Implemented
Microsoft Forefront Endpoint Protection 2010	2.x	6019	Implemented	Implemented	Implemented
Microsoft Security Essentials	2.x	6020	Implemented	Implemented	Not Implemented
Microsoft Security Essentials Microsoft Forefront Endpoint Protection 2012 System Center Endpoint Protection 2012	4.x	6020	Implemented	Implemented	Implemented
Microsoft Security Essentials [Antivirus]	1.x	6012	Implemented	Implemented	Implemented
System Center Endpoint Protection	2.x	6023	Implemented	Implemented	Implemented
System Center Endpoint Protection	4.x	6023	Implemented	Implemented	Implemented
Windows Defender	4.x	6009	Implemented	Implemented	Implemented
Windows Intune Endpoint Protection Windows Intune	2.x	6021	Implemented	Implemented	Not Implemented
Windows Intune Malware Protection [Antivirus] Windows Intune	1.x	6018	Implemented	Implemented	Implemented
Windows Live OneCare	1.5.x	6013	Not Implemented	Implemented	Not Implemented
Windows Live OneCare	1.x	6013	Not Supported	Implemented	Not Supported
Windows Live OneCare	2.x	6013	Implemented	Implemented	Not Implemented
Windows OneCare Live	0.8.x	6014	Not Implemented	Not Implemented	Not Supported
Other Microsoft Corp. Antivirus	x	6999	Implemented on Windows with	Implemented on Windows with	Not Implemented

[参考]ウィザード画面の Client Side Check：Enable Antivirus Check in Access Policy



5.5. SSL サーバ証明書の設定

BIG-IP が持つデフォルトのサーバ証明書は、正式な認証局で取得したものではないため、クライアント PC の Web ブラウザで Virtual Server へアクセスすると、以下のような警告が出ます。

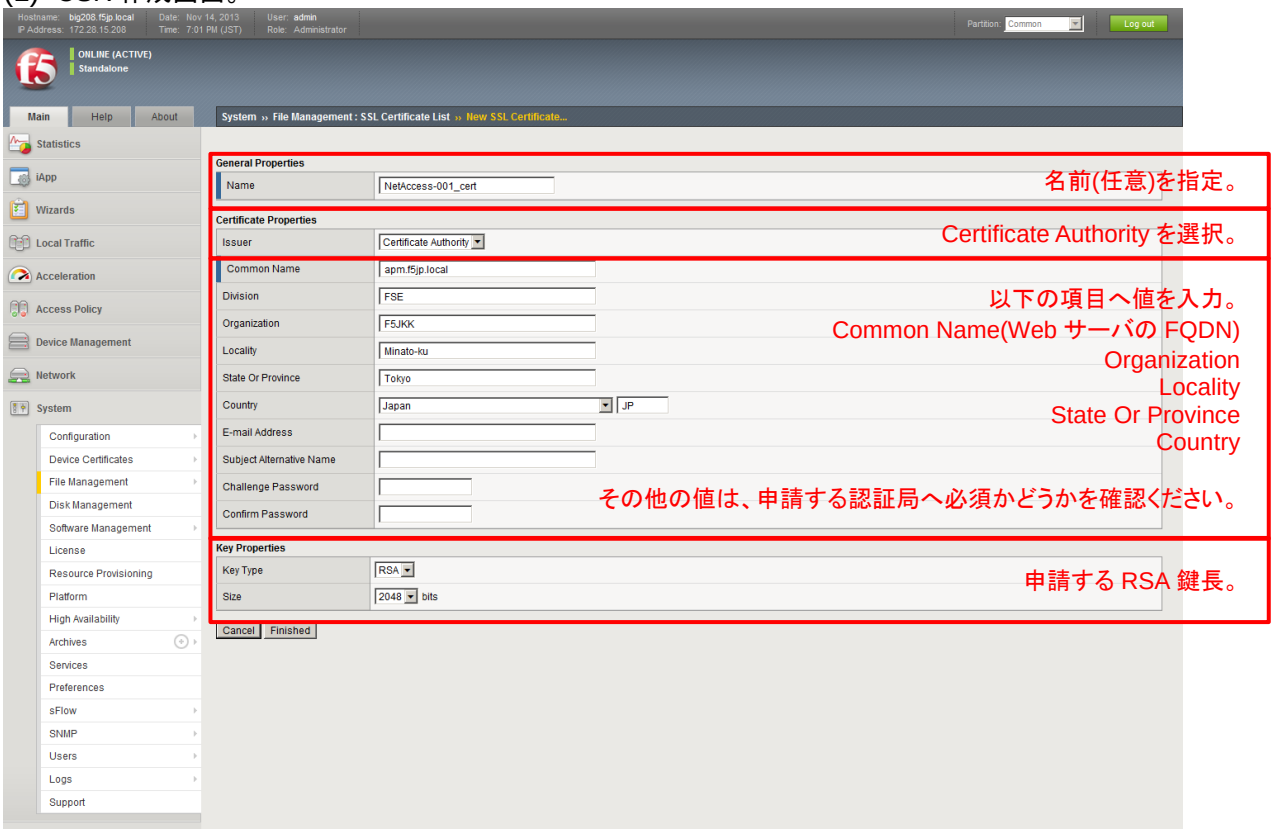


以降、正式な認証局(例：Verisign, CyberTrust 等)にて署名されたサーバ証明書をインポートして利用するまでの手順を示します。

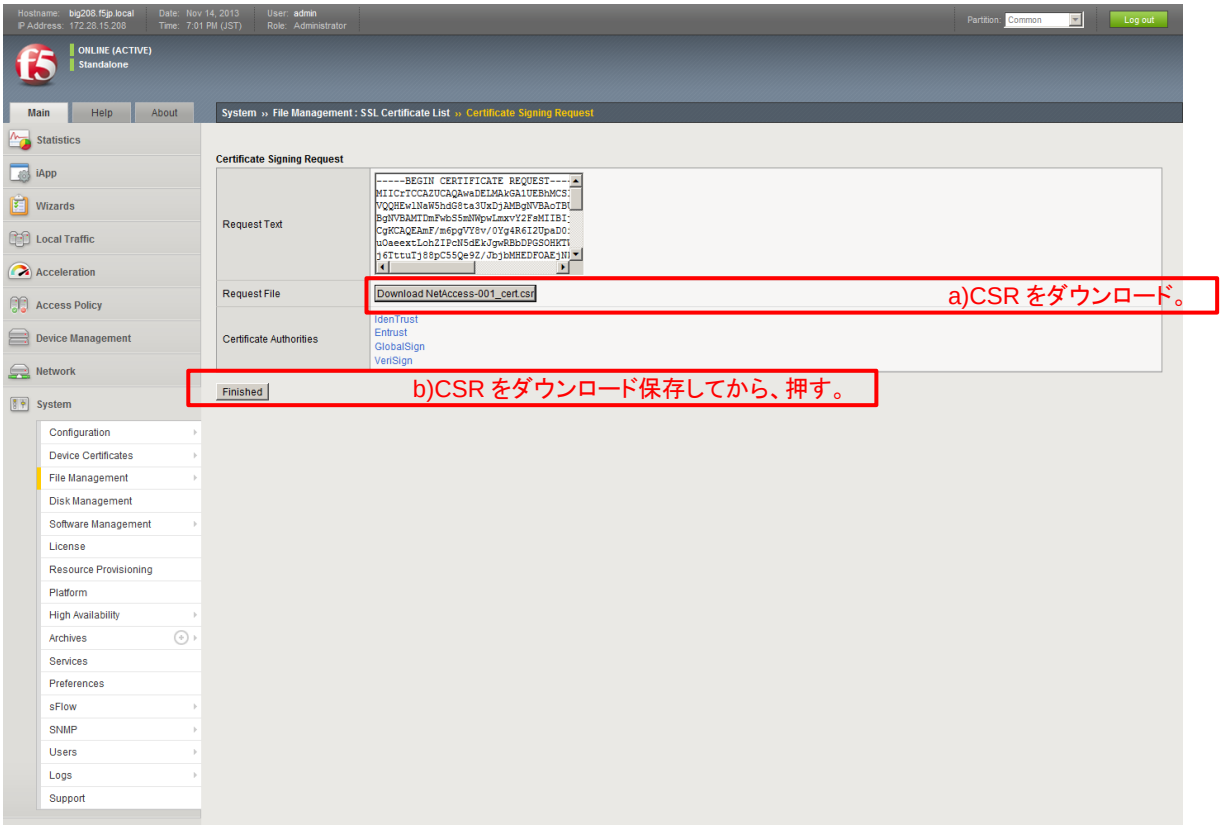
5.5.1. CSR の作成

認証局(CA)に対して、サーバ証明書の発行を依頼するための CSR(Certificate Signing Request)を作成します。
「Main」メニュー →「System」→「File Management」→「SSL Certificate List」タブで表示された画面右上の「Create」を押すと、以下の画面が表示されます。

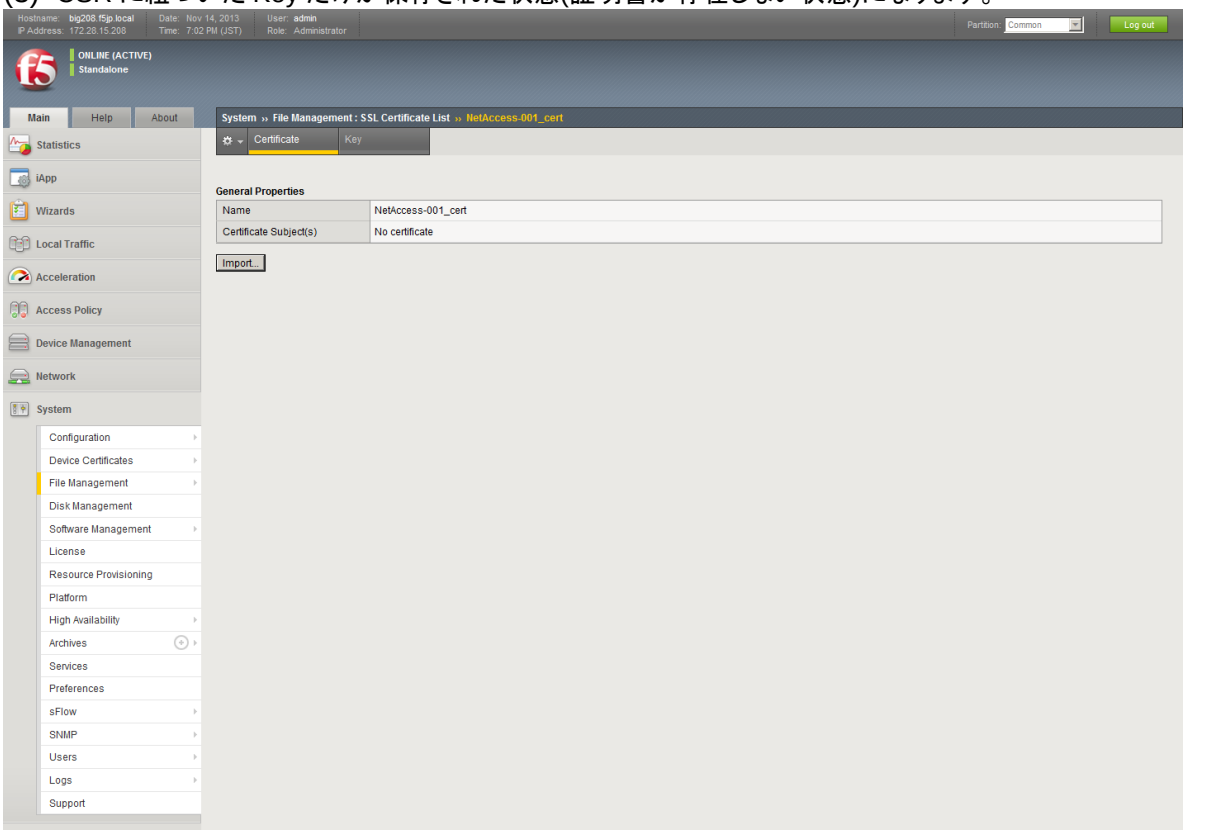
(1) CSR 作成画面。



(2) CSR を、ローカル PC へダウンロード保存します。
CSR を保存してから、「Finished」を押します。



(3) CSR に紐づいた Key だけが保存された状態(証明書が存在しない状態)になります。

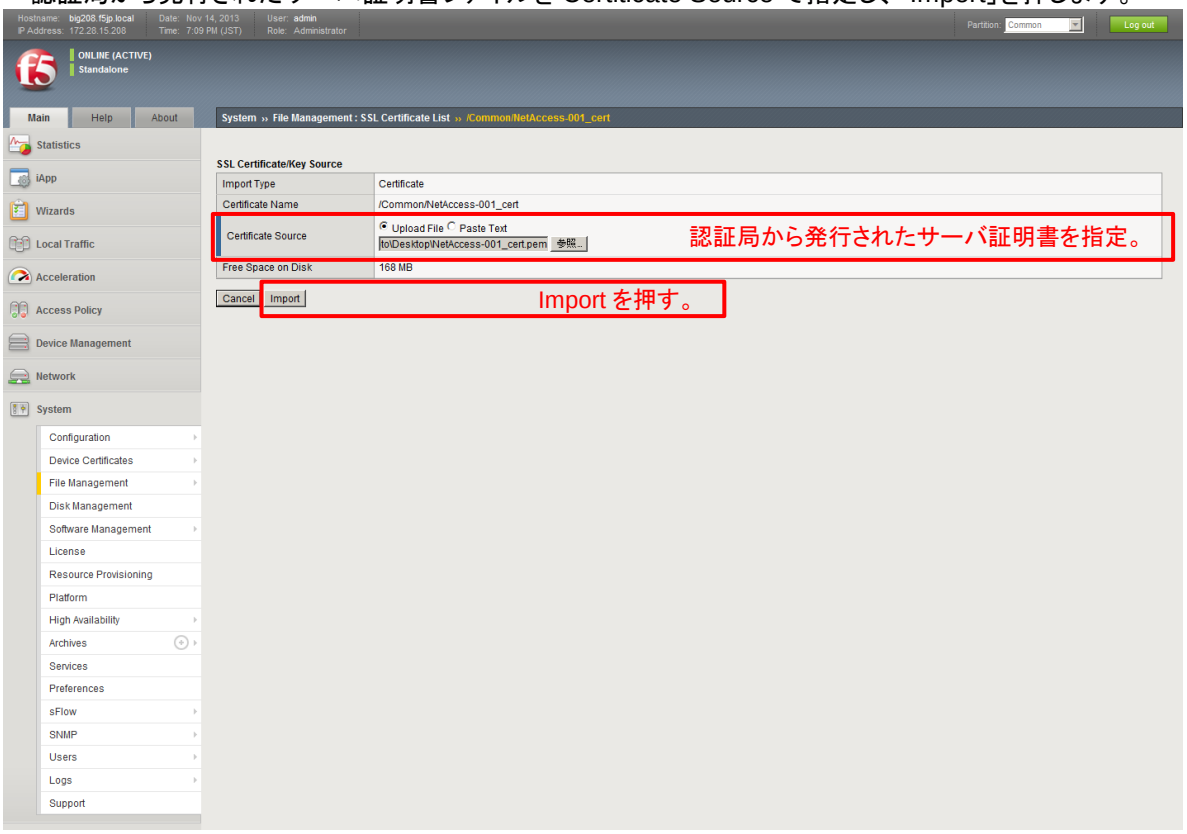


5.5.2. サーバ証明書の取得手続き

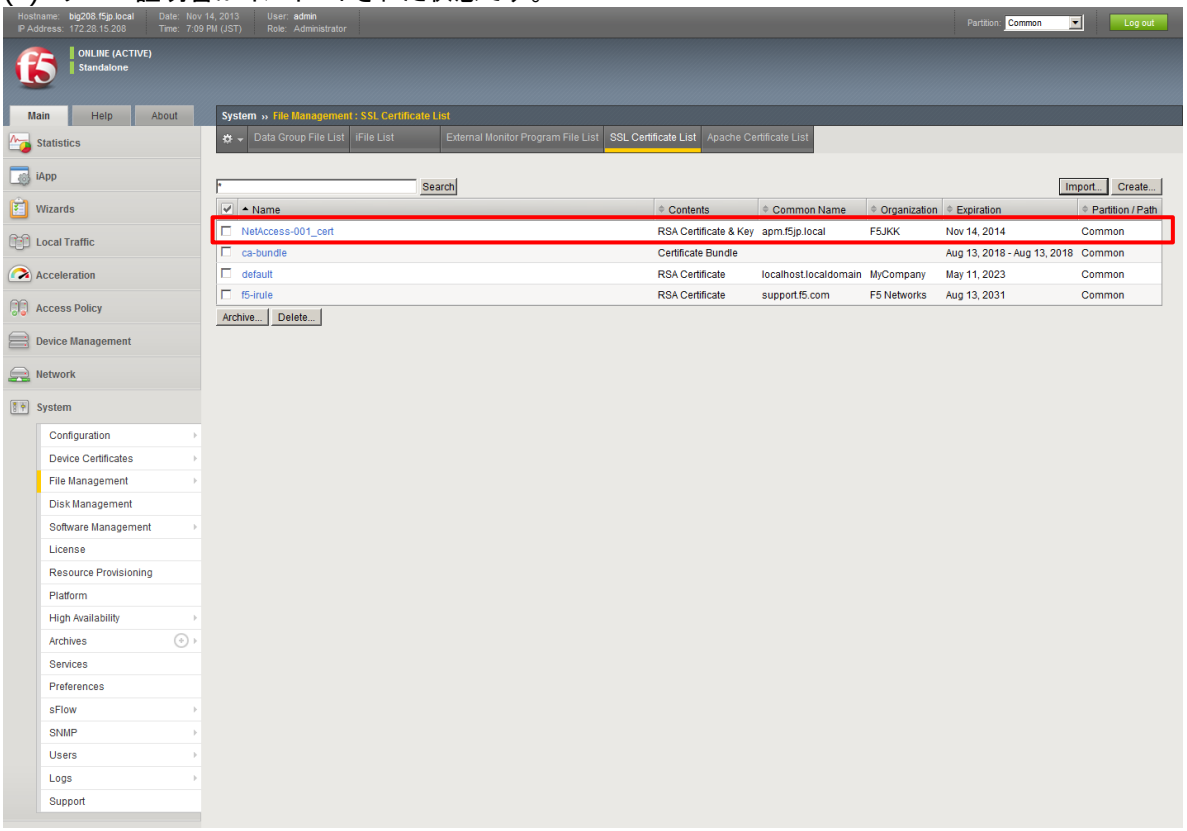
ダウンロードした CSR を商用の認証局(Verisign, CyberTrust 等)に送り、その CSR に署名してもらうことで、正式なサーバ証明書になります。
(本ガイドにおいては、OpenSSL を使って独自に認証局を作り、署名を行いました。)

5.5.3. 証明書のインポート

(1) 認証局から発行された SSL サーバ証明書をインポートします。
「Main」メニュー →「System」→「File Management」→「SSL Certificate List」から該当するもの(本例では、NetAcces-001_cert)を選択すると、以下の画面になります。
認証局から発行されたサーバ証明書ファイルを Certiticate Source で指定し、「Import」を押します。



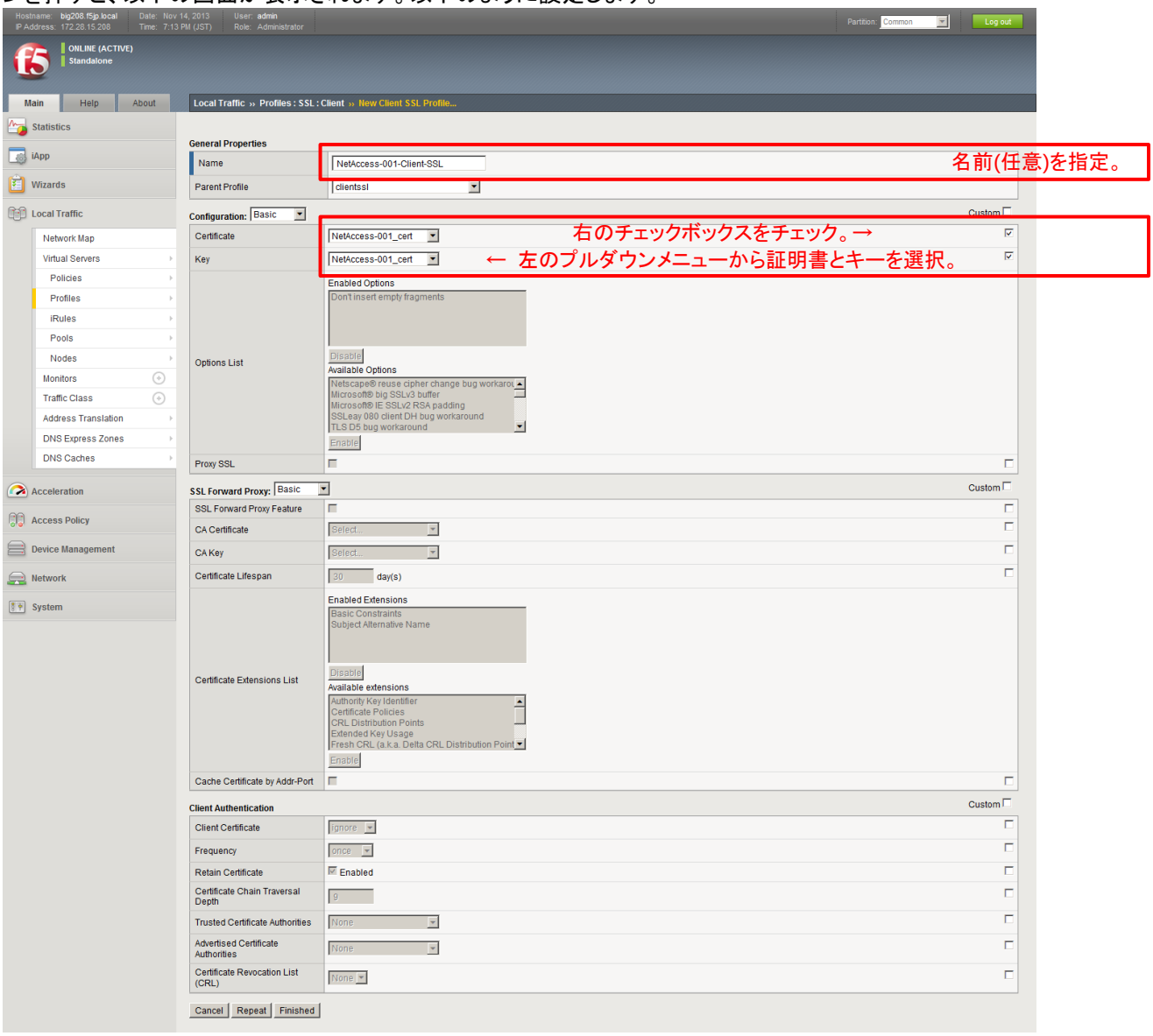
(2) サーバ証明書がインポートされた状態です。



5.5.4. Client SSL Profile の生成と VS への割当て

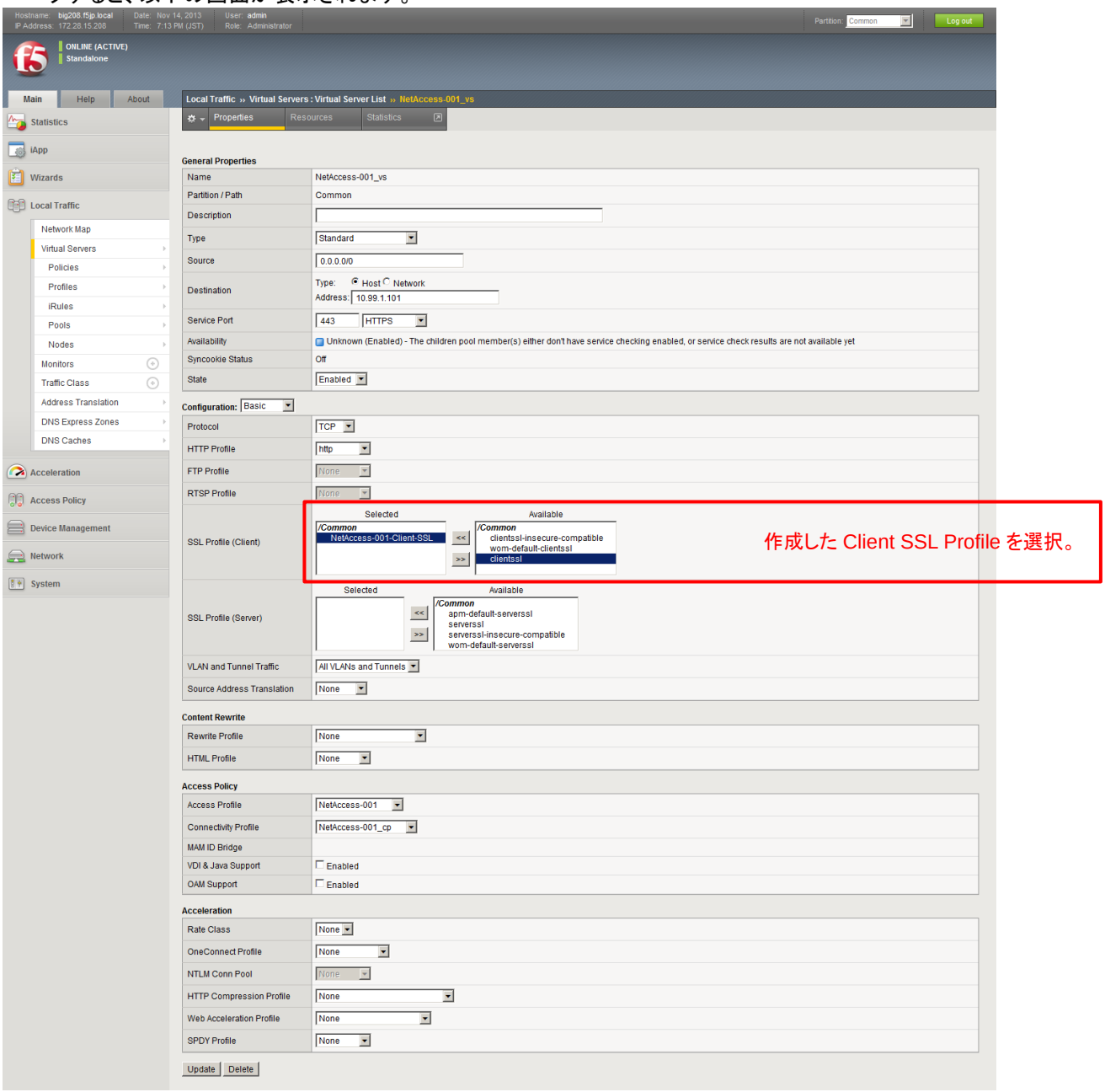
(1) Client SSL Profile の生成

「Main」メニュー →「Local Traffic」→「Profile」→「SSL」→「Client」で表示された画面右上の「Create」ボタンを押すと、以下の画面が表示されます。以下のように設定します。



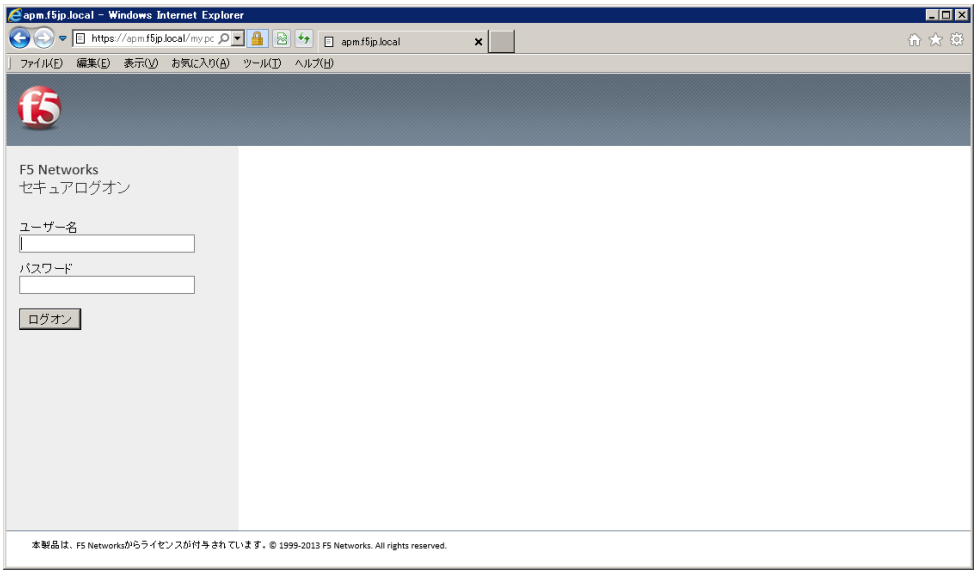
(2) Virtual Server への Client SSL Profile の割当て

「Main」メニュー →「Local Traffic」→「Virtual Servers」を選択し、APM 用に設定した Virtual Server をクリックすると、以下の画面が表示されます。



5.5.4.1. クライアント PC からのアクセス

正式なサーバ証明書を利用することで、クライアント PC から Virutal Server へのアクセス時に、警告が出なくなります。



初級編は以上で終了です。

ここまでで、ご要件を満たす設定になっていれば、「冗長化」へ進んでください。

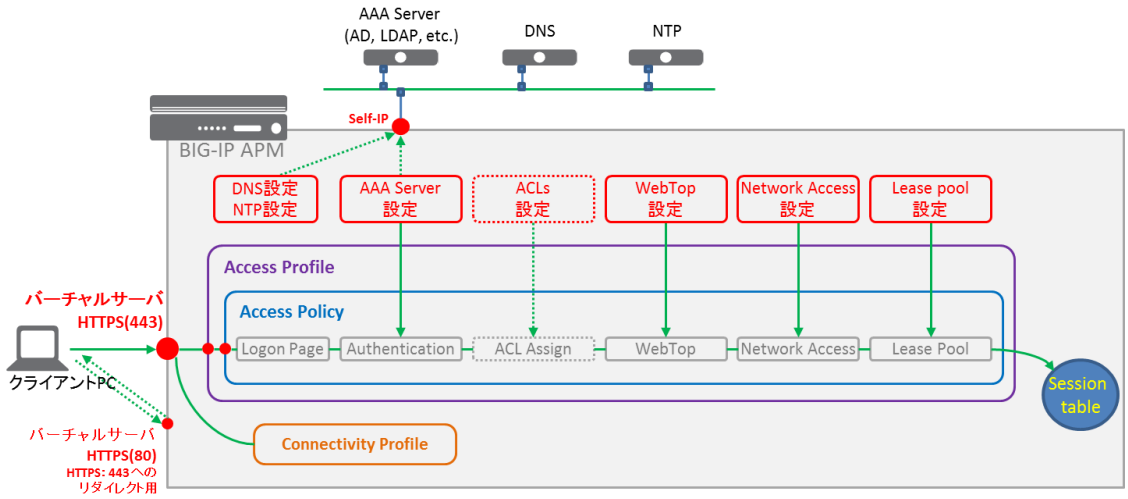
6. 中級編

6.1. APM オブジェクトを一つ一つ設定していく方法

ウィザードを利用せず、一つ一つオブジェクトを設定していき、ウィザード設定と同等の状態にする方法を示します。

6.1.1. 設定が必要な APM オブジェクトたち

APM のバーチャルサーバにアクセスしてから、ネットワークアクセス(SSL-VPN トンネル)を確立するまでには、下図に示すような、様々なオブジェクトを経由します。
このことで、BIG-IP APM に設定したポリシーが適用された、ネットワークアクセスセッションが生成されます。



設定が必要な各オブジェクトの概要を以下に記載します。

(1) DNS/NTP 設定
BIG-IP 自身が問合せを行うサーバ設定です。

(2) AAA Server 設定
Active Directory 認証に必要な設定を行います。

(3) ACL 設定
パケットフィルタリング設定です。このセクションでは設定しませんが、後の「VPE サンプル」で設定します。

(4) WebTop 設定
BIG-IP APM へのアクセス後に稼働する Web アプリケーションです。

(5) Network Access 設定
SSL-VPN トンネルを行うための設定です。

(6) Lease Pool 設定
クライアント PPP アダプタに割当てられるアドレス群です。

(7) Access Policy
上記のオブジェクトをフローチャート形式で紐づける設定です。

(8) Access Profile
Access Policy の親的位置づけです。利用する言語をここで設定します。

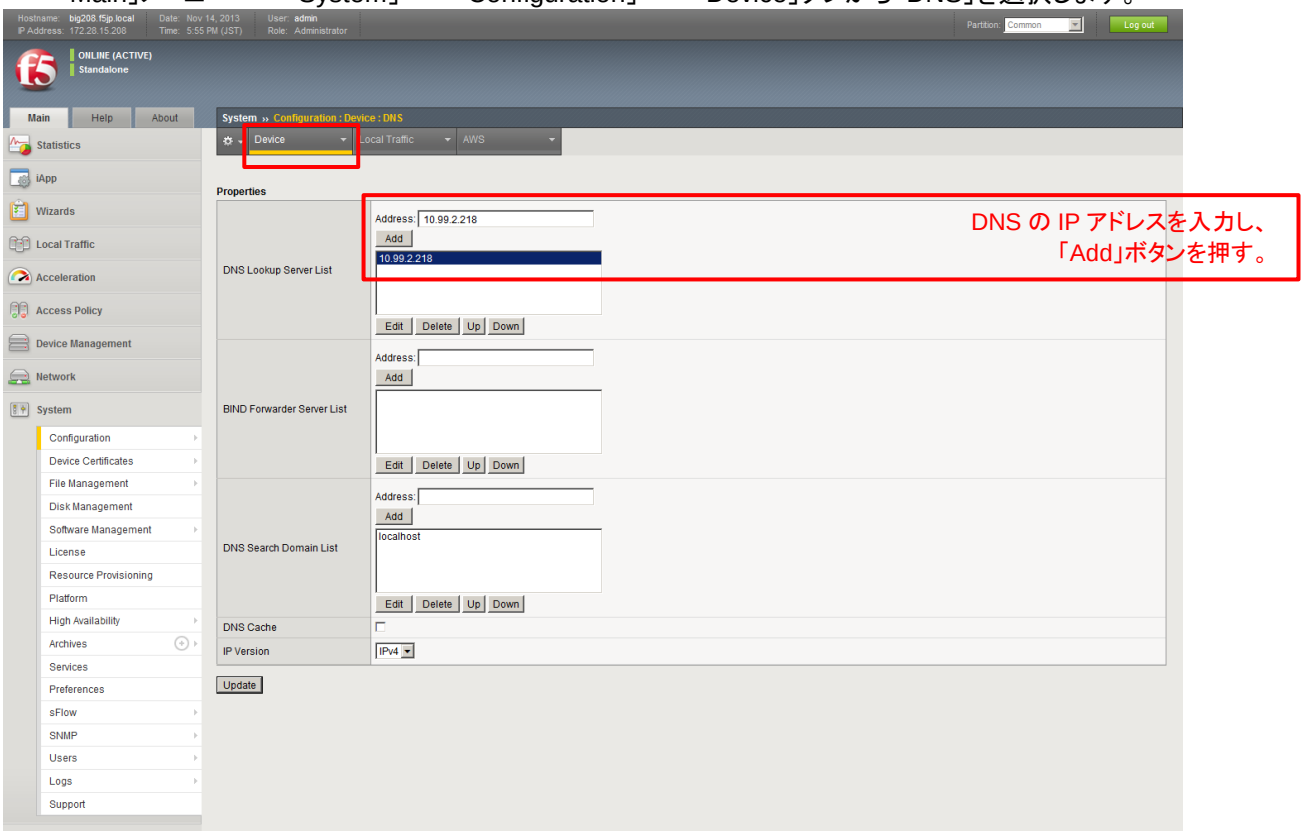
(9) Connectivity Profile
コネクション上の圧縮設定やクライアント用ソフトウェアの設定を行います。

以降、上記の各オブジェクトを設定していきます。
尚、既述の「ネットワーク設定」は完了しているものとして進めます。

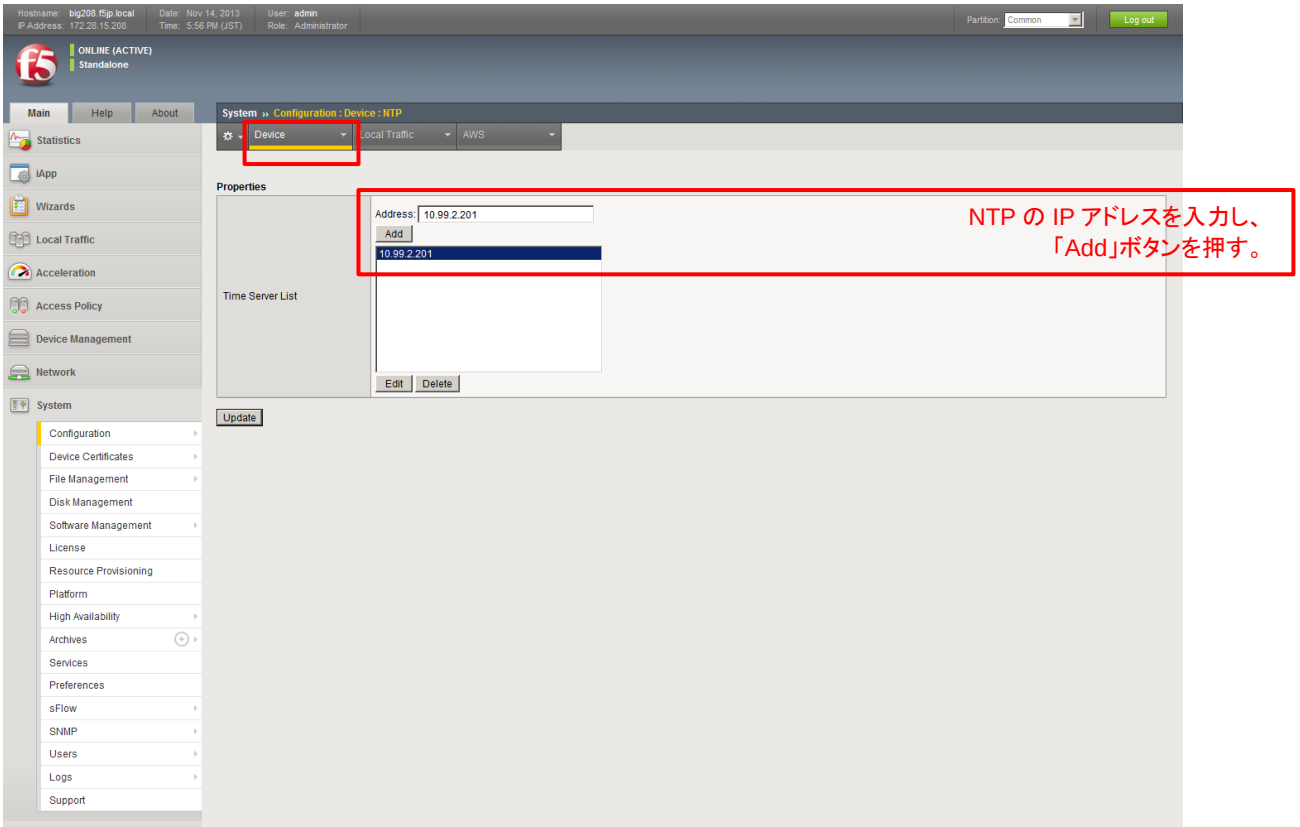
6.1.2. 各オブジェクトの設定

6.1.2.1. DNS / NTP 設定

(1) DNS を設定します。
「Main」メニュー → 「System」 → 「Configuration」 → 「Device」タブから「DNS」を選択します。

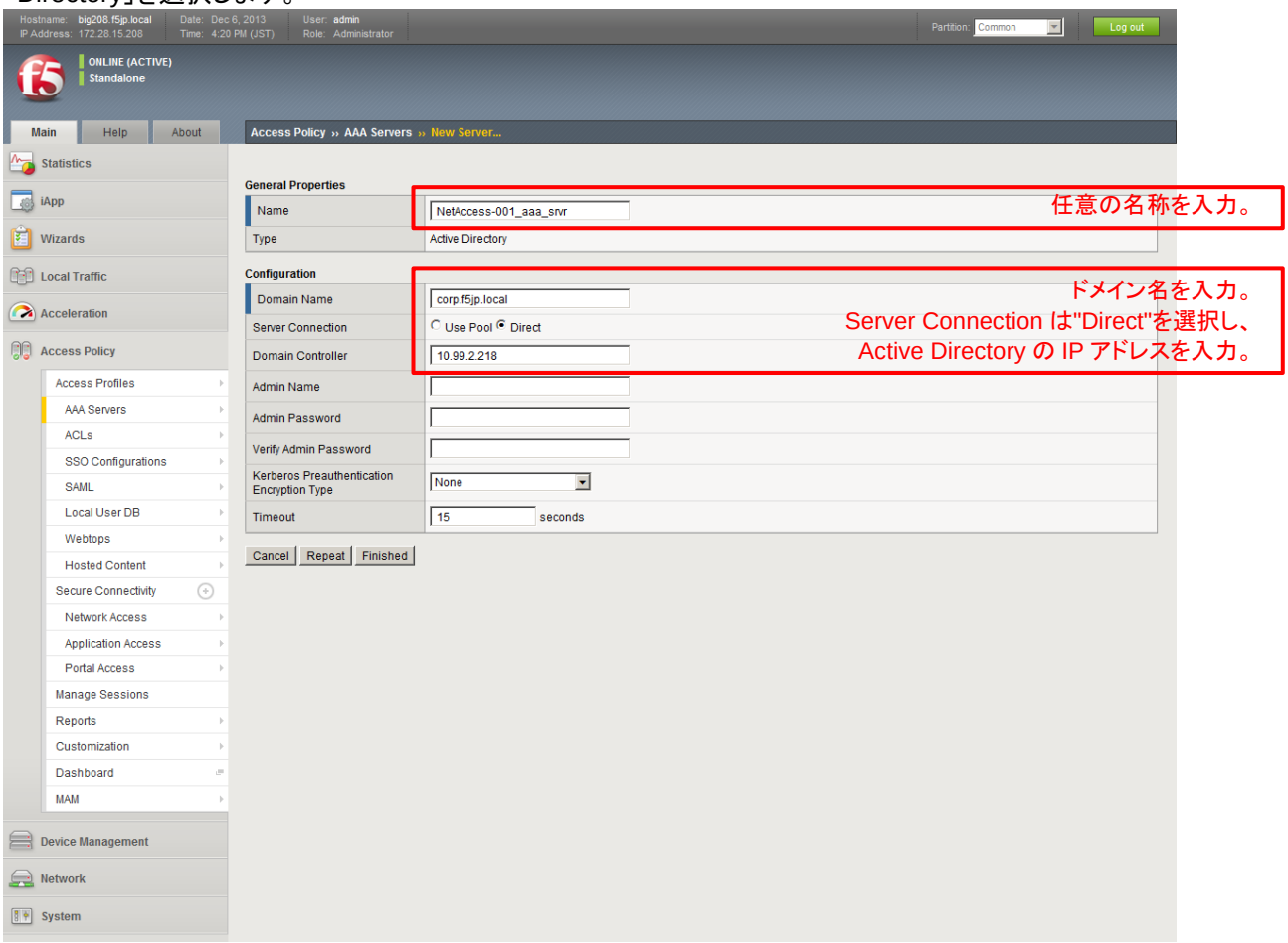


(2) NTP を設定します。
「Device」タブから「NTP」を選択します。



6.1.2.2. 認証サーバ：Active Directory の設定

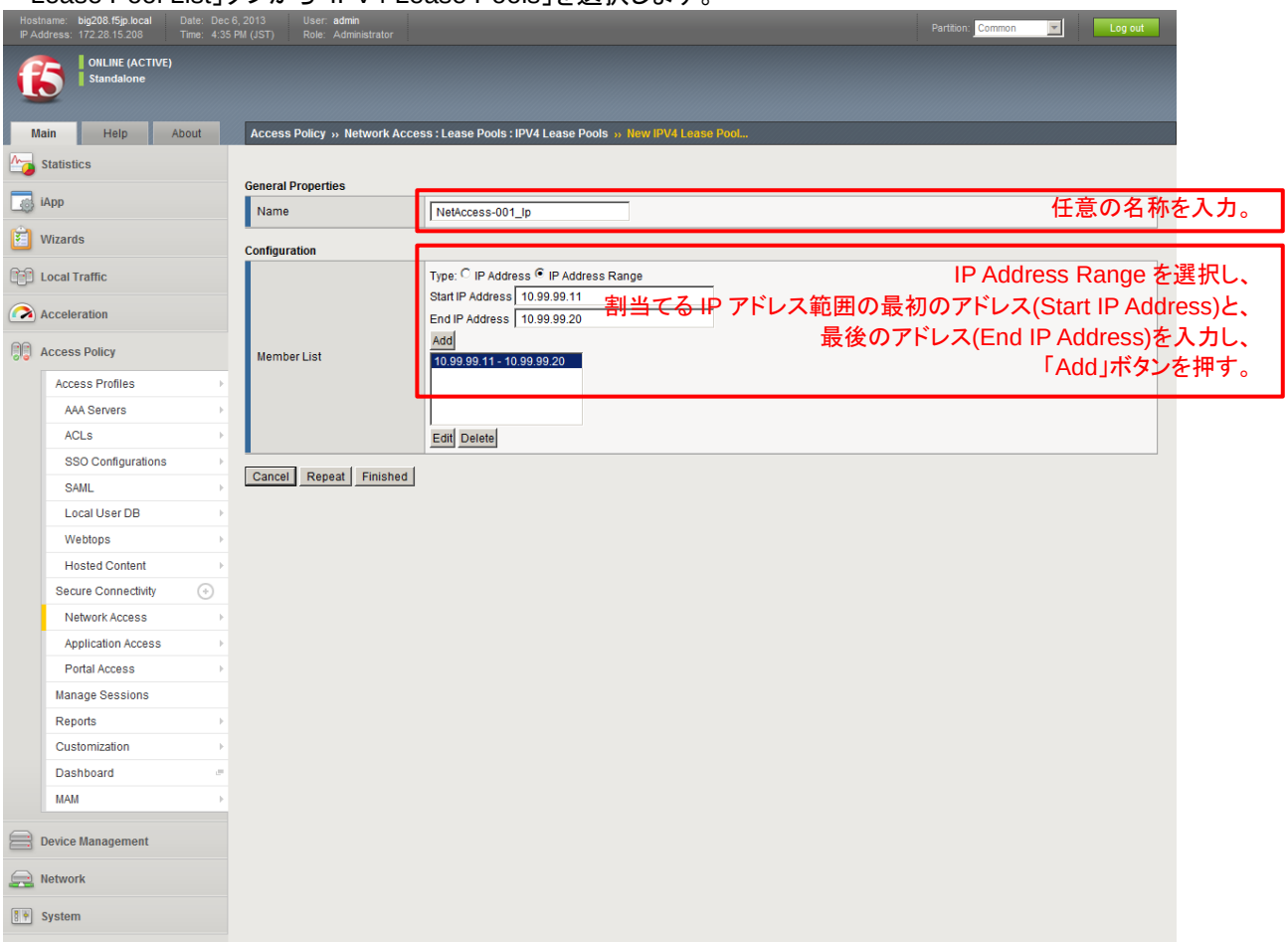
「Main」メニュー →「Access Policy」→「AAA Servers」へ移動し、「AAA Server by Type」タブから、「Active Directory」を選択します。



6.1.2.3. Lease Pool の設定

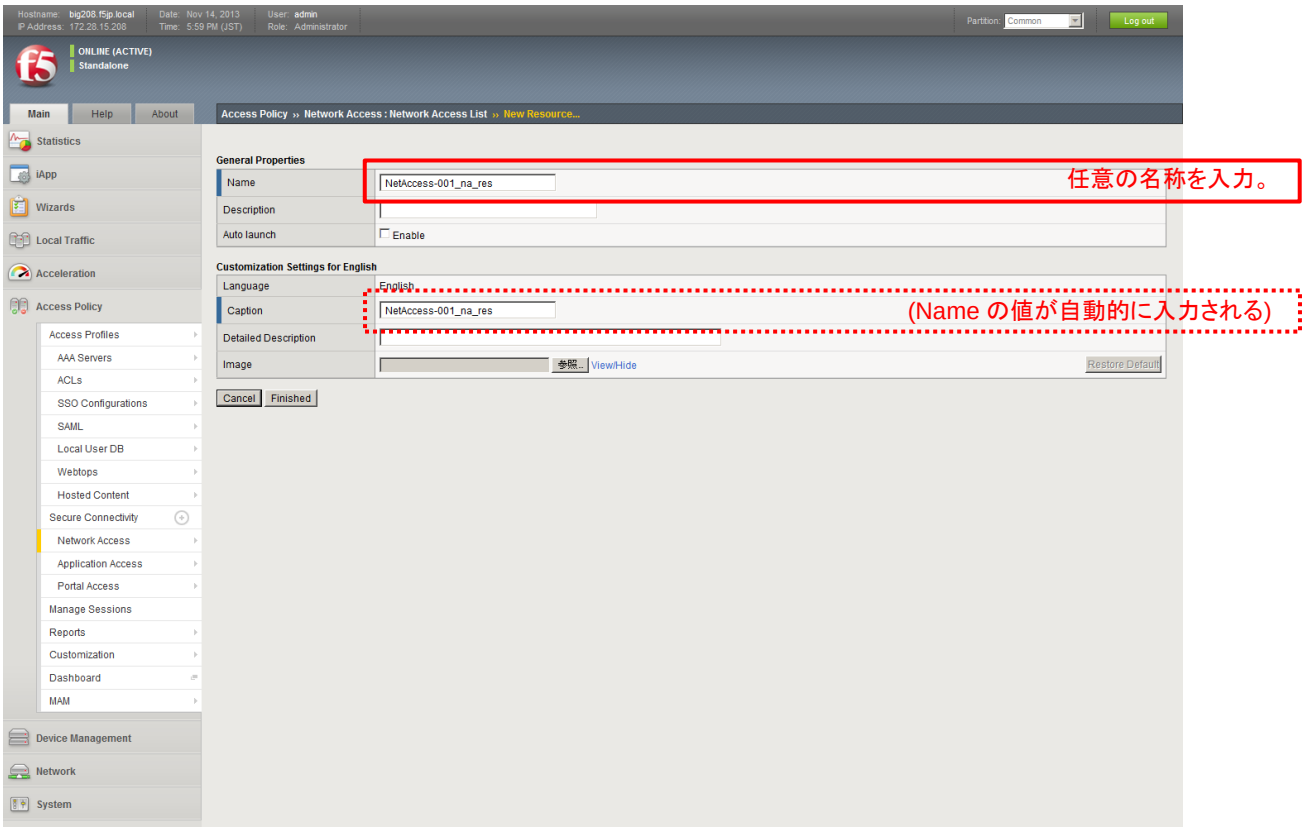
クライアントに割当てる IP アドレス群:リースプールを設定します。

「Main」メニュー →「Access Policy」→「Network Access」へ移動します。
「Lease Pool List」タブから「IPV4 Lease Pools」を選択します。

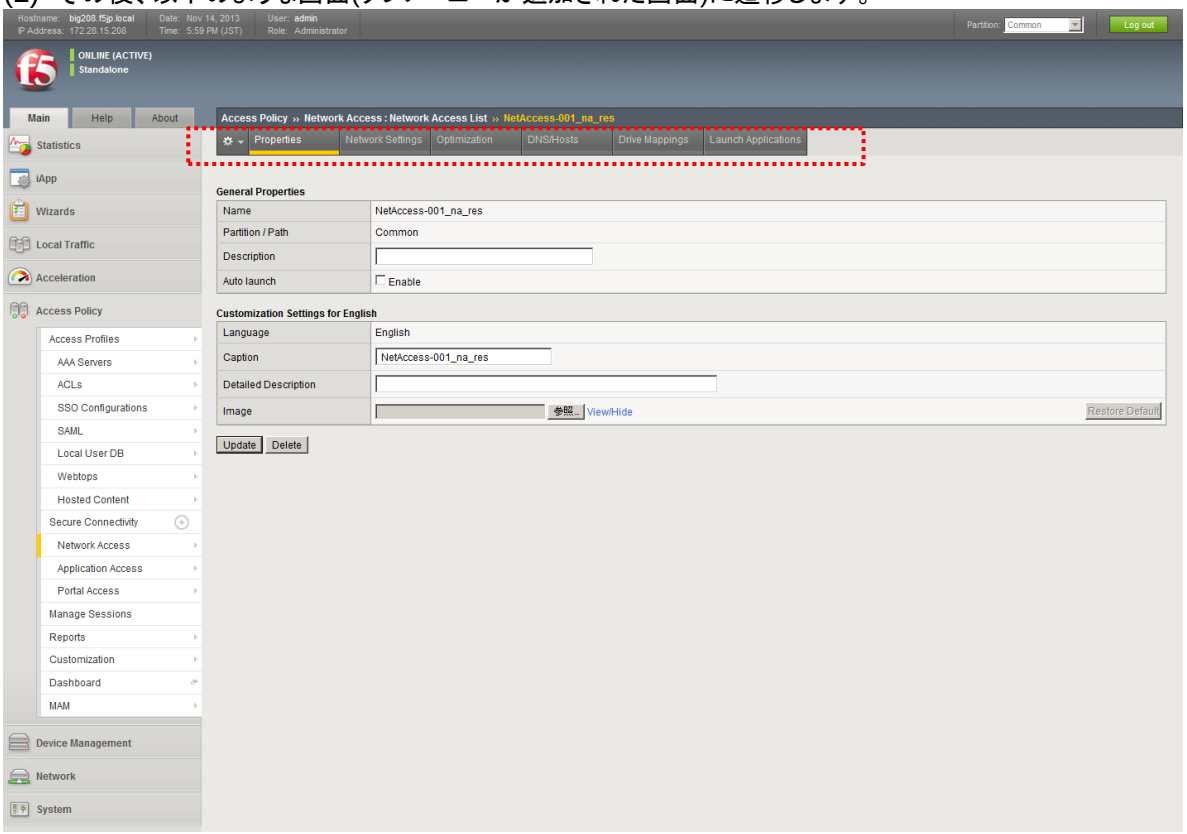


6.1.2.4. Network Access の設定

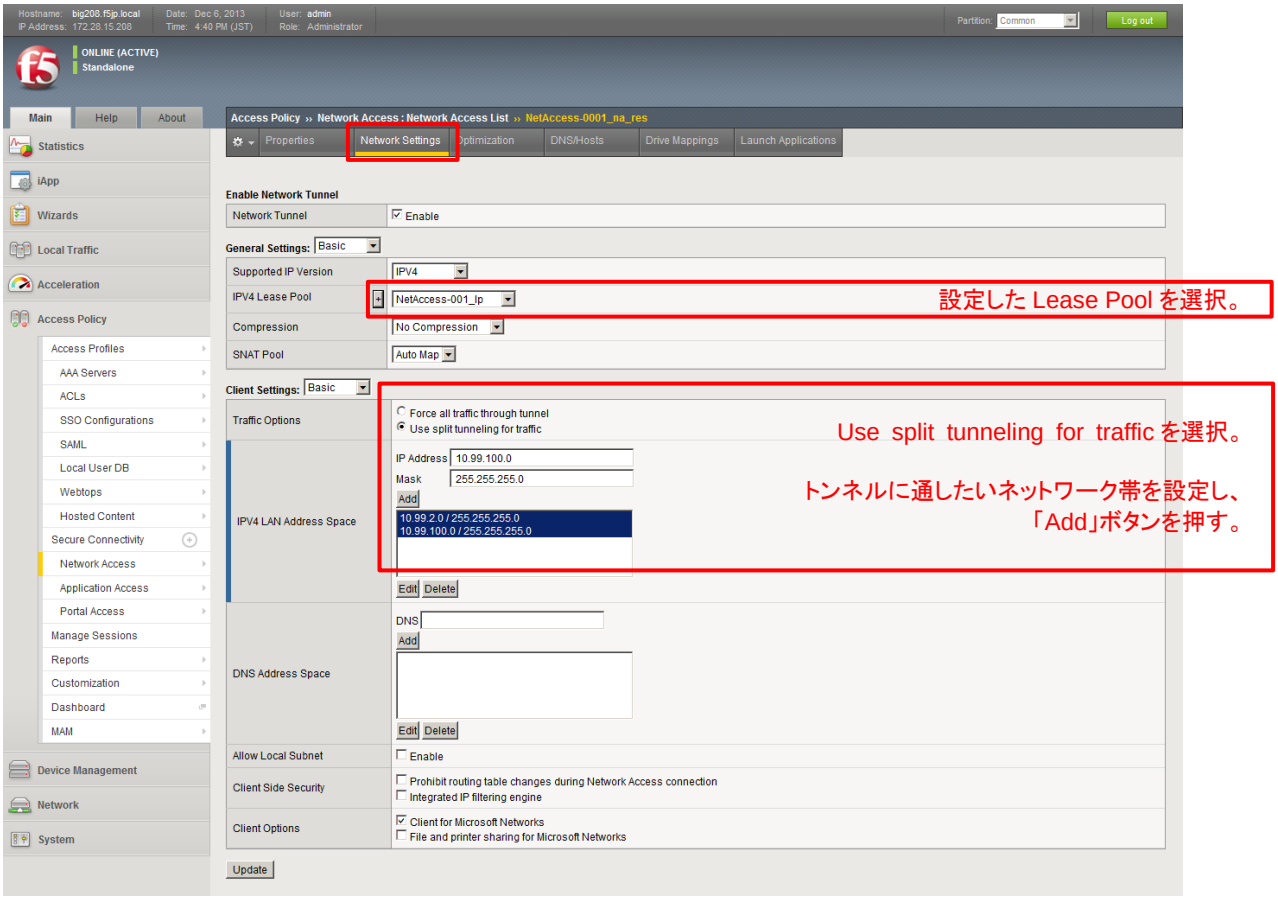
(1) 「Main」メニュー → 「Access Policy」 → 「Network Access」 へ移動します。
「Network Access List」タブを選択し、左に表示された「Create」ボタンを押すと、以下の画面が出ます。
以下のように、値を入力し、「Finished」ボタンを押します。



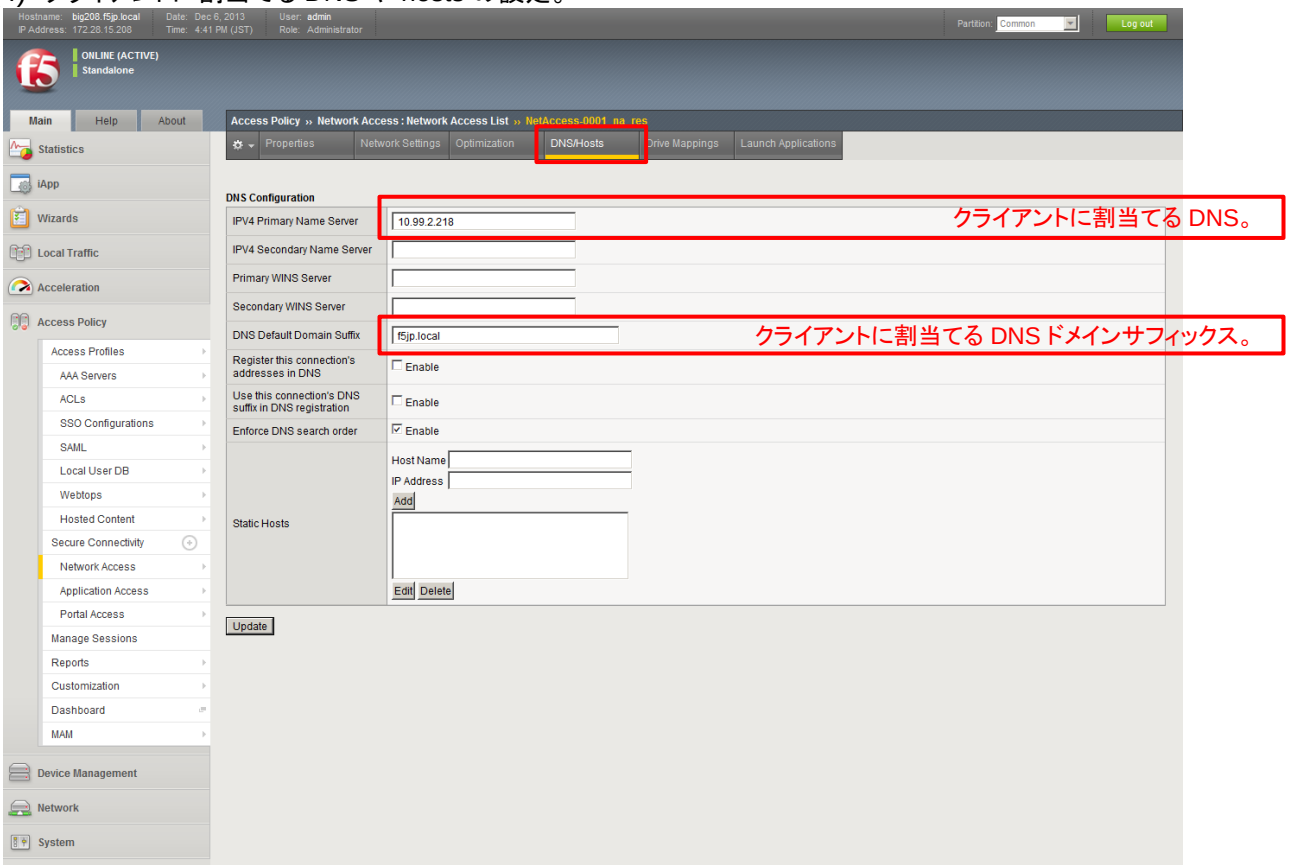
(2) その後、以下のような画面(タブメニューが追加された画面)に遷移します。



(3) Network Settings タブでの設定。
ここで、既に設定した Lease Pool を選択します。スプリット・トンネルの設定もここで行います。

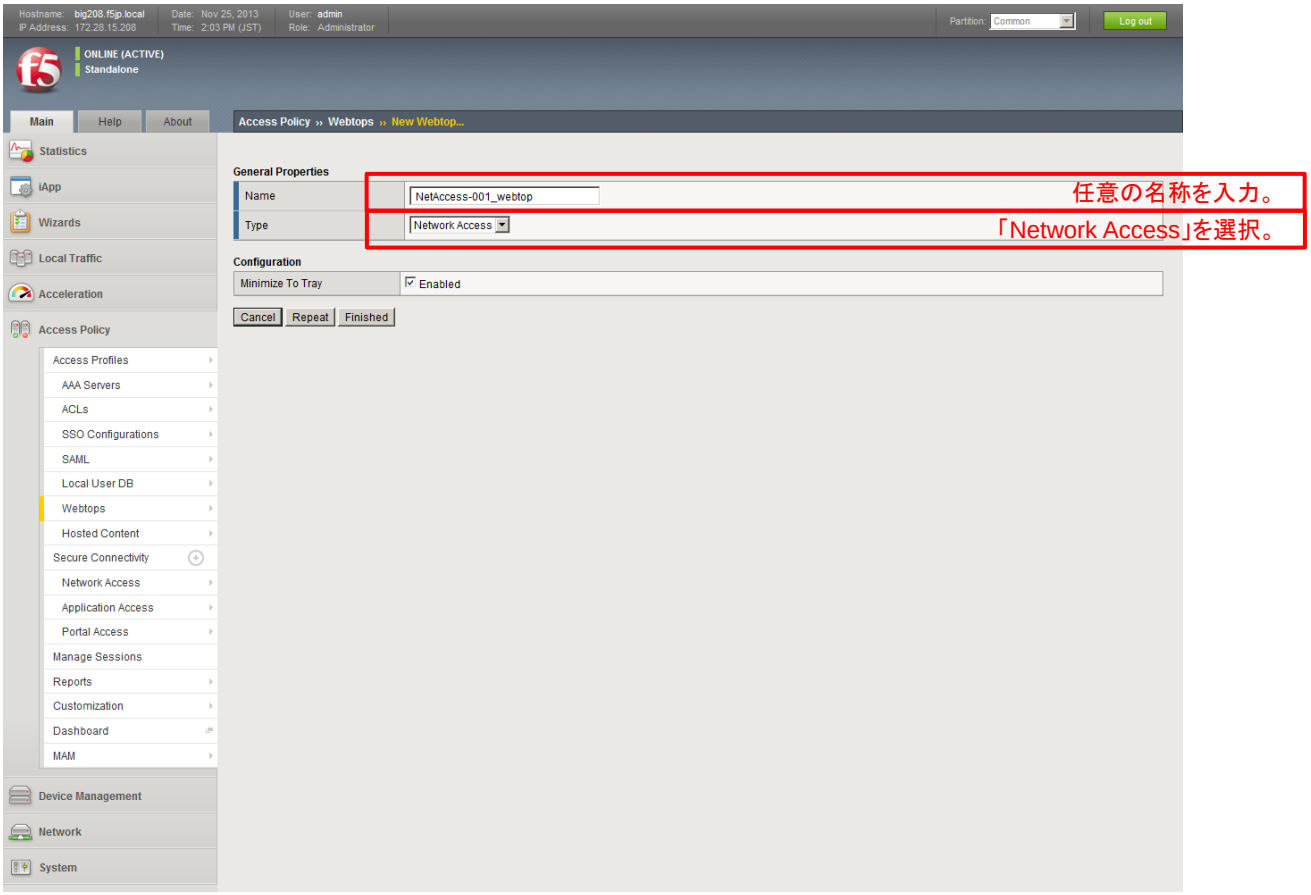


(4) クライアントに割当てる DNS や hosts の設定。



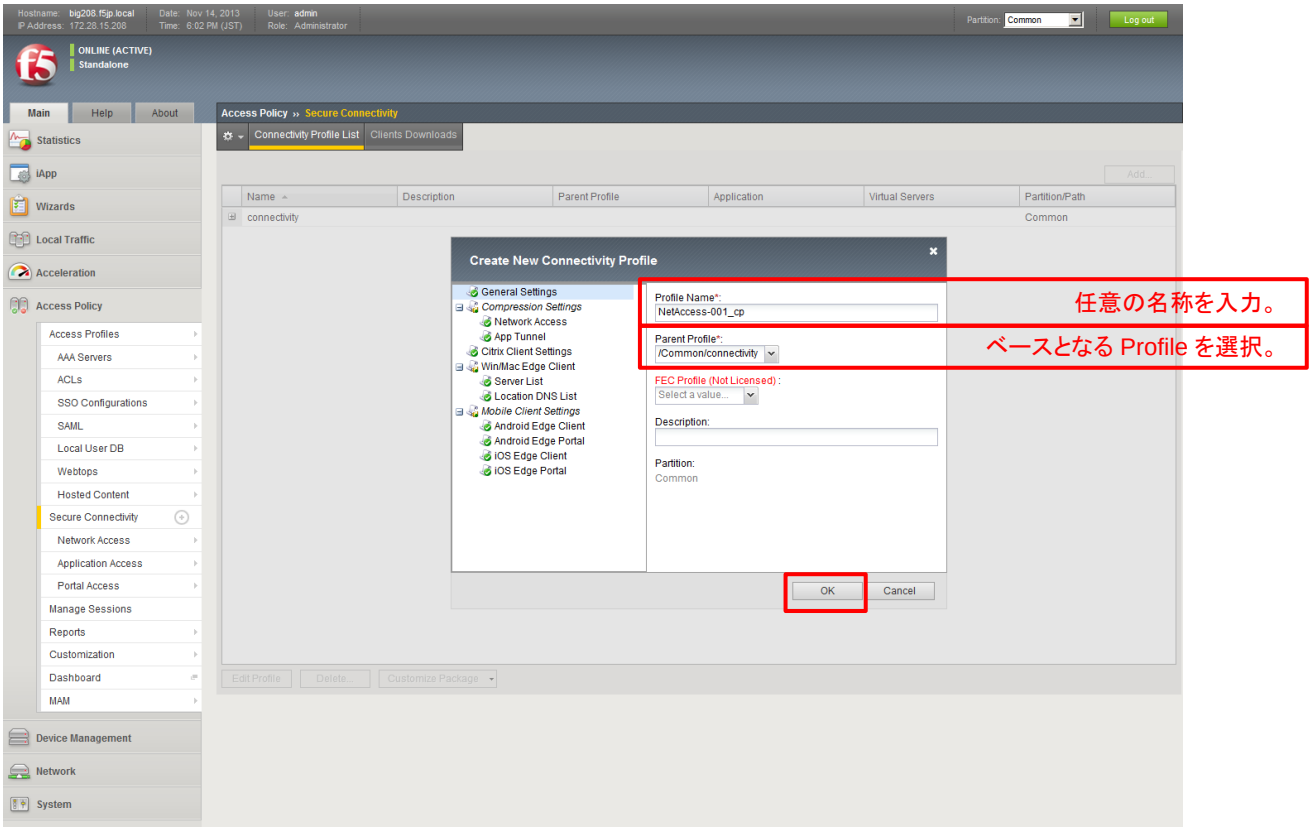
6.1.2.5. Webtop の設定

「Main」メニュー → 「Access Policy」 → 「Webtops」を選択します。
右上に表示された「Create」ボタンを押すと、以下の画面が現れます。
以下の 2 ヶ所を設定し、「Finished」ボタンを押します。



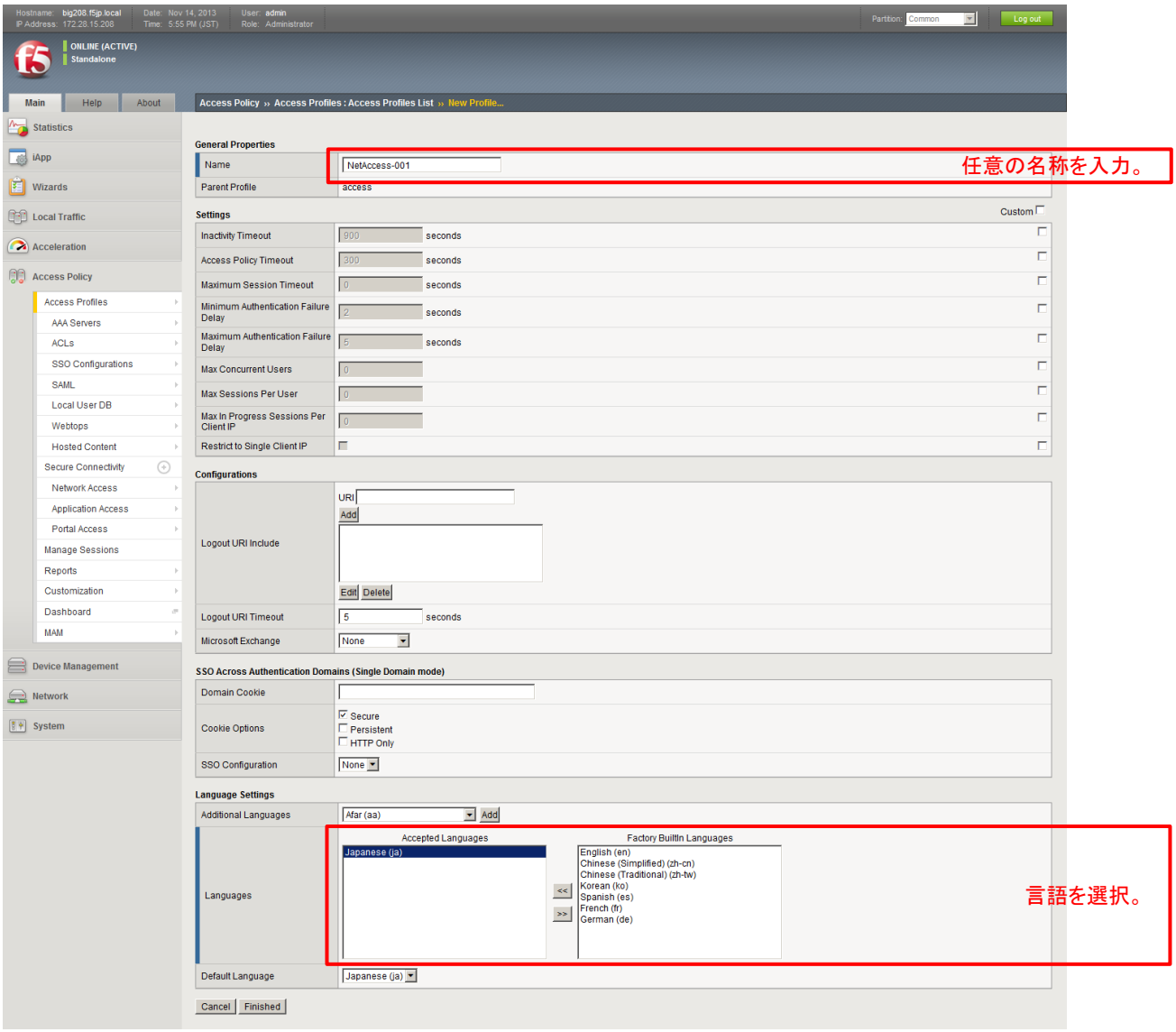
6.1.2.6. Connectivity Profile の設定

「Main」メニュー → 「Access Policy」 → 「Secure Connectivity」で以下の画面が現れます。
右上に表示される「Add」ボタンを押すと、以下の画面が現れます。
以下 2 ヶ所を設定し、「OK」ボタンを押します。

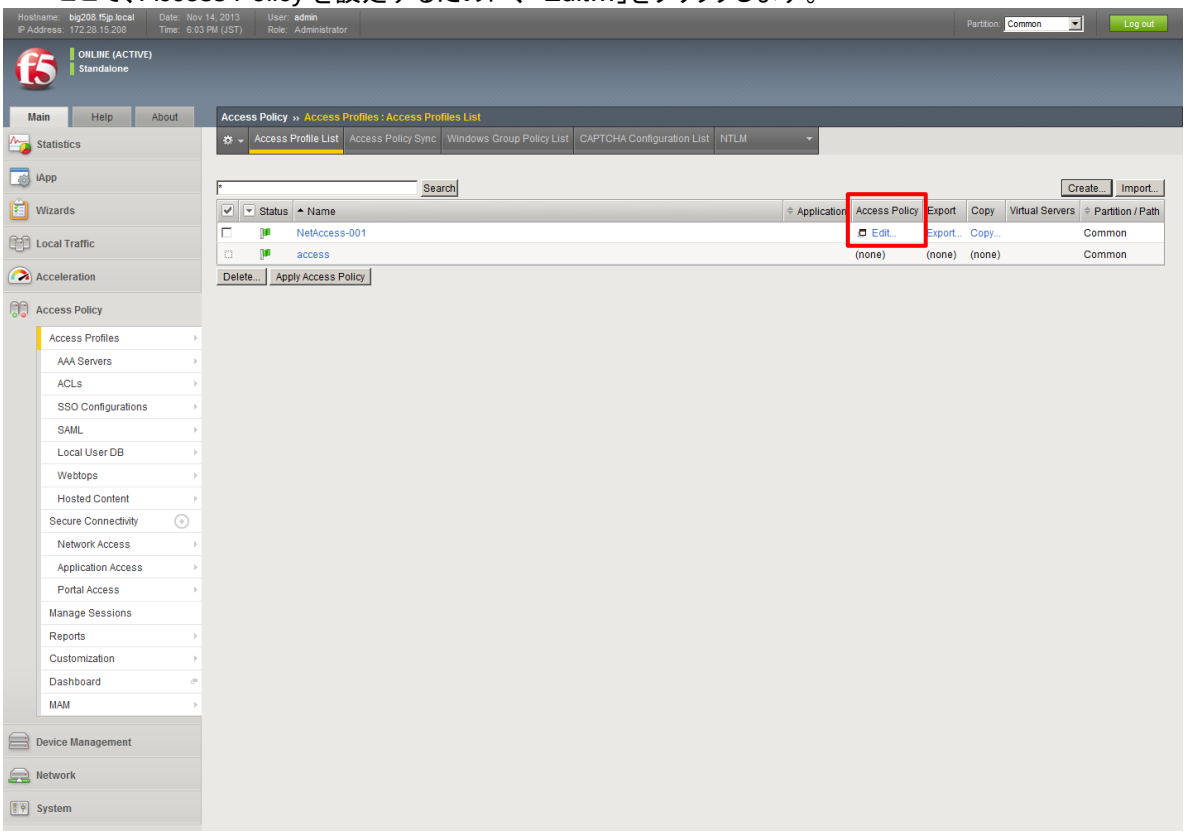


6.1.2.7. Access Profile と Access Policy の設定

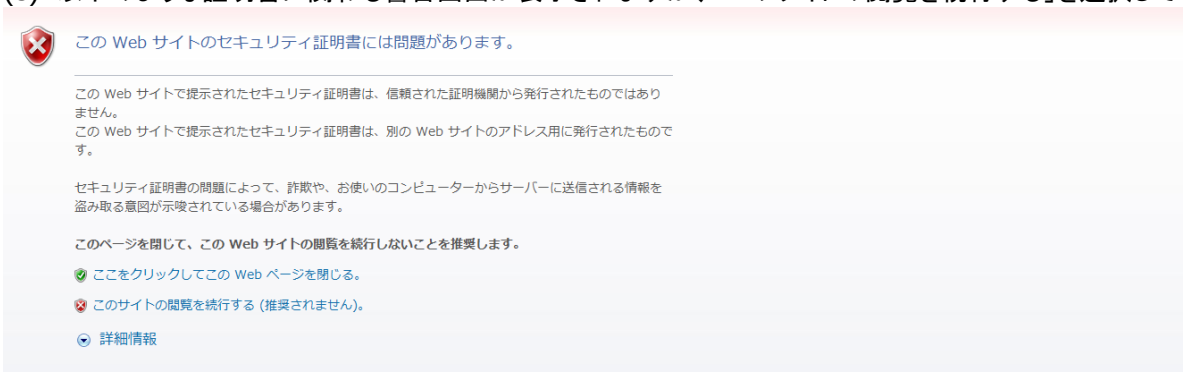
(1) 「Main」メニュー → 「Access Policy」 → 「Access Profile」 → 「Access Profile List」を選択。
右上に表示された「Create」ボタンを押すと、以下の画面が現れます。
以下 2 ヶ所を設定し、「Finished」ボタンを押します。



(2) その後、以下の画面に遷移します。
ここで、Access Policy を設定するために、「Edit…」をクリックします。

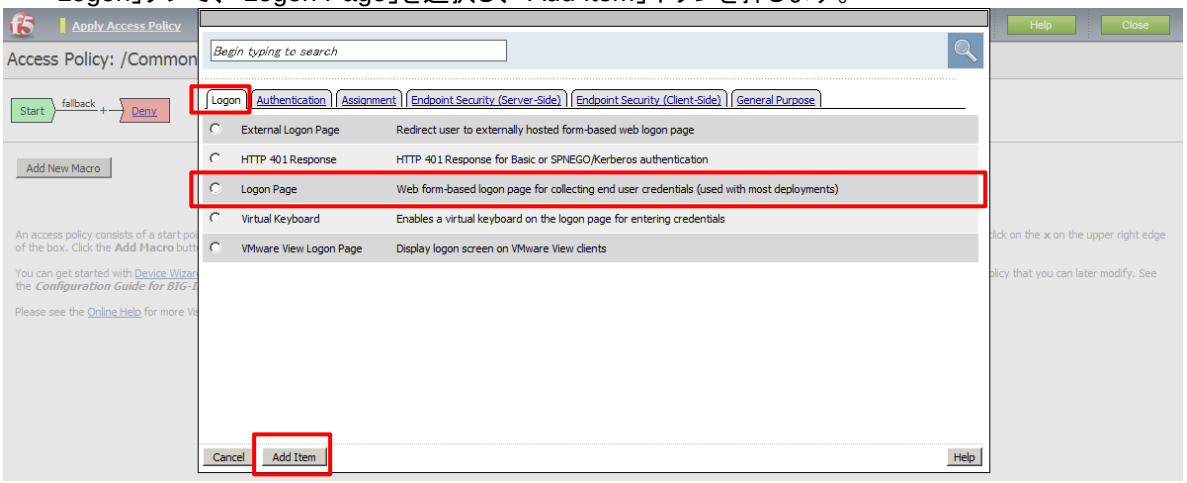


(3) 以下のような証明書に関わる警告画面が表示されますが、「このサイトの閲覧を続行する」を選択してください。

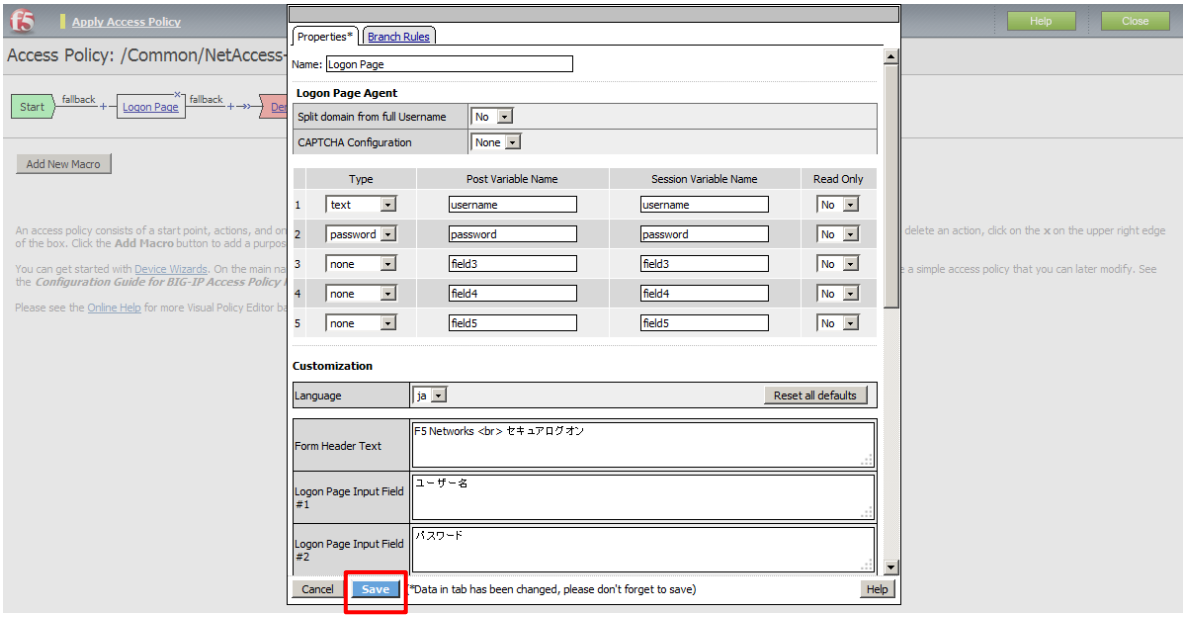


(4) 以下の画面：Visual Policy Editor (VPE) が表示されます。
"Start"と"Deny"の線上にある、「+」をクリックします。

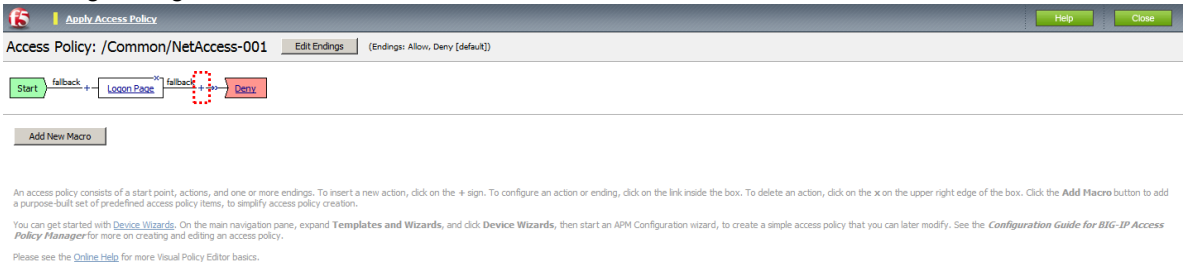
(5) その後、以下の画面が現れます。
「Logon」タブで、「Logon Page」を選択し、「Add Item」ボタンを押します。



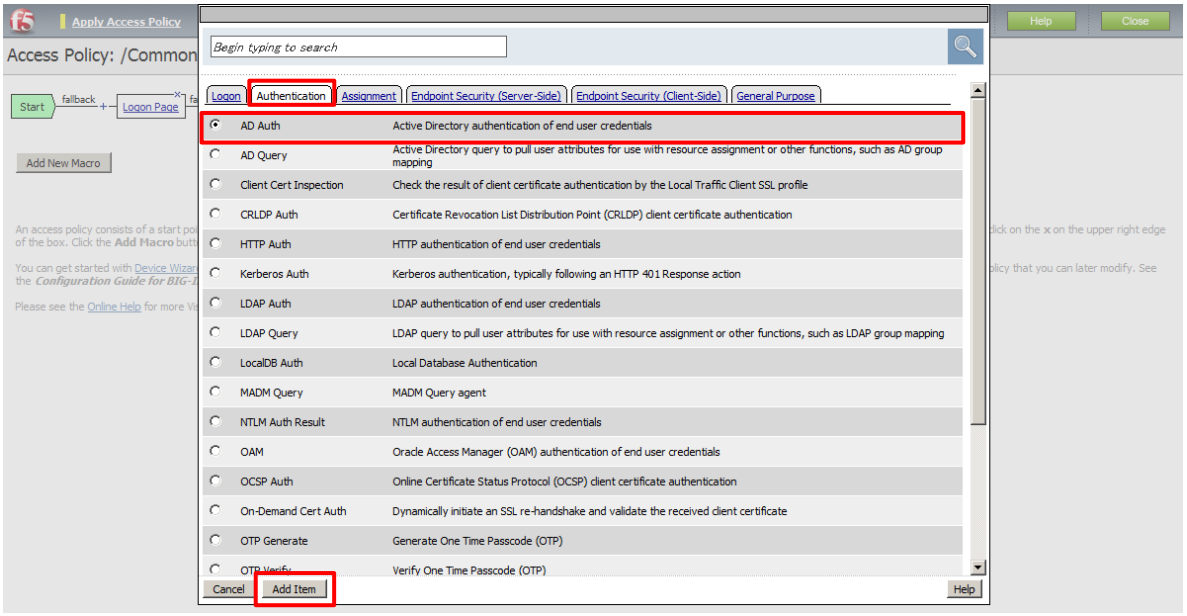
(6) その後、以下の画面が現れます。
ここでは、特に変更は行わず、「save」ボタンを押します。



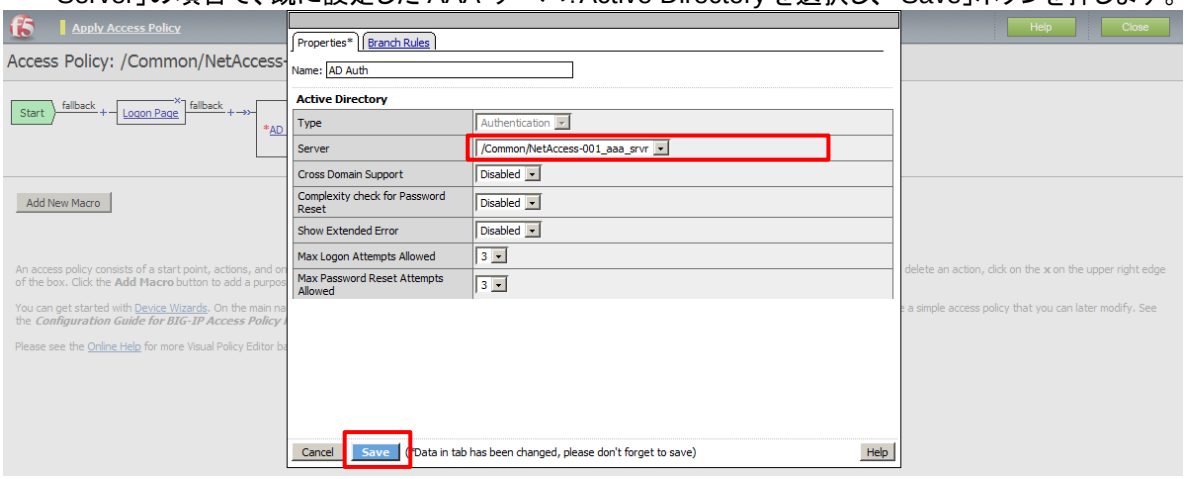
(7) 以下のような状態になります。
Logon Page の後ろにある「+」をクリックします。



(8) その後、以下の画面が現れます。
「Authentication」タブで、「AD Auth」を選択し、「Add Item」ボタンを押します。

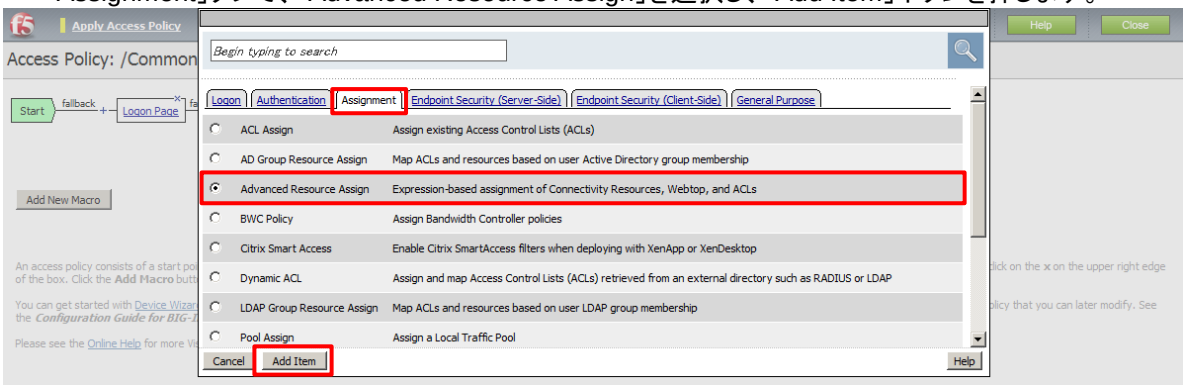


(9) その後、以下の画面が現れます。
「Server」の項目で、既に設定した AAA サーバ：Active Directory を選択し、「Save」ボタンを押します。

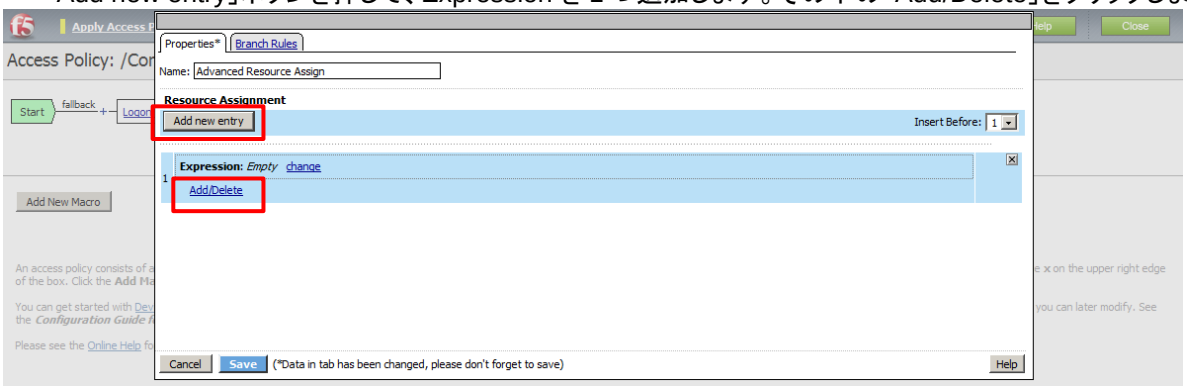


(10)以下のような状態になります。
「AD Auth」の後ろにある、Successful 側の「+」をクリックします。

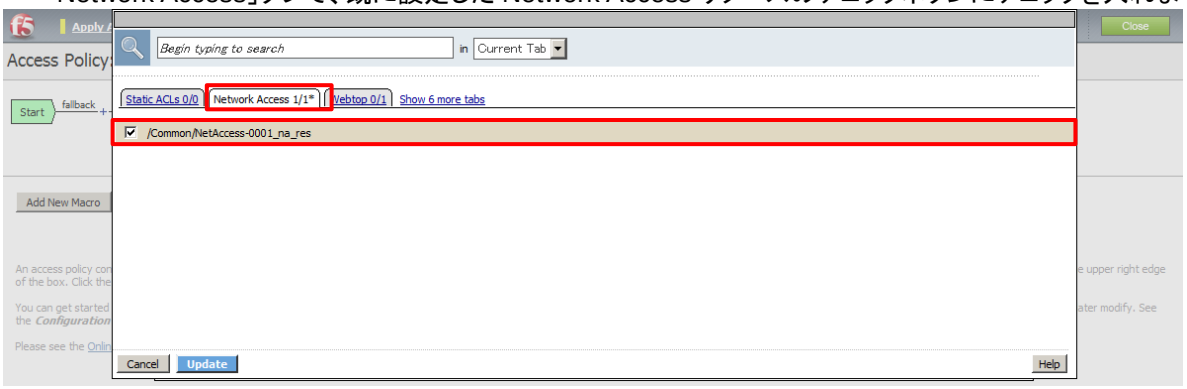
(11)その後、以下の画面が現れます。
「Assignment」タブで、「Advanced Resource Assign」を選択し、「Add Item」ボタンを押します。



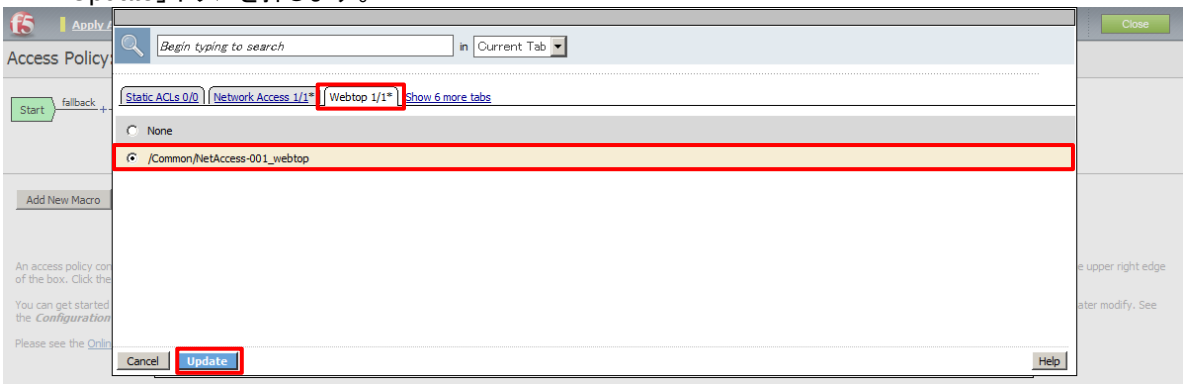
(12)その後、以下の画面が現れます。
「Add new entry」ボタンを押して、Expression を 1 つ追加します。その下の「Add/Delete」をクリックします。



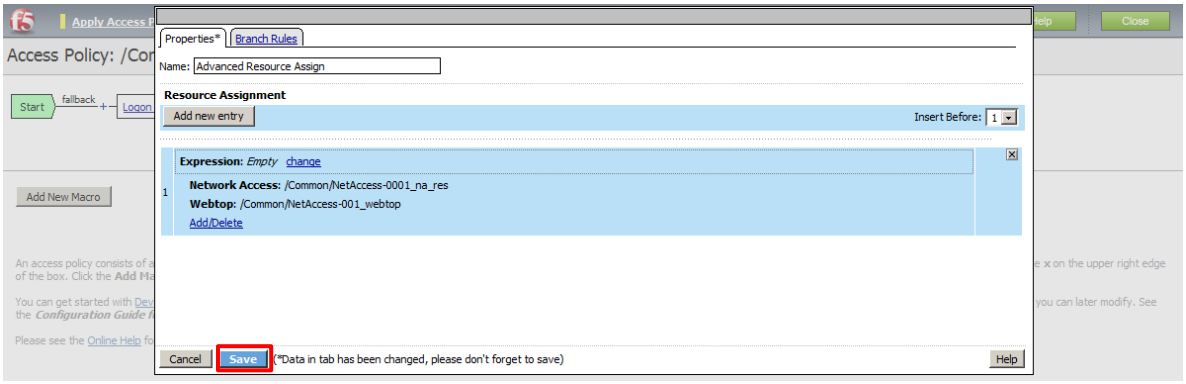
(13)その後、以下の画面が現れます。
「Network Access」タブで、既に設定した Network Access リソースのチェックボタンにチェックを入れます。



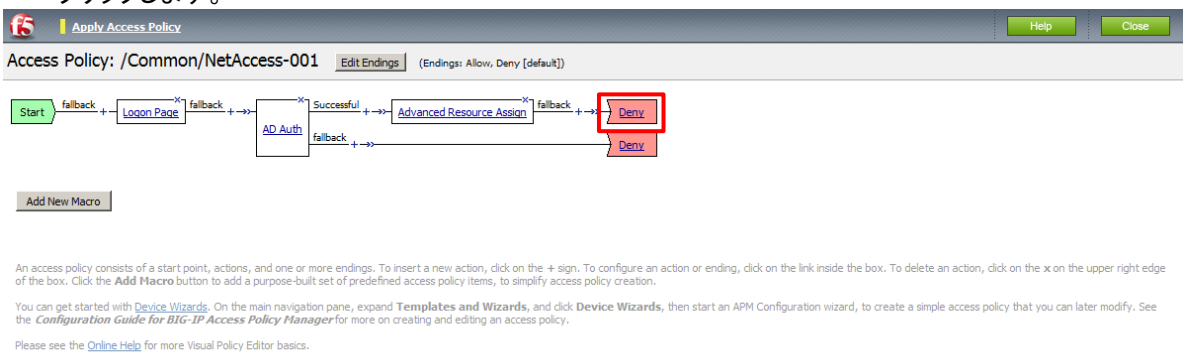
(14)「Webtop」タブで、既に設定した Netowrk Access 用 Webtop のチェックボタンにチェックを入れます。
「Update」ボタンを押します。



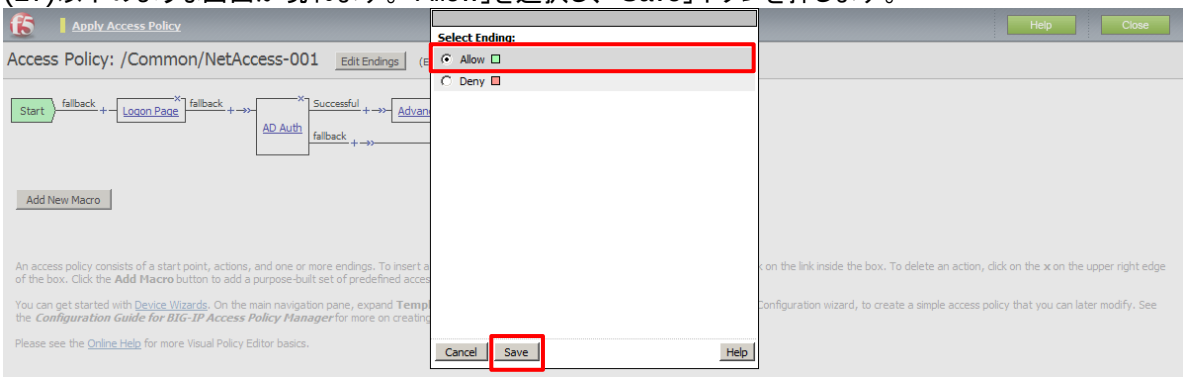
(15)その後、以下のような状態になります。
「Save」ボタンを押します。



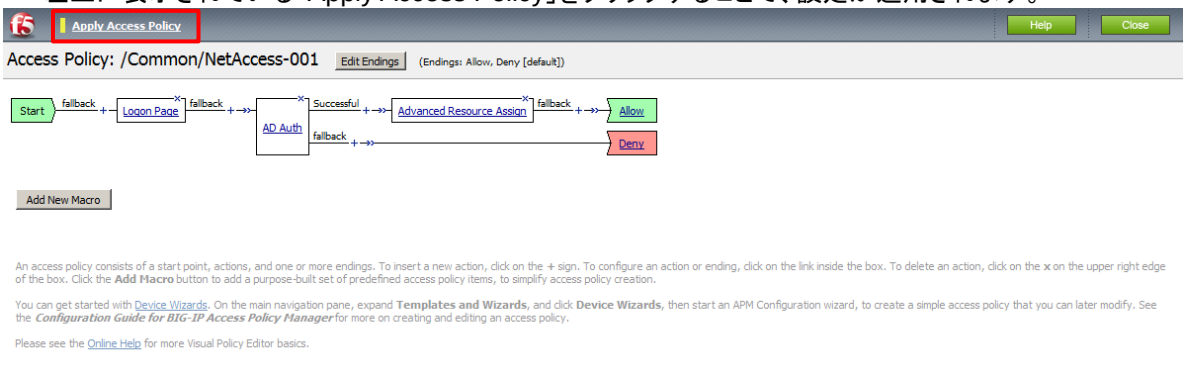
(16)以下のような状態になります。
最後に「Advance Resource Assign」の後ろにある「Deny」を「Allow」に変更する必要があるので、その「Deny」をクリックします。



(17)以下のような画面が現れます。「Allow」を選択し、「Save」ボタンを押します。

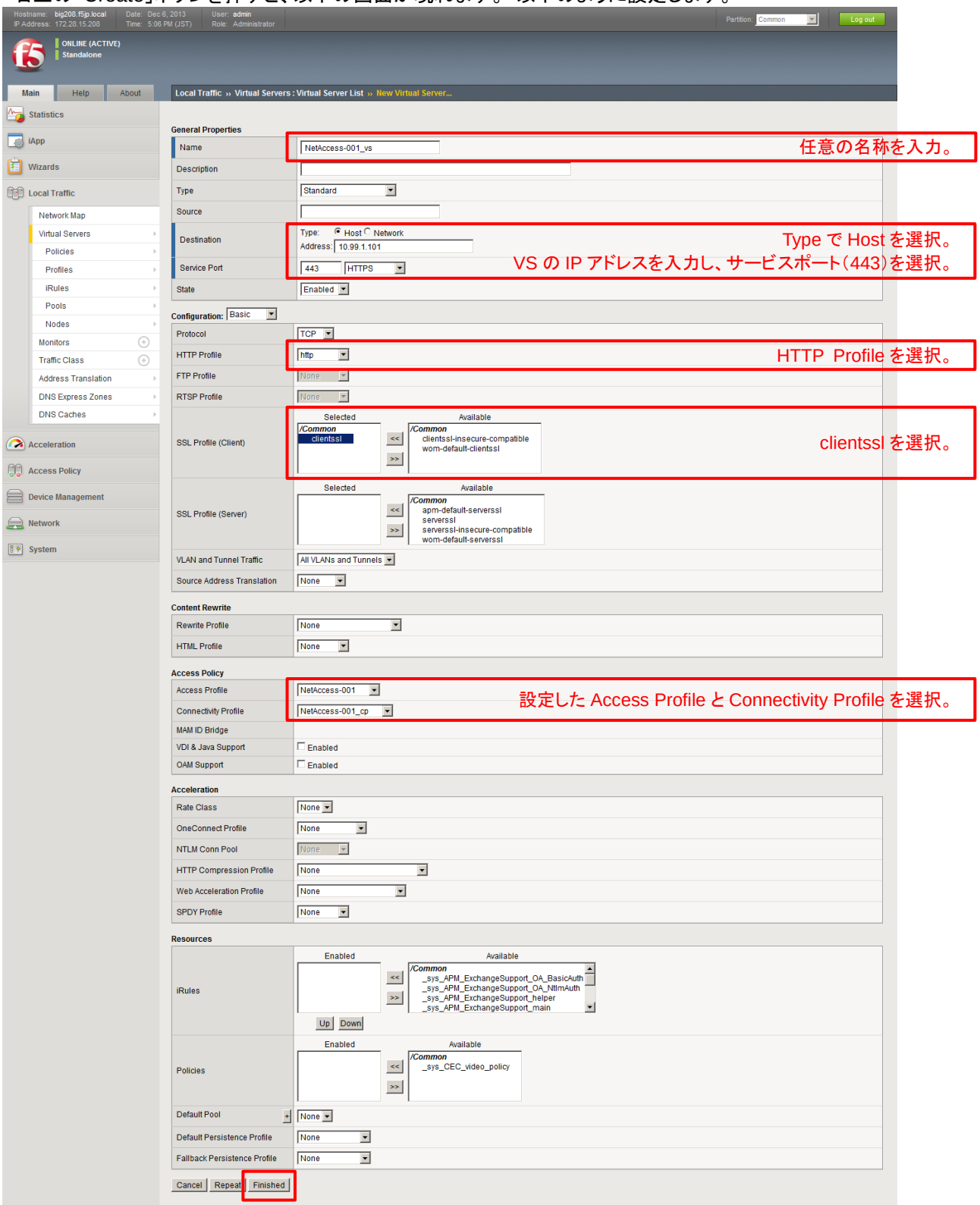


(18)VPE の設定は以上ですが、まだ設定した値は適用されていません。
左上に表示されている「Apply Access Policy」をクリックすることで、設定が適用されます。



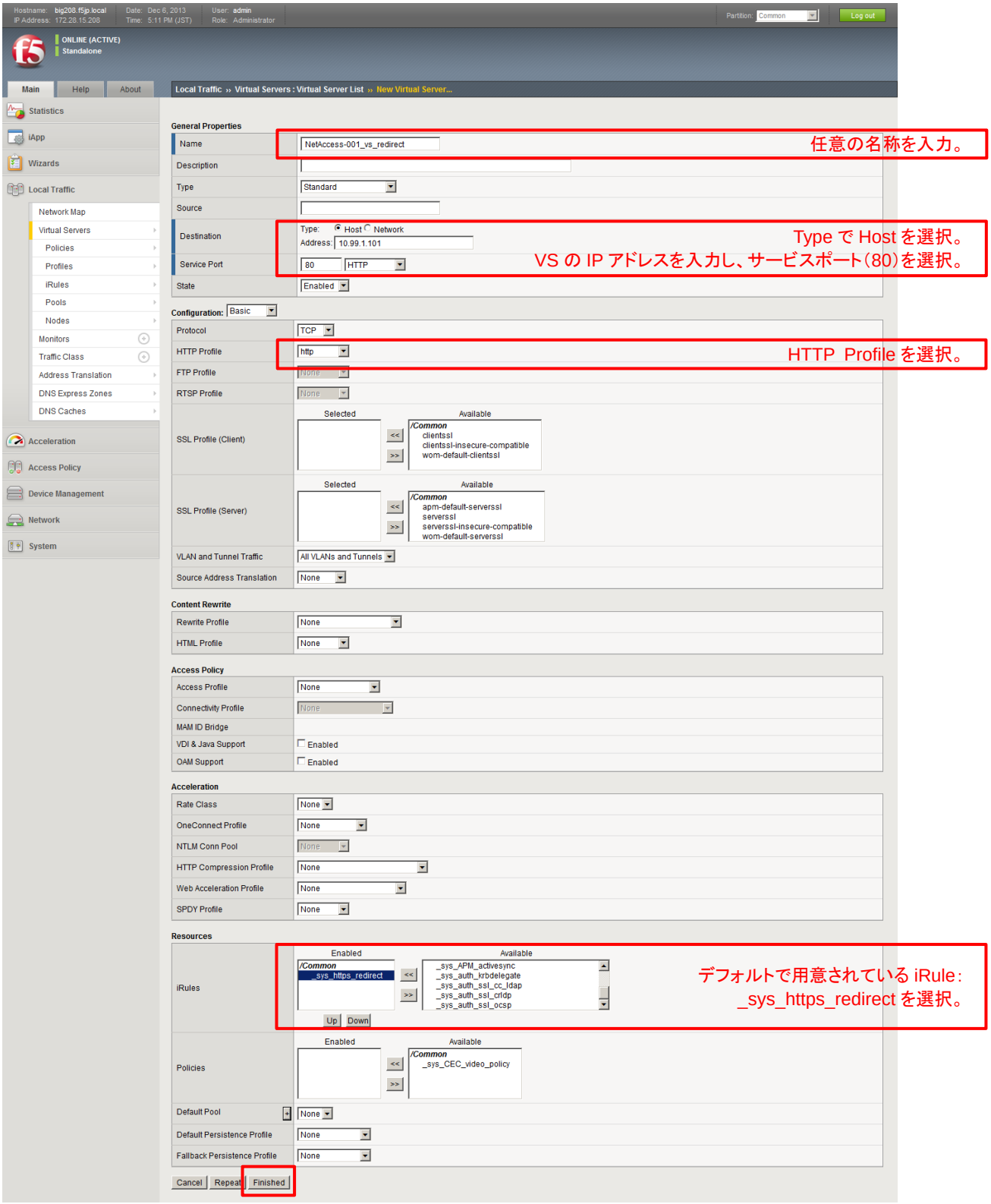
6.1.2.8. APM 用 Virtual Server の設定

「Main」メニュー →「Local Traffic」→「Virtual Servers」を選択します。
右上の「Create」ボタンを押すと、以下の画面が現れます。 以下のように設定します。



6.1.2.9. リダイレクト用 Virtual Server の設定

HTTP(80)でアクセスしても、APM 用 Virtual Server(HTTPS(443))へリダイレクトされるように、リダイレクト用の Virtual Server を新規に設定します。



以上で、ウィザードで設定した内容と同等の状態になります。

6.1.2.10. クライアント PC からのアクセス

クライアント PC から、設定した Virtual Server へのアクセスが完了することを確認します。

6.1.3. SSL サーバ証明書の設定

初級編での設定と同様です。
既述の「SSL サーバ証明書の設定」を参照してください。

6.2. クライアント証明書認証の設定

クライアント証明書による認証を行う設定方法を記載します。

6.2.1. クライアント証明書の発行

クライアント証明書認証の設定を行うためには、以下 2 つの証明書が必要です。

① 認証局の証明書
BIG-IP 側で利用します。

② クライアント証明書
クライアント PC 側で利用します。

クライアント証明書の発行には、大きくは以下 2 つの方法があります。

a) 商用の認証局(Verisign、CyberTrust 等)から発行してもらう
b) 独自の認証局(例：OpenSSL の利用)を建てて、発行する

本ガイドでは、b)の方法：OpenSSL を使って独自の認証局を建てて、クライアント証明書を発行しました。

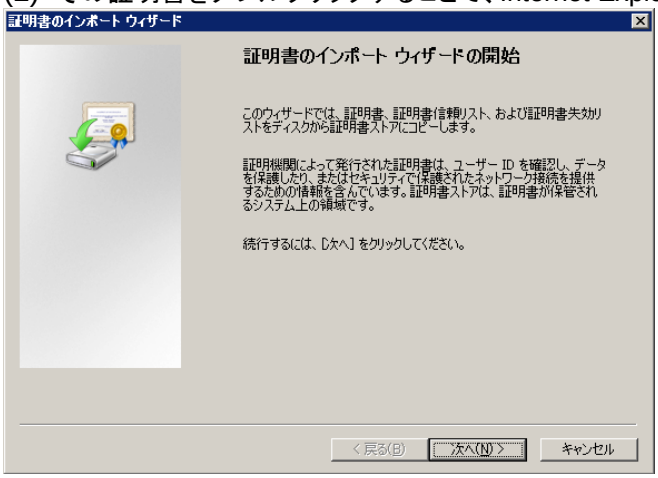
クライアント証明書を発行する際、PKCS#12 形式で発行することで、キーと証明書を一つのファイルとしてクライアントに提供することが可能です。
本例では、PKCS#12 形式で、「apmclient001.p12」というファイル名のクライアント証明書を発行しました。

6.2.2. クライアント PC へクライアント証明書をインポート

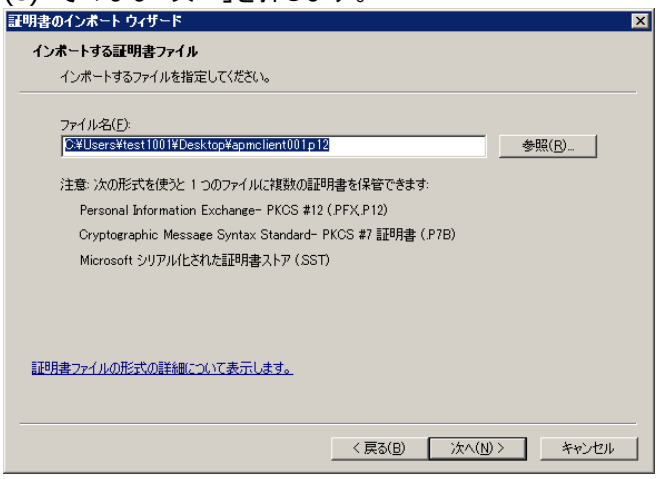
クライアント証明書(PKCS#12)を、クライアント PC へインストールする手順について、参考までに記載します。
本ガイドのクライアント PC は、Windows7＋Internet Explorer 10 を利用しています。

(1) クライアント証明書：「apmclient001.p12」を Windows へコピーします。

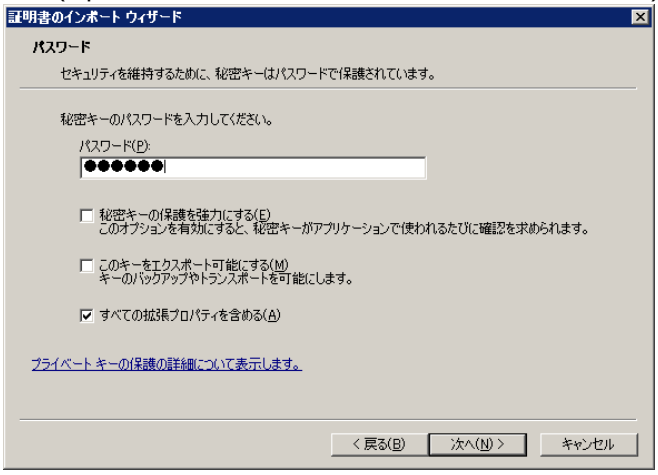
(2) その証明書をダブルクリックすることで、Internet Explorer へのインポートが開始されます。



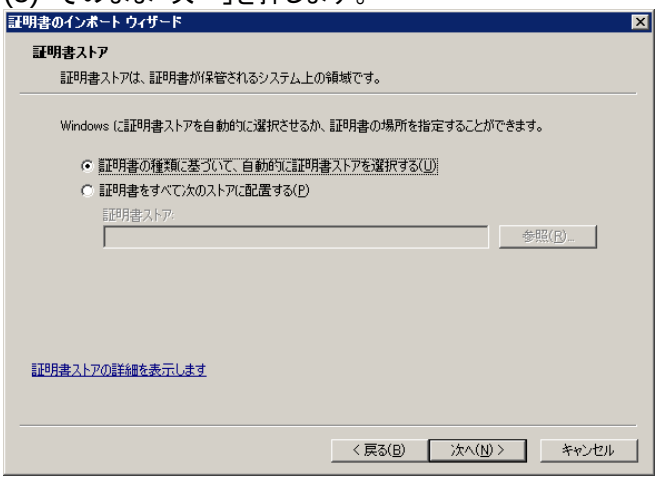
(3) そのまま「次へ」を押します。



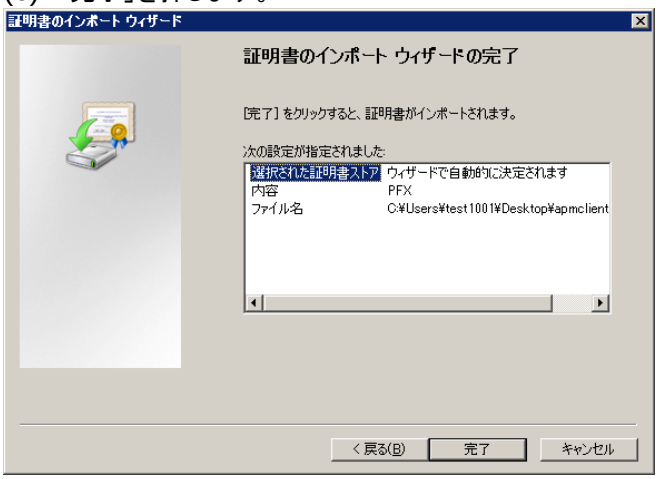
(4) 秘密キーがパスワードで保護されているので、パスワードを入力します。
(OpenSSL で発行する際に指定したパスワードです。)



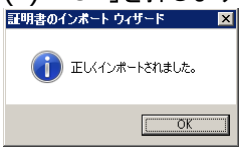
(5) そのまま「次へ」を押します。



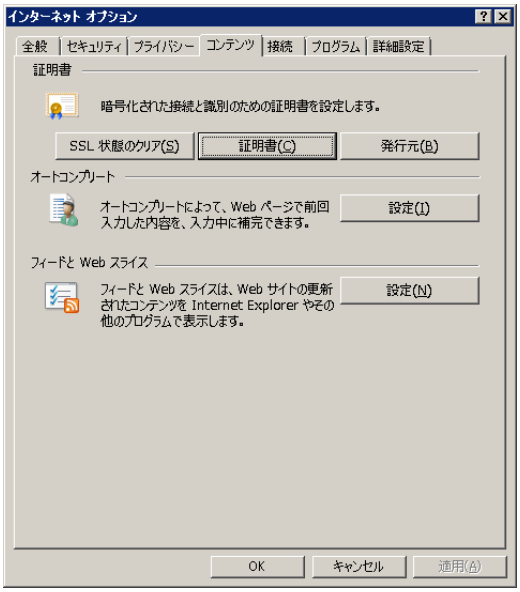
(6)「完了」を押します。



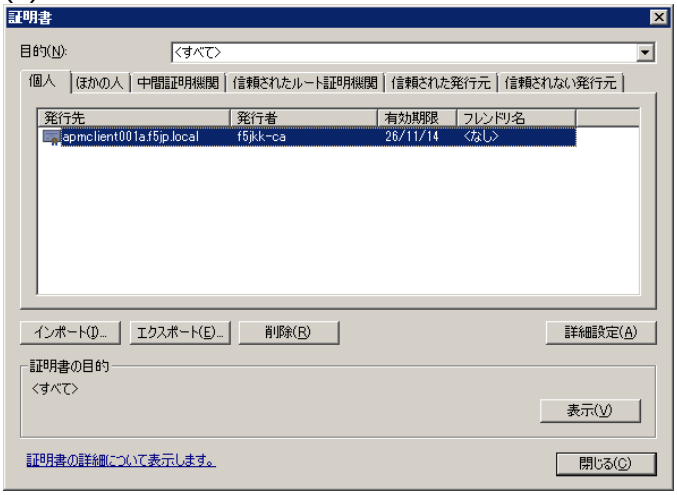
(7)「OK」を押します。



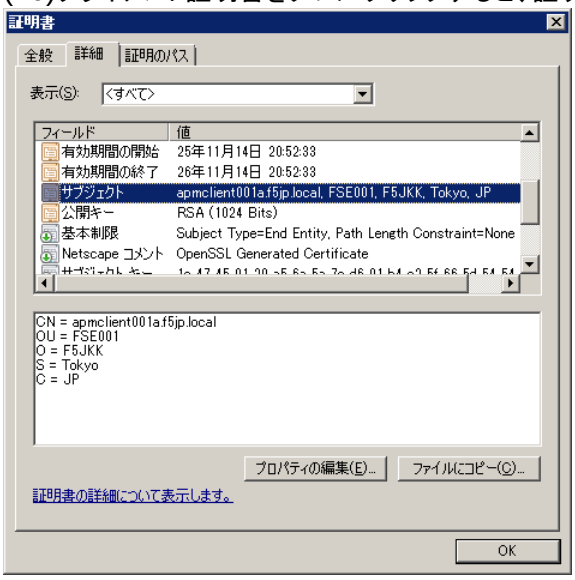
(8) 証明書がインストールされた状態を確認するには、
IE10 の「ツール」→「インターネットオプション」→「証明書」ボタンを押します。



(9)「個人」タブで、クライアント証明書がインストールされていることを確認できます。



(10)クライアント証明書をダブルクリックすると、証明書の詳細が確認できます。



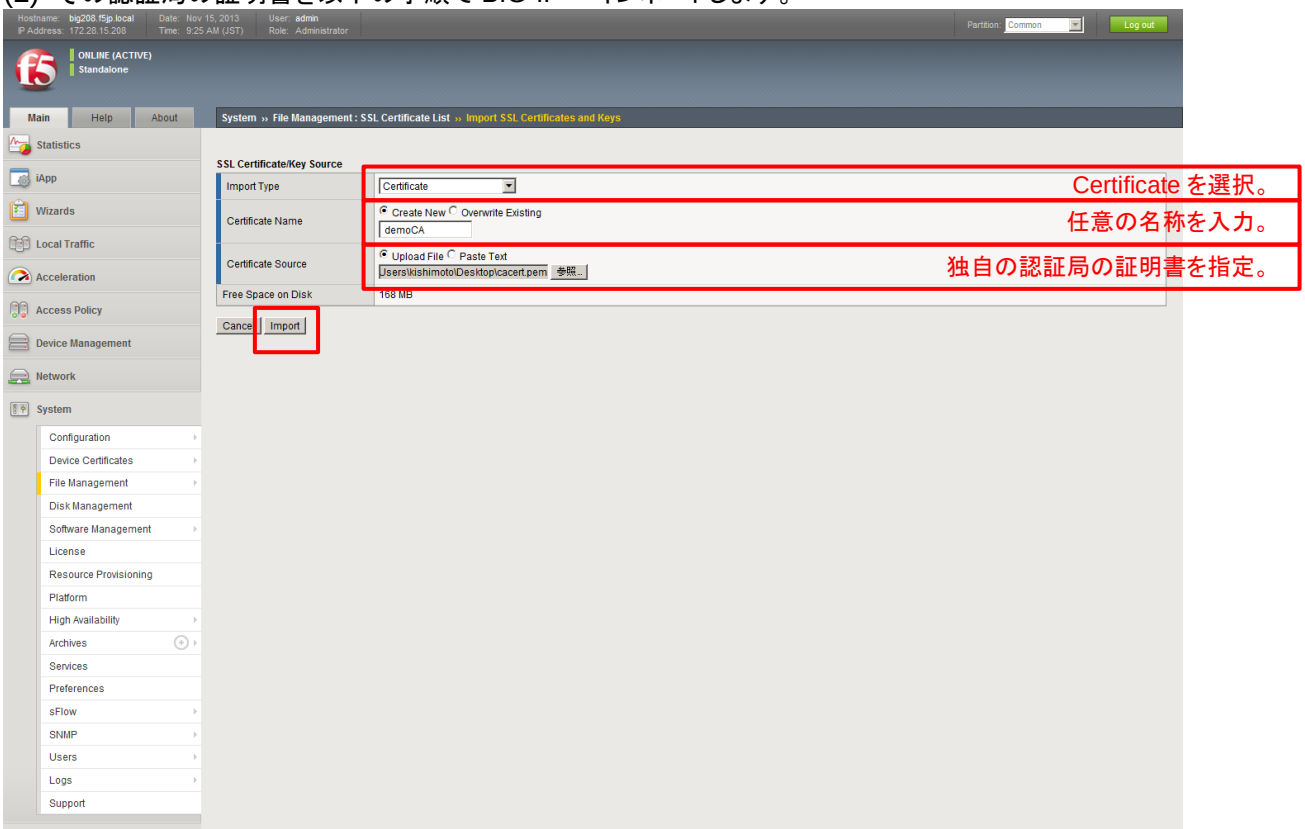
6.2.3. BIG-IP の設定

クライアント証明書認証に必要な BIG-IP の設定を示します。

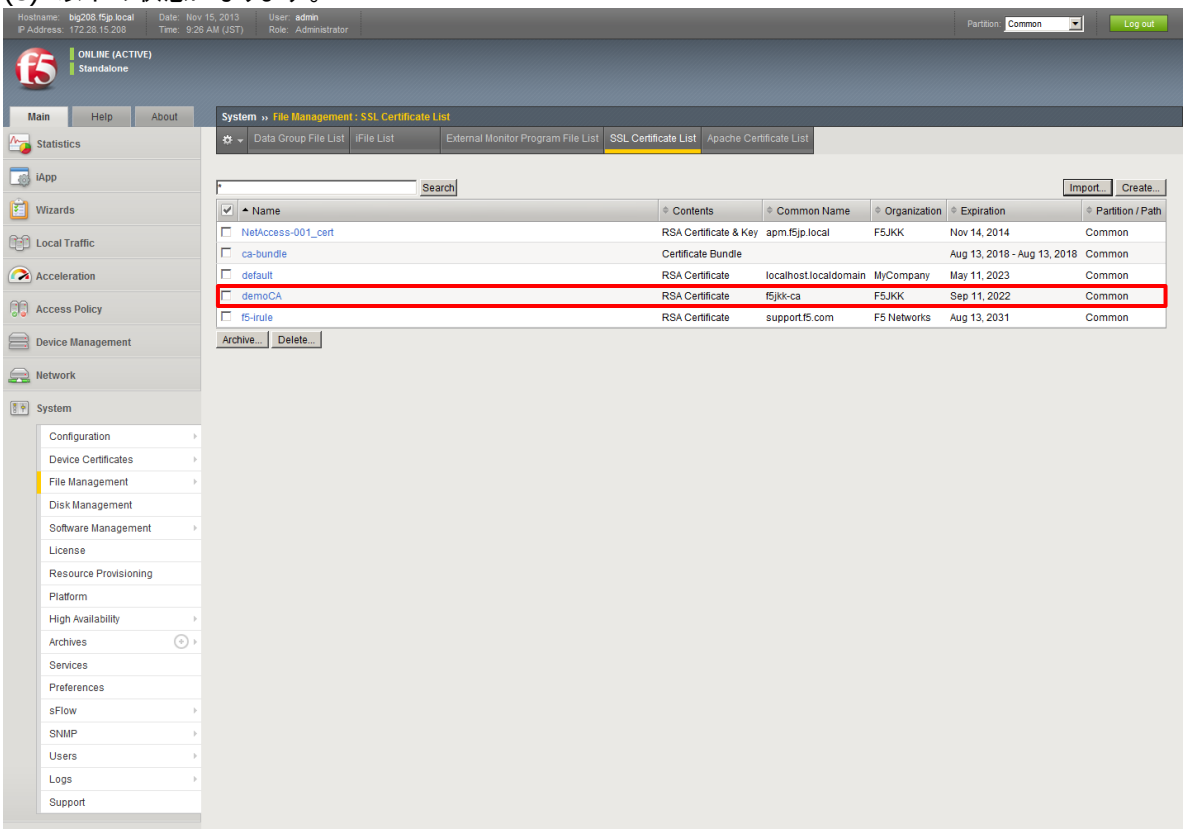
6.2.3.1. 認証局の証明書のインポート

(1) あらかじめ、認証局の証明書を、BIG-IP の設定用 GUI へアクセスする PC にコピーしておきます。

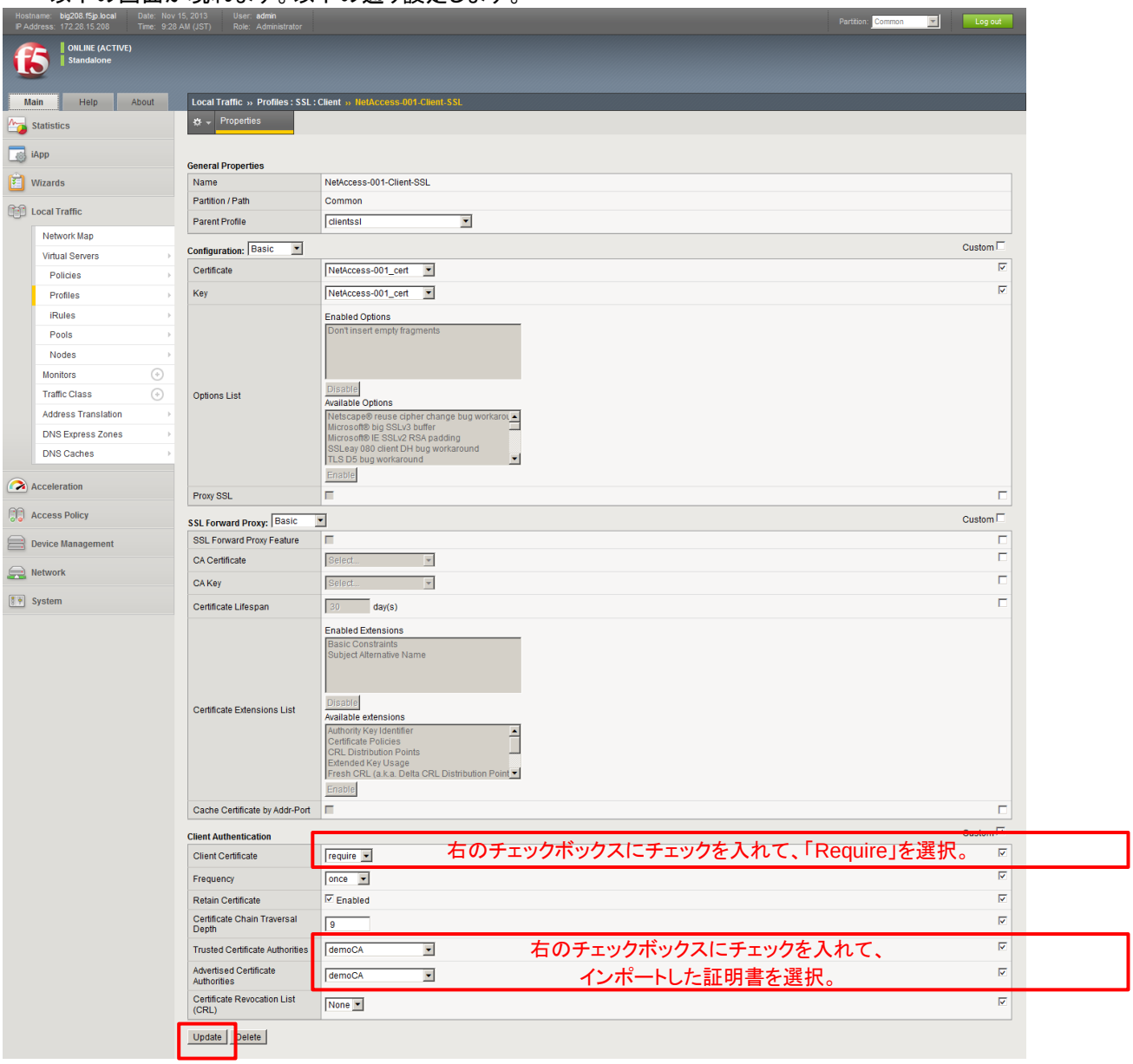
(2) その認証局の証明書を以下の手順で BIG-IP へインポートします。



(3) 以下の状態になります。



(4) 「SSL サーバ証明書の設定」で生成した、Client SSL Profile を編集します。
「Main」メニュー → 「Local Traffic」 → 「Profile」 → 「SSL」 → 「Client」で、該当する Profile をクリックすると、以下の画面が現れます。以下の通り設定します。



以上で、クライアント証明書認証の設定は完了です。

6.2.4. クライアントからのアクセス

(1) クライアント PC から、APM VS へアクセスします。

(2) クライアント証明書の選択画面が出たら、該当する証明書をクリックします。

(3) APM へのアクセスが完了することを確認します。

6.3. セッション変数について

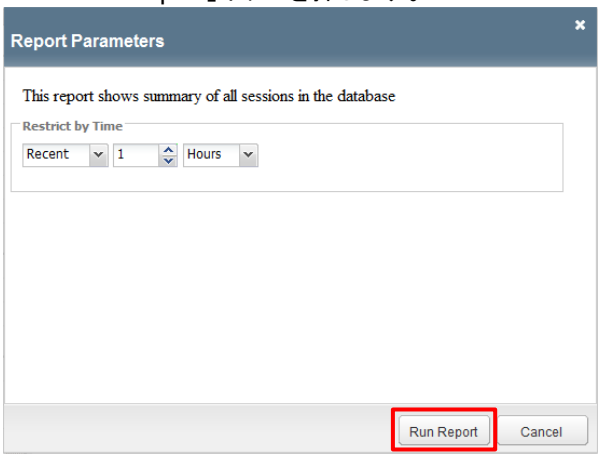
BIG-IP APM には、セッション変数(Session Variables)という便利な機能が実装されています。

このセッション変数を利用することで、例えば、クライアント端末が持つ情報と、Active Directory で管理している情報を突き合わせて、情報が一致すれば次のアクションを実施する、というようなポリシーを生成することが可能です。

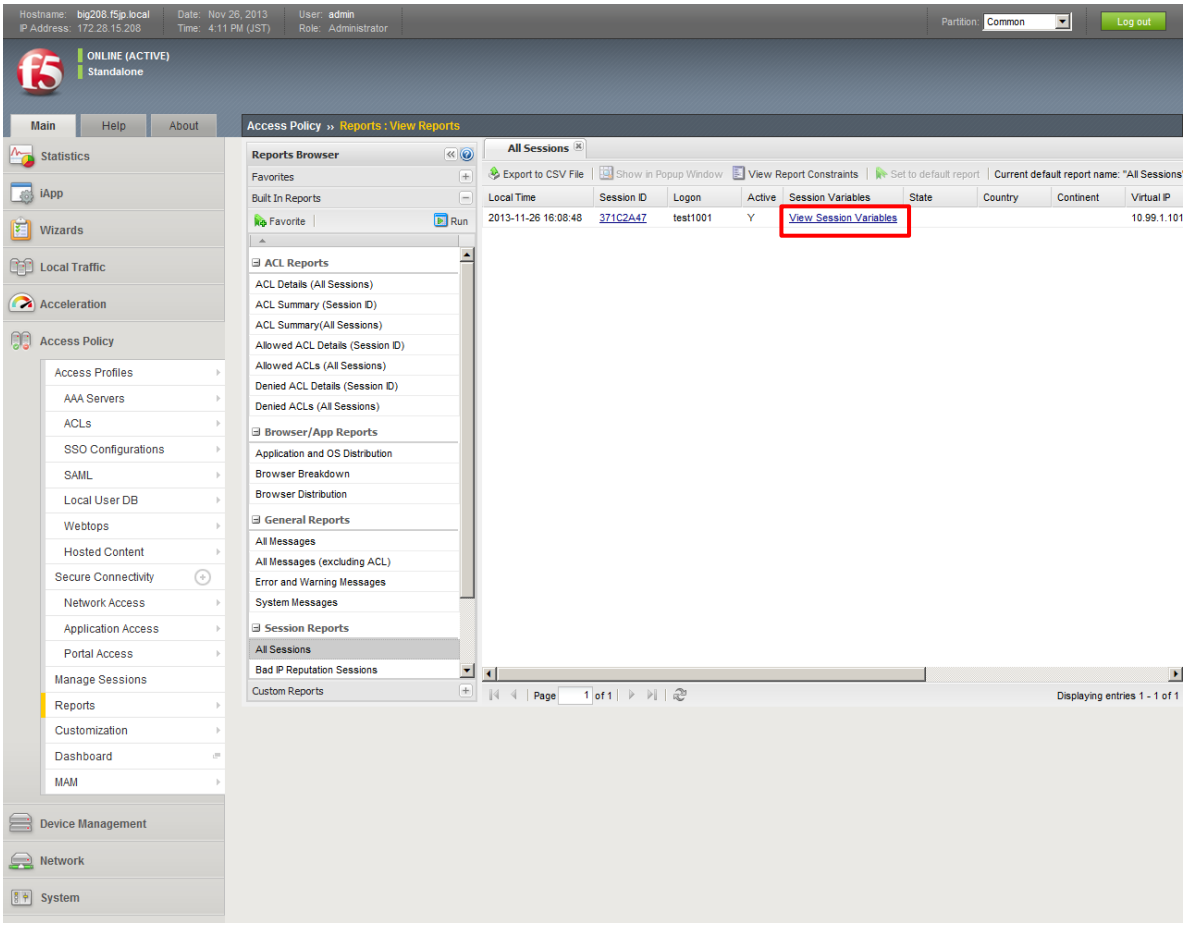
例えば、先のセクションで設定したクライアント証明書認証において、そのクライアント証明書内の値がセッション変数に取り込まれますので、その情報を利用することも可能です。
セッション変数の確認方法を以下に示します。

(1) クライアントが APM に接続された状態にします。

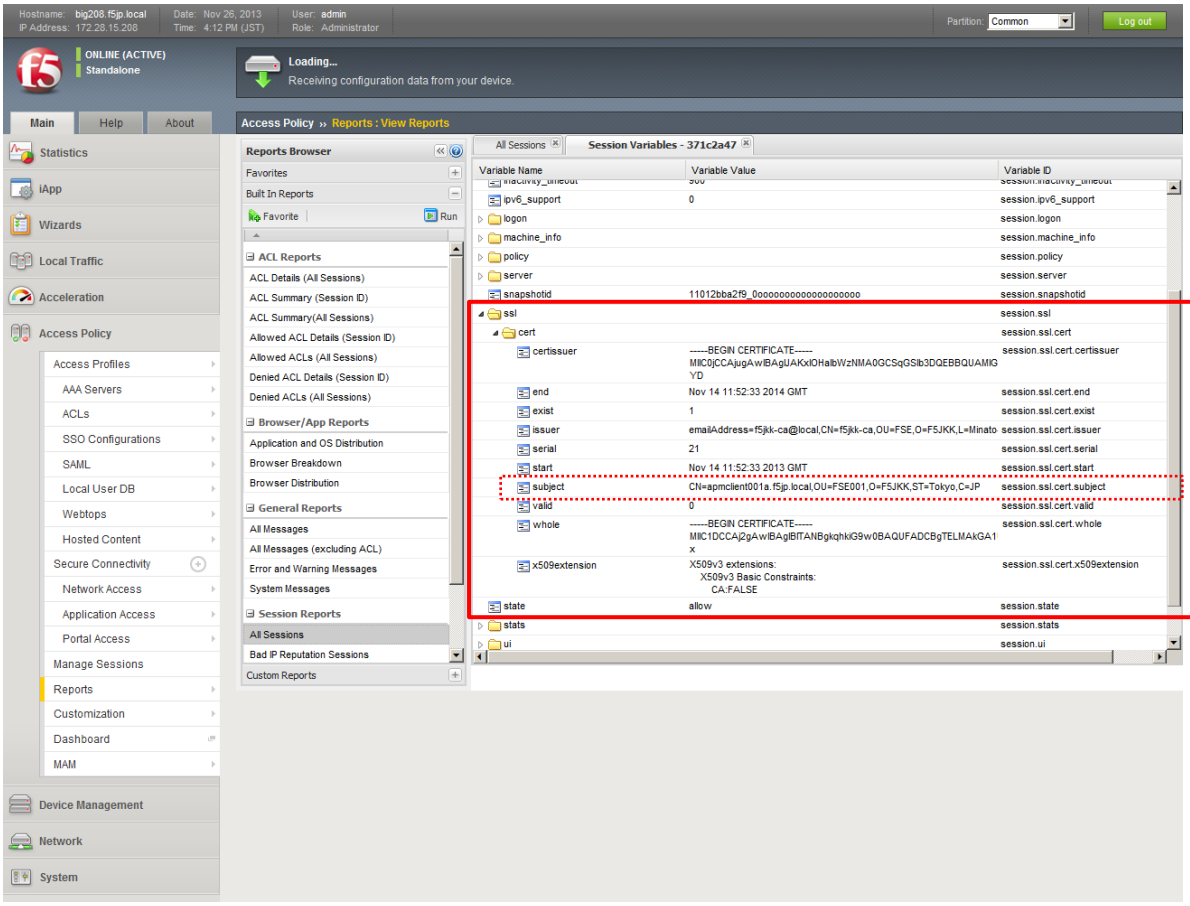
(2) 「Main」メニュー → 「Access Policy」 → 「Reports」を選ぶと、以下の画面が現れます。
「Run Report」ボタンを押します。



(3) アクセスした Logon ユーザ(本例では test1001)の行に表示されている、「View Session Variables」をクリックします。



(4) 表示された画面の Variable Name の中で、「ssl」を捜し、△ボタンをクリックして展開すると、クライアント証明書の詳細が表示されます。



上図の赤点線囲みの部分を例にとりますと、
「session.ssl.cert.subject」がセッション変数であり、
「CN=apmclient001a.f5jp.local,OU=FSE001,O=F5JKK,ST=Tokyo,C=JP」がその値です。

クライアント証明書情報を APM のセッション変数に取り込む、というのはほんの一例であり、その他にもクライアントが持つ固有の情報(例：Windows であれば、NIC の MAC アドレス、マザーボードの ID 等)を取り込むことが可能です。
このセッション変数を利用することで、ユーザ単位にアクセス制御を行うことが可能です。

以降、このセッション変数を利用したポリシーの設定例をいくつか紹介します。

6.4. ［VPE サンプル-1］クライアント証明書の OU で ACL を割当てる

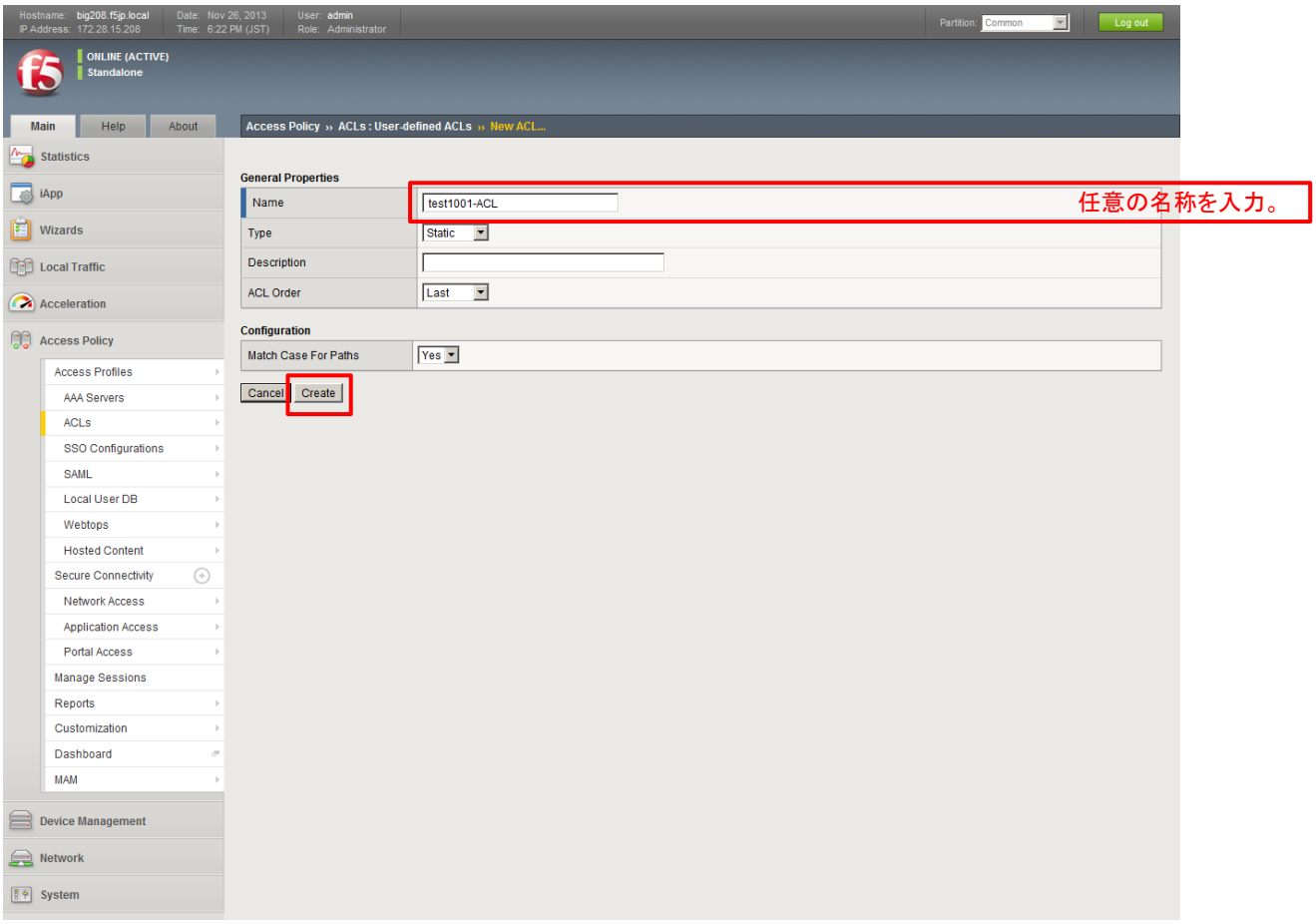
クライアント証明書の OU 単位（＝組織単位）に、アクセスできるサーバを制限したい＝Access Control List を適用したい、という要件があると仮定します。

本例では、クライアント証明書の Sbject に、"OU=FSE001"が含まれている場合に、ある ACL を割当てる、という設定を行います。

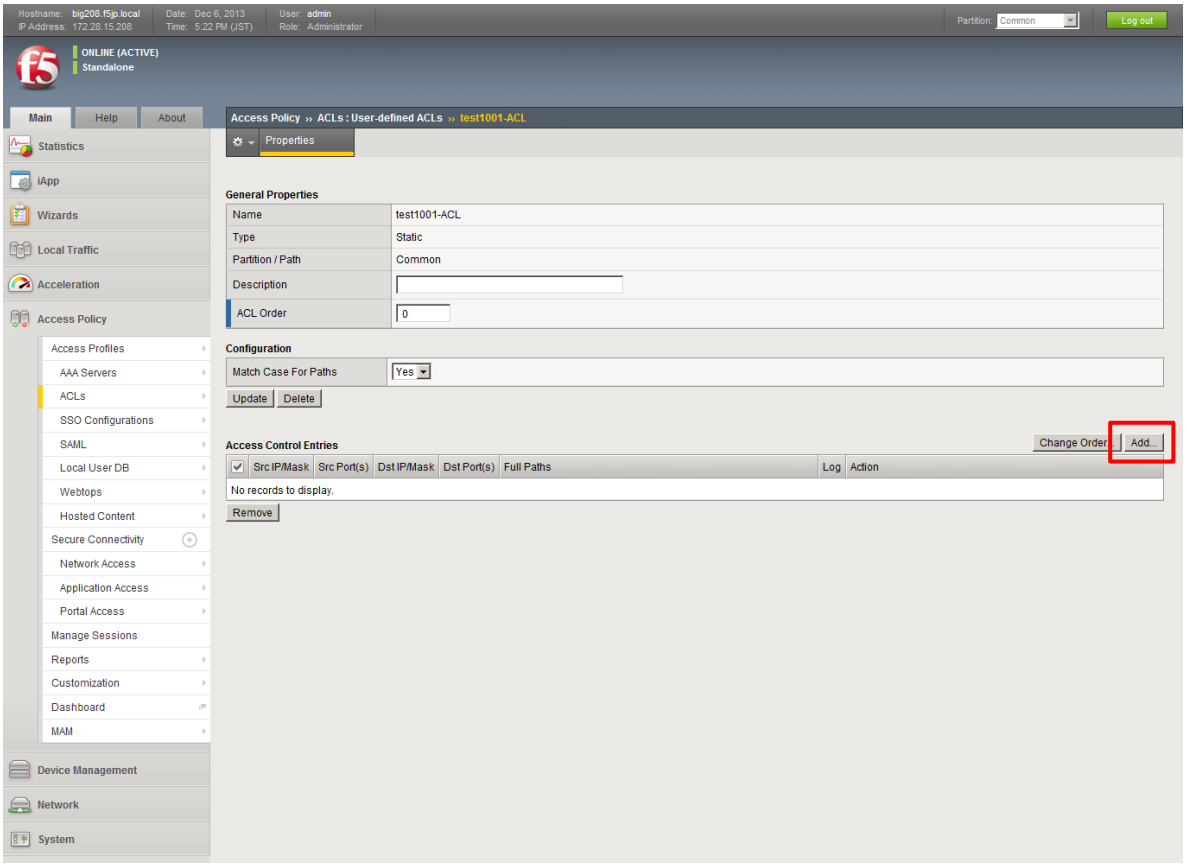
6.4.1. ACL の作成

サンプルとして、実サーバ：10.99.2.215 への SSH(Port：22)アクセスを止める ACL を作成します。

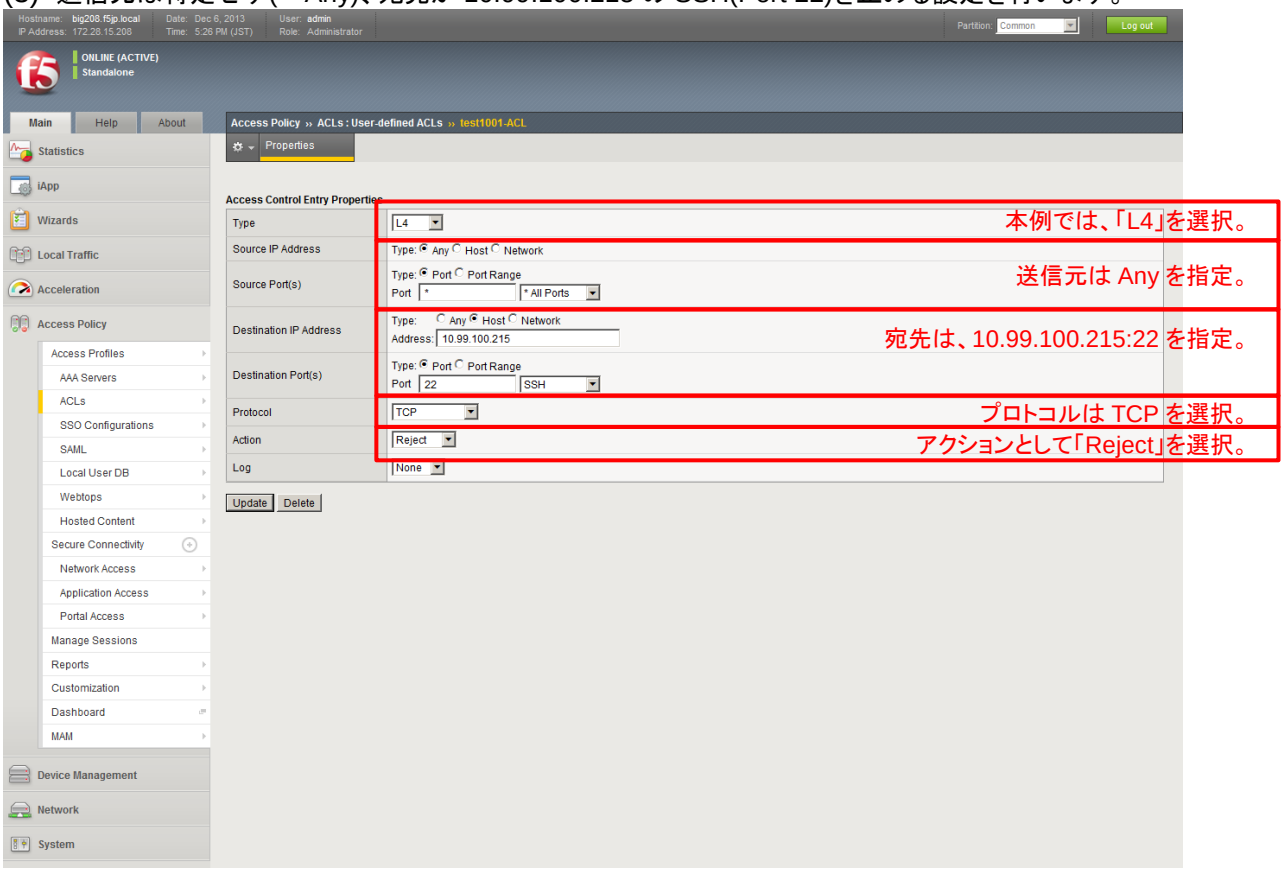
(1) 「Main」メニュー → 「Access Policy」 → 「ACLs」で表示された画面の右上の「Create」ボタンを押すと、以下の画面が表示されます。以下のように設定します。



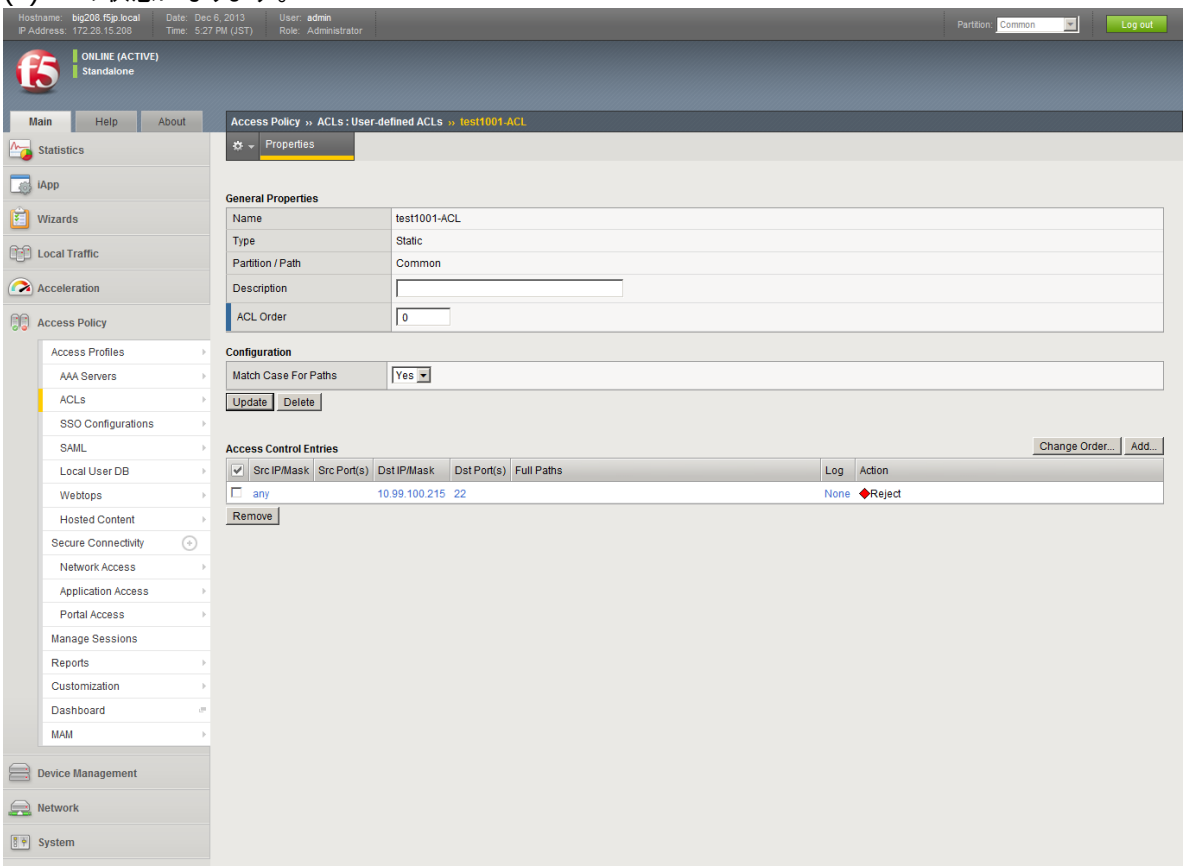
(2) 以下の状態になります。
「Access Control Entries」の横の「Add」ボタンを押します。



(3) 送信元は特定せず(＝Any)、宛先が 10.99.100.215 の SSH(Port 22)を止める設定を行います。

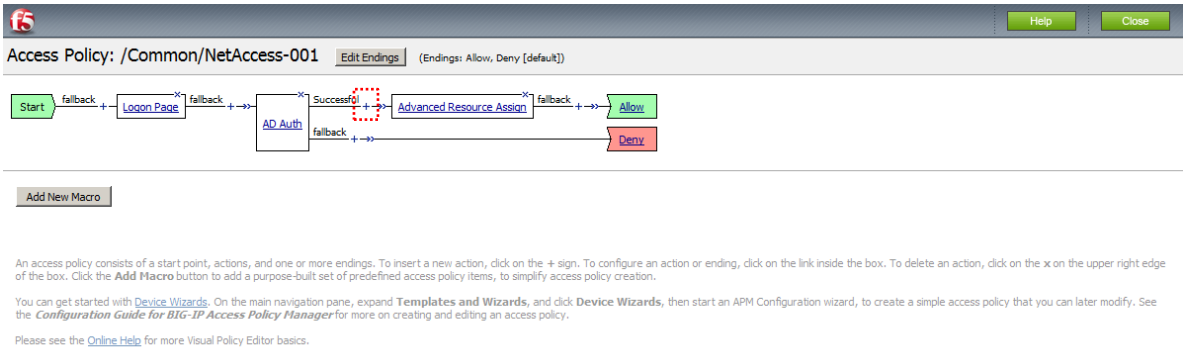


(4) この状態になります。

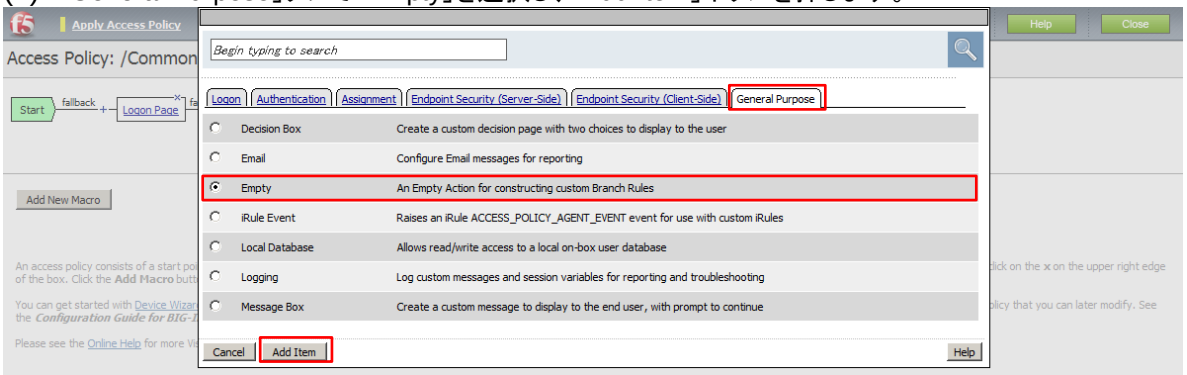


6.4.2. VPE の設定

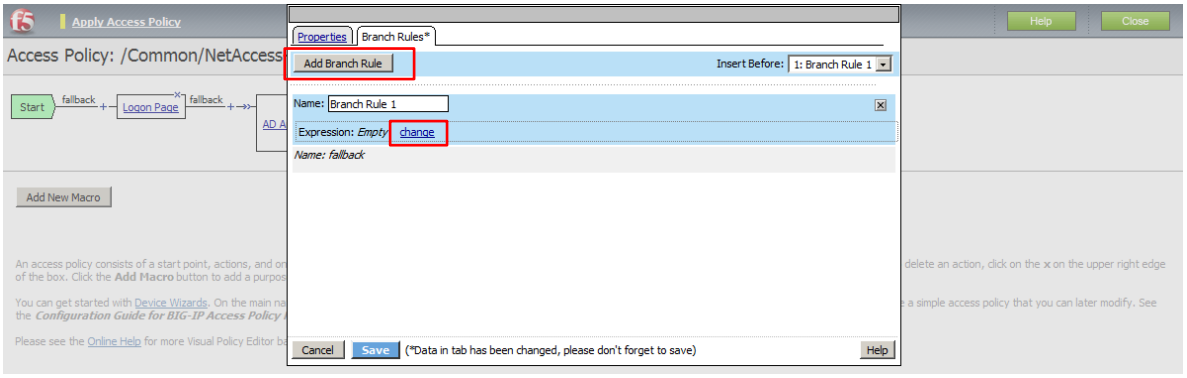
(1) ここまでの設定では、VPE は以下の状態になっています。
AD Auth の後ろにある「+」をクリックします。



(2) 「General Purpose」タブで「Empty」を選択し、「Add Item」ボタンを押します。

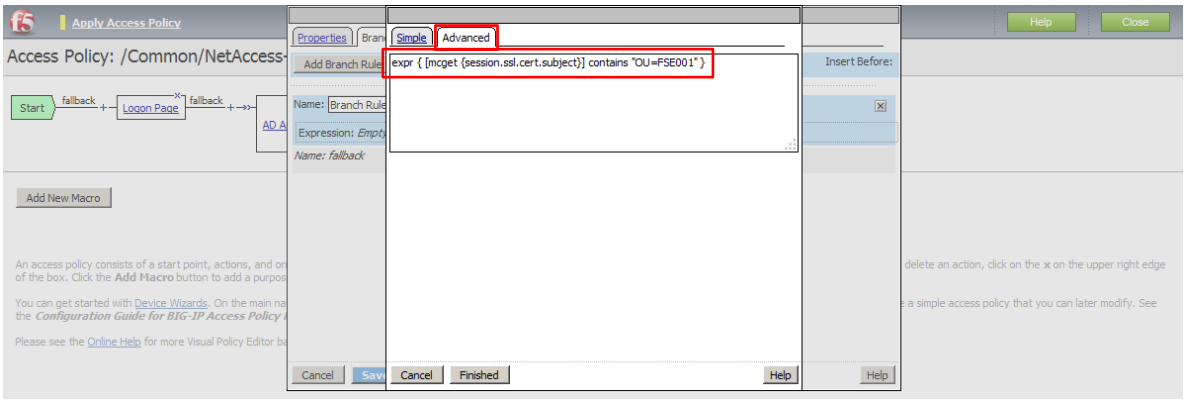


(3) 「Branch Rules」タブを選択します。「Add Branch Rule」ボタンを押して、Expression を 1 つ追加し、「Change」をクリックします。



(4) 「Advanced」タブを選択し、以下のように TCL 形式で入力します。

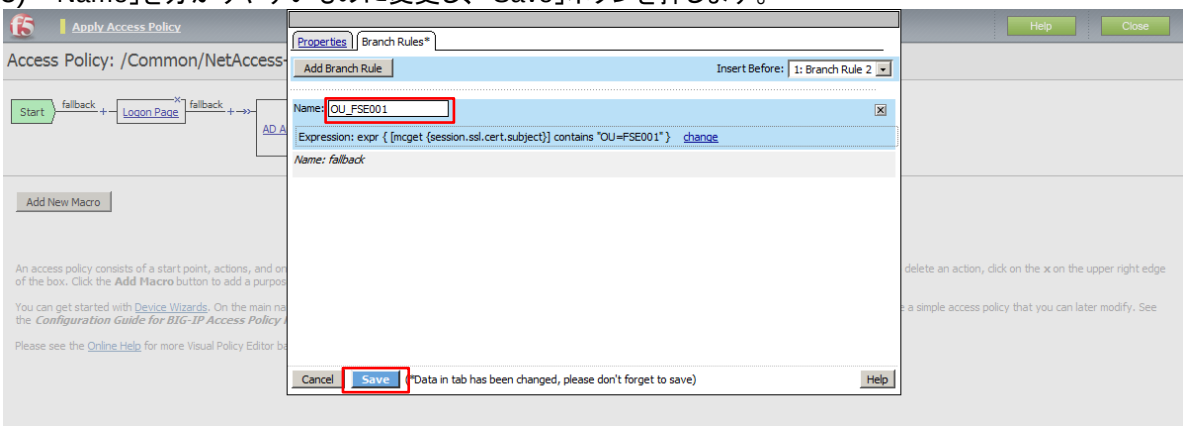
expr { [mcget {session.ssl.cert.subject}] contains "OU=FSE001" }



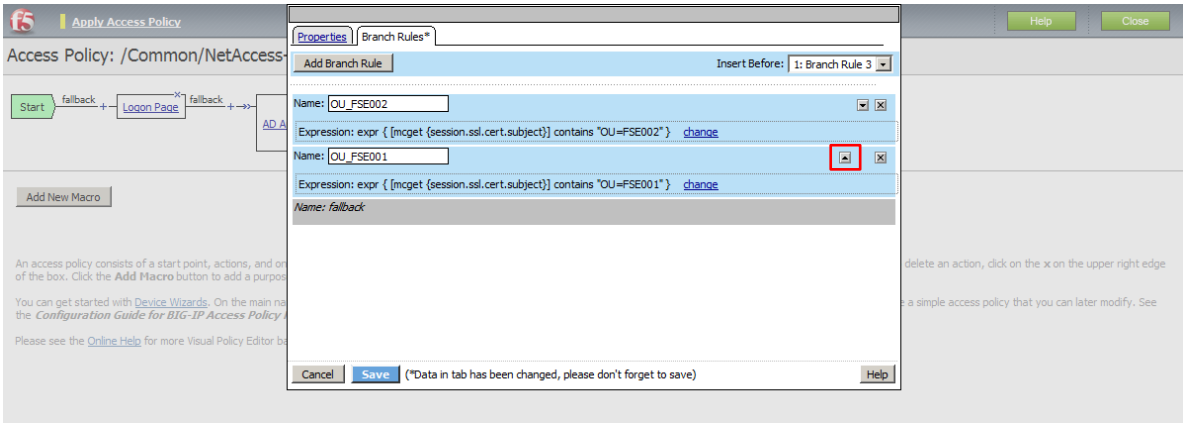
「mcget」コマンド：このコマンドによって、BIG-IP APM のセッション変数(Session Variable)に取り込まれた値を取り出します。

この構文によって、セッション変数："session.ssl.cert.subject"の値に、"OU=FSE001"が含まれているかどうかを確認します。確認結果が OK であれば、次のボックスへ進みます。

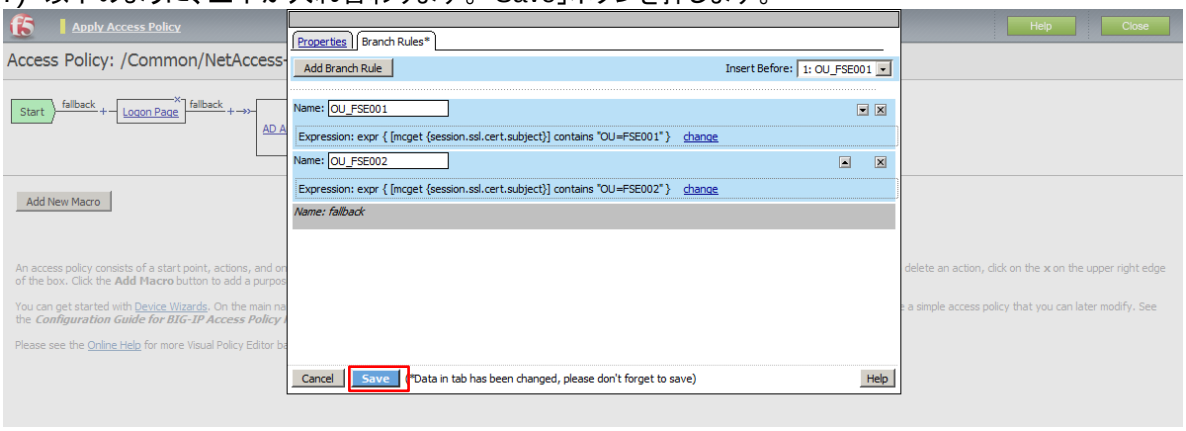
(5) 「Name」を分かりやすいものに変更し、「Save」ボタンを押します。



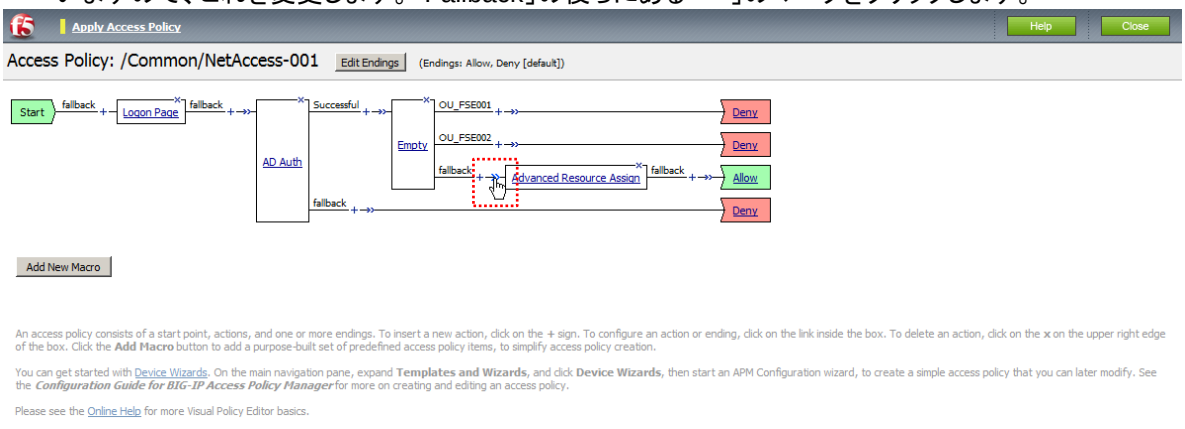
(6) 同様の方法で、2 つ目の分岐(OU=FSE002 の場合)も追加してみた状態です。
VPE の見た目上、FSE001 を一番上にしたい場合、以下の▲ボタンを押します。



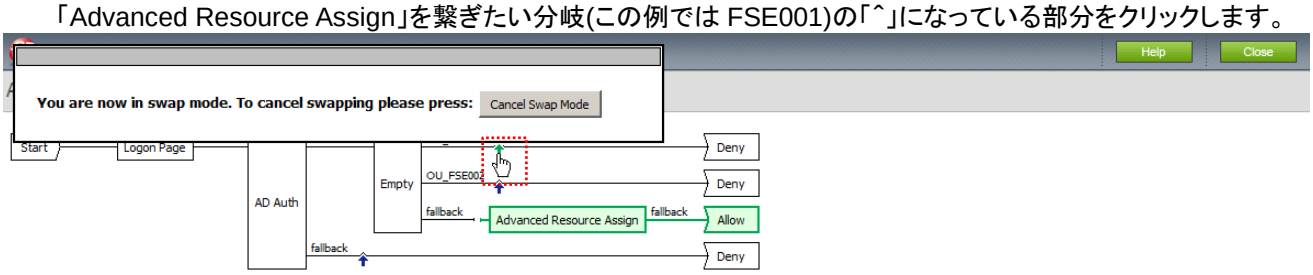
(7) 以下のように、上下が入れ替わります。「Save」ボタンを押します。



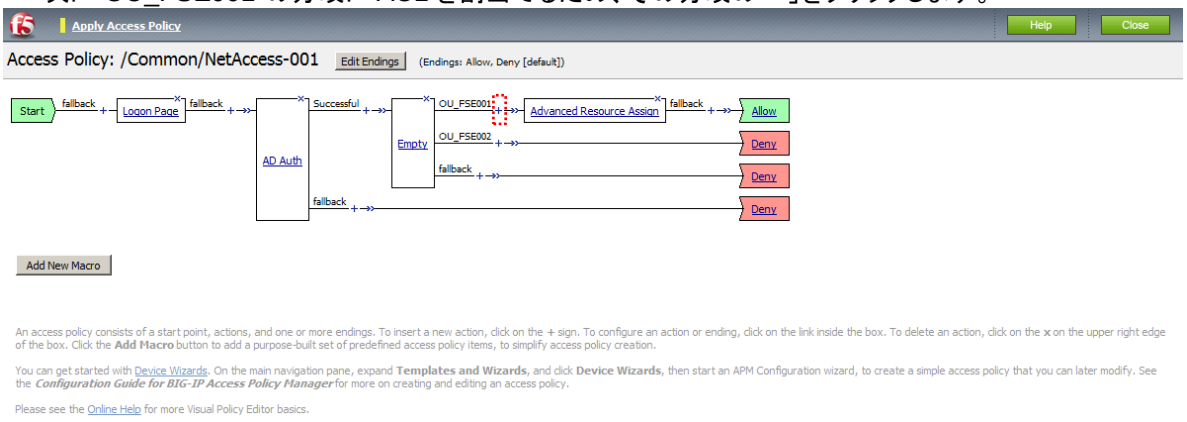
(8) この例では、以下のように、「Fallback」に「Asdvanced Resouce Assign」がつながっています。
このままだと、OU=FSE001 でも、OU＝FSE002 でもないものに対して、リソースがアサインされる状態になっていますので、これを変更します。「Fallback」の後ろにある「>>」のマークをクリックします。



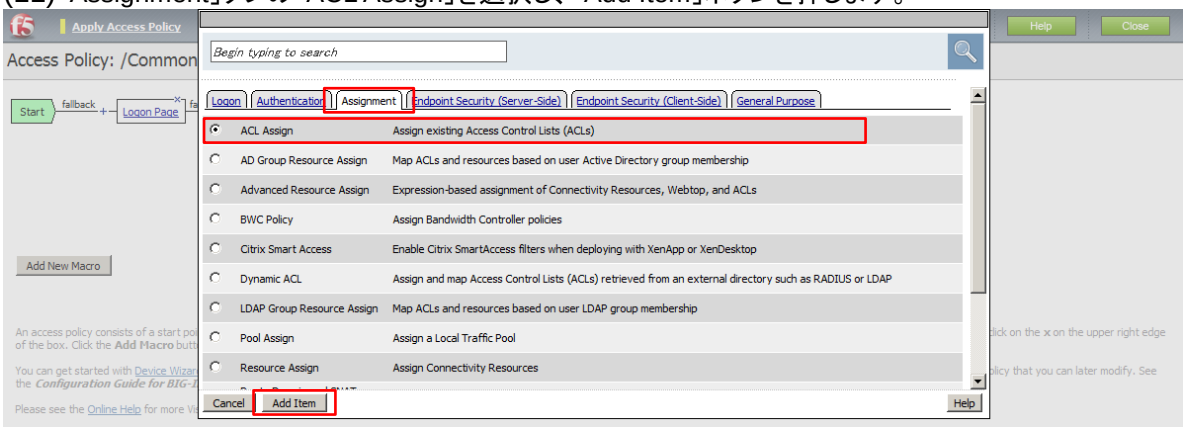
(9) 以下のような画面に変わります。
「Advanced Resource Assign」を繋ぎたい分岐(この例では FSE001)の「^」になっている部分をクリックします。



(10)以下のように、「Advanced Resource Assign」が移動します。
次に"OU_FSE001"の分岐に ACL を割当てるため、その分岐の「+」をクリックします。

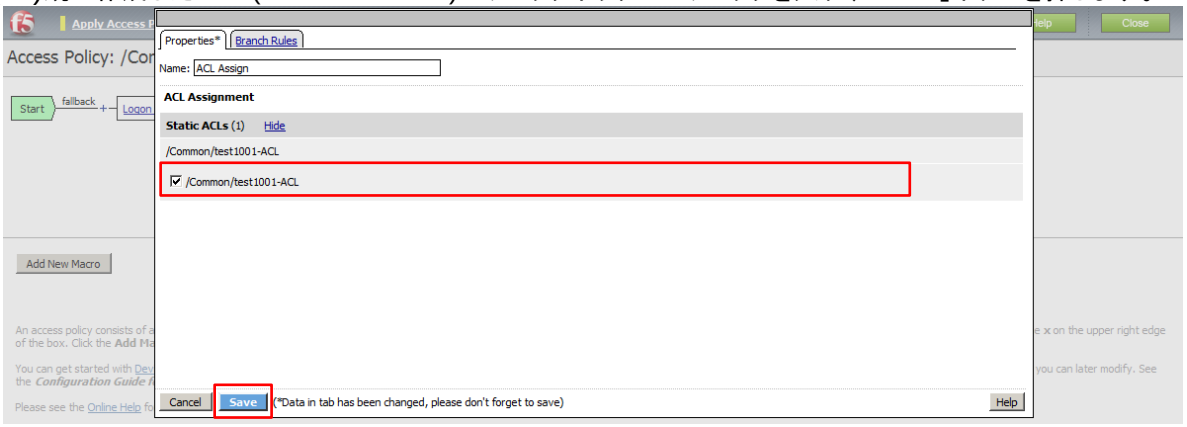


(11)「Assignment」タブの「ACL Assign」を選択し、「Add Item」ボタンを押します。

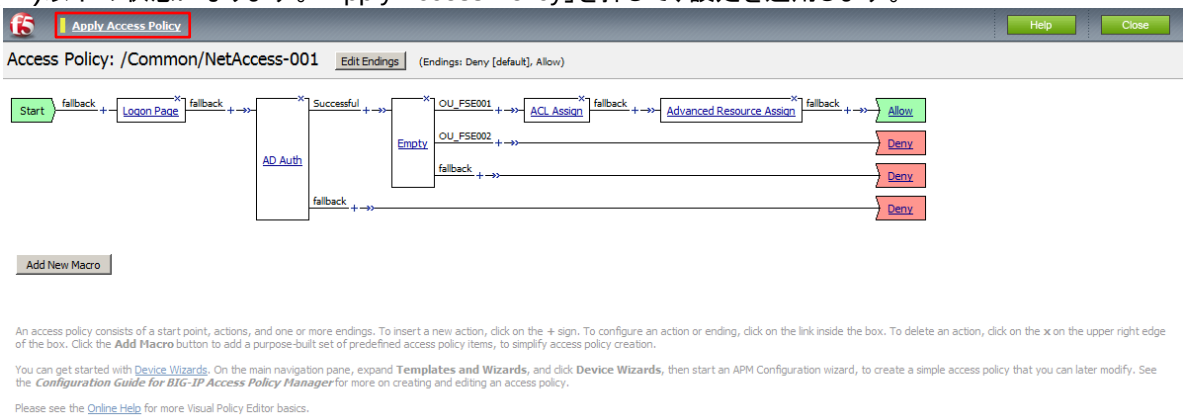


(12)「Add/Delete」をクリックします。

(13)既に作成した ACL(TEST1001-ACL)のチェックボックスにチェックを入れ、「Save」ボタンを押します。



(14)以下の状態になります。「Apply Access Policy」を押して、設定を適用します。



6.4.3. クライアントからのアクセス

(1) OU=FSE001 のクライアント証明書を持つクライアント PC から、APM の VS へアクセスします。

(2) アクセス完了後、10.99.2.215 の SSH(Port 22)へのアクセスだけが Reject されることを確認します。

6.5. ［VPE サンプル-2］Active Directory の Group で ACL を割当てる

Active Directory のユーザが属する Group 毎に、アクセスできるサーバを制限したい＝Access Control List を適用したい、という要件があると仮定します。

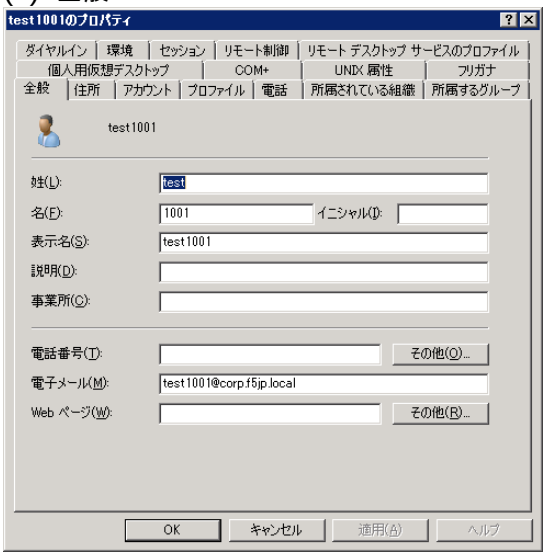
本例では、"CorpA-Group"に属するユーザ：test1001"に対して ACL を適用し、"CorpB-Group"に属するユーザ：test1002"には ACL を適用しない、という設定を行います。

6.5.1. ACL の作成

"［VPE サンプル-1］"で作成した ACL：Test1001-ACL を利用しますので、設定例は省略します。

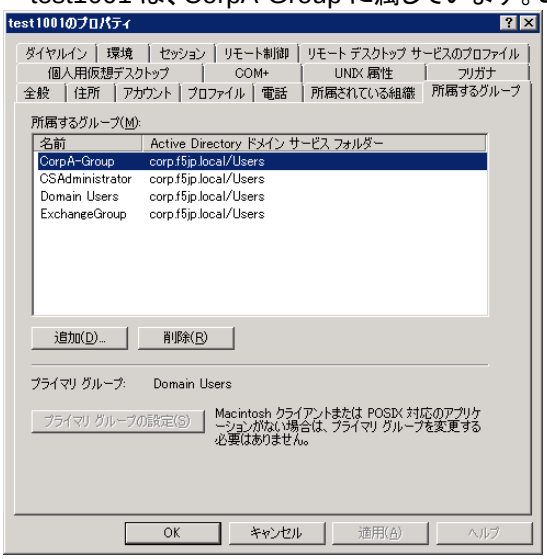
6.5.2. Active Directory ユーザ：test1001

(1) 全般



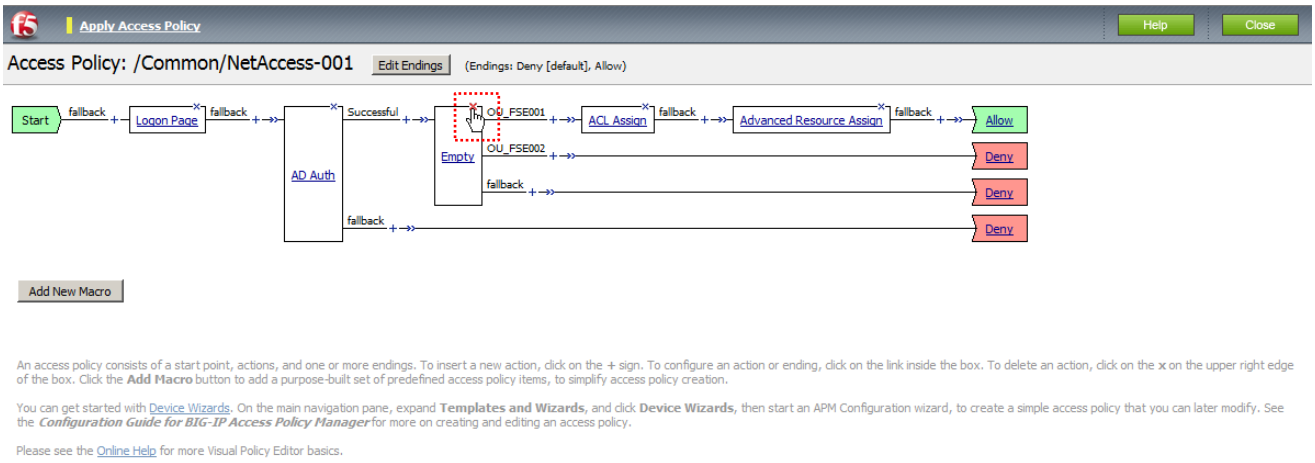
(2) 所属するグループ

test1001 は、CorpA-Group に属しています。この CorpA-Group に対して、ACL を割当てる設定を行います。

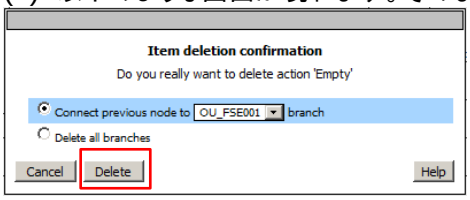


6.5.3. VPE の設定

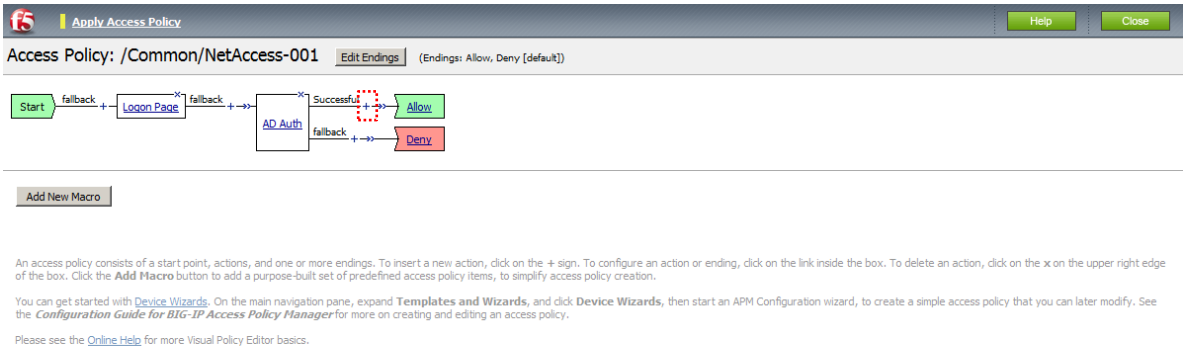
(1) ここまでの設定では、VPE は以下のようになっています。
一旦、Empty 以降をすべて削除します。
ボックスの右上の「×」をクリックします。



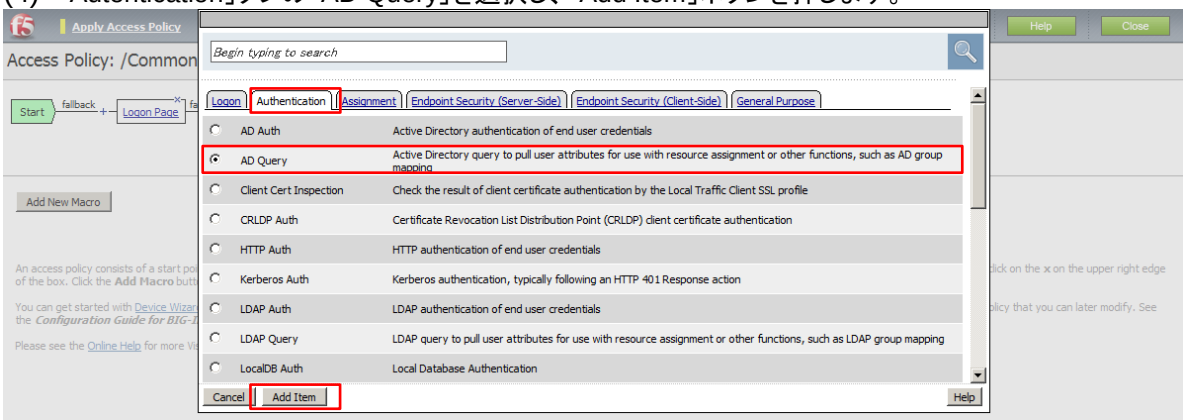
(2) 以下のような画面が現れます。そのまま、「Delete」を押します。



(3) 同様の手順で、「ACL Assign」も「Advanced Resource Assign」も削除し、以下の状態にします。
「AD Auth」の Successful 分岐上の「+」をクリックします。



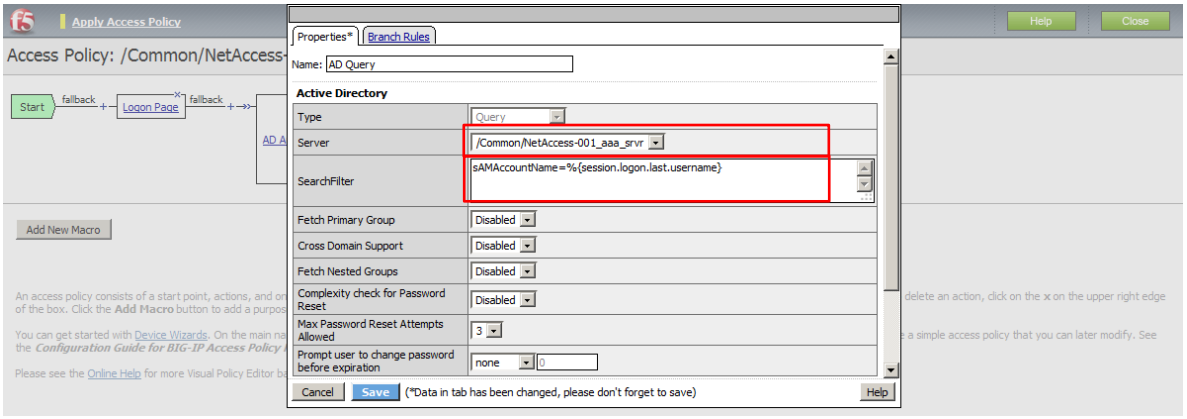
(4) 「Autentication」タブの「AD Query」を選択し、「Add Item」ボタンを押します。



(5) 「Server」として、既に設定した Active Directory 設定(NetAccess-001_aaa_srvr)を選択します。

「SerchFilter」には、以下を入力します。

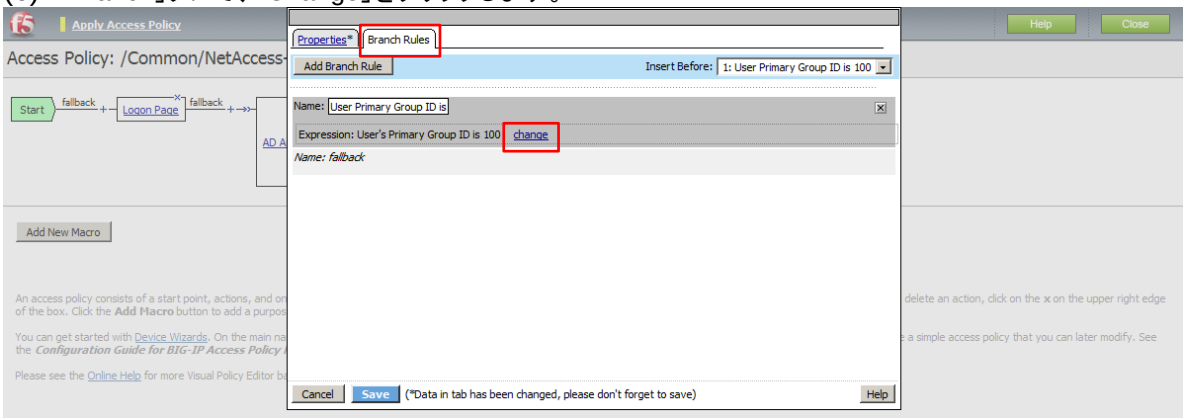
sAMAccountName=%{session.logon.last.username}



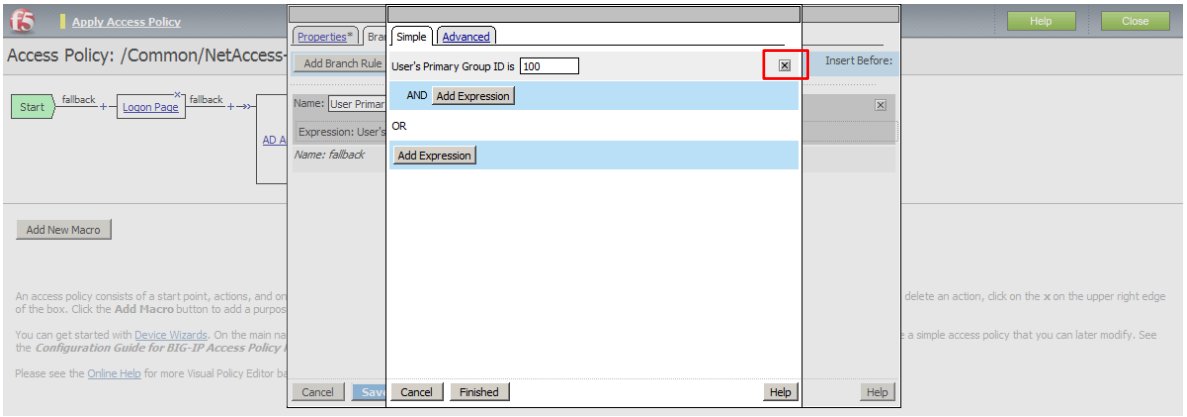
SearchFilter に入力した「sAMAccountName」は、Active Directory で定義されている、ユーザ名の変数です。この変数に、APM にログインしたときのユーザ名(例:test1001)を代入して、AD Query を実施する、という定義です。

APM にログインしたときのユーザ名は、セッション変数:「session.logon.last.username」の値として格納されていますので、「=%{session.logon.last.username}」で代入を行います。

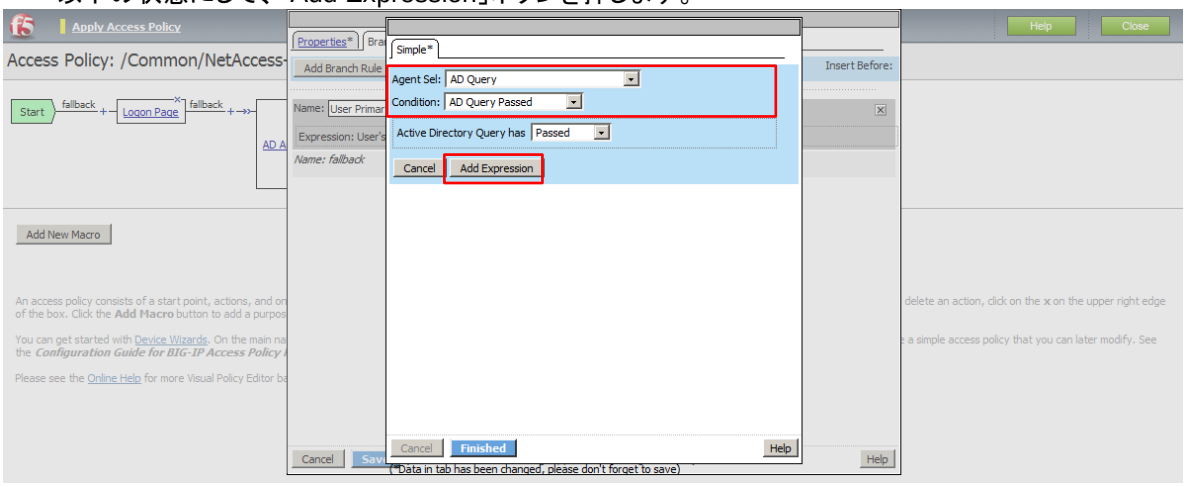
(6) 「Branch」タブで、「Change」をクリックします。



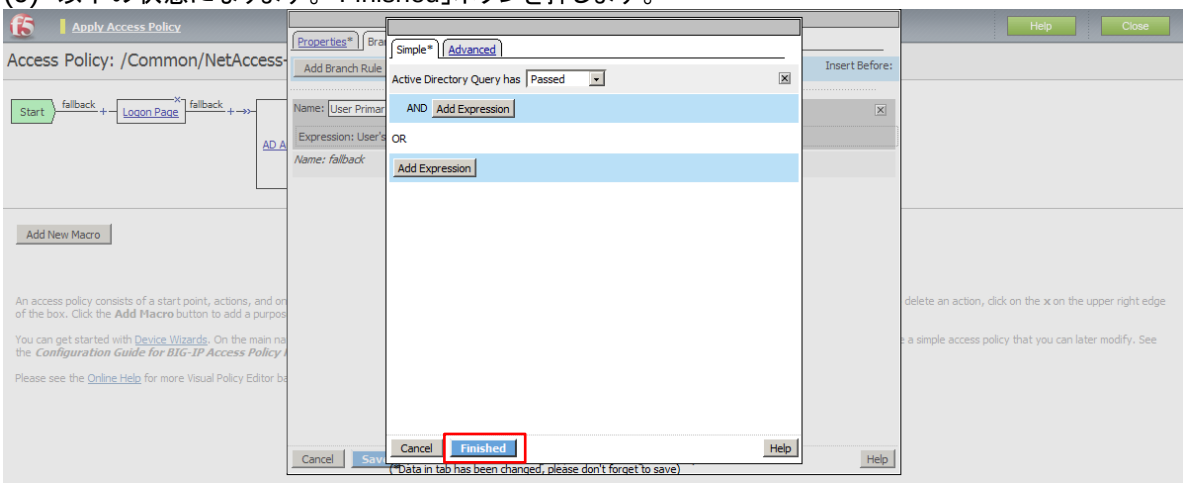
(7) 「Simple」タブ上で、デフォルトで設定されている「User's Primary Group ID is 100」を、「×」ボタンを押して削除します。



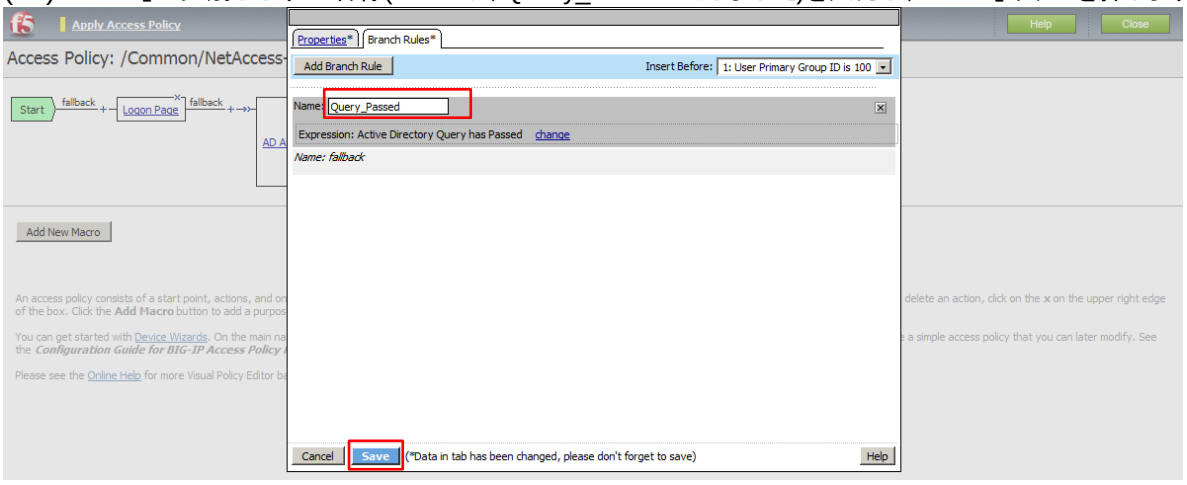
(8) 「Add Expression」ボタンをクリックすると、以下の画面が現れます。
ここでは、単純に、AD Query が成功したら、次の BOX に移動する定義にしています。
以下の状態にして、「Add Expression」ボタンを押します。



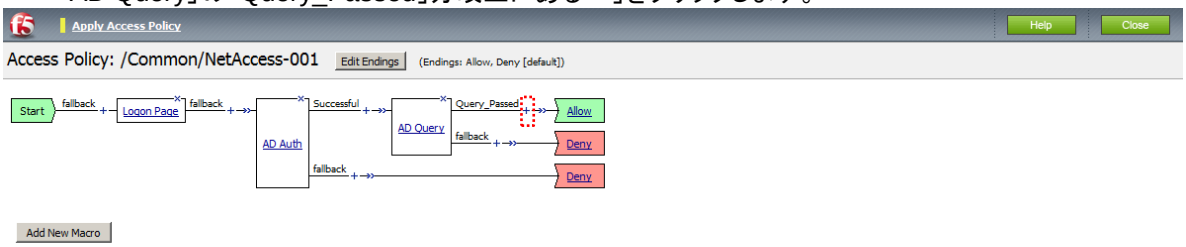
(9) 以下の状態になります。「Finished」ボタンを押します。



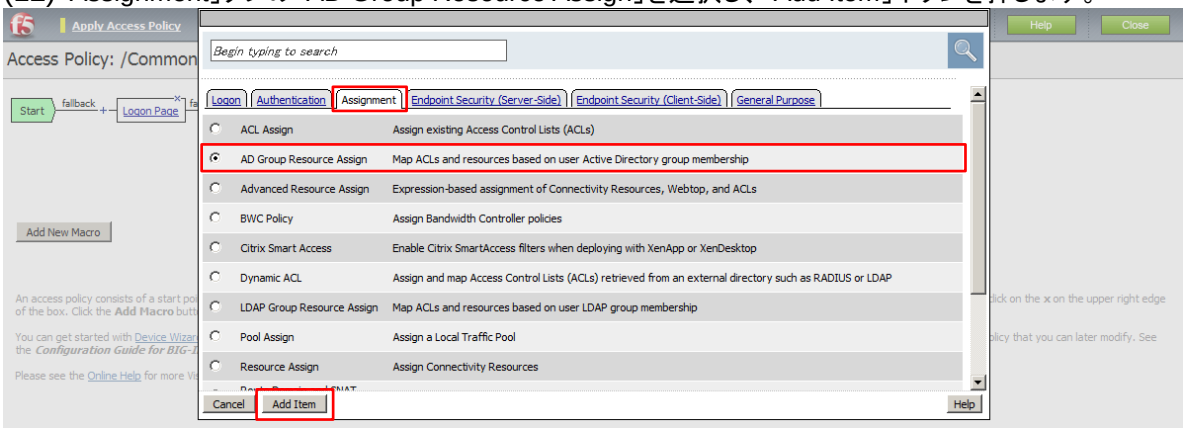
(10)「Name」に区別しやすい名称(ここでは、Query_Passed としました)を入力し、「Save」ボタンを押します。



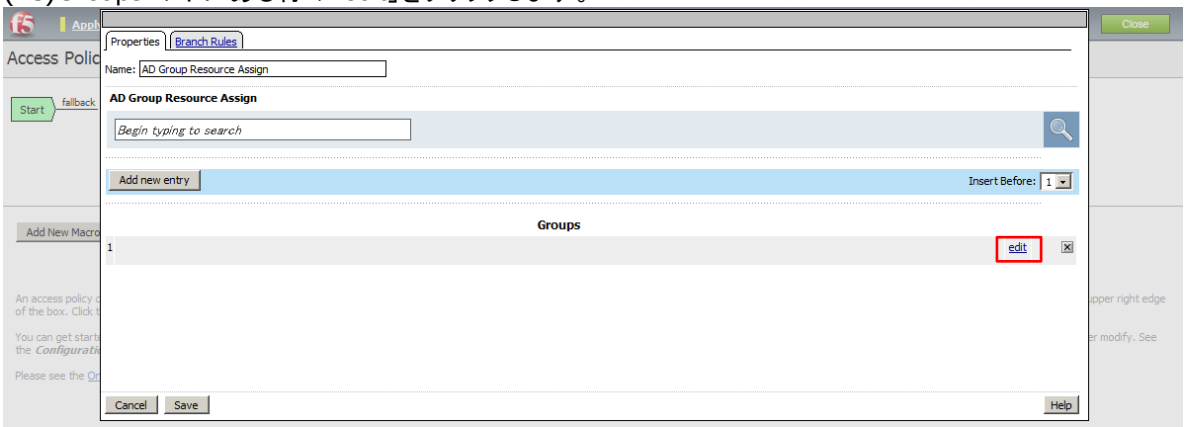
(11)以下の状態になります。
「AD Query」の「Query_Passed」分岐上にある「+」をクリックします。



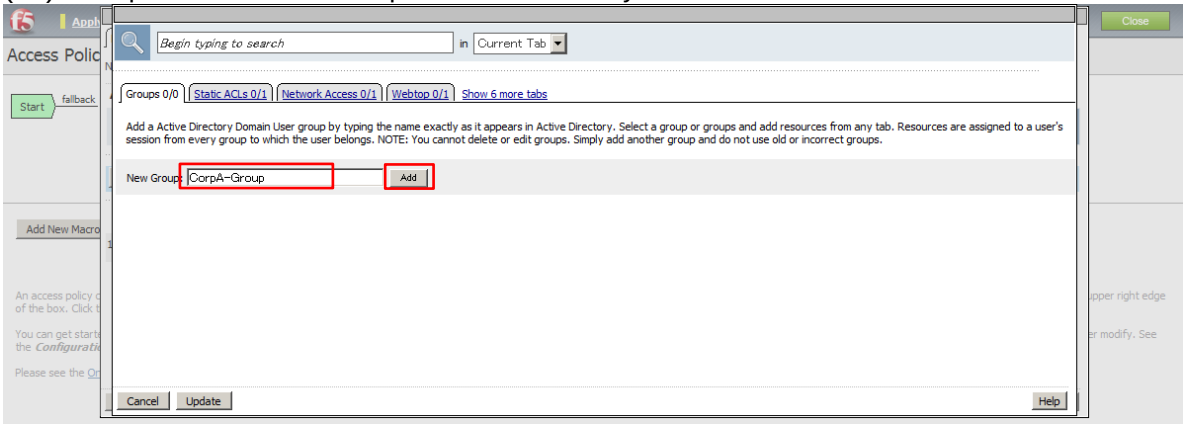
(12)「Assignment」タブの「AD Group Resource Assign」を選択し、「Add Item」ボタンを押します。



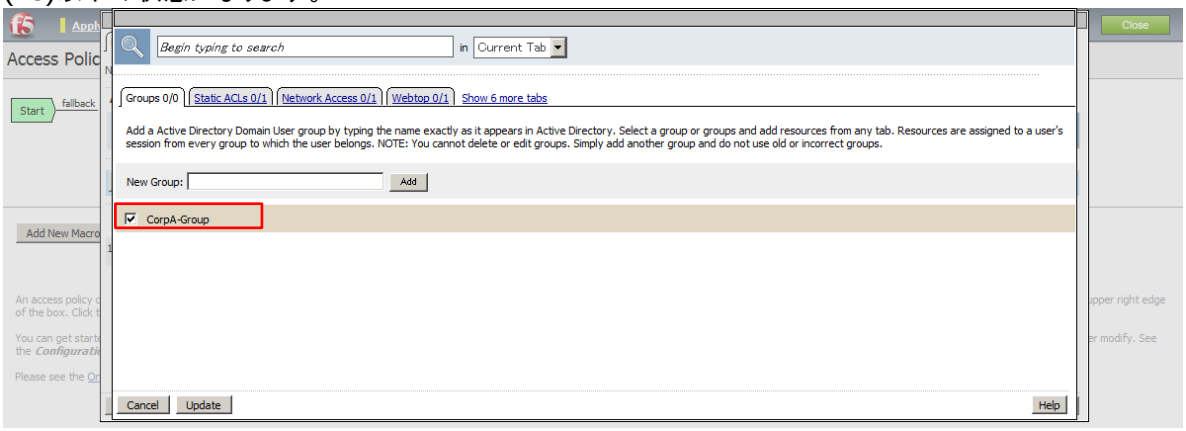
(13)Groups の下にある行の「edit」をクリックします。



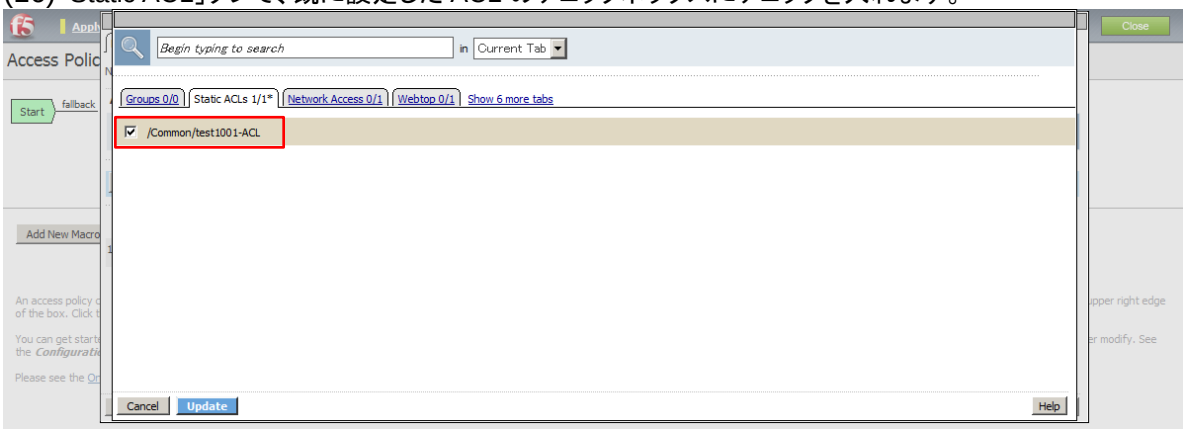
(14)「Groups」タブで、「New Group」に Active Directory のグループ名を入力し、「Add」ボタンを押します。



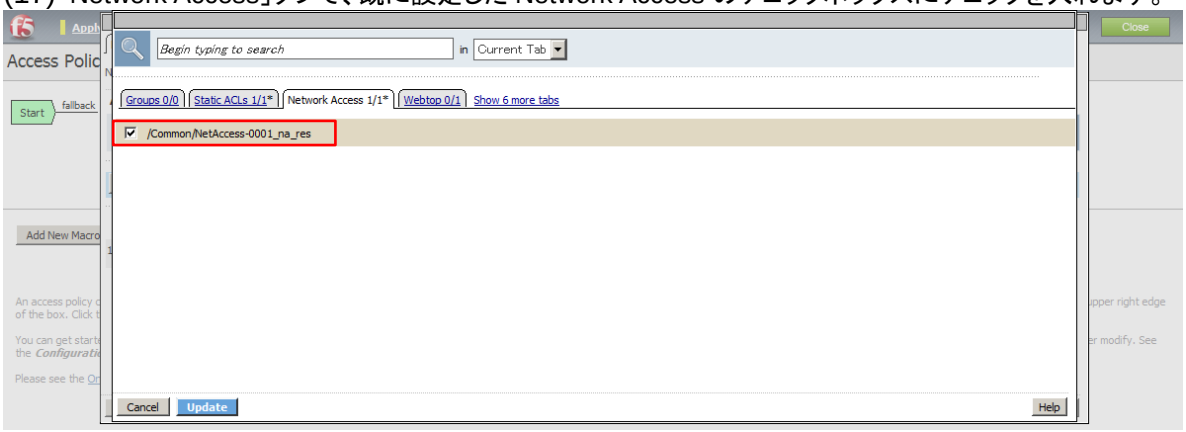
(15)以下の状態になります。



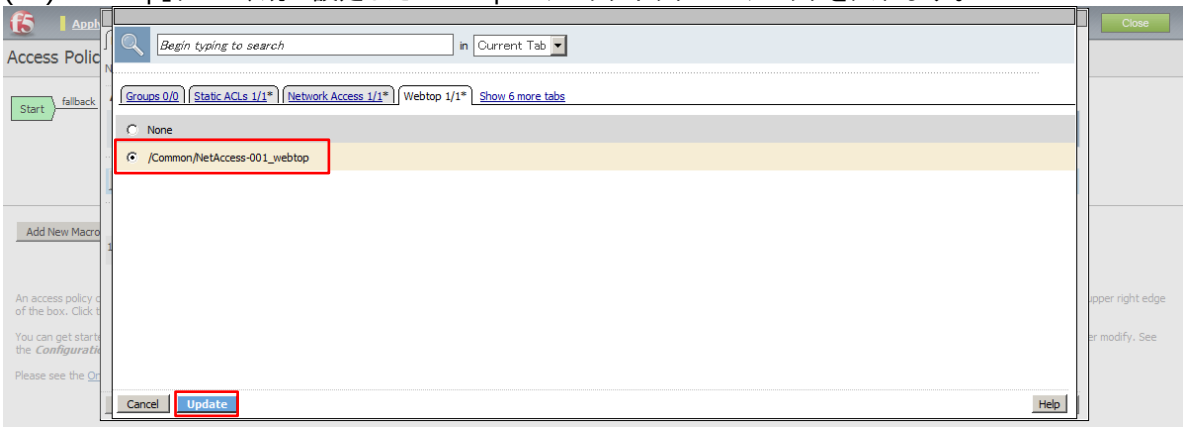
(16)「Static ACL」タブで、既に設定した ACL のチェックボックスにチェックを入れます。



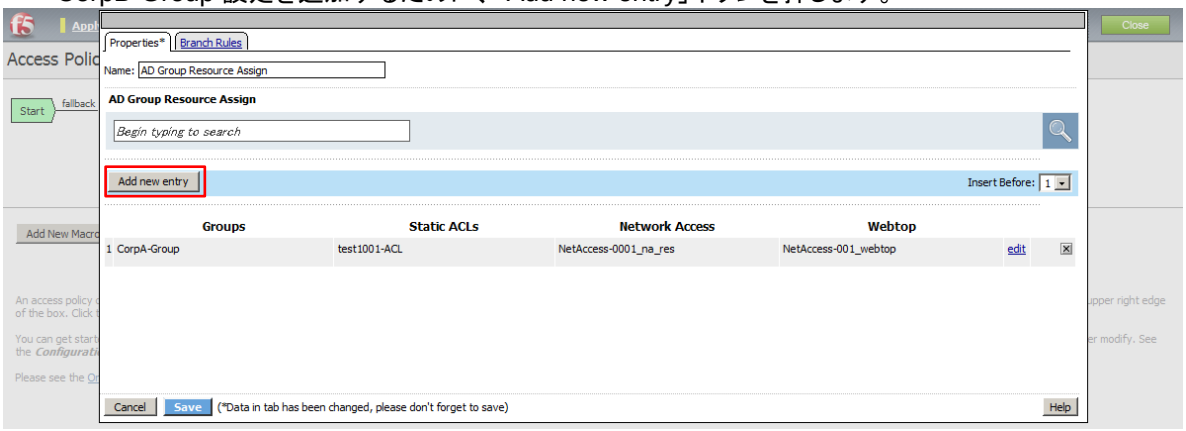
(17)「Network Access」タブで、既に設定した Network Access のチェックボックスにチェックを入れます。



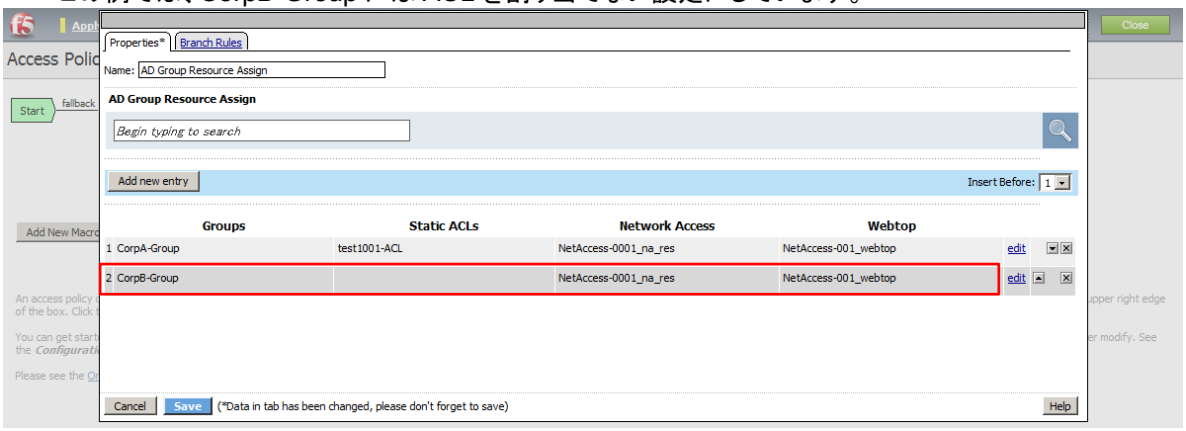
(18)「Webtop」タブで、既に設定した Webtop のチェックボックスにチェックを入れます。



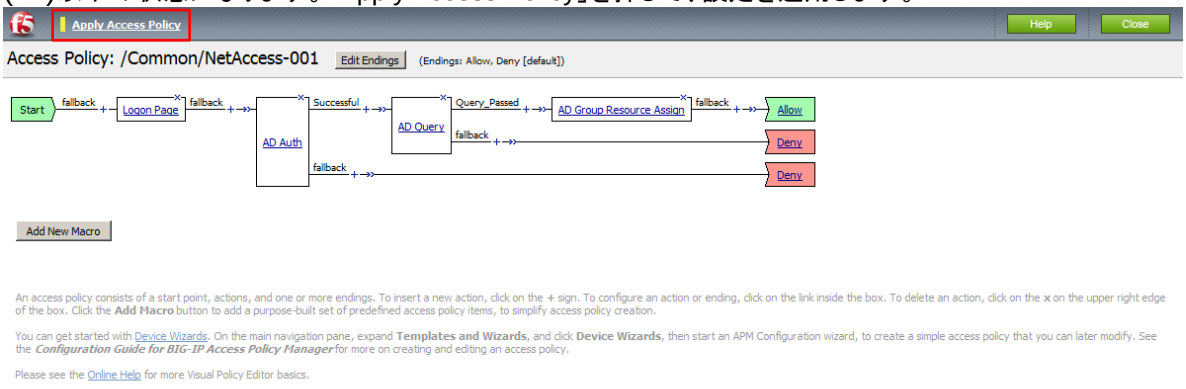
(19)以下の状態になります。
CorpB-Group 設定を追加するために、「Add new entry」ボタンを押します。



(20)同様の手順で CorpB-Group の設定を行います。
この例では、CorpB-Group には ACL を割り当てない設定にしています。



(21)以下の状態になります。「Apply Access Policy」を押して、設定を適用します。



6.5.4. クライアントからのアクセス

(1) クライアント PC から、CorpA-Group に属するユーザ："test1001"で、APM の VS へアクセスします。

(2) アクセス完了後、10.99.2.215 の SSH(Port 22)へのアクセスだけが Reject されることを確認します。

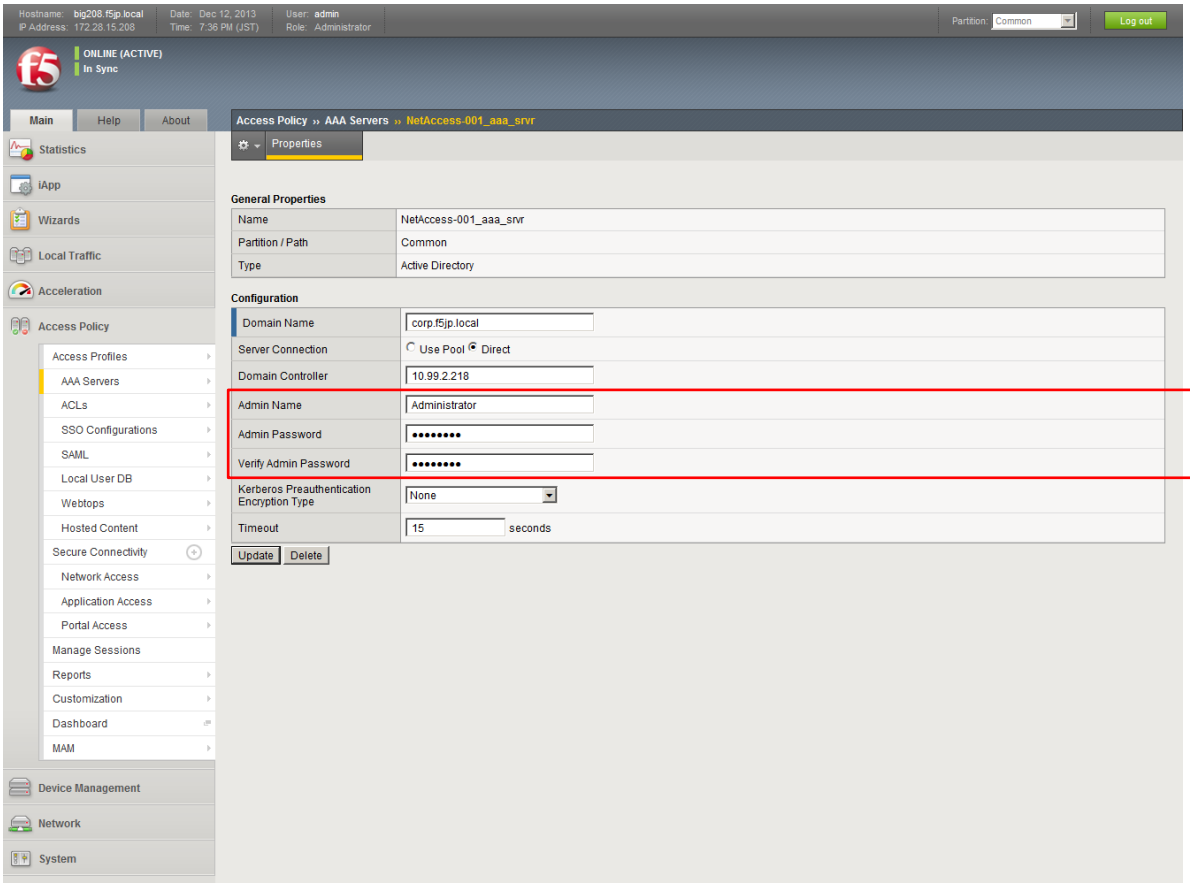
(3) クライアント PC から、CorpB-Group に属するユーザ："test1002"で、APM の VS へアクセスします。

(4) CorpB-Group には ACL が割り当てられていないので、すべてのアクセスが通過する（なにも Reject されない）ことを確認します。

6.5.5. AD Query がうまく行かない場合：AAA 設定の変更

Active Directory 設定またはそのユーザ設定によっては、Administrator 権限が必要となる場合があります。その場合には、以下の部分を追加してみてください。

「Main」メニュー →「Access Policy」→「AAA Servers」→「Active Directory」→ 設定済みの AAA サーバをクリックすることで、以下の画面が現れます。以下の赤囲み部分を追加してみてください。



6.6. ［VPE サンプル-3］アクセスできるクライアント端末を限定する

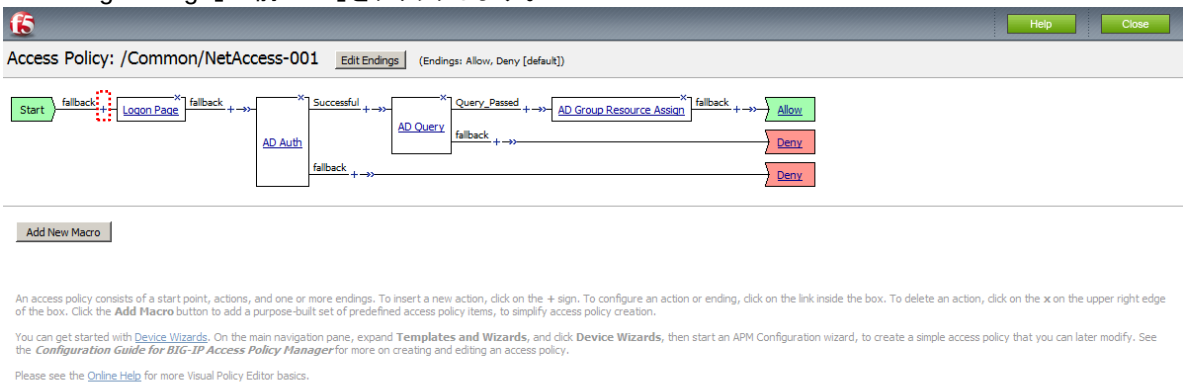
Active Directory のユーザが利用する端末を限定したい、という要件があると仮定します。

本例では、"test1001"が使うことができる端末は、その端末のマザーボードシリアル番号が Active Directory に登録されているものだけにする、という設定を行います。

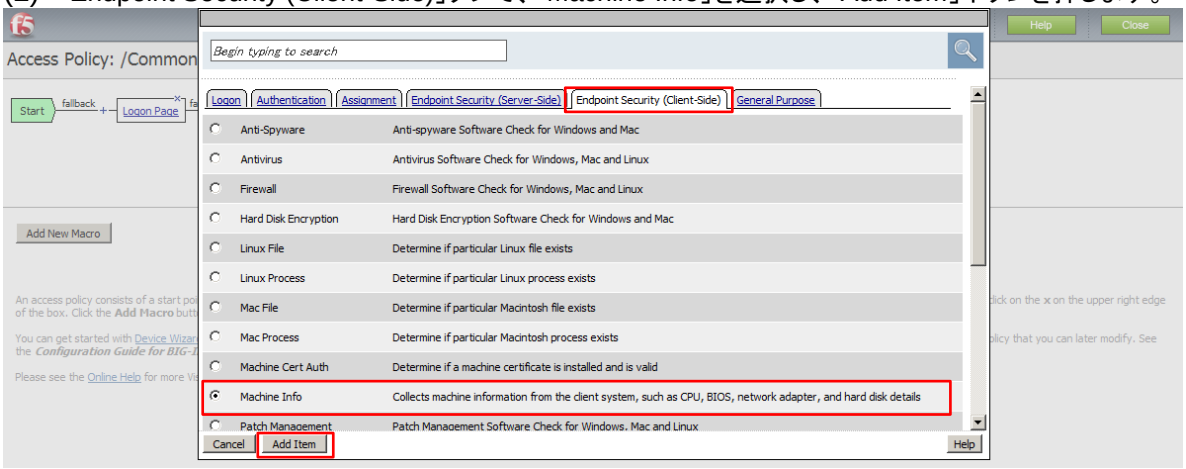
6.6.1. クライアント端末固有の情報の取得

クライアント端末のマザーボードシリアル番号情報が入手できない場合、APM で調べる事も可能です。
以下、クライアント PC のマザーボードのシリアル番号を取得するためのステップです。

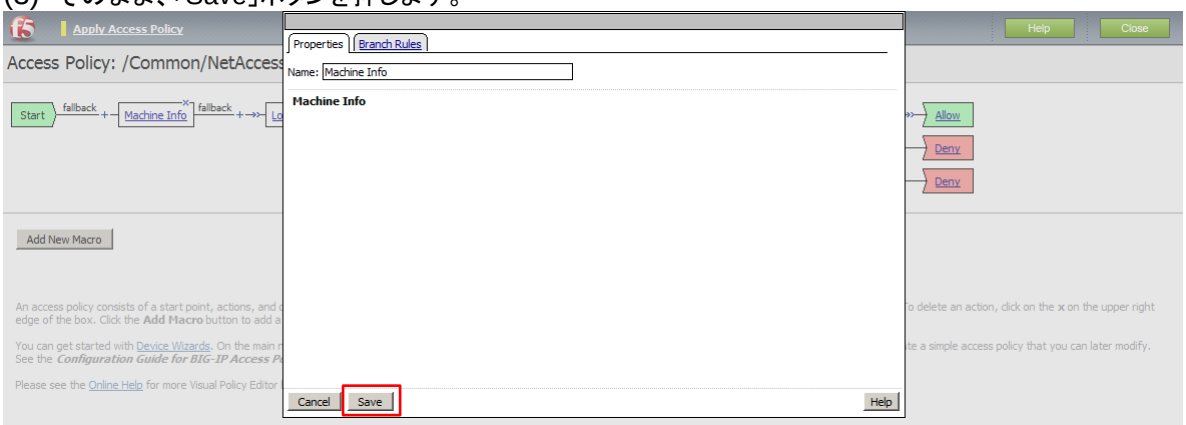
(1) ここまでの設定では、以下の状態になっています。
「Logon Page」の前の「+」をクリックします。



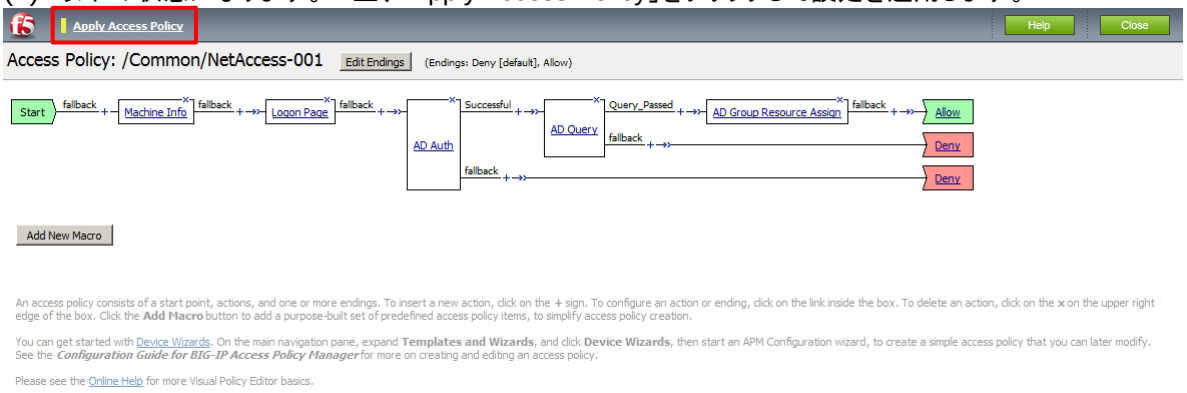
(2) 「Endpoint Security (Client-Side)」タブで、「Machine Info」を選択し、「Add Item」ボタンを押します。



(3) そのまま、「Save」ボタンを押します。

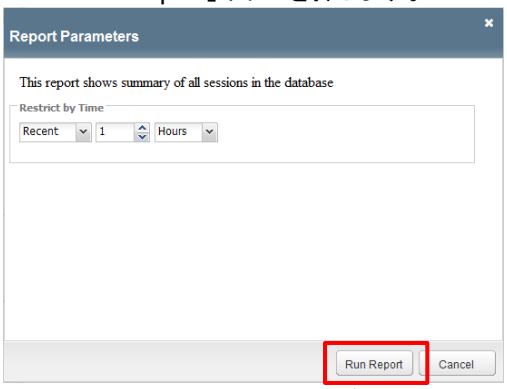


(4) 以下の状態になります。一旦、「Apply Access Policy」をクリックして設定を適用します。

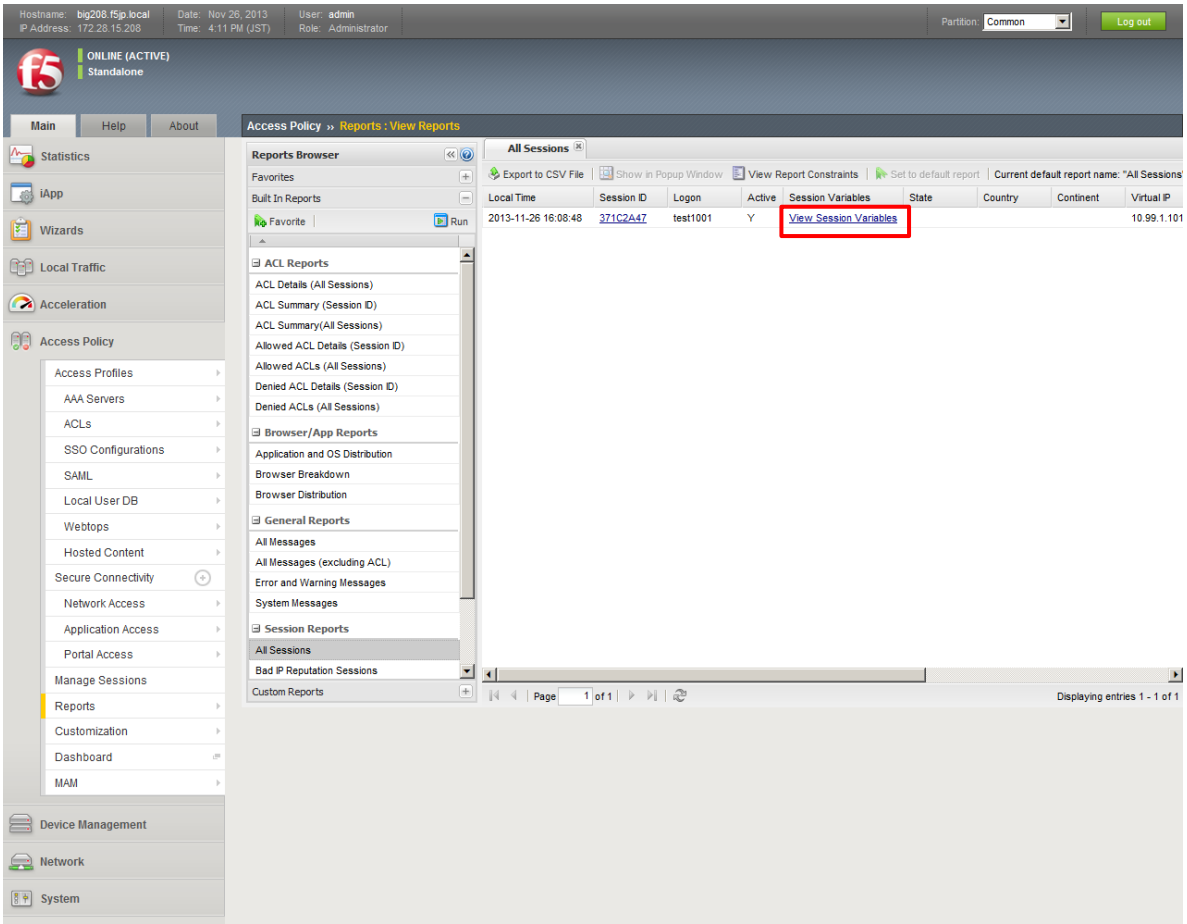


(5) クライアント PC から APM Virtual Server へアクセスします。

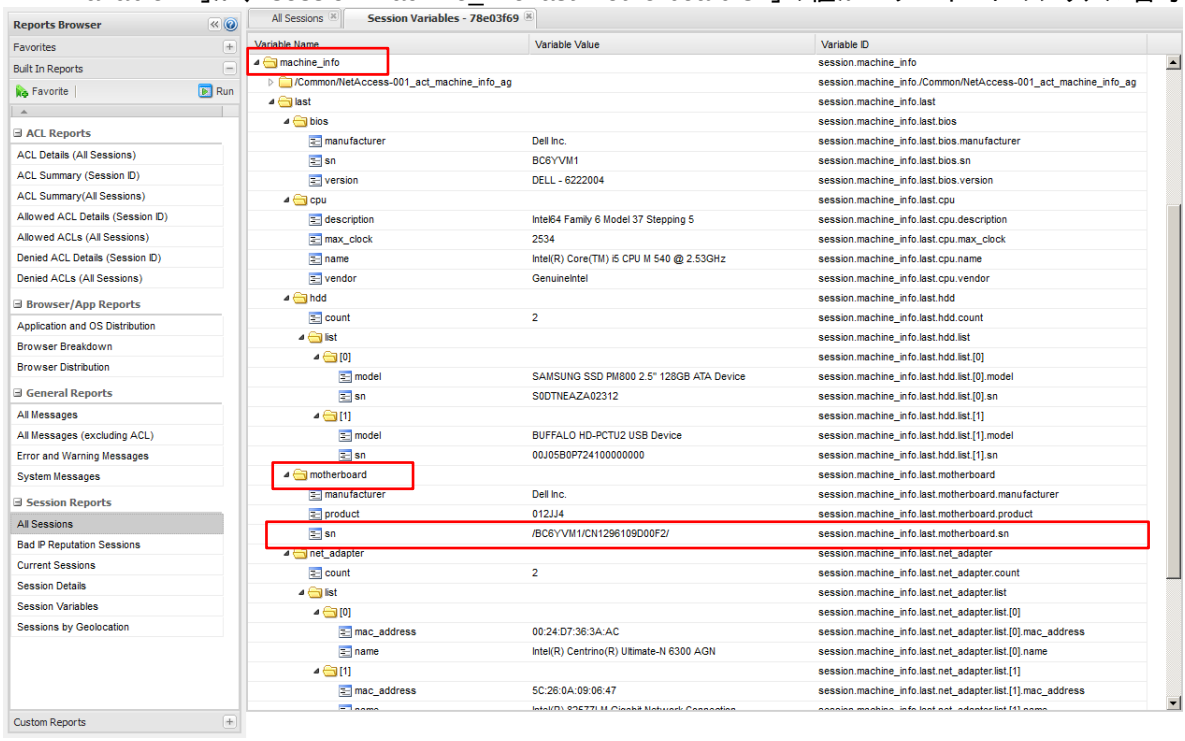
(6) 「Main」メニュー → 「Access Policy」 → 「Reports」を選ぶと、以下の画面が現れます。
「Run Report」ボタンを押します。



(7) アクセスした Logon ユーザ（本例では test1001）の行に表示されている、「View Session Variables」をクリックします。



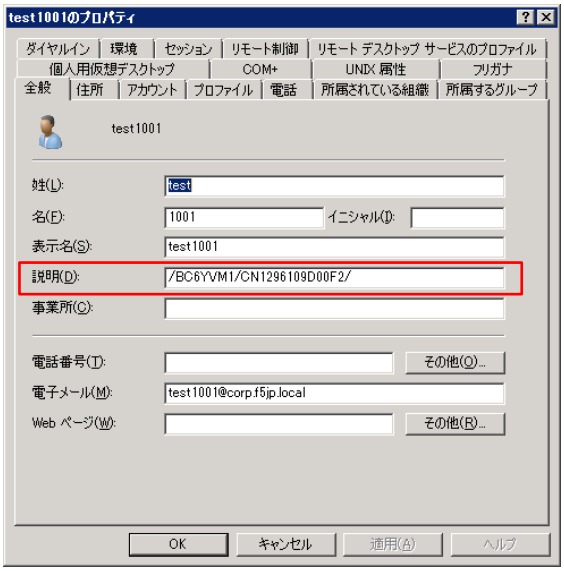
(8) 「Variable Name」の「Machine_info」の△をクリックして展開します。
その中に、「Motherboard」ディレクトリがあるので、△をクリックして展開します。
「Variable ID」が、「session.machine_info.last.motherboard.sn」の値がマザーボードのシリアル番号です。



マザーボードシリアル番号がチェックできたら(またはコピーできたら)、一旦、ネットワークアクセスを切断します。

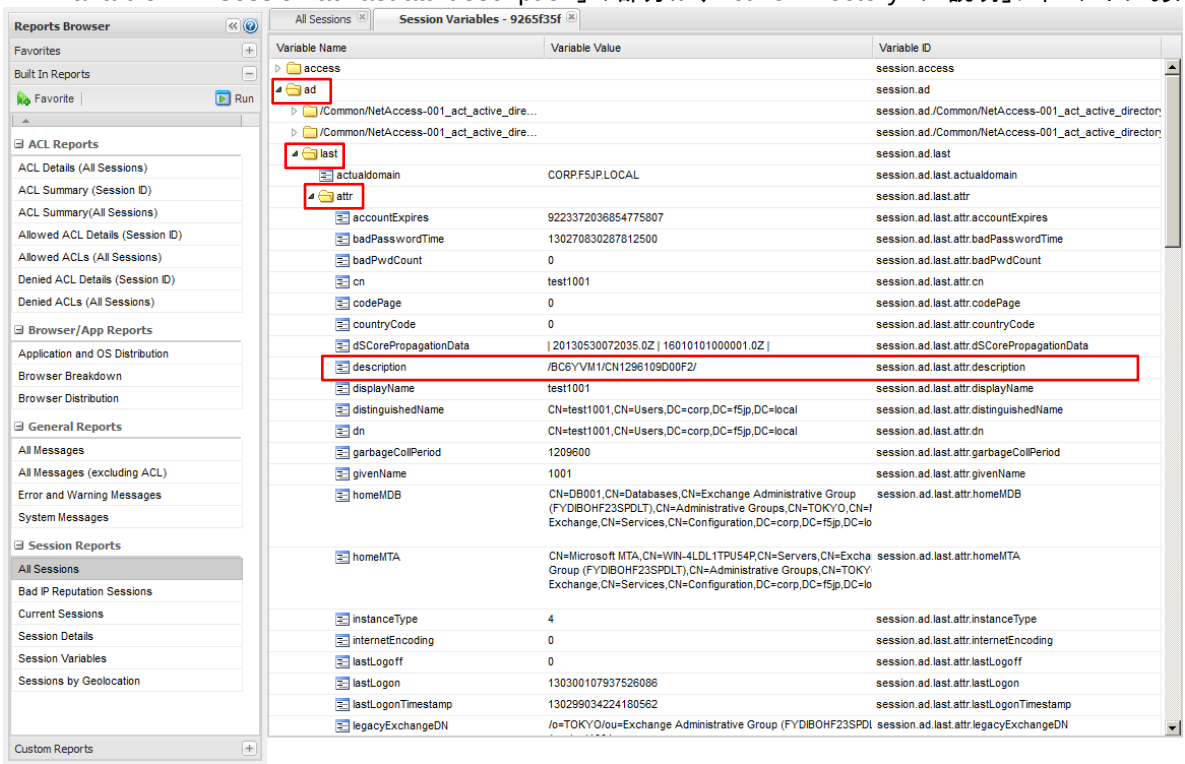
6.6.2. Active Directory の設定

(1) Active Directory 上の"test1001"設定を開きます。本例では、「説明」フィールドを使うことにします。
ここに、クライアント PC のマザーボードシリアル番号を入力します。

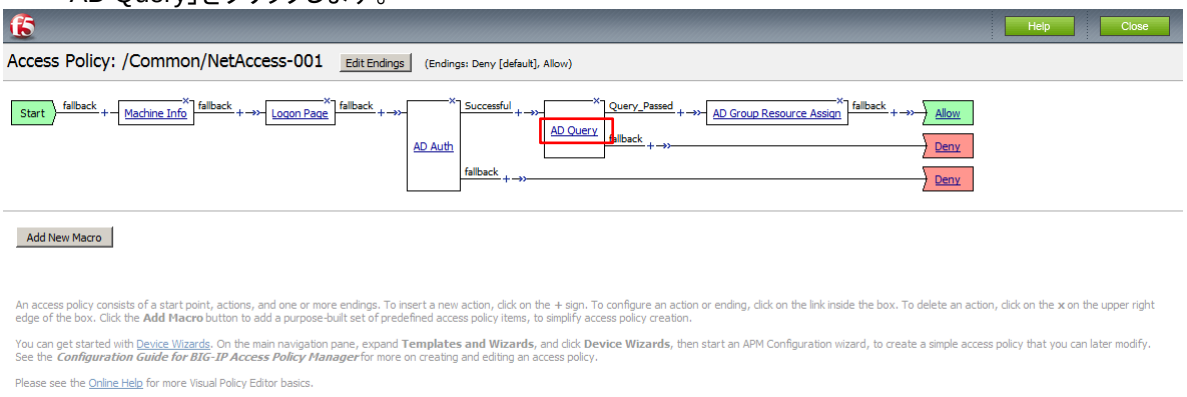


(2) 今一度、クライアント PC から、APM の Virtual Server へアクセスします。

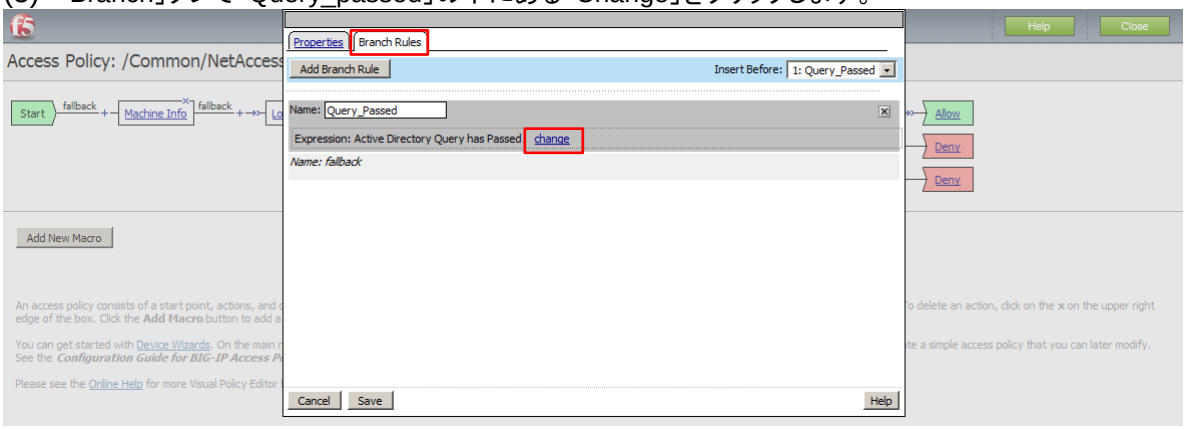
(3) もう一度、「Main」メニュー → 「Access Policy」 → 「Reports」で、test1001 の Session Variable を確認します。
「ad」 → 「last」 → 「attr」を展開します。
Varialble ID:「session.ad.last.attr.description」の部分が、Active Directory の「説明」フィールドにあたります。



(4) クライアントPCのマザーボードシリアル番号と、Active Directoryに登録したそのシリアル番号を比較して、同じであれば次のボックスへ進む、という設定を行います。
「AD Query」をクリックします。

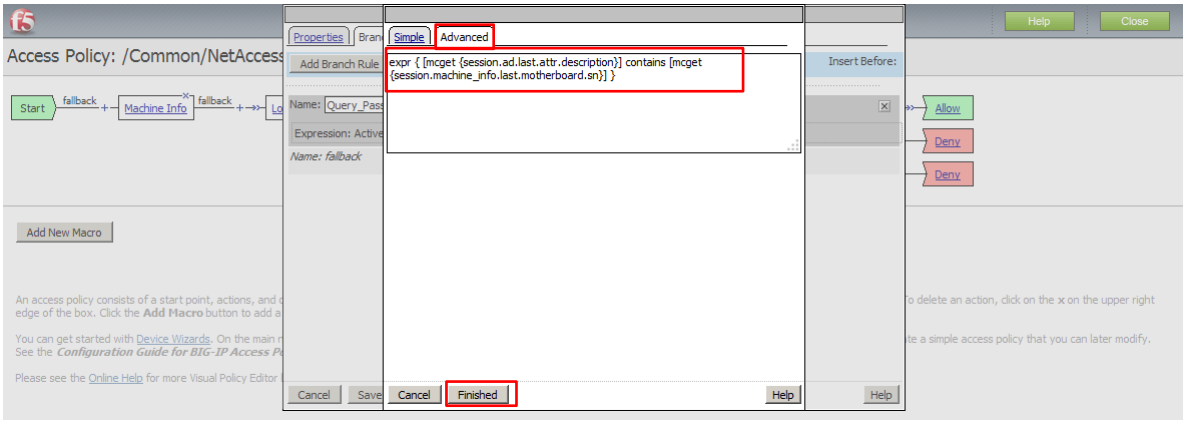


(5) 「Branch」タブで「Query_passed」の下にある「Change」をクリックします。



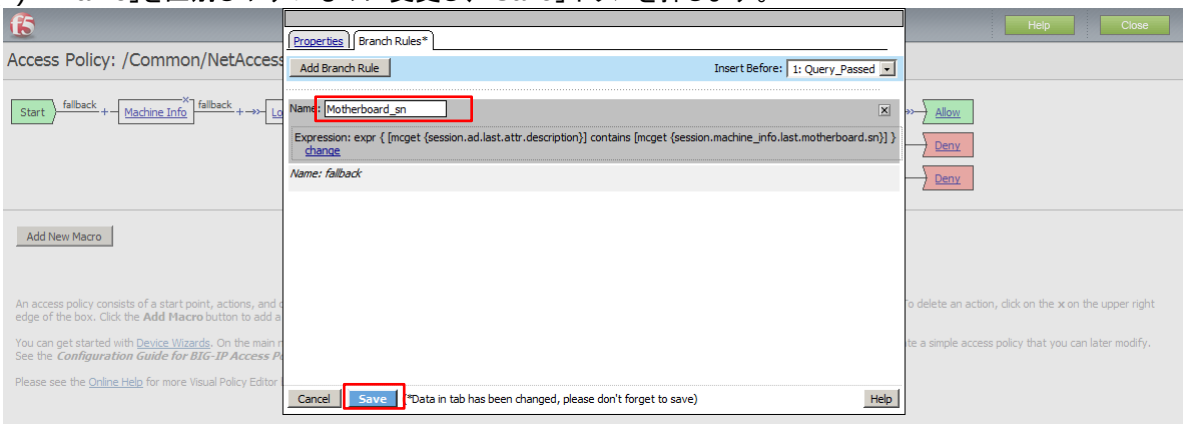
(6) 「Advanced」タブで、以下を入力します。

expr { [mcget {session.ad.last.attr.description}] contains [mcget {session.machine_info.last.motherboard.sn}] }

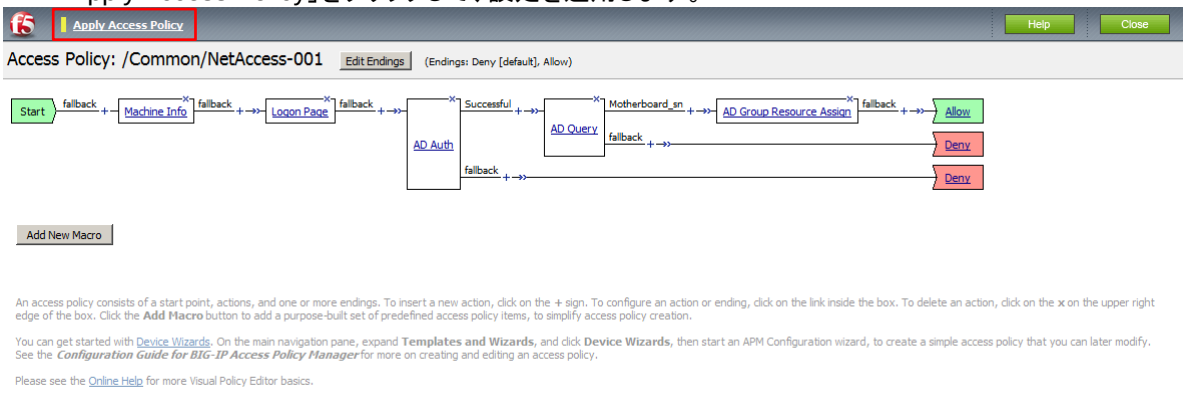


セッション変数:「session.ad.last.attr.description」の値(＝Active Directory の「説明」フィールド値)を mcget で取得しています。
また、「session.machine_info.last.motherboard.sn」の値(＝クライアントPCのマザーボードシリアル番号)もmcgetで取得しています。
この例では、「session.ad.last.attr.description」の値が「session.machine_info.last.motherboard.sn」の値を含んでいるかどうかをチェックし、含んでいる(≒同じである)場合には次のボックスに進む、という設定にしています。

(7) 「Name」を区別しやすいものに変更し、「Save」ボタンを押します。



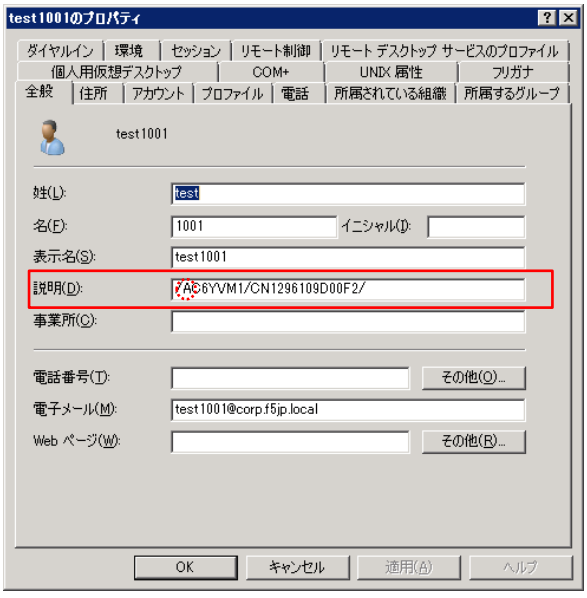
(8) 以下の状態になります。
「Apply Access Policy」をクリックして、設定を適用します。



6.6.3. クライアントからのアクセス

(1) マザーボードシリアル番号:「/BC6YVM1/CN1296109D00F2/」を持つクライアント PC から、"test1001"で、APM の VS へアクセスし、アクセスができることを確認します。

(2) Active Directory のユーザ:"test1001"の「説明」フィールドに記載されたマザーボードシリアル番号:「/BC6YVM1/CN1296109D00F2/」を、例えば、「/AC6YVM1/CN1296109D00F2/」に変更してみます。



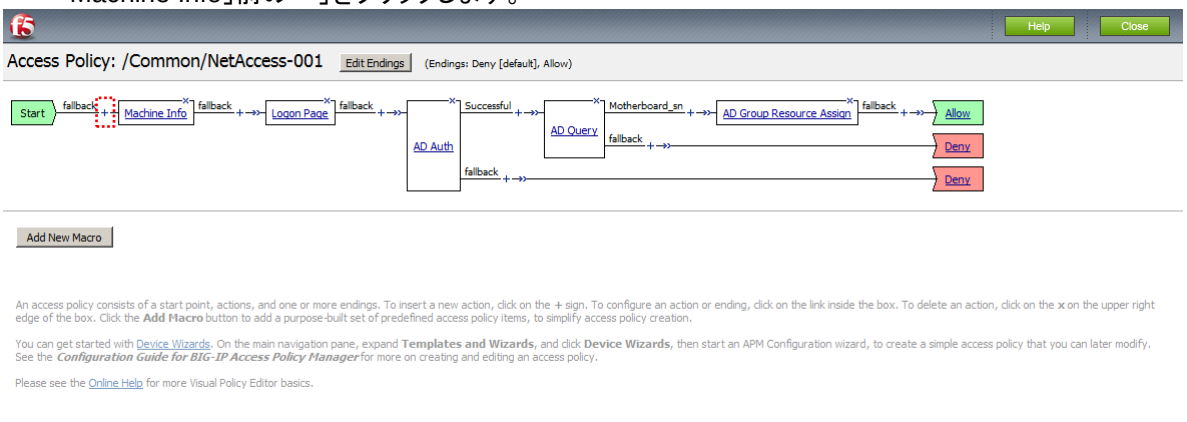
(3) もう一度、マザーボードシリアル番号:「/BC6YVM1/CN1296109D00F2/」を持つクライアント PC から、"test1001" で、APM の VS へアクセスすると、シリアル番号が異なるので、接続ができなくなります。

6.7. ［VPE サンプル-4］クライアント OS の種類に応じてポリシーを変える

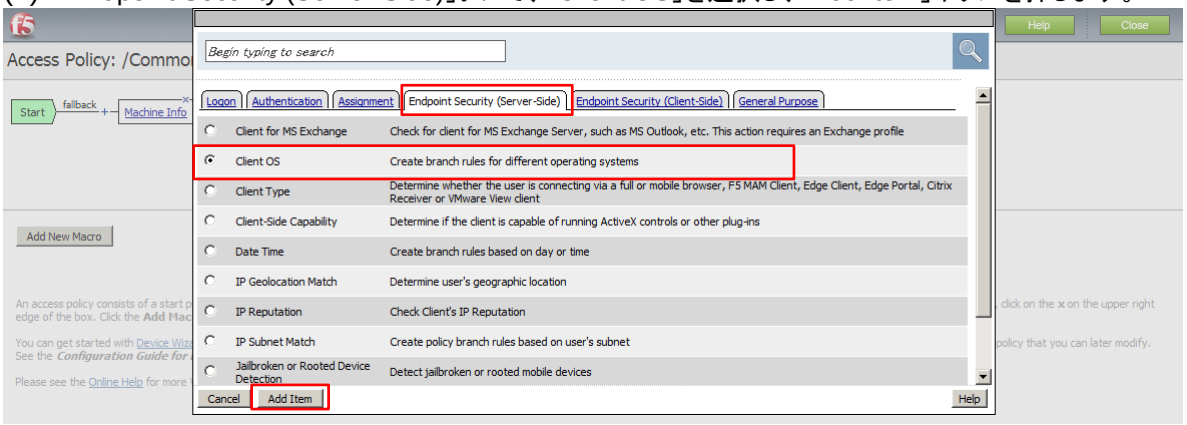
クライアント OS 毎にポリシーを変更したい、という要件があると仮定します。

本例では、Windows クライアントには、［VPE サンプル-3］で設定したポリシーを適用し、iOS(Apple iPhone/iPad)にはそれとは異なるポリシーを適用する、という設定を行います。

(1) ここまでの設定では、以下の状態になっています。
「Machine Info」前の「+」をクリックします。

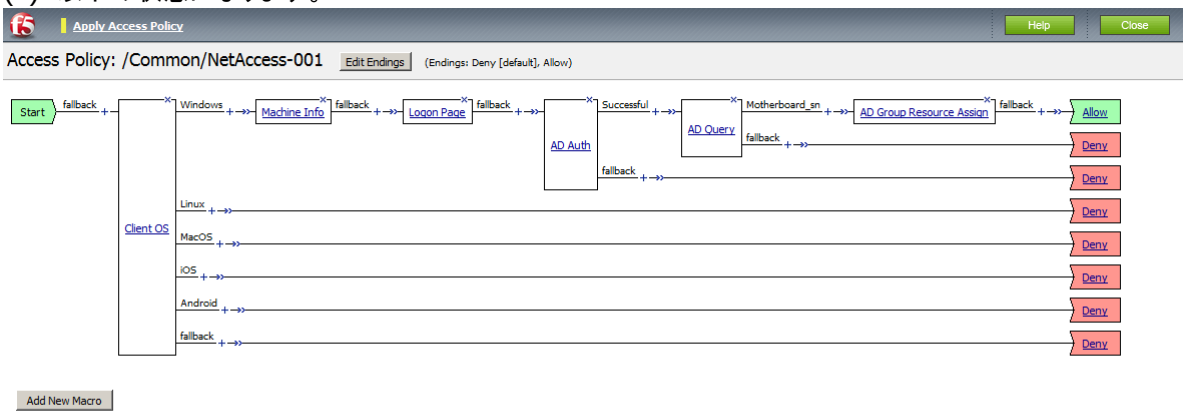


(2) 「Endpoint Security (Server-Side)」タブで、「Client OS」を選択し、「Add Item」ボタンを押します。

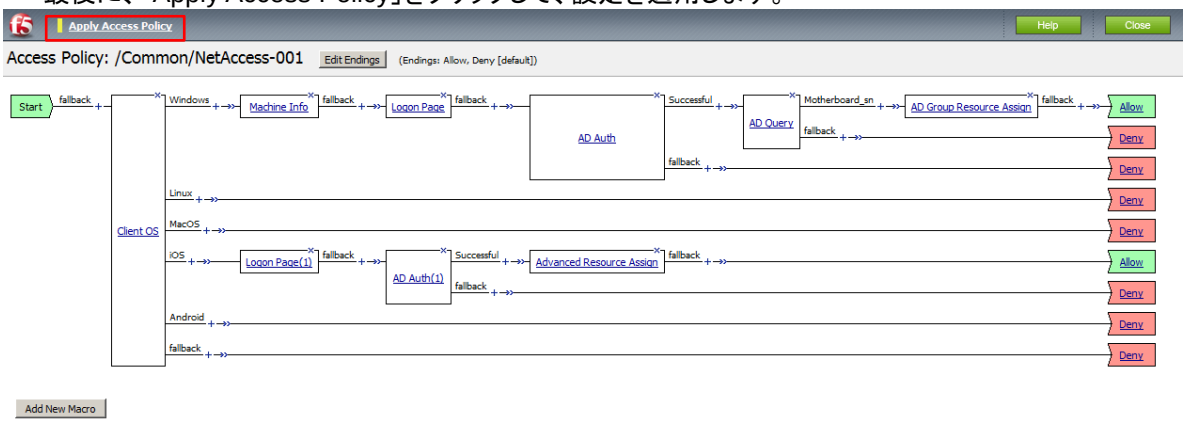


(3) そのまま、「Save」ボタンを押します。

(4) 以下の状態になります。



(5) iOS 設定には、「Logon Page」,「AD Auth」,「Advanced Resource Assign」のみ追加してみました。
最後に、「Apply Access Policy」をクリックして、設定を適用します。



この設定によって、クライアント OS 毎に異なるポリシーを適用することができます。

6.8. ［VPE サンプル-5］マクロを使う

VPE には、マクロ機能があります。繰り返し利用されるポリシーをマクロ化して再利用する、またはデフォルトで用意されている便利なマクロを利用することもできます。

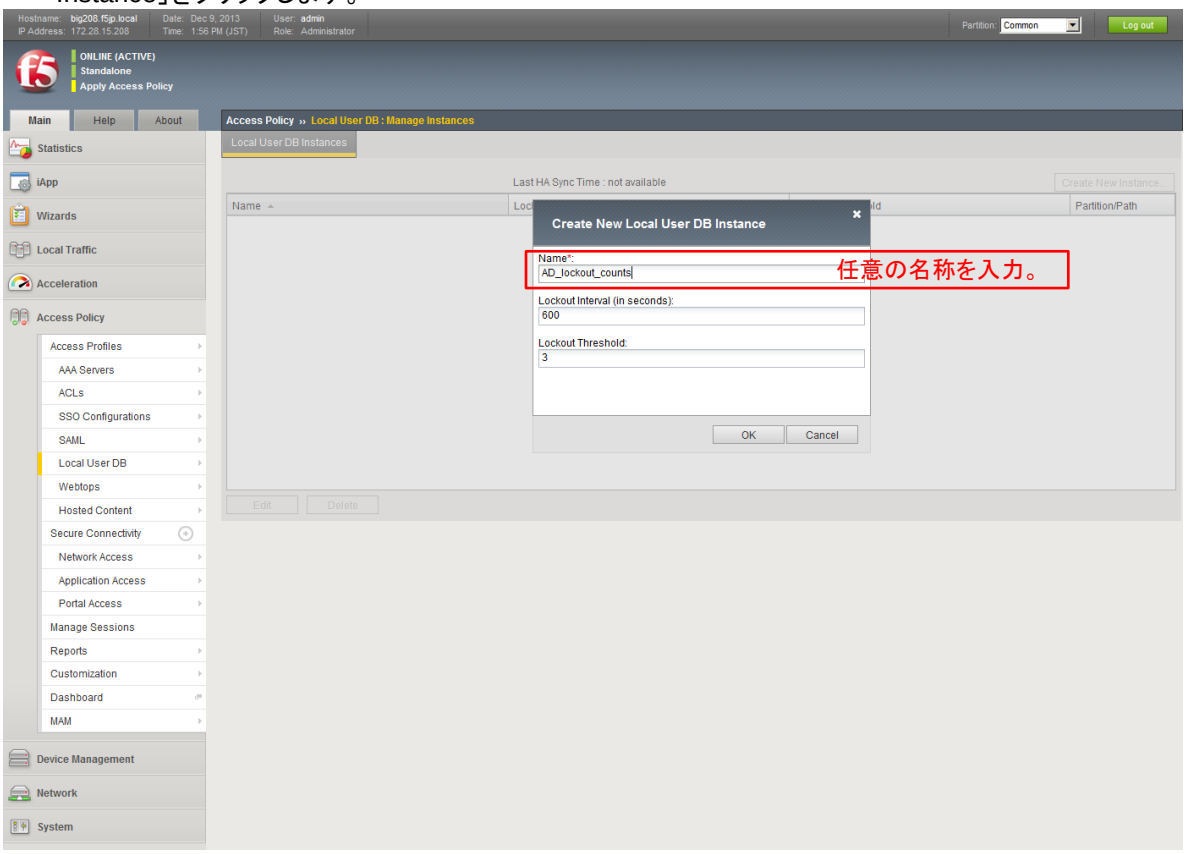
ここでは、以下 2 つの要件に対して、デフォルトで用意されているマクロを利用する例を示します。

① Active Directory 認証の誤り回数をカウントしたい。
さらに指定回数を超えたらロックし、ロック解除するまで使えないようにしたい。

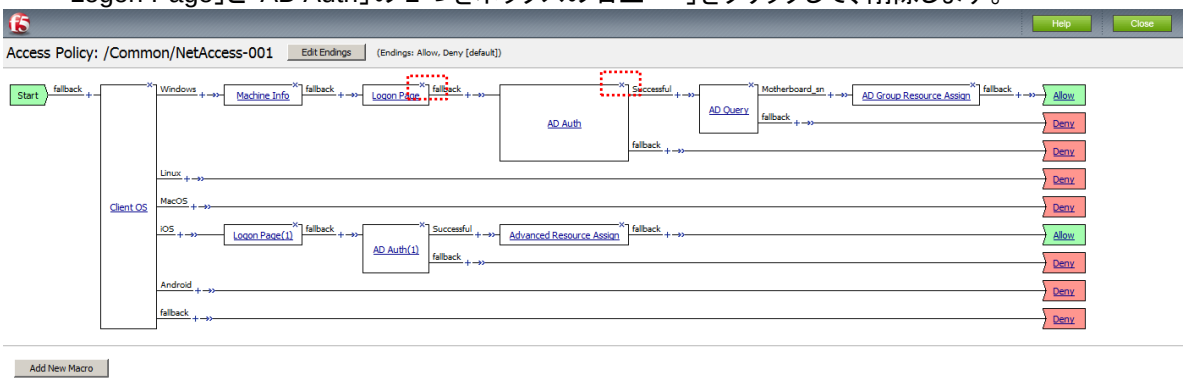
② Android と iOS は同じ設定なので、一つの設定にまとめたい。

6.8.1. AD 認証の誤り回数カウント

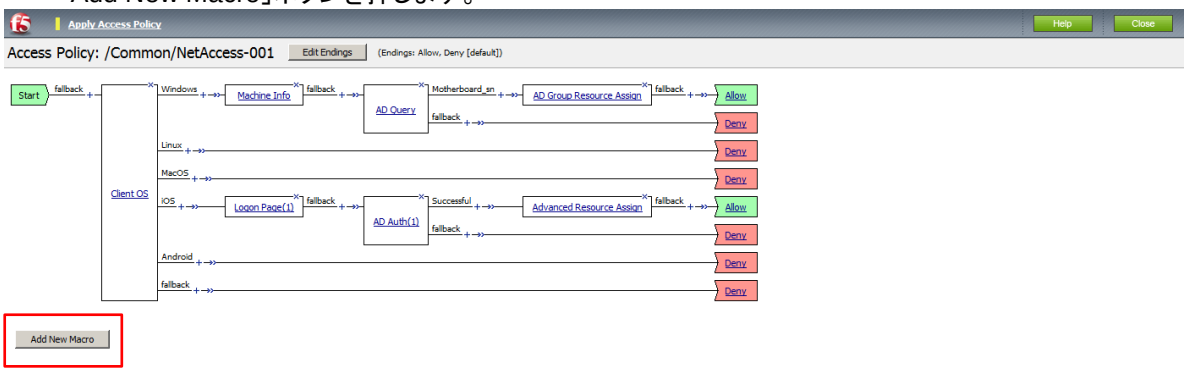
(1) まず、ユーザエントリの存在しない、空の Local User DB の Instance を作ります。
「Main」メニュー → 「Access Policy」 → 「Local User DB」 → 「Manage Instances」で、左上の「Create New Instance」をクリックします。



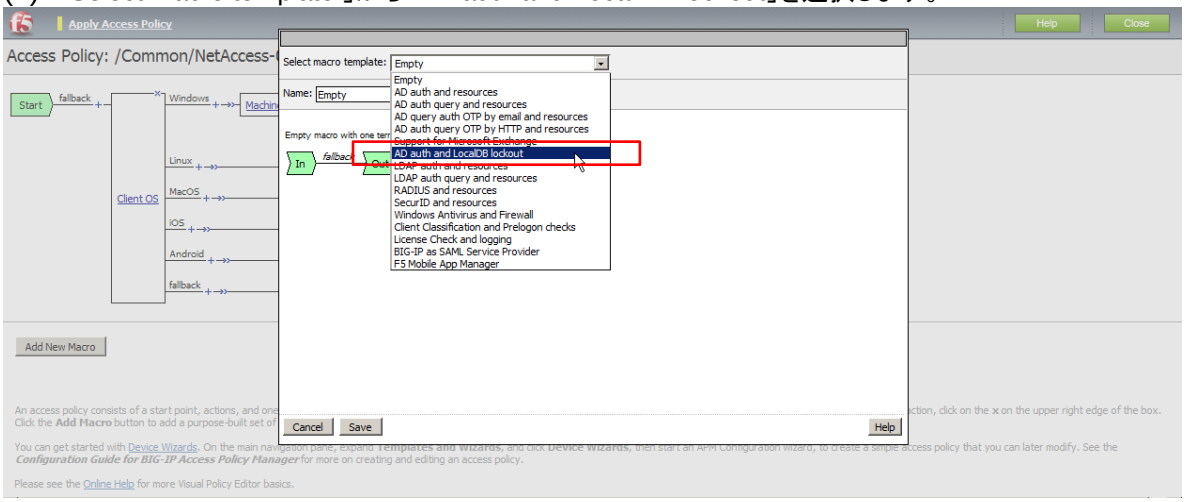
(2) VPE 設定に戻ります。
ここまでの設定では、以下の状態になっています。
「Logon Page」と「AD Auth」の 2 つをボックスの右上「×」をクリックして、削除します。



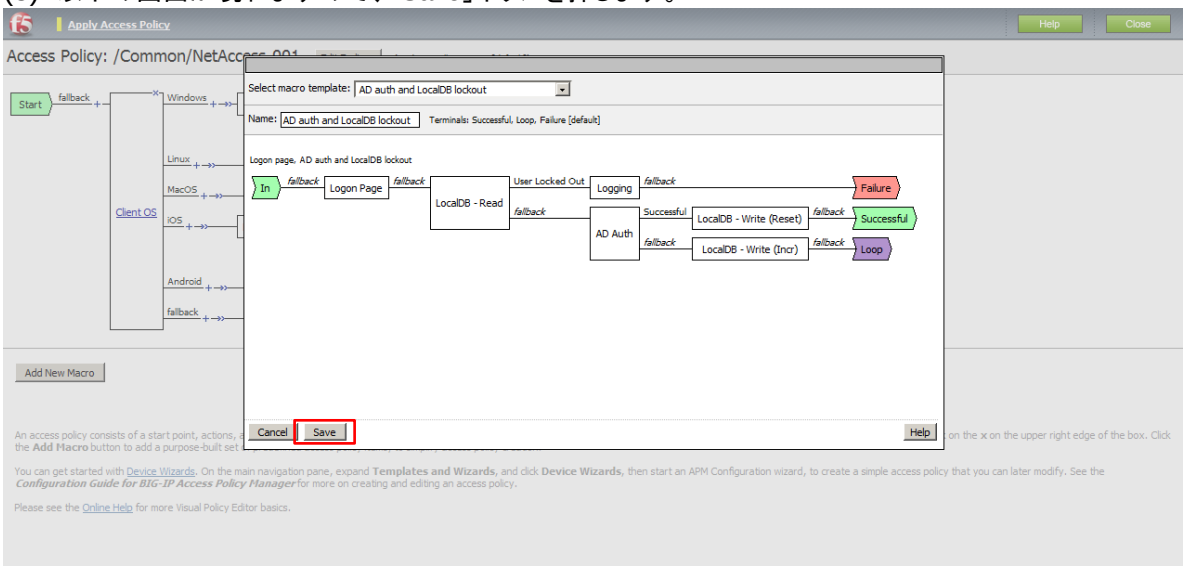
(3) 以下の状態になります。
「Add New Macro」ボタンを押します。



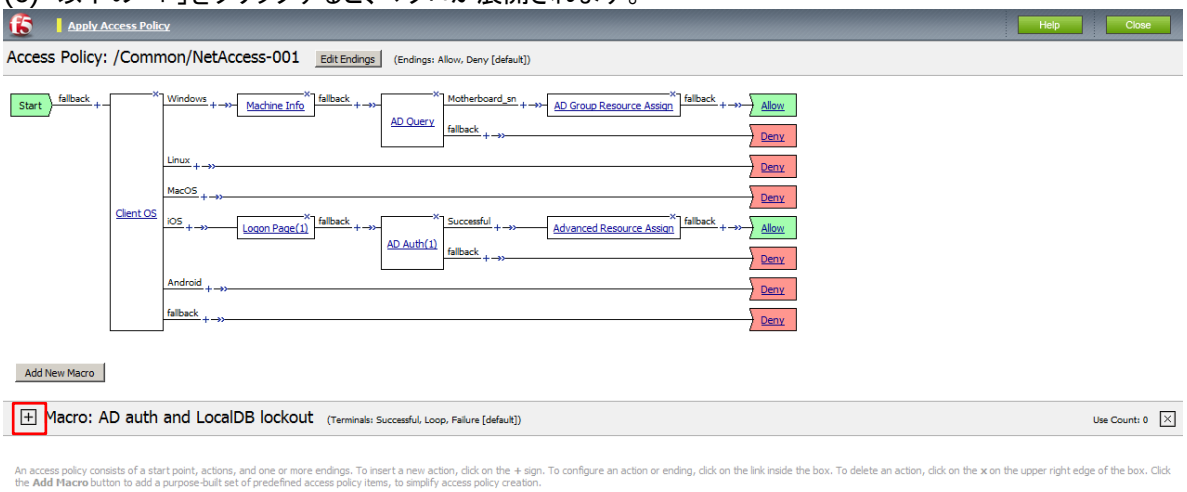
(4) 「Select macro template:」から「AD auth and LocalDB lockout」を選択します。



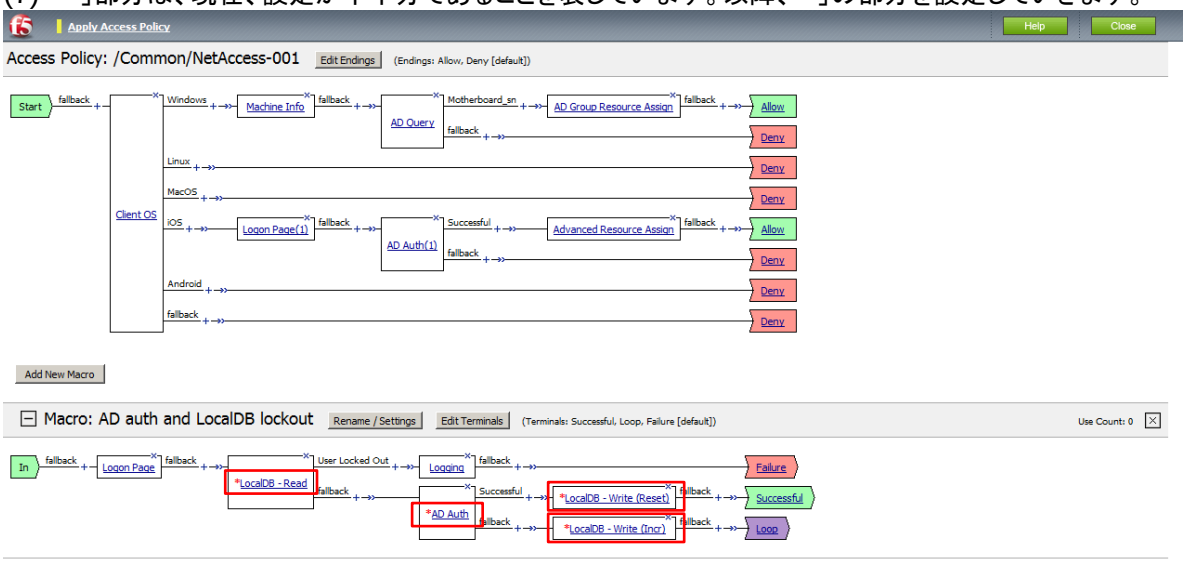
(5) 以下の画面が現れますので、「Save」ボタンを押します。



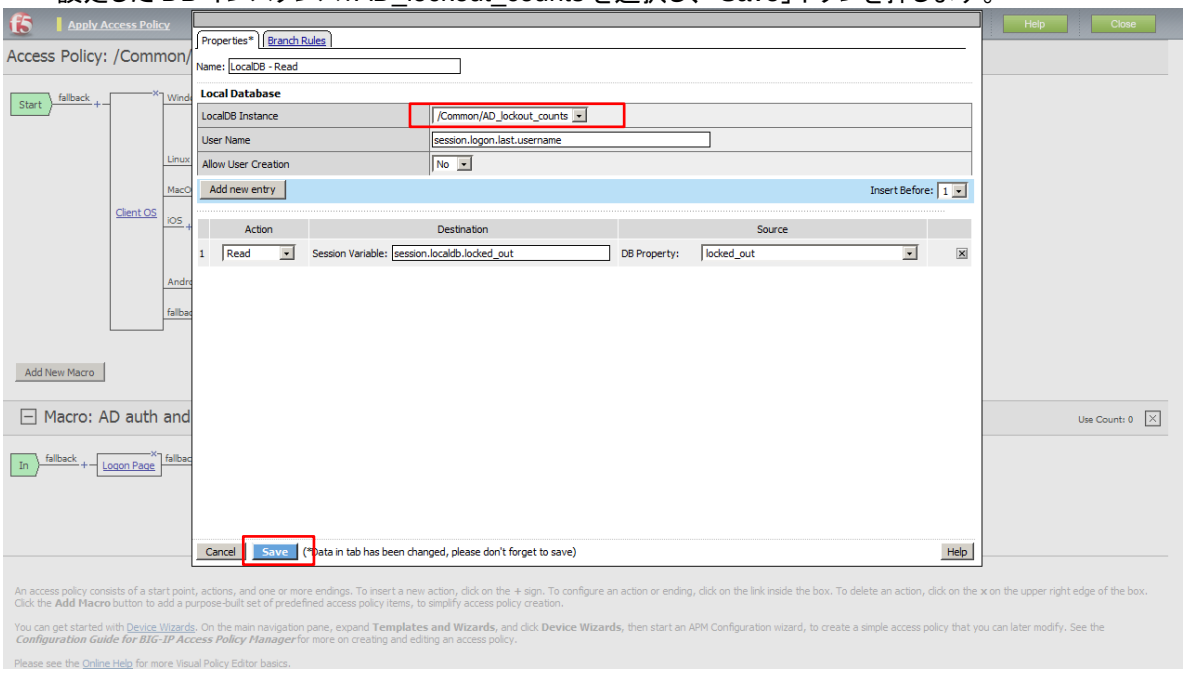
(6) 以下の「＋」をクリックすると、マクロが展開されます。



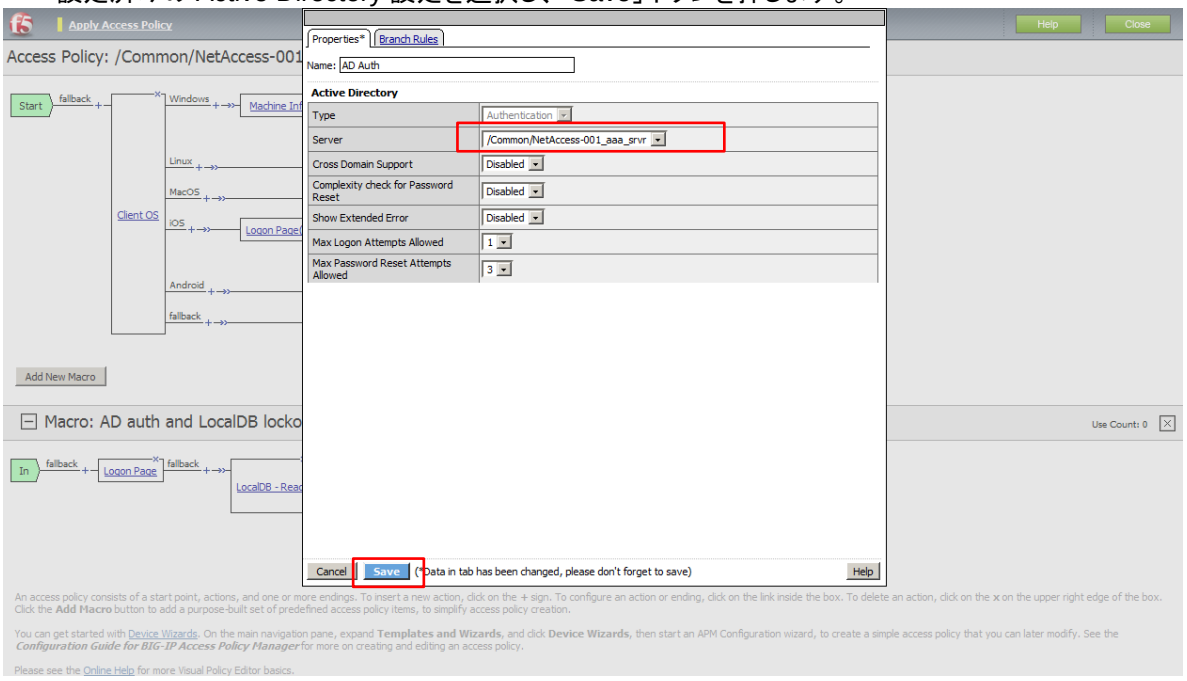
(7) 「*」部分は、現在、設定が不十分であることを表しています。以降、「*」の部分を設定していきます。



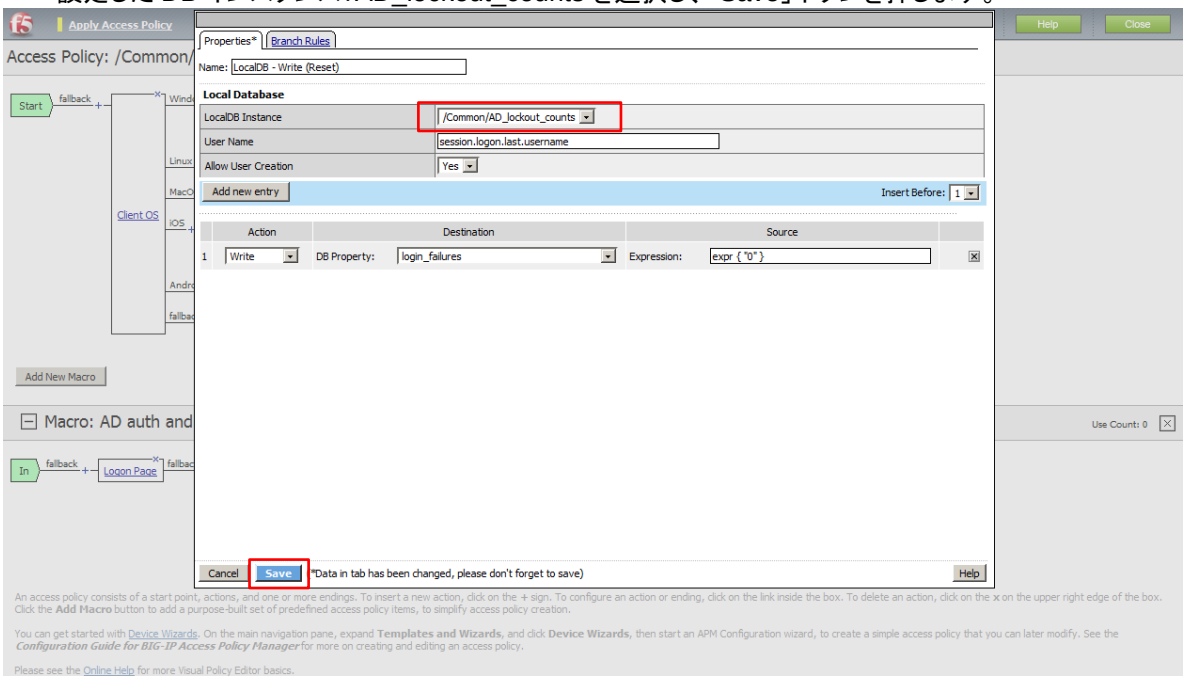
(8) 「LocalDB - Read」をクリックすると、以下の画面が現れます。
設定した DB インスタンス：AD_lockout_counts を選択し、「Save」ボタンを押します。



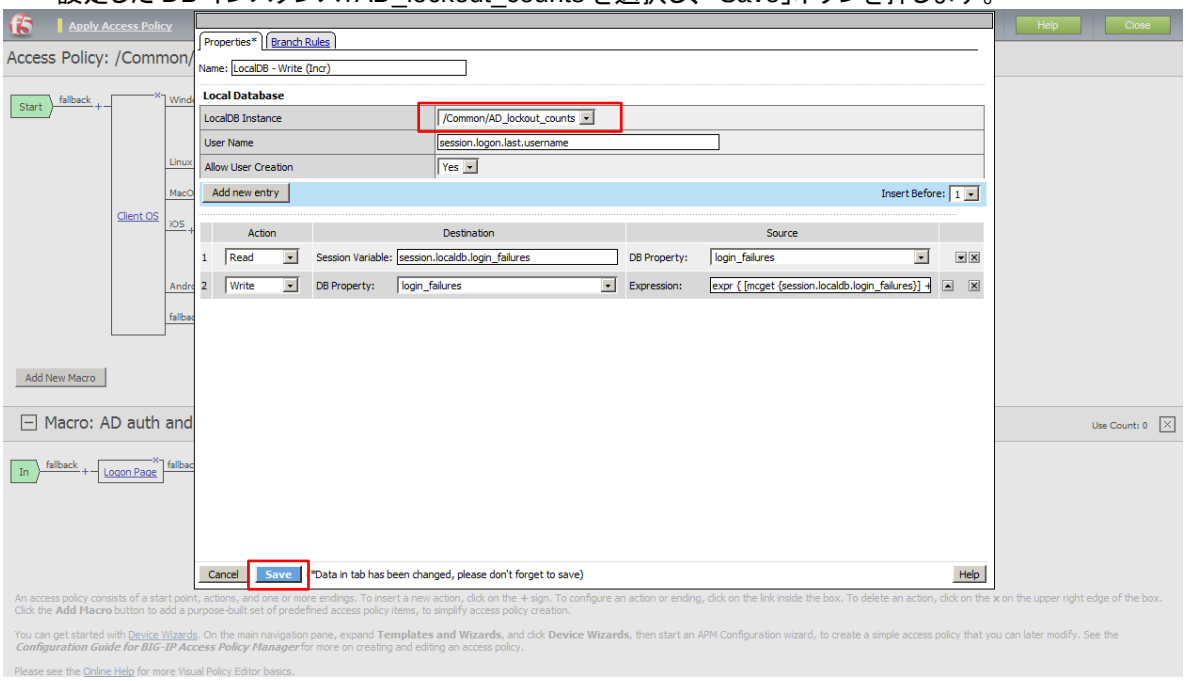
(9) 「AD Auth」をクリックすると、以下の画面が現れます。
設定済みの Active Directory 設定を選択し、「Save」ボタンを押します。



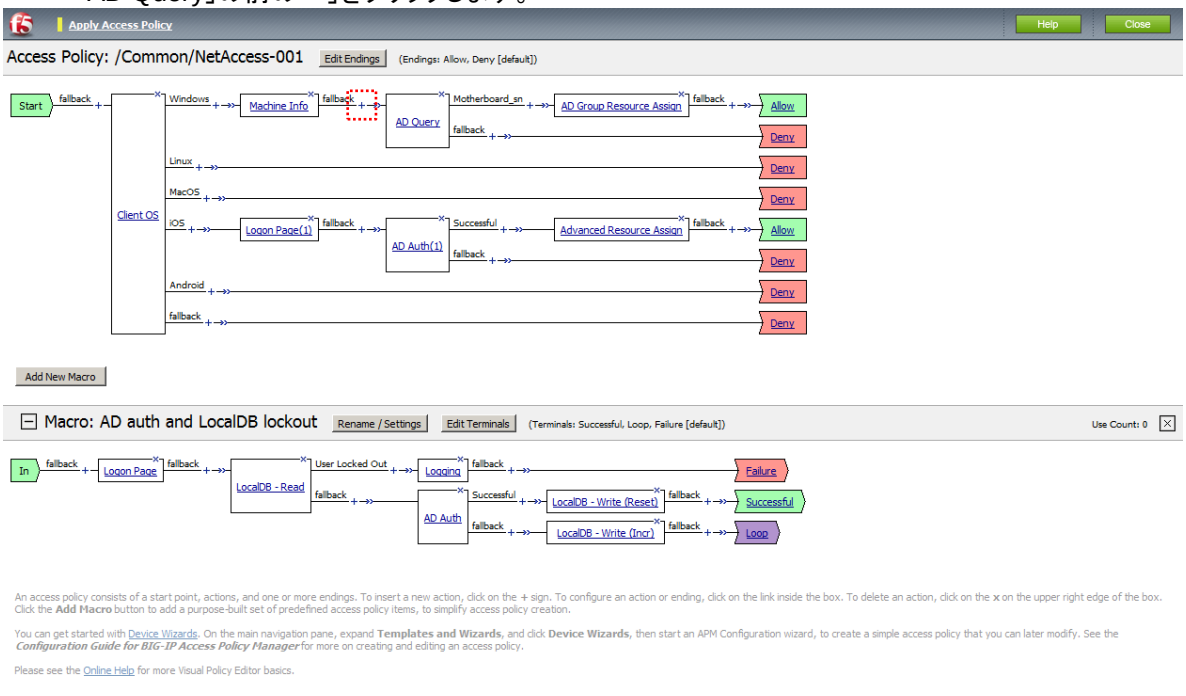
(10)「LocalDB - Write (Reset)」をクリックすると、以下の画面が現れます。
設定した DB インスタンス：AD_lockout_counts を選択し、「Save」ボタンを押します。



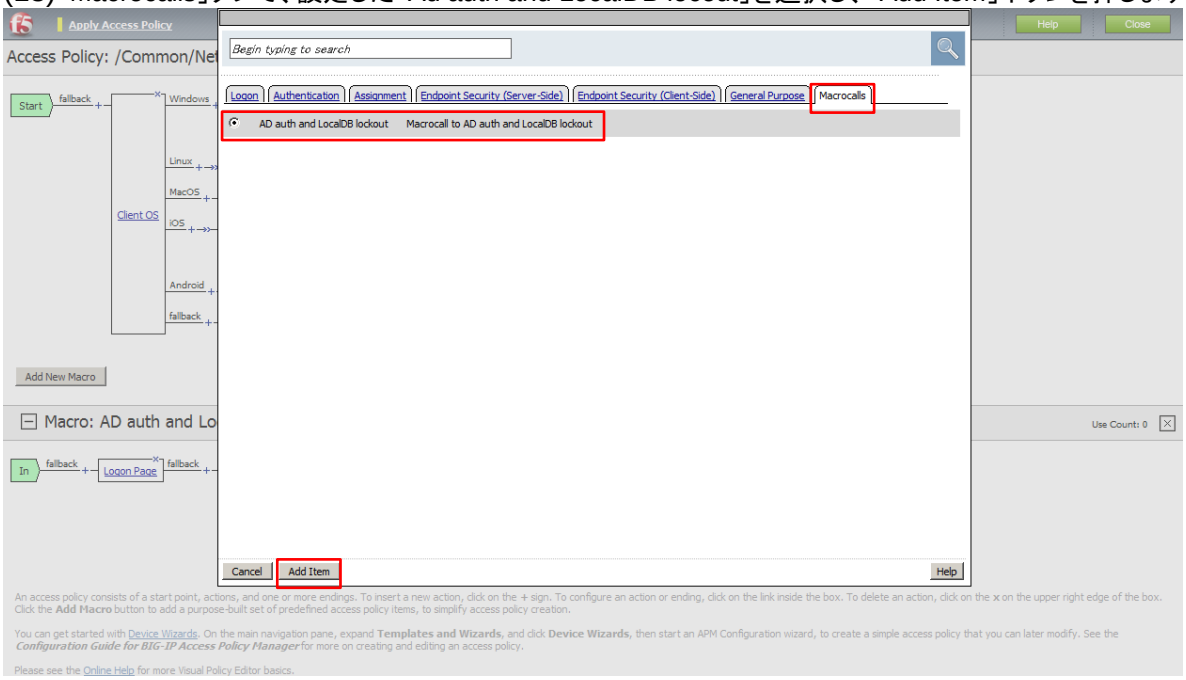
(11)「LocalDB - Write (Incr)」をクリックすると、以下の画面が現れます。
設定した DB インスタンス：AD_lockout_counts を選択し、「Save」ボタンを押します。



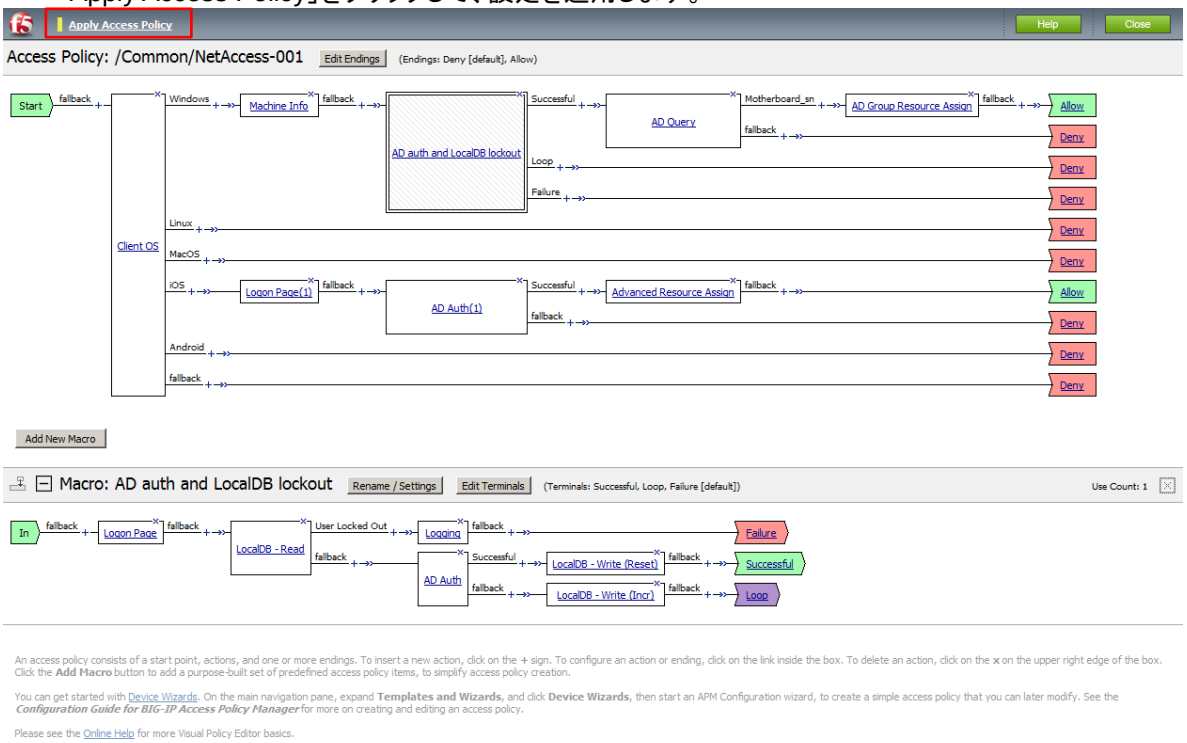
(12) 本サンプルでは、「AD Query」の前に、マクロを入れることにします。
「AD Query」の前の「+」をクリックします。



(13)「Macrocalls」タブで、設定した「Ad auth and LocalDB locout」を選択し、「Add Item」ボタンを押します。

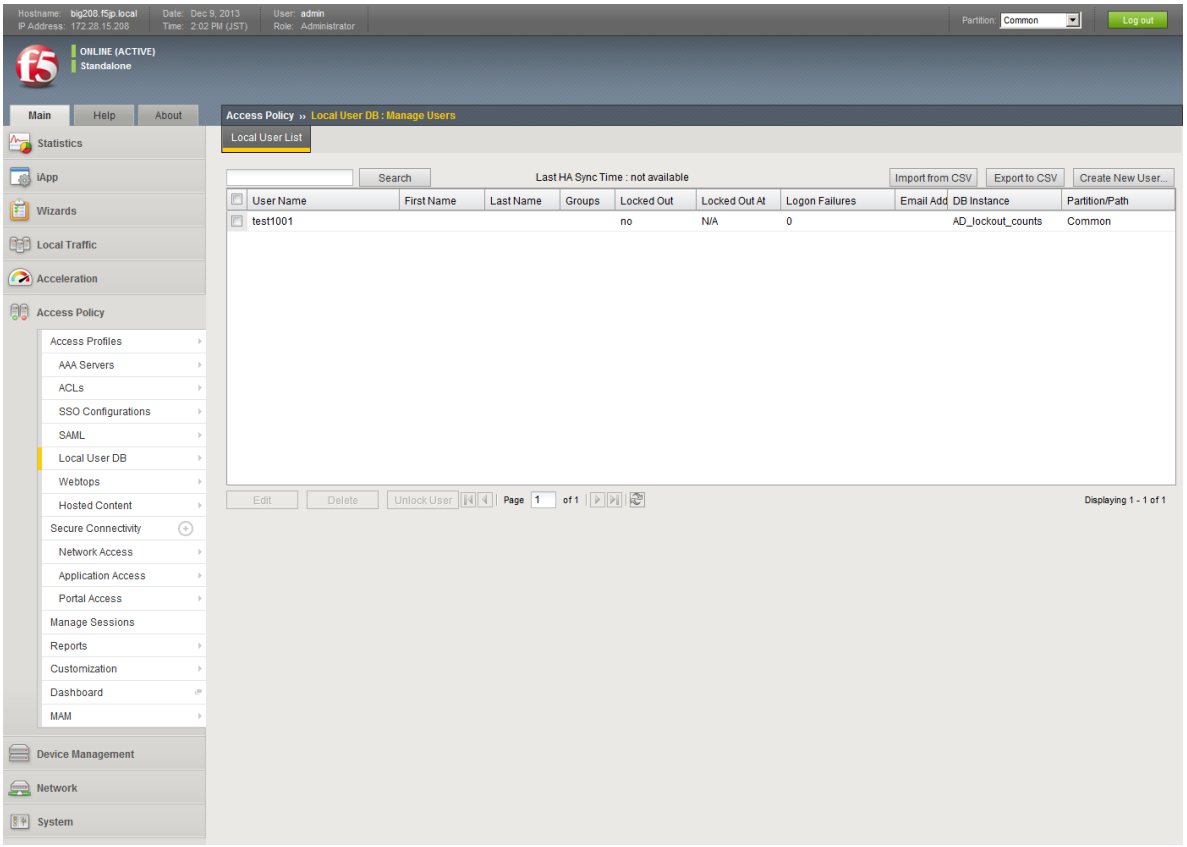


(14) 以下の状態になります。
「Apply Access Policy」をクリックして、設定を適用します。



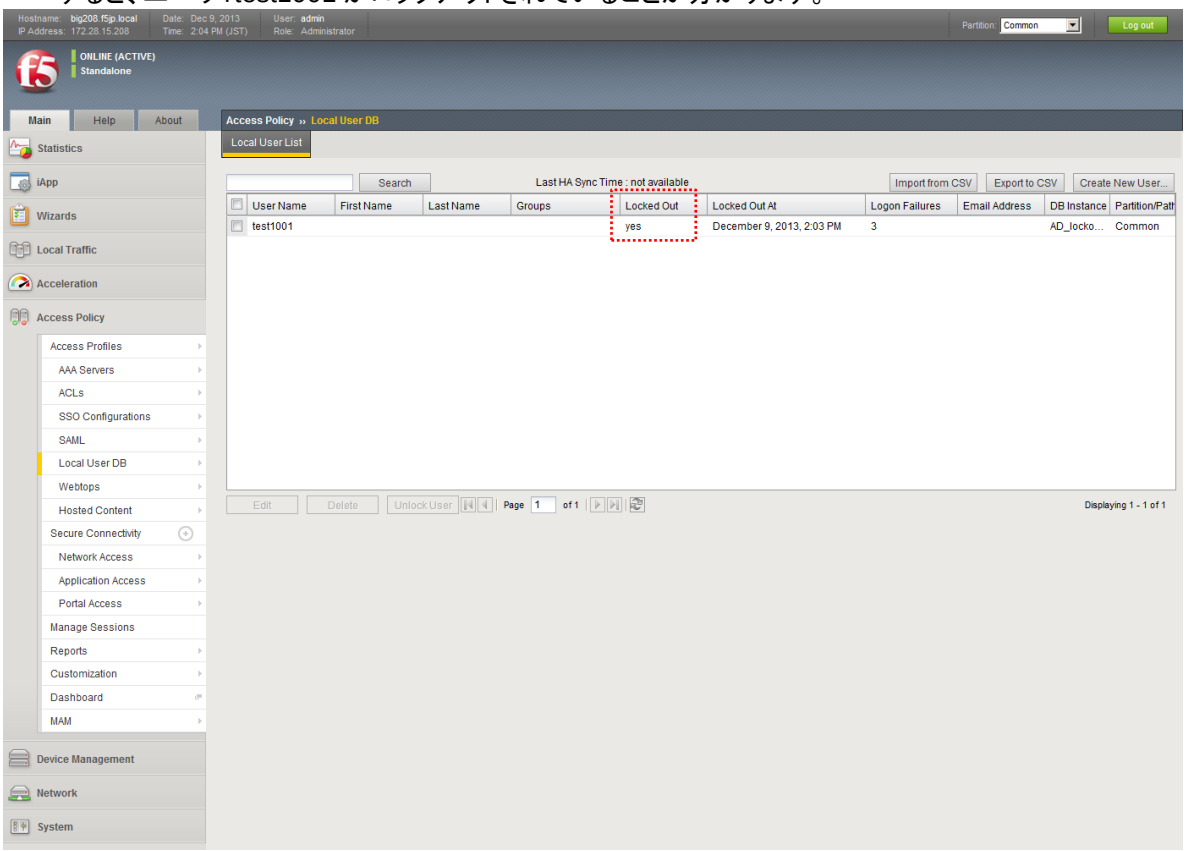
6.8.1.1. クライアントからのアクセス

(1) まずは、クライアント PC から正しい ID とパスワード(test1001/test1001)でアクセスしてみます。
「Main」メニュー →「Access Policy」→「Local User DB」→「Manage Users」を確認します。
すると、ユーザ：test1001 がエントリされていることが分かります。



(2) 今度は、誤ったパスワードで、3 回程度アクセスしてみます。
以下のように、アクセスが拒否されたメッセージが表示されます。

(3) 「Main」メニュー →「Access Policy」→「Local User DB」→「Manage Users」を確認します。
すると、ユーザ：test1001 がロックアウトされていることが分かります。



(4) ロックされたユーザのロック解除

V11.4.1(HF1 含む)では、GUI からのロック解除ができず、コマンドラインで実施する必要があります。
(詳細は以下 SOL を参照ください)
http://support.f5.com/kb/en-us/solutions/public/14000/700/sol14746.html

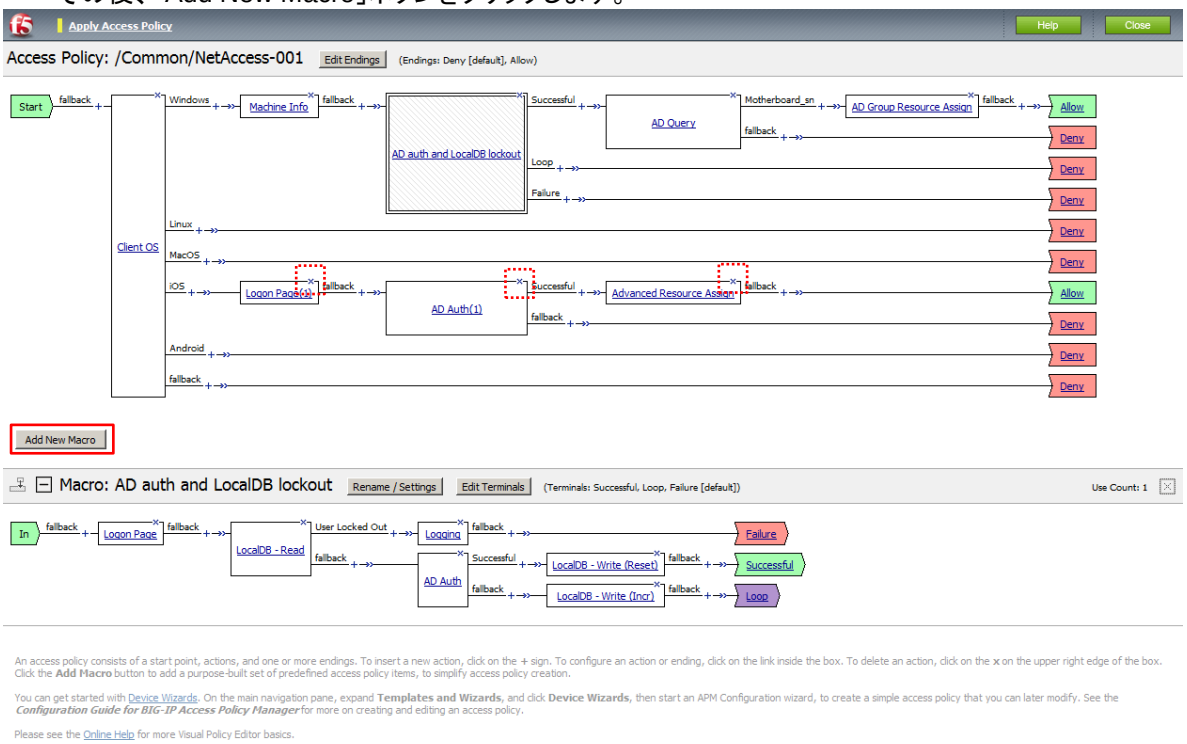
① SSH で BIG-IP へログイン(デフォルト ID/Pass：root/default)
② 以下のコマンドを実行。(赤文字部分のみ変更してご利用ください。)

```
[root@big208:Active:Standalone] config # ldbutil --update --uname=test1001
--instance=/Common/AD_lockout_counts --locked_out=0 --lockout_start=0 --login_failures=0
```

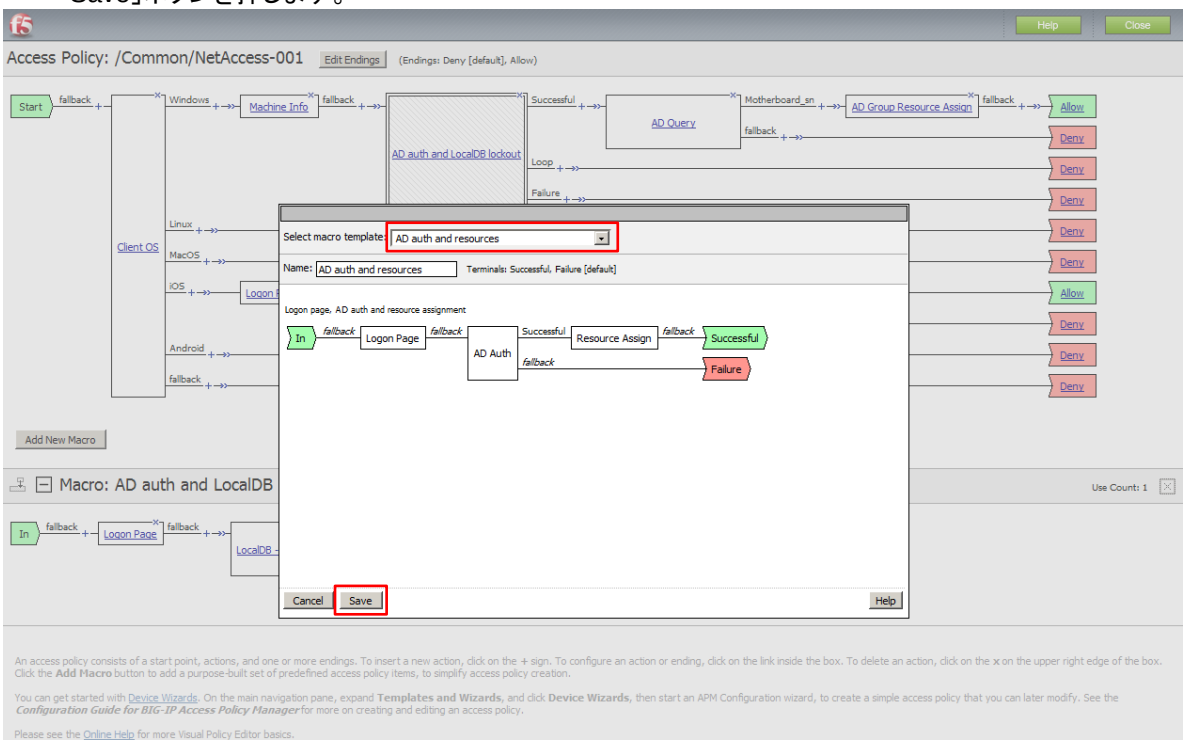
6.8.2. 同じ設定をまとめる

ご要件として、iOS と Android は同じ設定を行う、と仮定します。
iOS と Android それぞれに同じ設定を追加しても全く問題はないのですが、見た目上、少し煩雑になります。
そこで、ここではサンプルとして、共通のマクロを生成して、それを再利用する、という設定を行ってみます。

(1) ここでは一旦、iOS の分岐上にあるボックス全てを削除します。
その後、「Add New Macro」ボタンをクリックします。

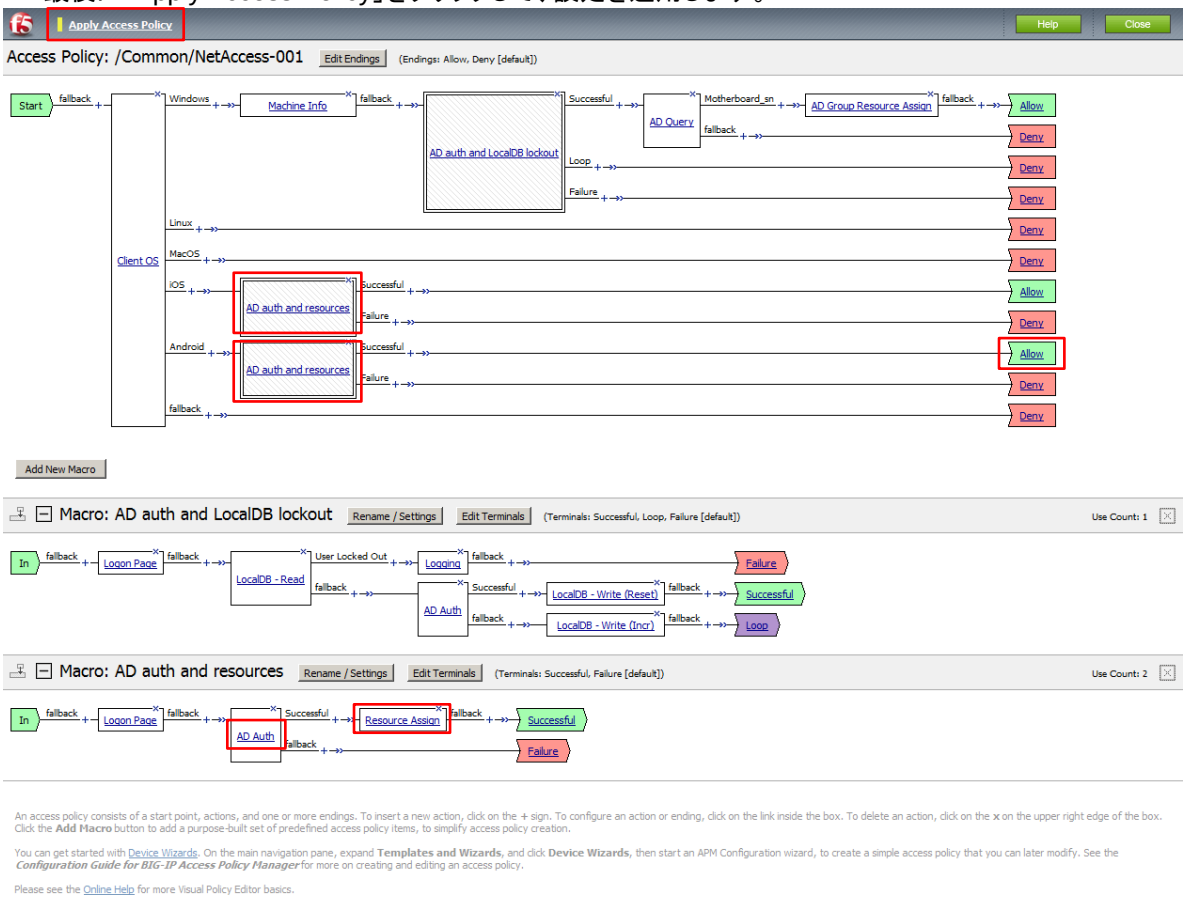


(2) ここでは、サンプルとして、「AD auth and resources」を選択してみました。
「Save」ボタンを押します。



(3) 追加したマクロ：「AD Aurh and resources」の「*」マークの付いたボックス：「AD Auth」と「Resource Assign」をそれぞれ設定します。
その後、iOS と Android の分岐の「+」をクリックして、そのマクロを追加します。

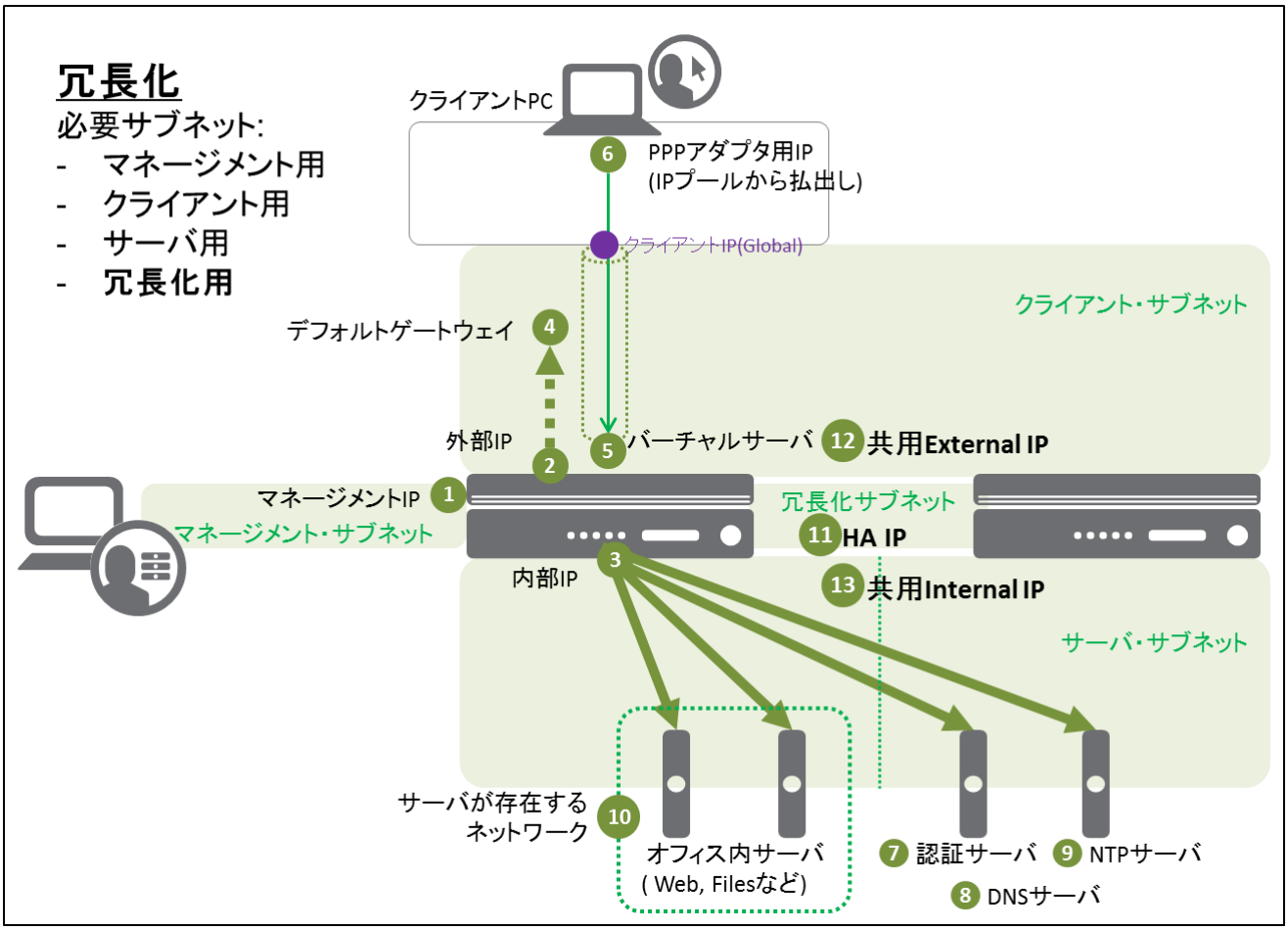
Android は Ending が「Deny」になっているので、「Allow」に変更します。
最後に「Apply Access Policy」をクリックして、設定を適用します。



以上で設定は完了です。

7. 冗長化

7.1. 冗長化イメージ

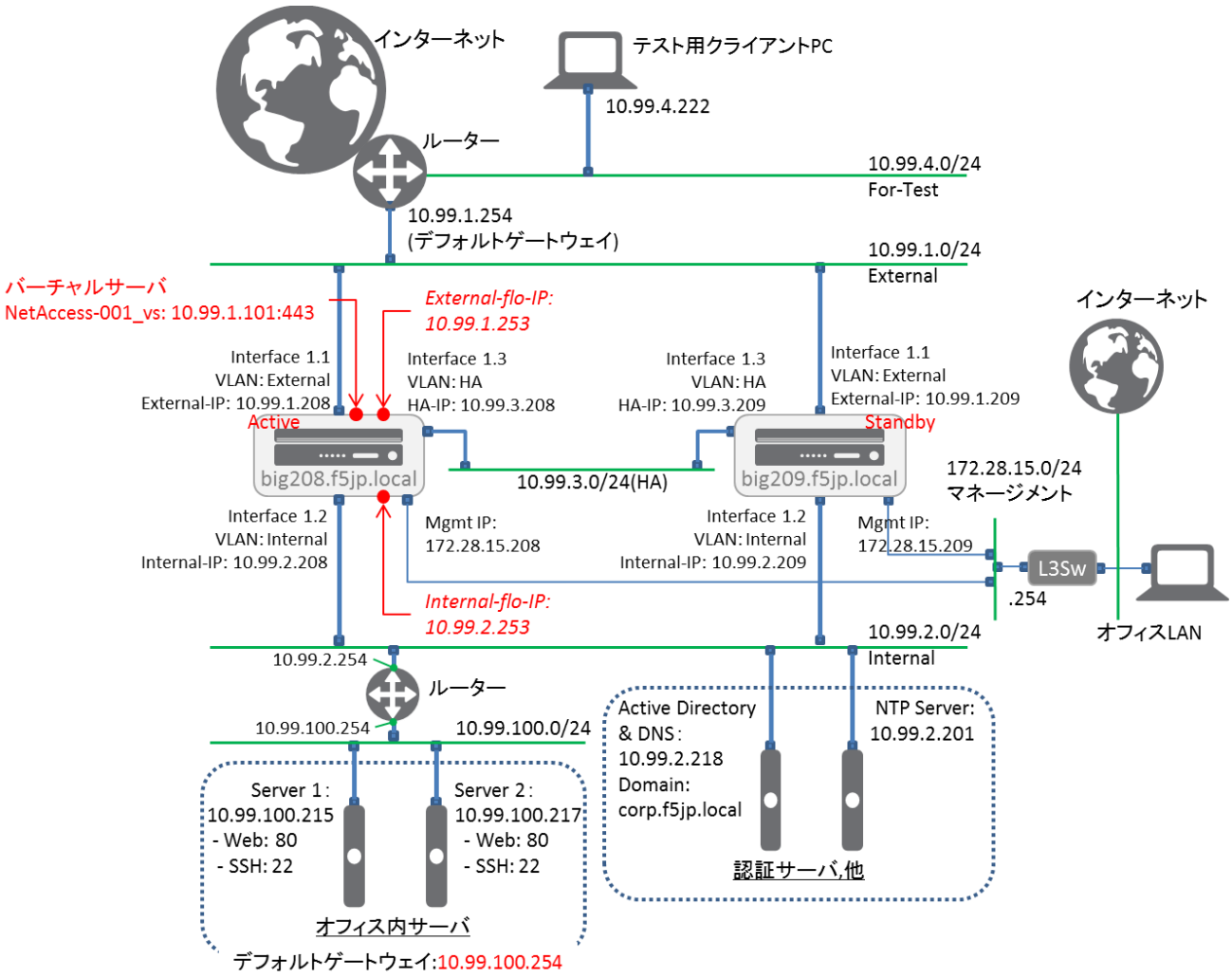


スタンドアローン構成に加え、冗長化用サブネットが必要になります。また、2 台で共有し、どちらかが Active に動作する共用 IP アドレスを設定し、サーバのデフォルト GW として指定します。

	項目	名前	値	名前	値
		1 号機		2 号機	
-	ホスト名	big208.f5jp.local			big209.f5jp.local
①	管理 IP	---	172.28.15.208/24	---	172.28.15.209/24
②	External インタフェース	external	10.99.1.208	external	10.99.1.209/24
③	Internal インタフェース	internal	10.99.2.208	internal	10.99.2.209/24
④	デフォルトゲートウェイ	default-GW	10.99.1.254	⇒	設定同期によりコピー
⑤	バーチャルサーバアドレス	NetAccess-001_vs	10.99.1.101:443	⇒	設定同期によりコピー
⑥	PPP アダプタ用 IP プール	NetAccess-001_lp	10.99.99.11-20	⇒	設定同期によりコピー
⑦	認証サーバ(Active Directory)	NetAccess-001_aaa_srvr	10.99.2.218	⇒	設定同期によりコピー
⑧	DNS サーバ(Active Directory)	---	10.99.2.218	⇒	設定同期によりコピー
⑨	NTP サーバ	---	10.99.2.201	⇒	設定同期によりコピー
⑩	サーバが存在するネットワーク	---	10.99.100/0/24	⇒	設定同期によりコピー
⑪	HA インタフェース	HA	10.99.3.208/24	HA	10.99.3.209/24
⑫	共用 External	External-flo-ip	10.99.1.253	⇒	設定同期によりコピー
⑬	共用 Internal	Internal-flo-ip	10.99.2.253	⇒	設定同期によりコピー

7.2. 冗長化のネットワークサンプル

もう一台 BIG-IP を追加して、L3 構成の冗長化設定を行います。



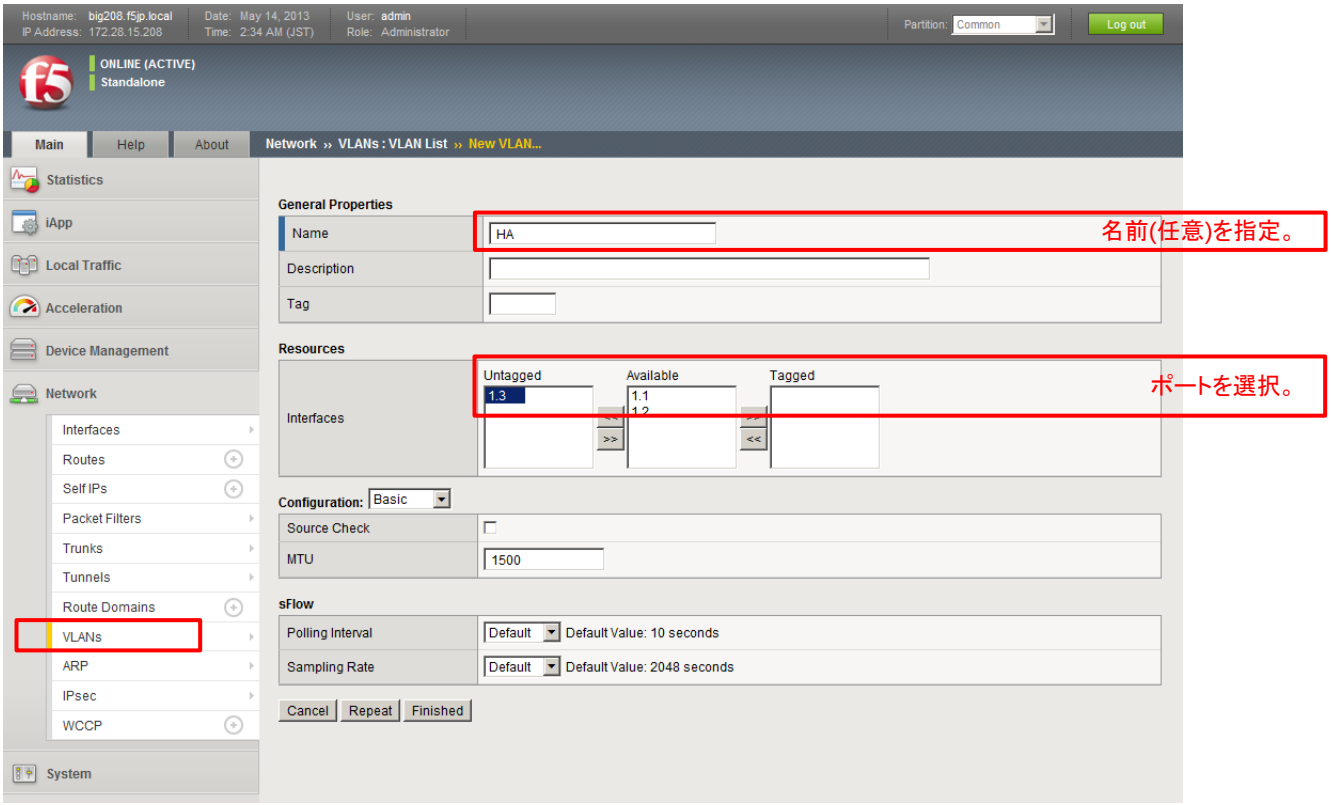
BIG-IP 間の HA (High Availability) VLAN は、冗長化の制御パケットをやり取りする専用の VLAN です。External や Internal VLAN を利用することも可能ですが、HA 専用の VLAN を追加することを推奨しています。

よって、本構成においては、HA VLAN を追加しています。

7.3. Active 機(big208.f5jp.local)の設定

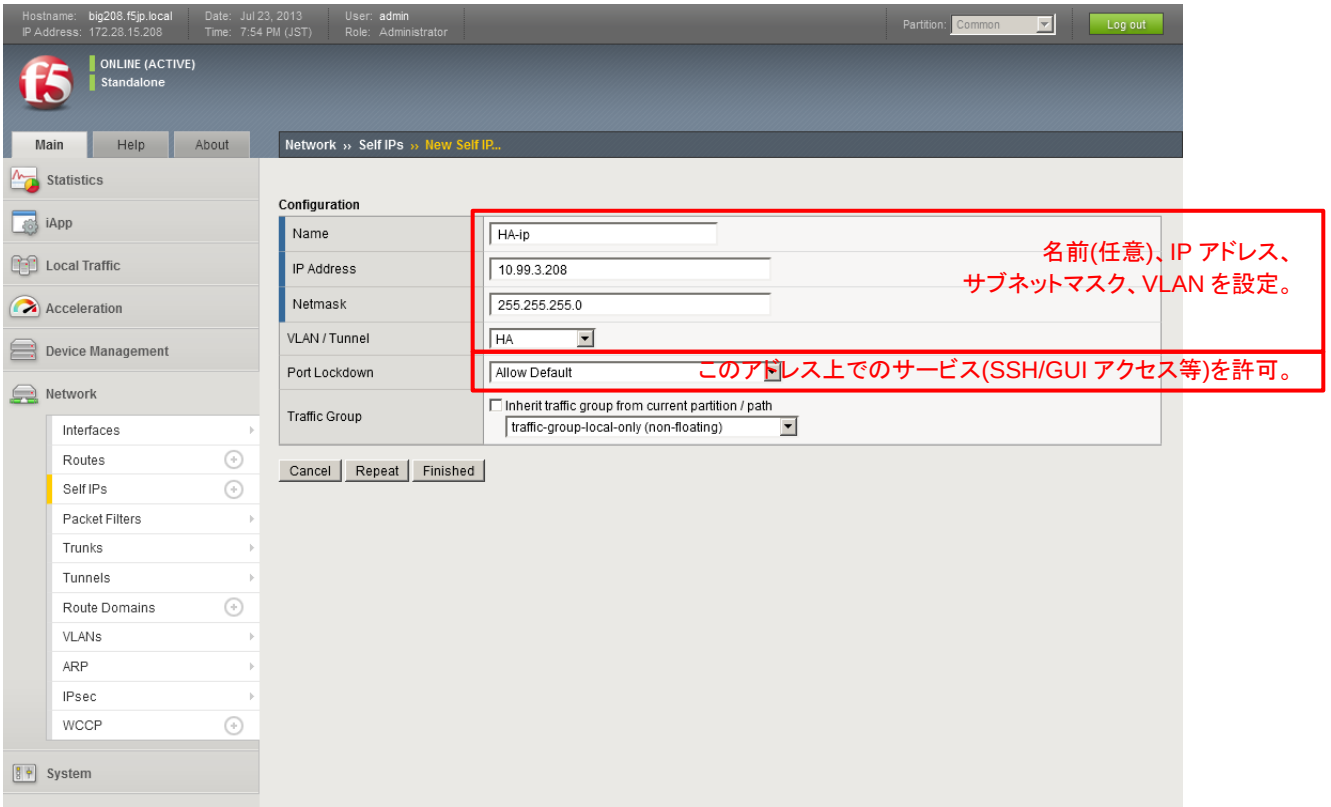
(1) HA VLAN の設定

「Main」メニュー →「Network」→「VLANs」で表示された画面の右上にある「Create」ボタンを押し、HA 用 VLAN を設定します。

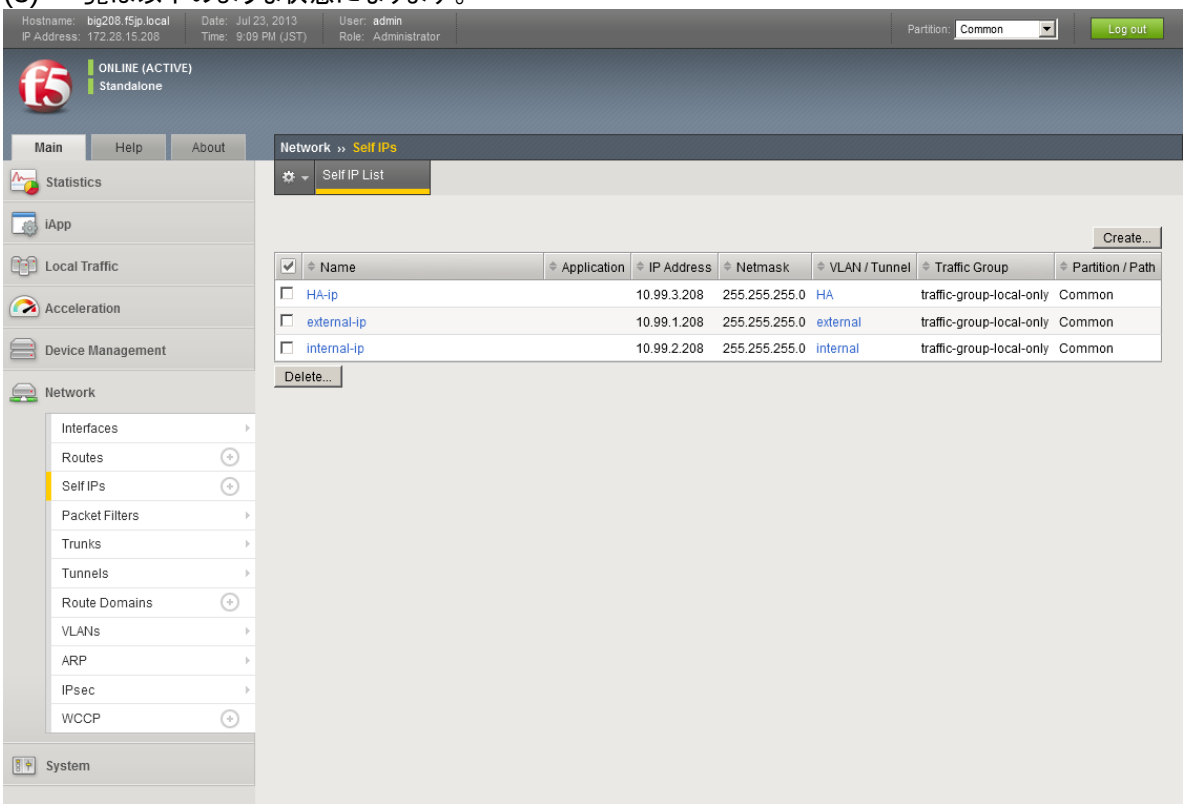


(2) HA VLAN の IP 設定

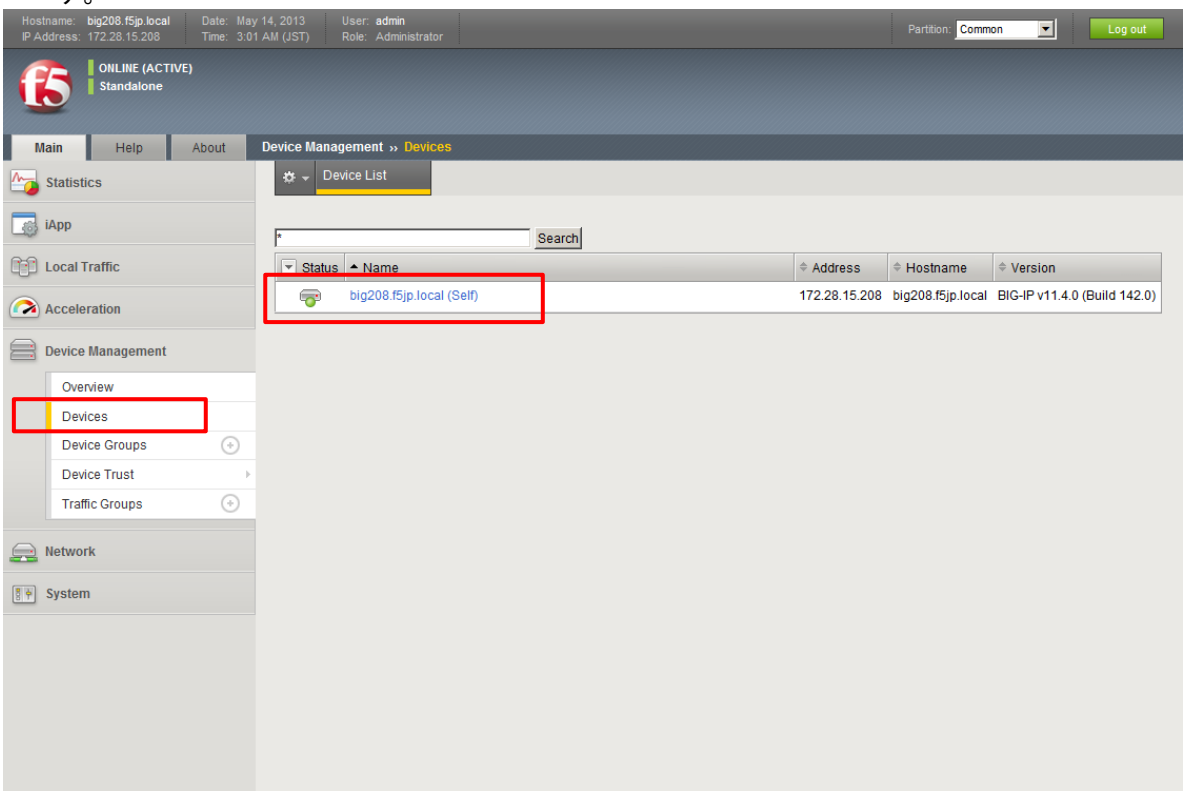
「Main」メニュー →「Network」→「Self IPs」で表示された画面の右上にある「Create」ボタンを押し、HA 用 VLAN の IP を設定します。



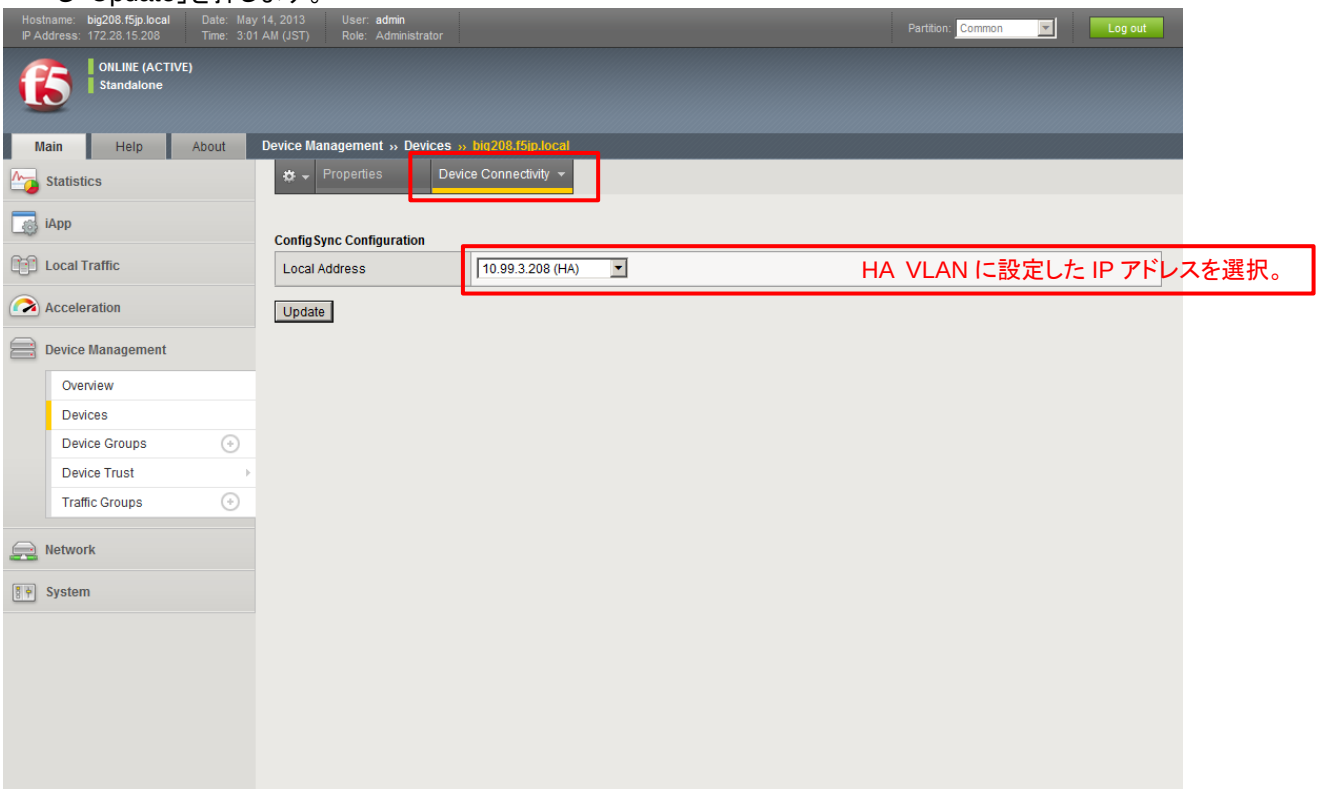
(3) 一覧は以下のような状態になります。



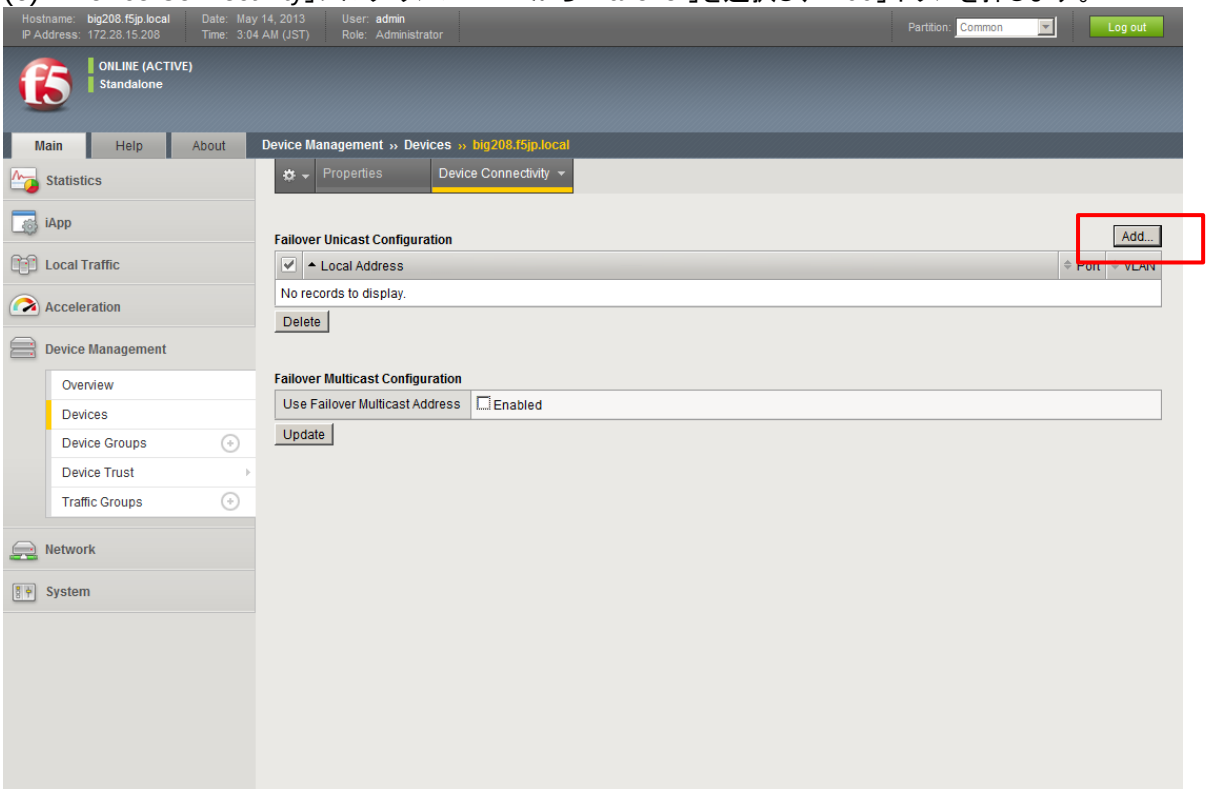
(4) 次に、「Main」メニュー →「Device Management」→「Devices」で、自分自身：big208.f5jp.local(self)を選択します。



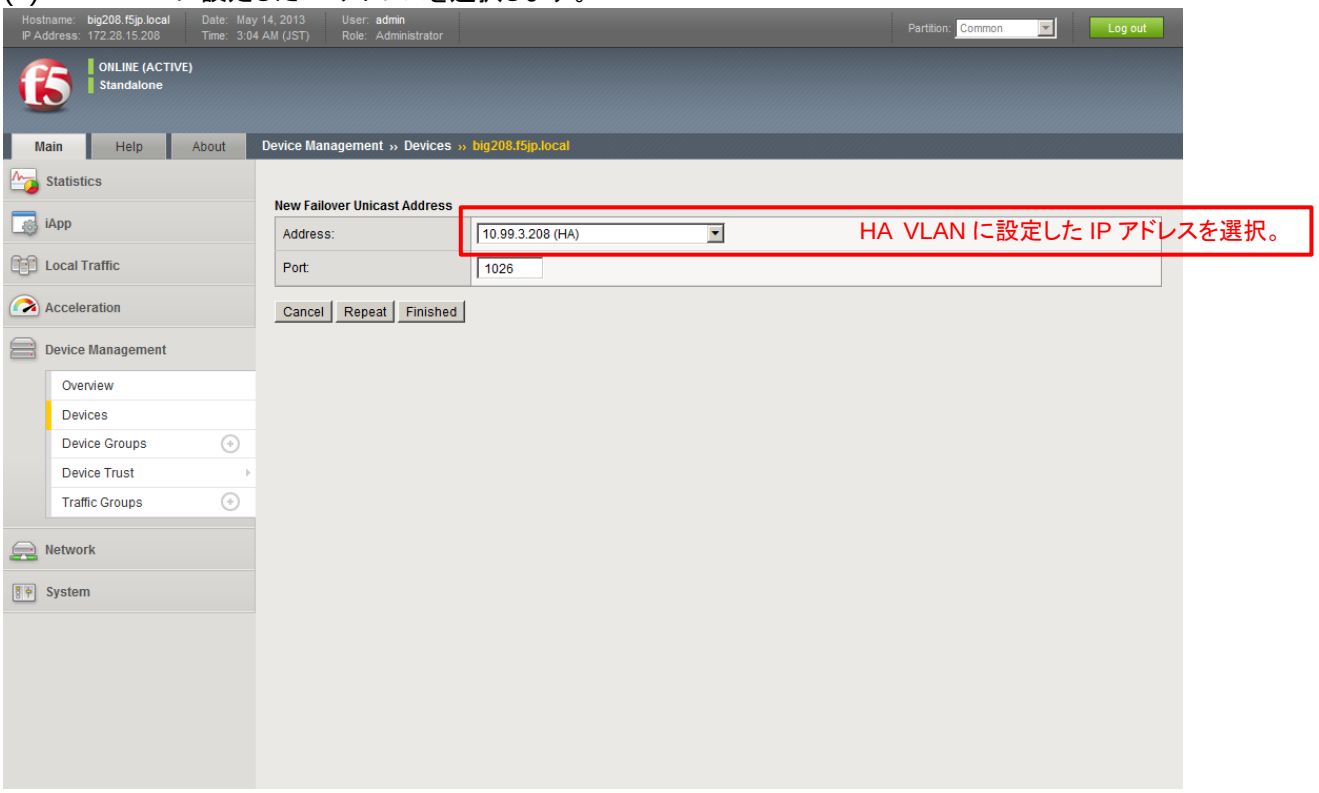
(5) 「Device Connectivity」プルダウンメニューから「ConfigSync」を選択し、HA VLAN に指定した IP アドレスを選択し「Update」を押します。



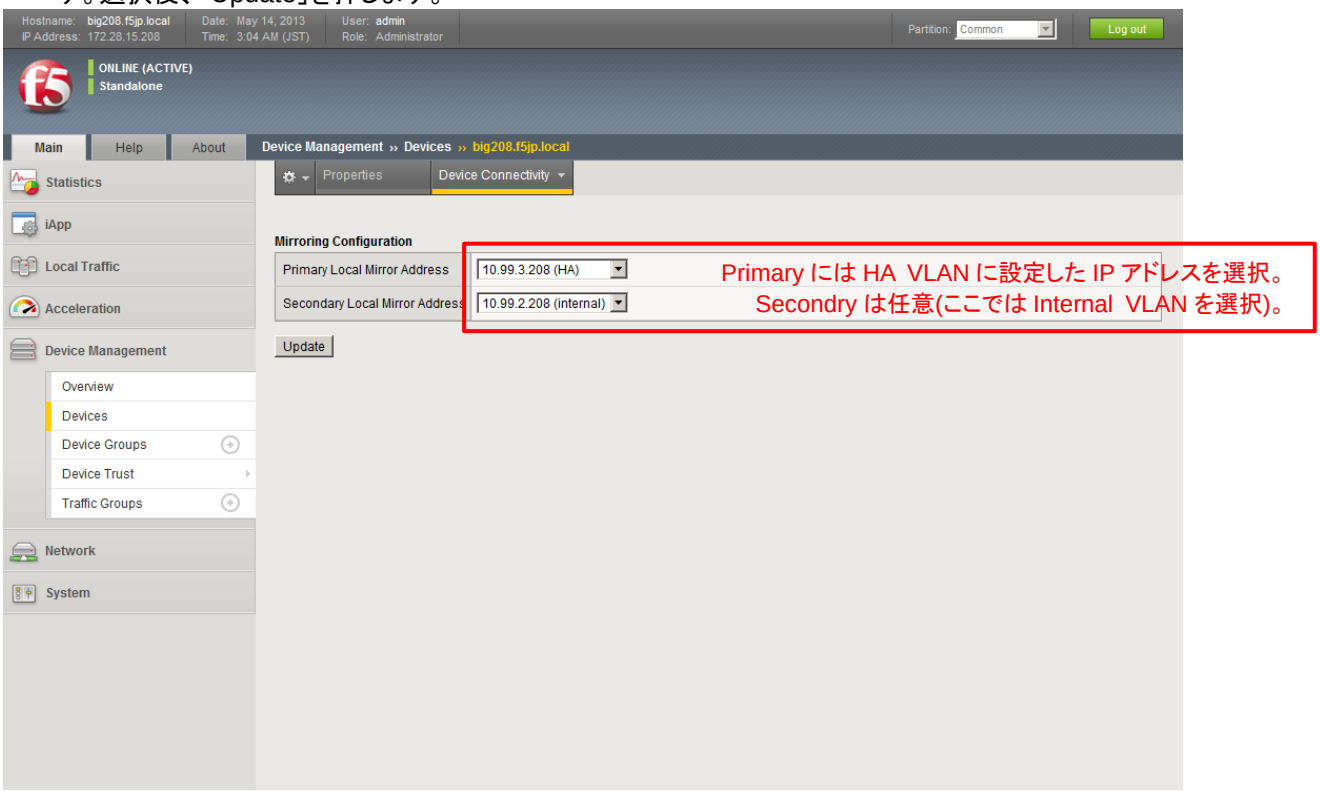
(6) 「Device Connectivity」プルダウンメニューから「Failover」を選択し、「Add」ボタンを押します。



(7) HA VLAN に設定した IP アドレスを選択します。



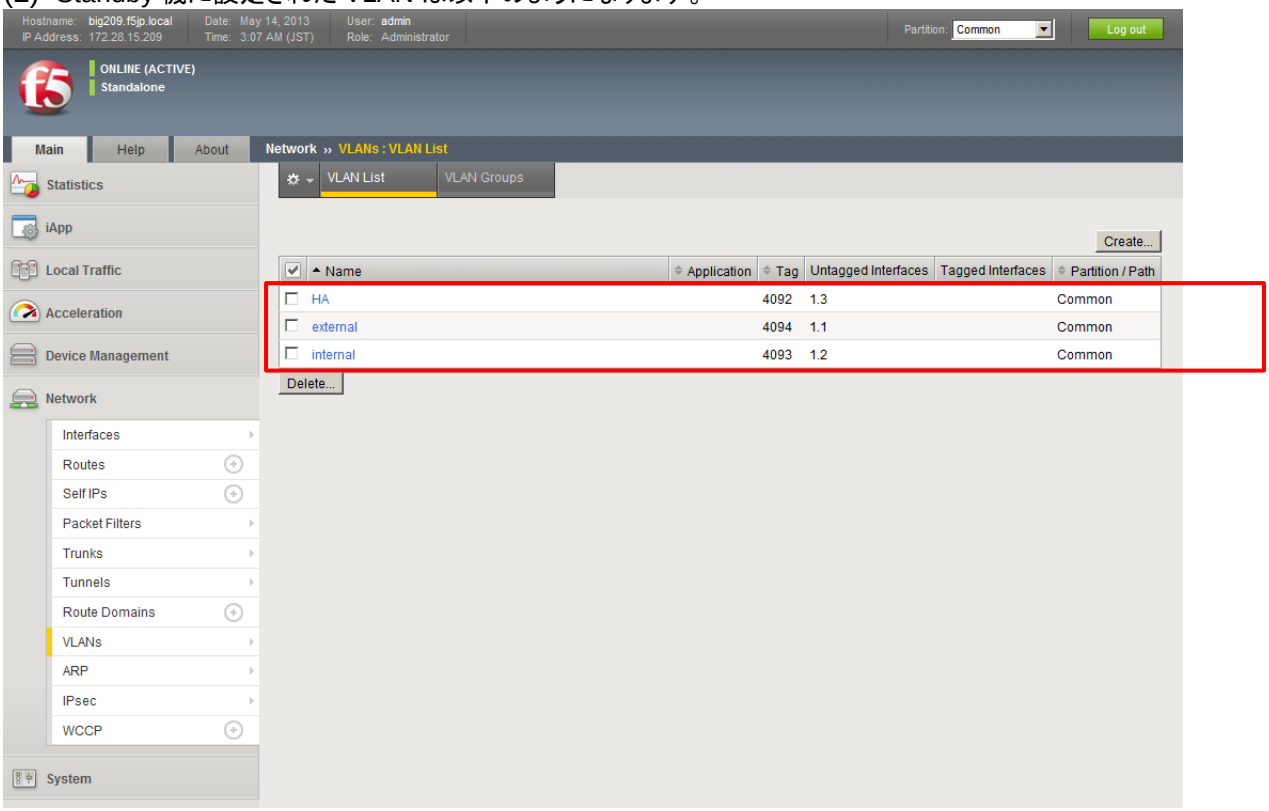
(8) 「Device Connectivity」プルダウンメニューから「Mirroring」を選択し、HA VLAN に指定した IP アドレスをプライマリに指定します。任意ですが、ここでは Secondary として、Internal VLAN に指定した IP アドレスを選択しています。選択後、「Update」を押します。



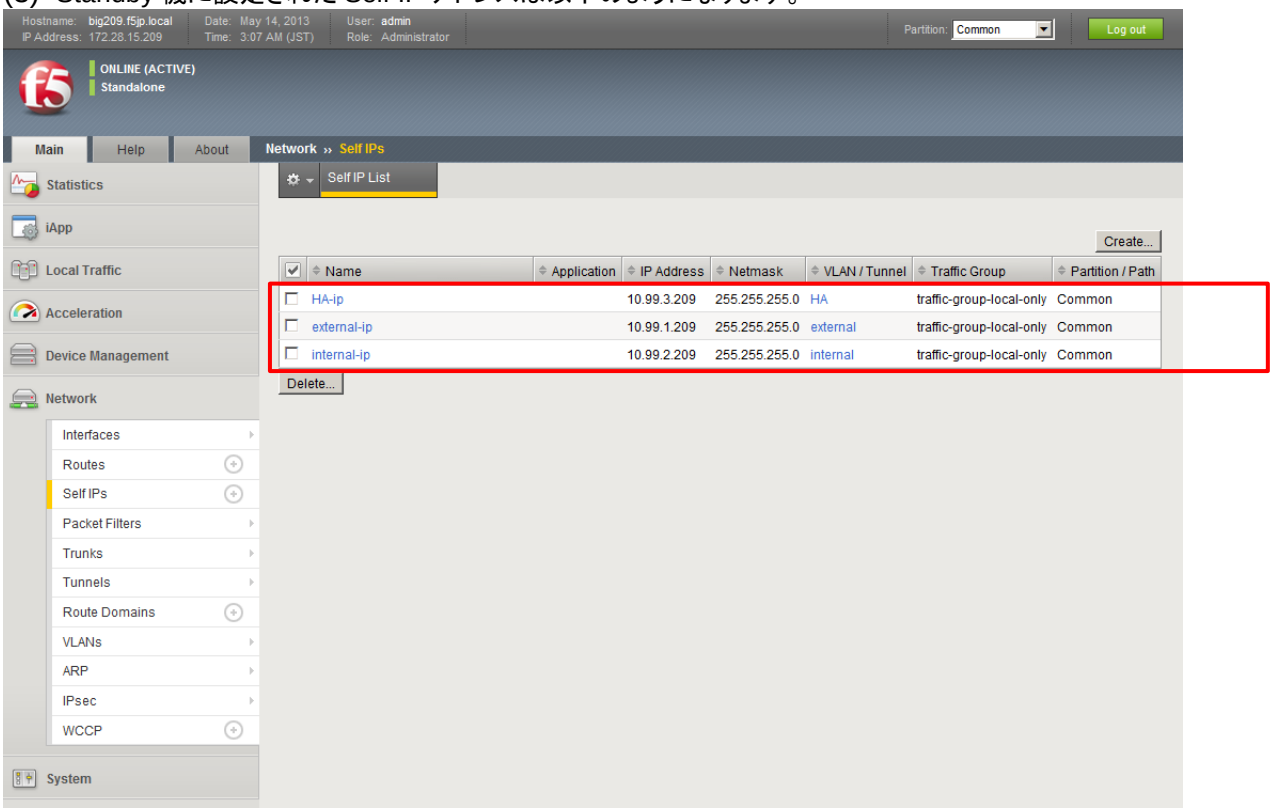
7.4. Standby 機(big209.f5jp.local)の設定

(1) Active 機での VLAN，Self IP，Devices の設定と同様の設定を Standby 機に対しても行います。

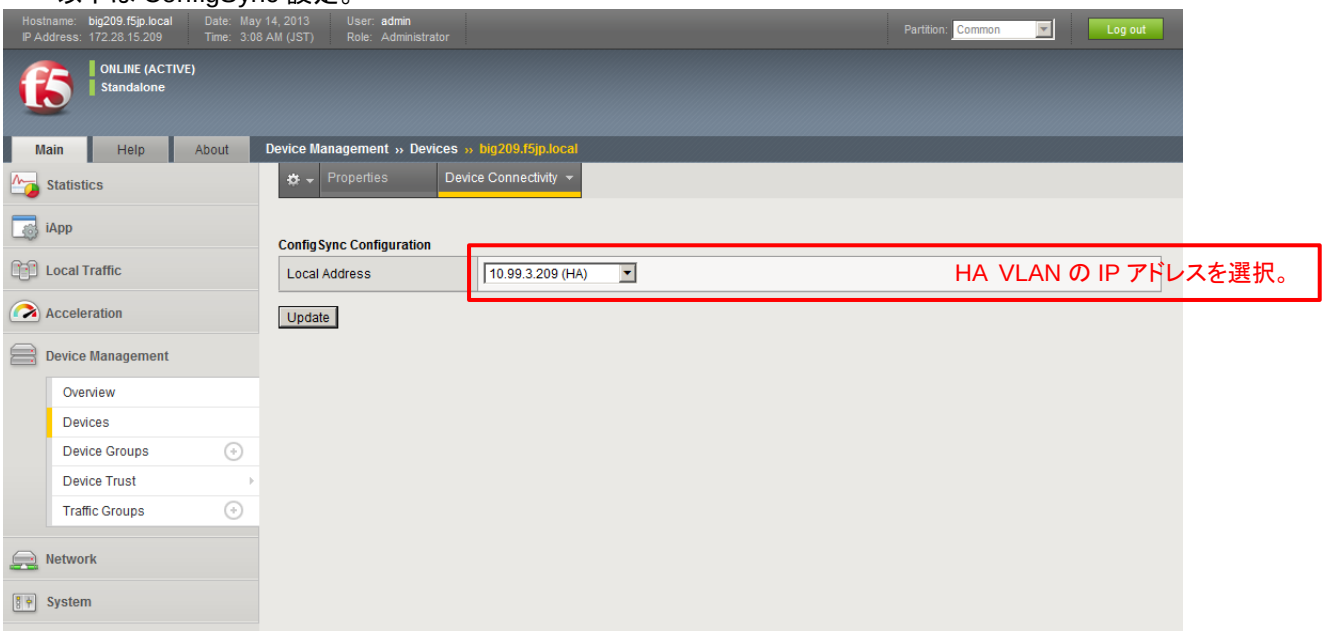
(2) Standby 機に設定された VLAN は以下のようになります。



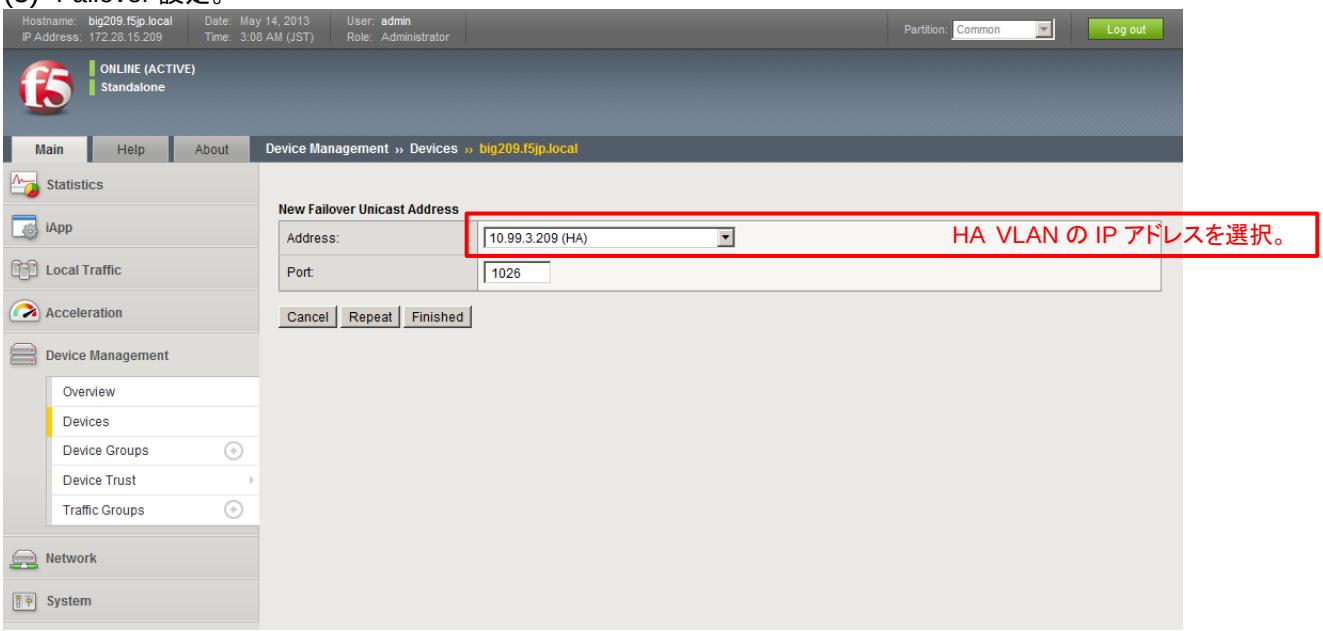
(3) Standby 機に設定された Self IP アドレスは以下のようになります。



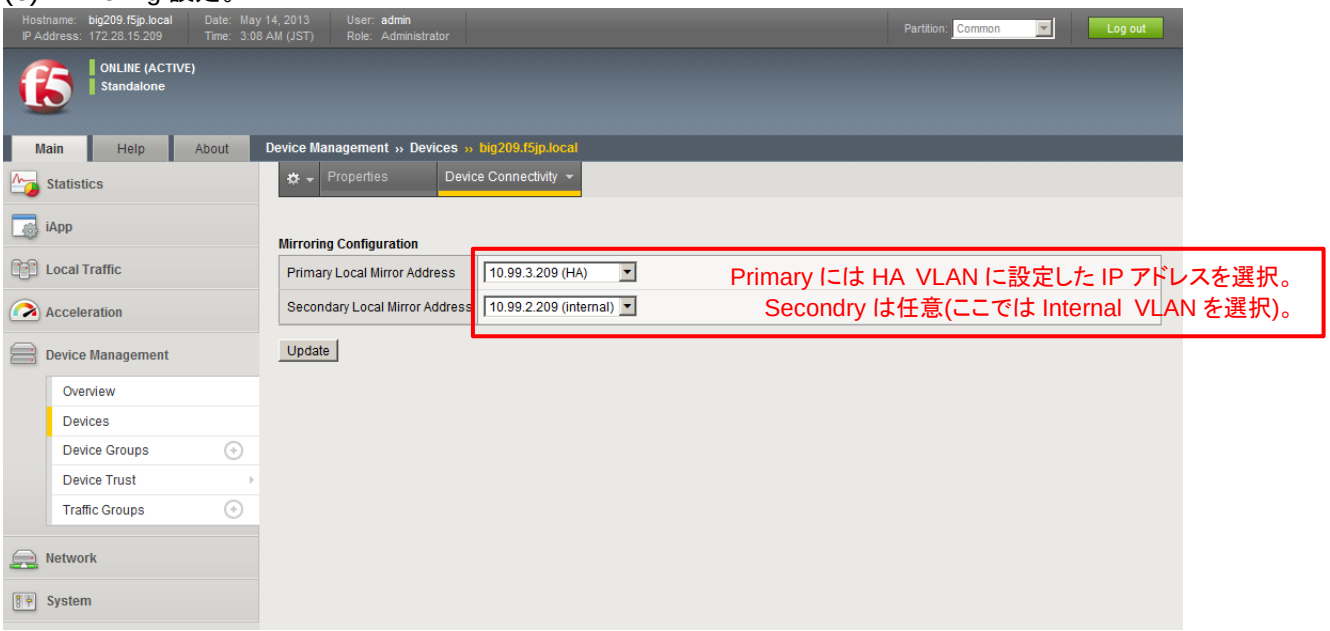
(4) 次に、「Main」メニュー →「Device Management」→「Devices」で、自分自身：big209.f5jp.local(self)を選択し、Active 機同様に、Device Connectivity の設定を行います。
以下は ConfigSync 設定。



(5) Failover 設定。



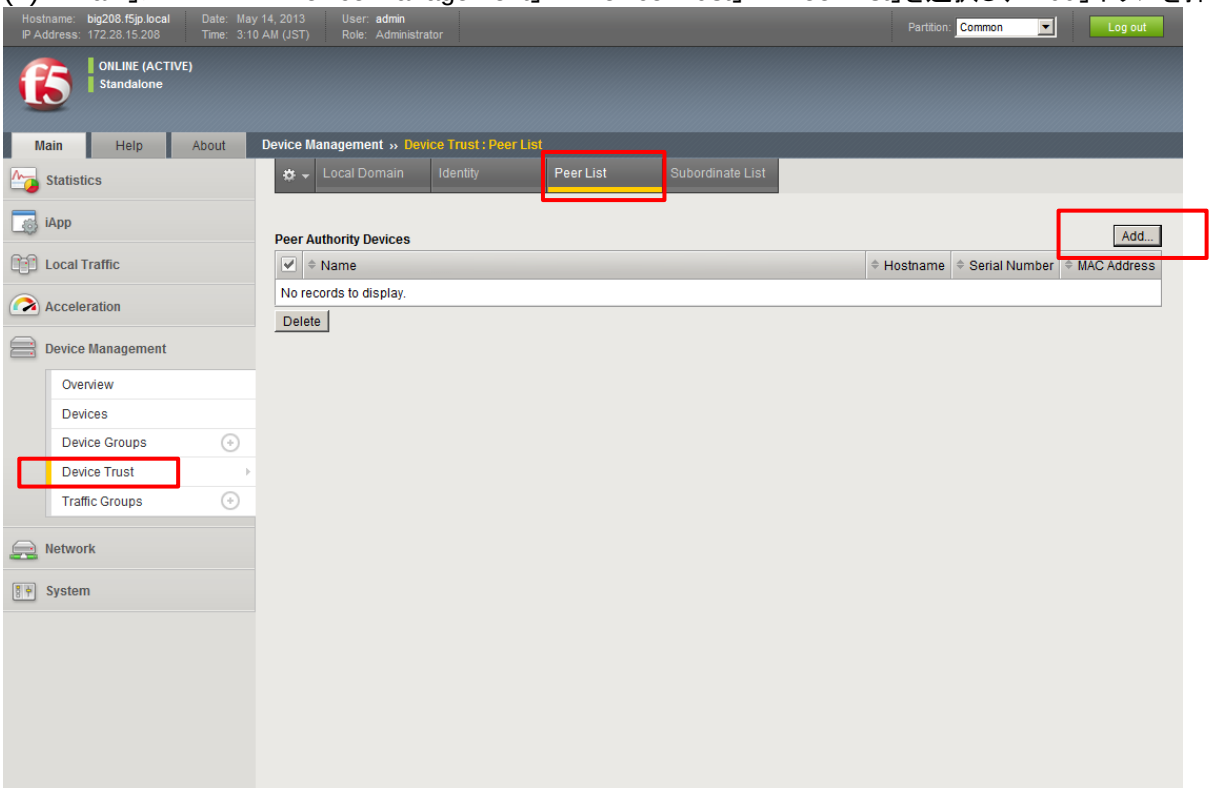
(6) Mirroring 設定。



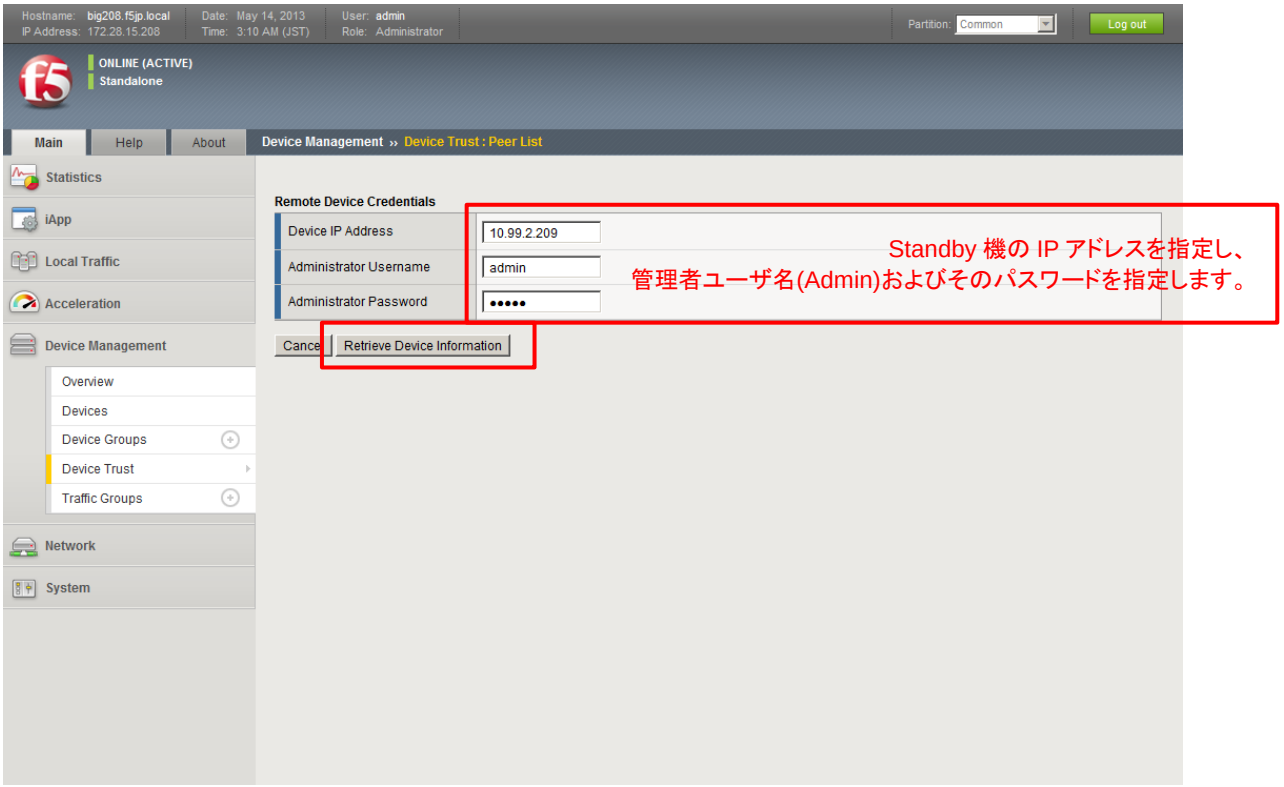
7.5. デバイストラスト設定 (Active 機：big208.f5jp.local 側から実施)

デバイストラスト設定にて、冗長化する機器間で信頼関係を結びます。
以降は、Active 機：big208.f5jp.local からのみ、設定します。

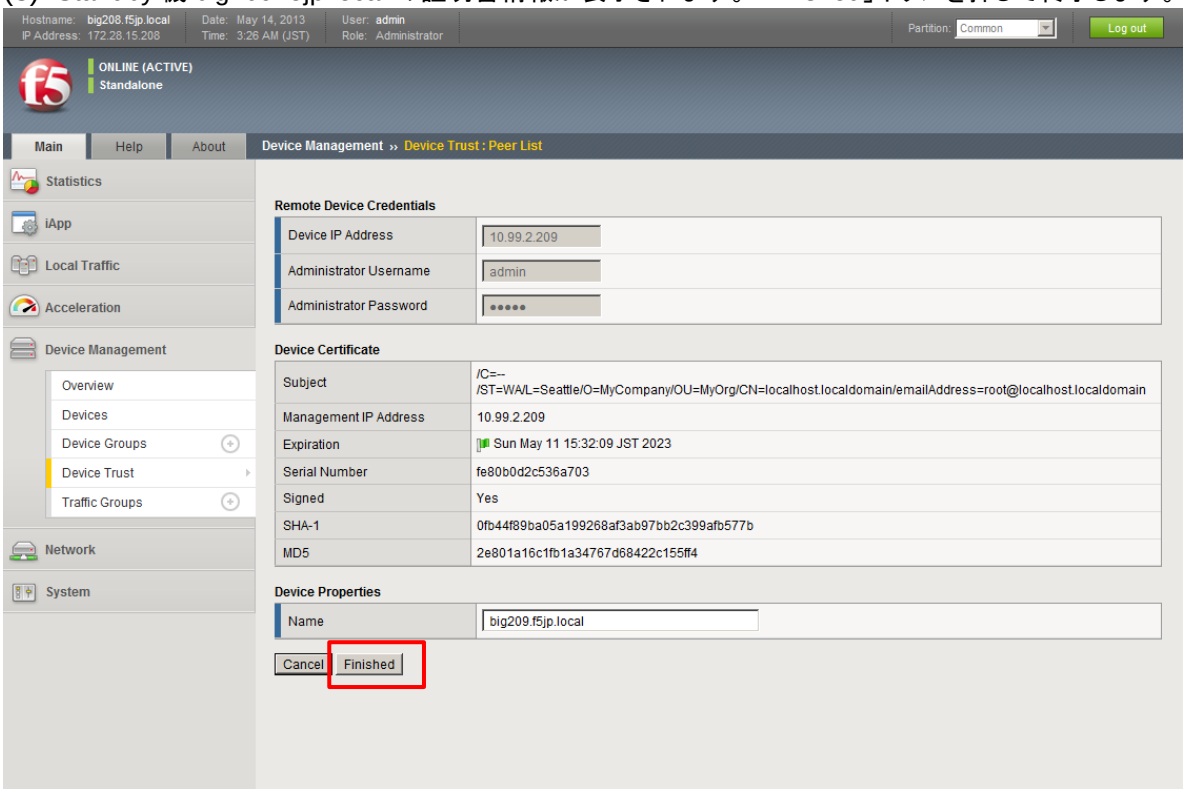
(1) 「Main」メニュー →「Device Management」→「Device Trust」→「Peer List」を選択し、「Add」ボタンを押します。



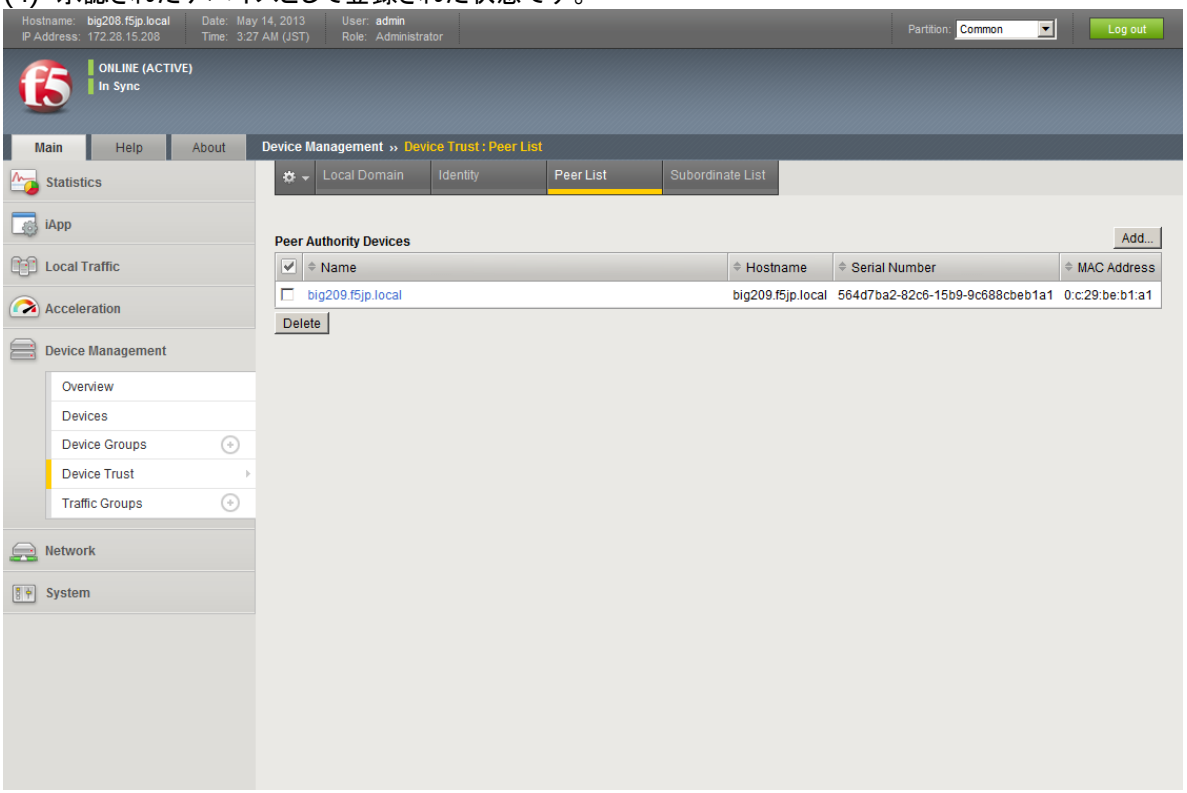
(2) Standby 機：big209.f5jp.local の IP アドレスと管理者 ID(Admin)とパスワードを指定します。「Retrieve Device Information」ボタンを押します。



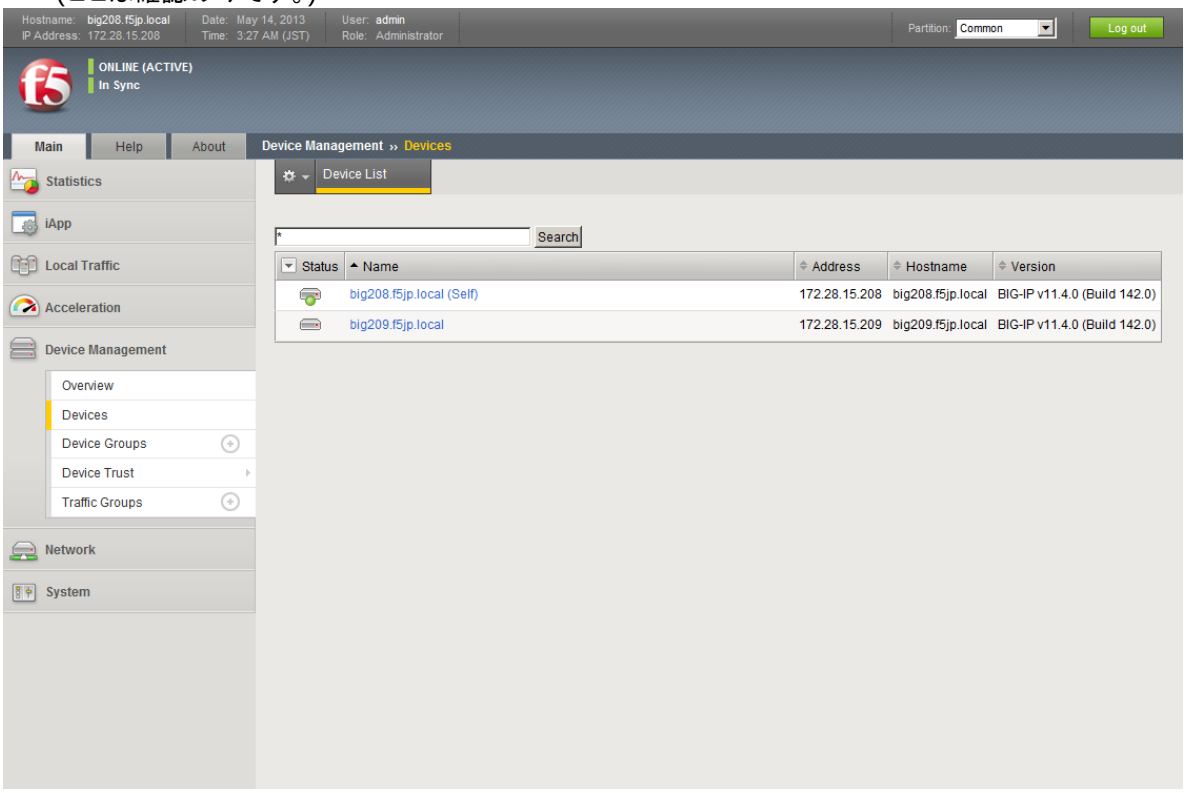
(3) Standby 機 big209.f5jp.local の証明書情報が表示されます。「Finished」ボタンを押して終了します。



(4) 承認されたデバイスとして登録された状態です。



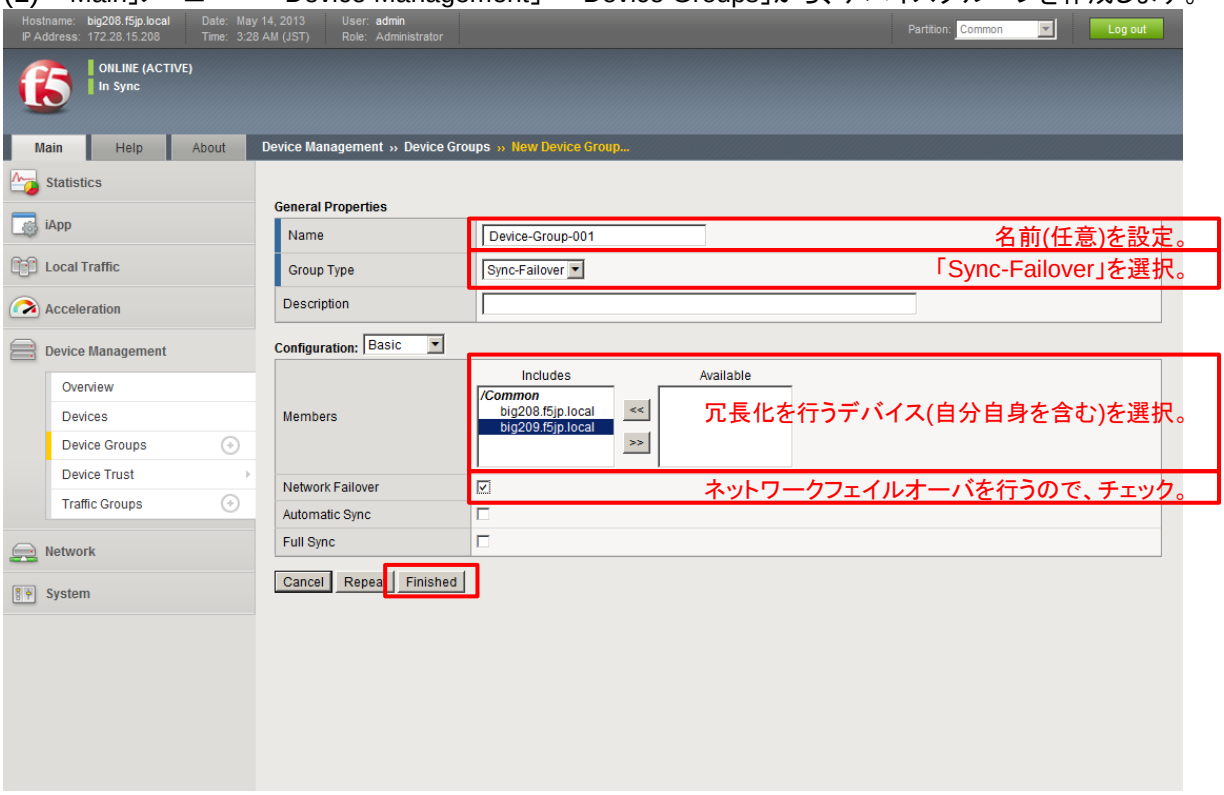
(5) 「Device Management」→「Devices」で見ると、(self)に加え、Standby 機：big209.f5jp.local も表示されます。
(ここは確認のみです。)



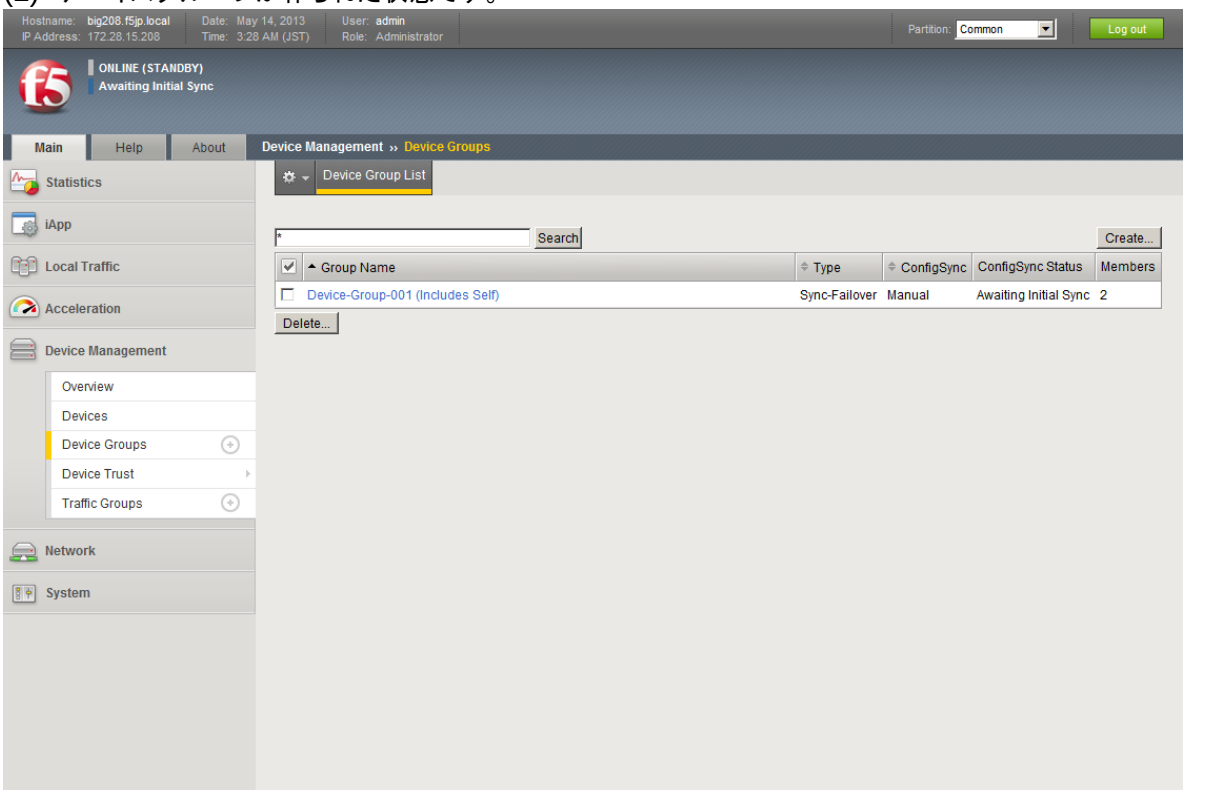
7.6. デバイスグループの設定

デバイスグループは、デバイストラストで信頼関係を結んだ機器の間で、どの機器間で冗長化を行うかの指定です。
デバイストラストは BIG-IP×3 台以上で構成することも可能で、例えば、(1)と(2)で冗長化を行い、(2)と(3)はコンフィグ同期のみ行う、という組合せが可能となっています。この組み合わせをデバイスグループで指定します。
2 台で冗長化を行う場合はデバイスグループの組み方をあまり意識する必要はありませんが、設定は必要です。

(1) 「Main」メニュー →「Device Management」→「Device Groups」から、デバイスグループを作成します。



(2) デバイスグループが作られた状態です。

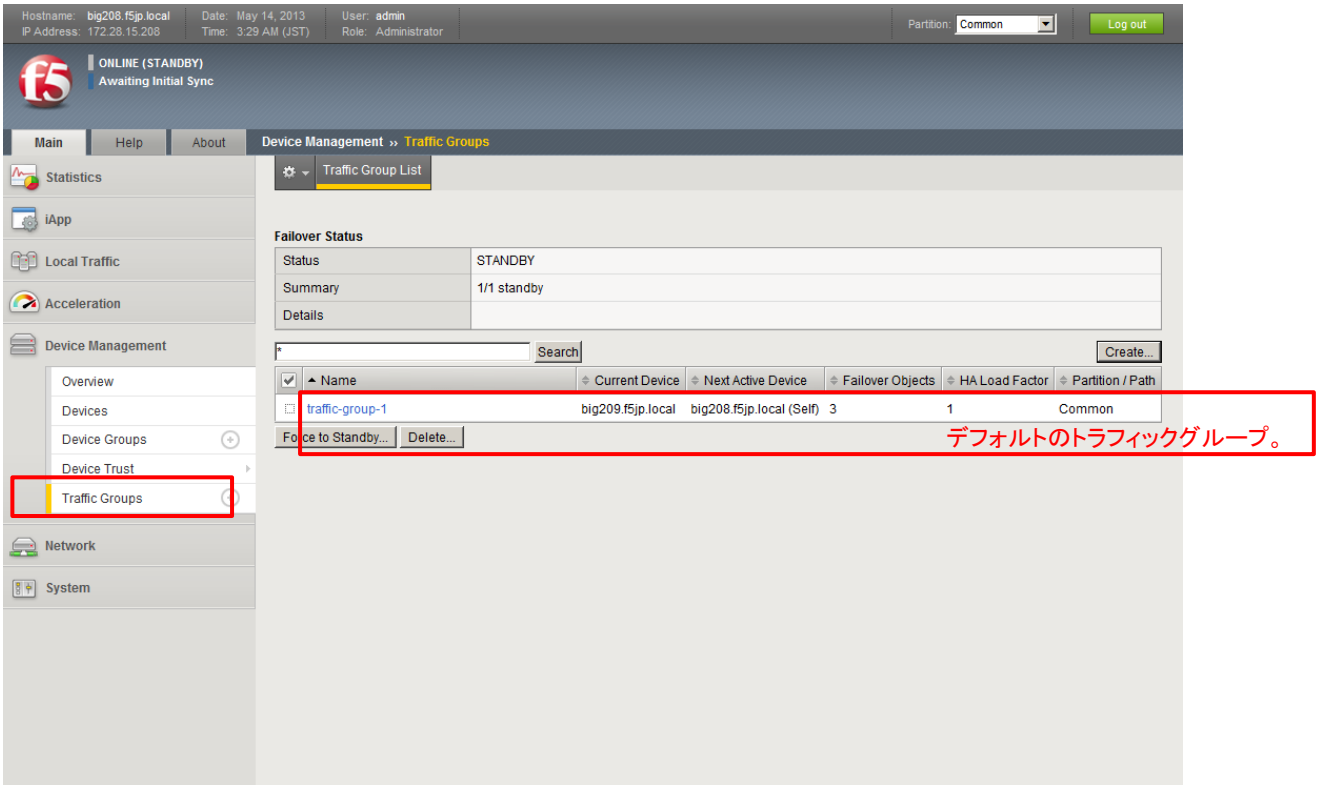


7.7. トラフィックグループの設定

トラフィックグループは、デバイスグループ内で移動するオブジェクトの集合です。
主に、Virtual Server と共用 IP(Floating IP)がトラフィックグループのオブジェクトです。

「Main」メニュー →「Device Management」→「Traffic Groups」を確認します。

(1) デフォルトで、「Traffic-group-1」という名前のトラフィックグループが存在しています。
以降、この Traffic-group-1 に対して、Floating IP および Virtual Server を割当てていきます。

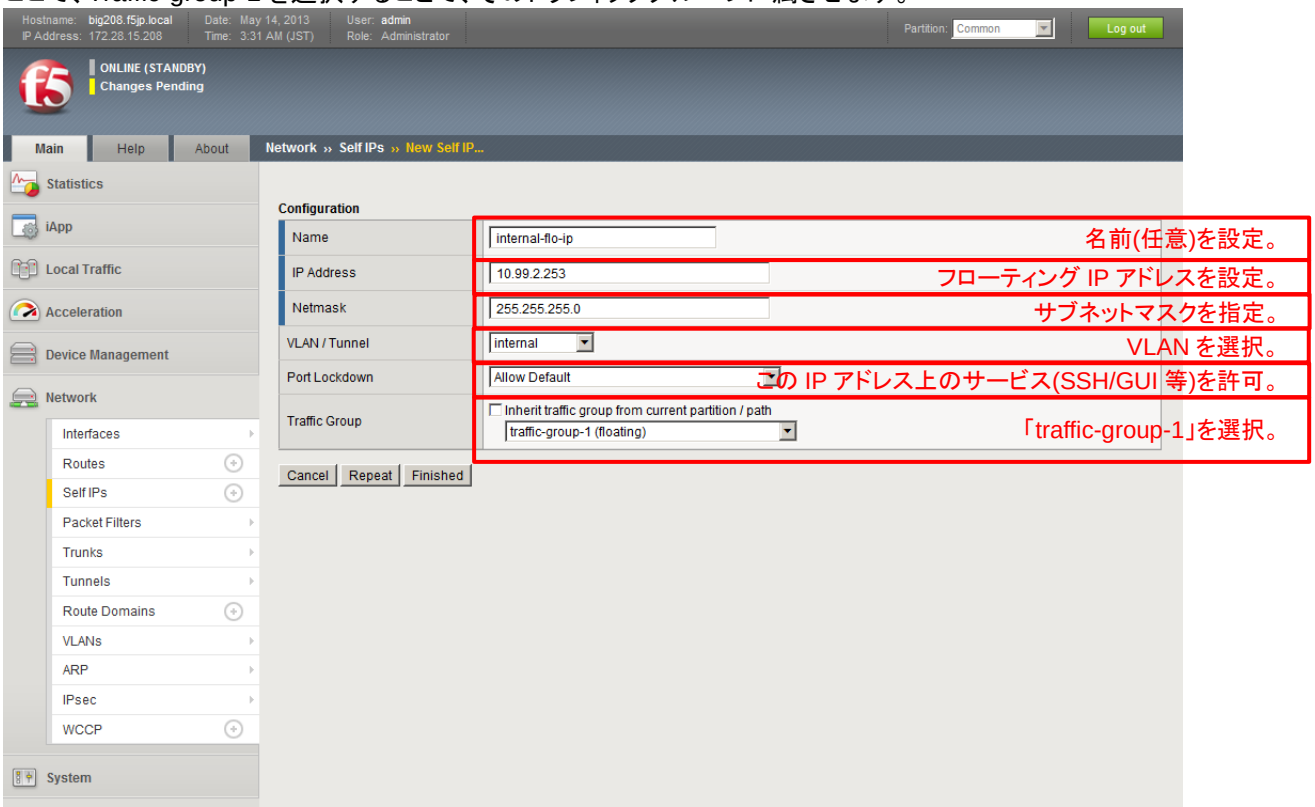


(2) Internal VLAN 側の共用 IP(Floating IP)を追加設定します。

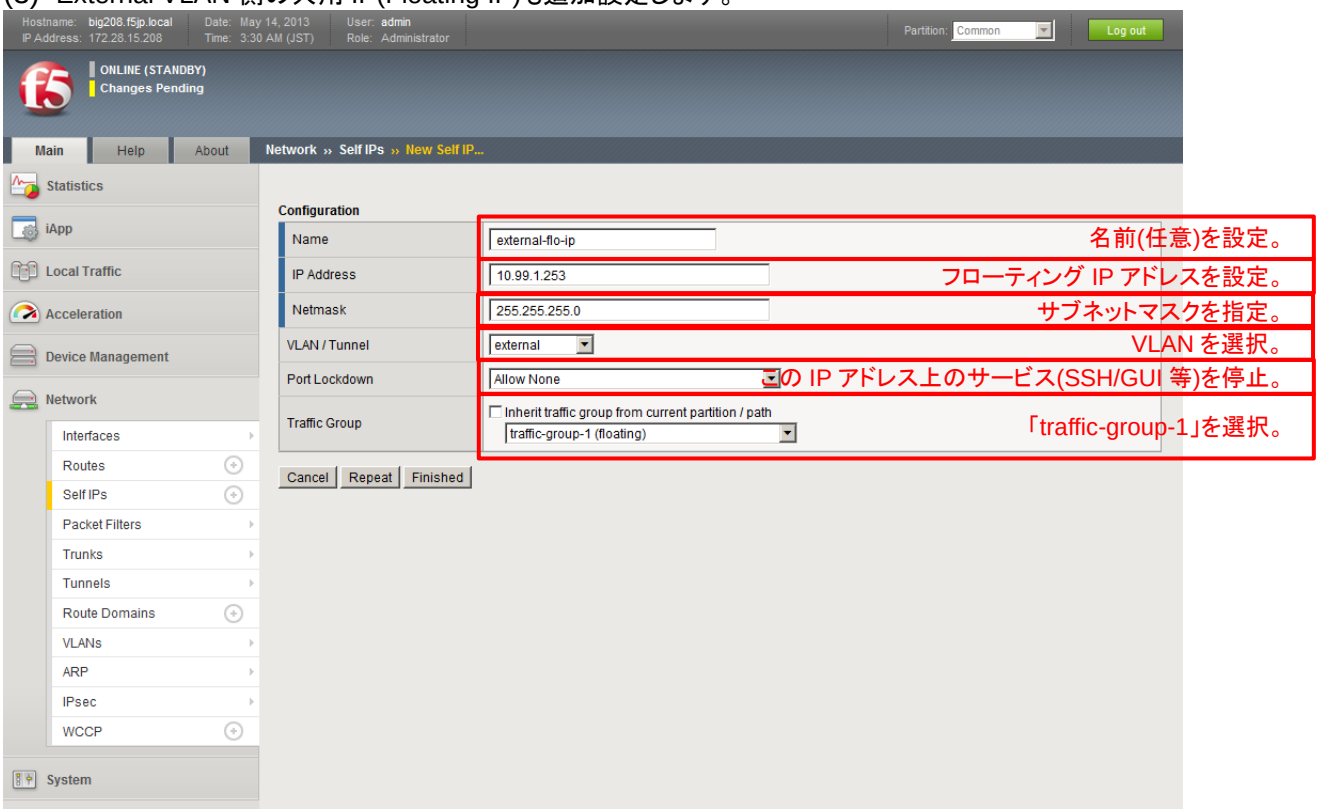
Floating IP は、Active 機ダウン時に Standby 機が引き継ぐ、自身に設定された IP アドレス(Self IP)を指します。
実サーバは、この IP アドレスをデフォルトゲートウェイに指定することで、Active/Standby の切り替わり発生時にも、即座に通信を再開できます。

「Main」メニュー →「Network」→「Self IPs」から設定します。

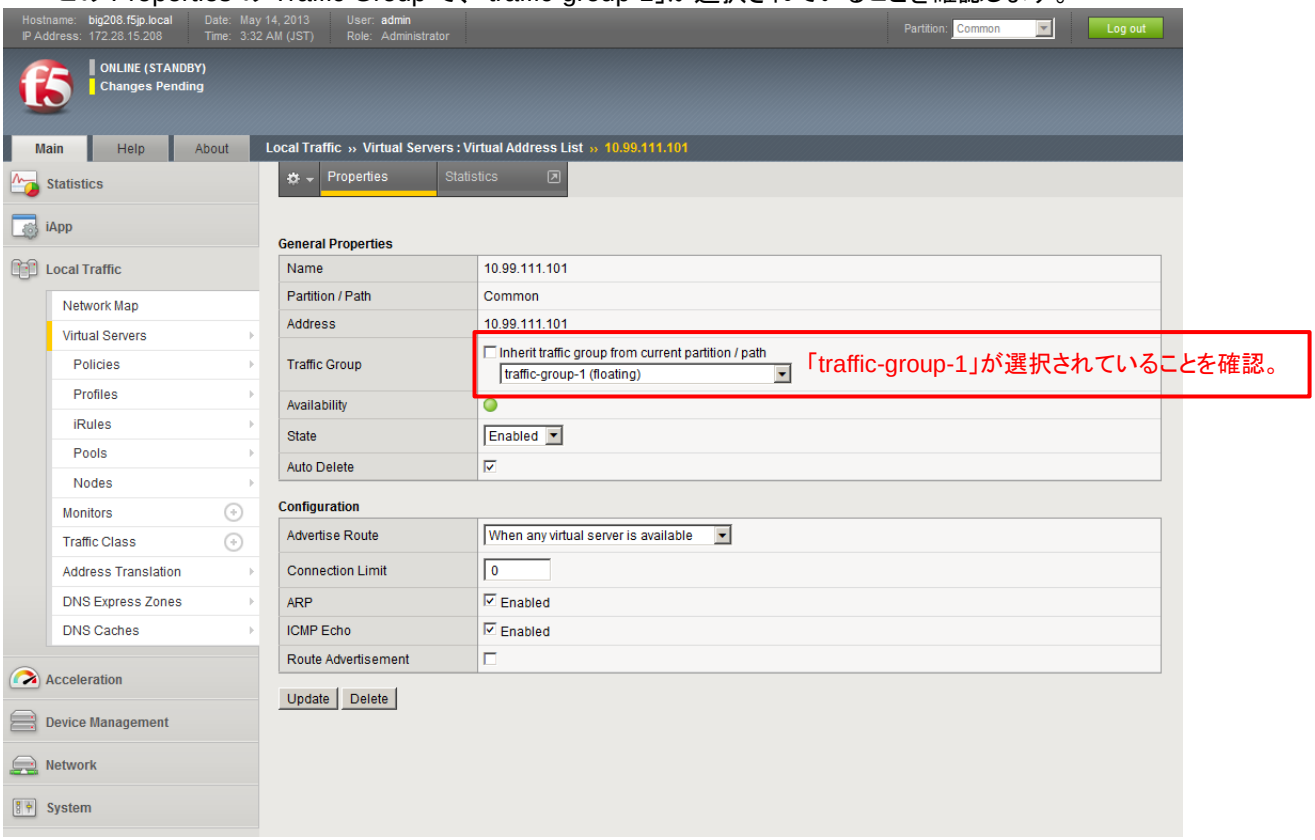
ここで、Traffic-group-1 を選択することで、そのトラフィックグループに属させます。



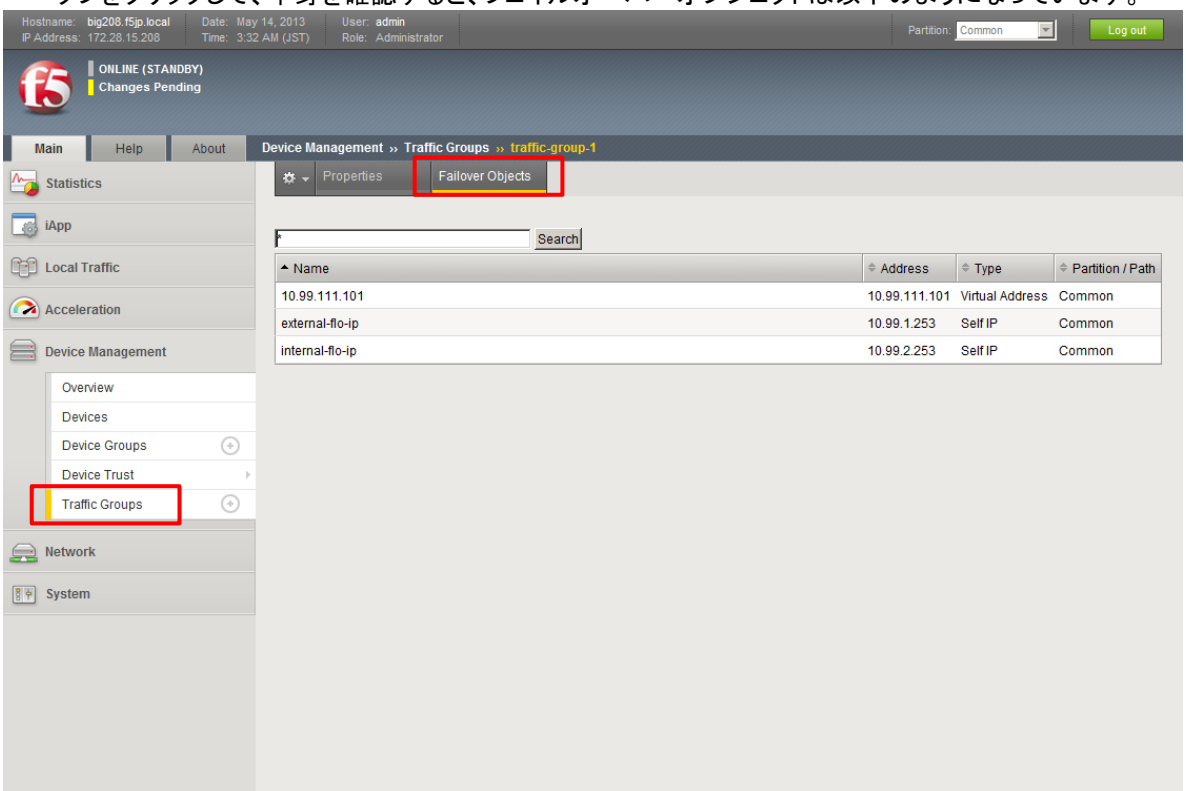
(3) External VLAN 側の共用 IP(Floating IP)も追加設定します。



(4) 「Main」メニュー→「Local Traffic」→「Virtual Servers」→「Virtual Address List」を選択します。
この Properties の Traffic Group で、「traffic-group-1」が選択されていることを確認します。



(5) 「Main」メニュー→「Device Management」→「Traffic Groups」の Traffic-group-1 をクリック→「Failover Objects」タブをクリックして、中身を確認すると、フェイルオーバーオブジェクトは以下のようになっています。

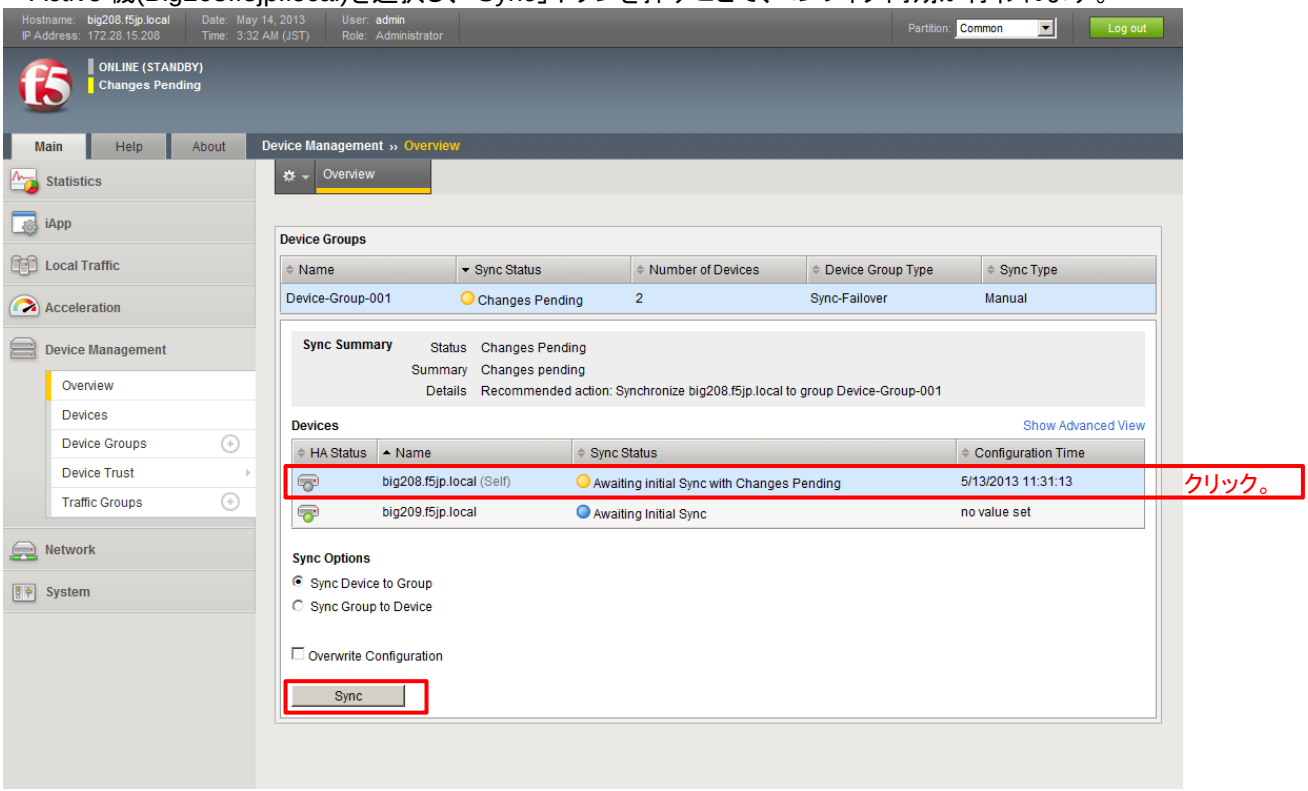


7.8. ConfigSync

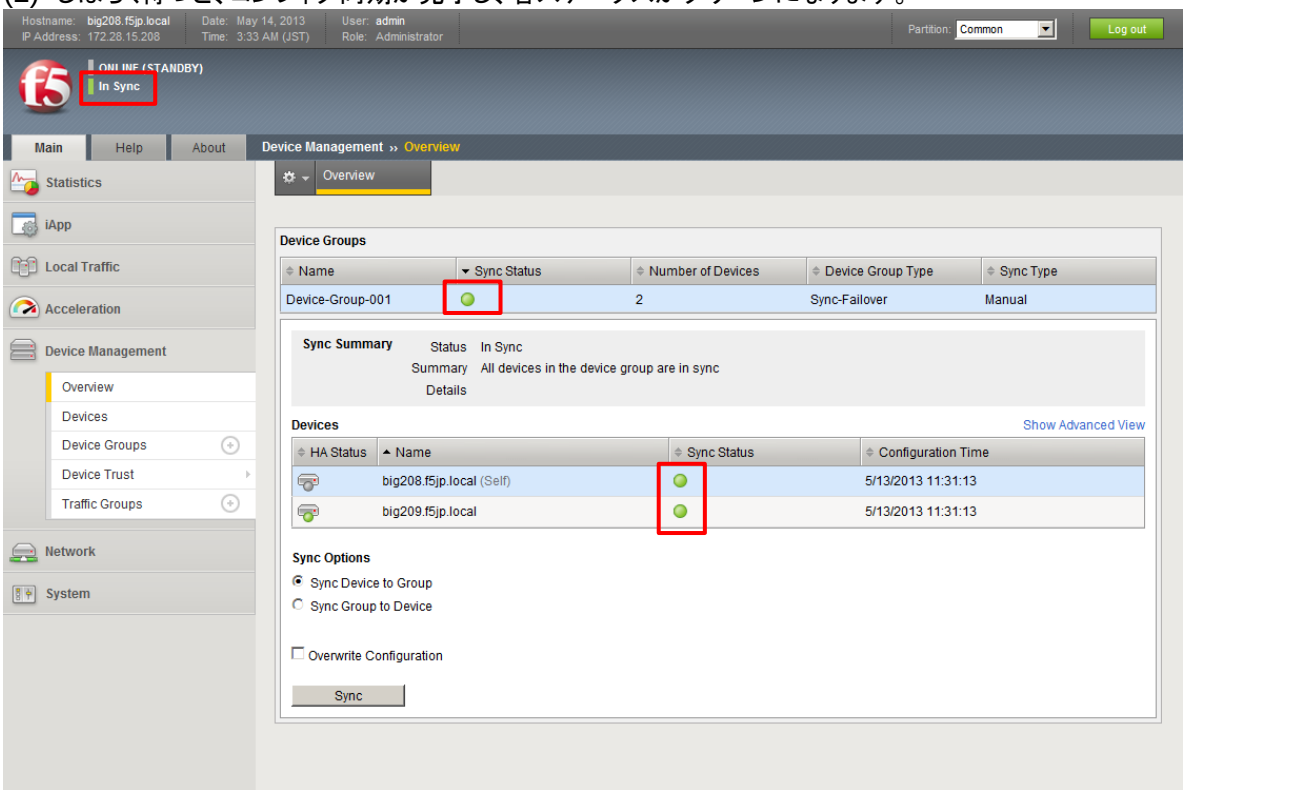
Active 機：big208.f5jp.local にのみに行った設定を、Standby 機：big209.f5jp.local に同期するために、ConfigSync を行します。

(1) 「Main」メニュー→「Device Management」→「Overview」を選択します。

Active 機(Big208.f5jp.local)を選択し、「Sync」ボタンを押すことで、コンフィグ同期が行われます。



(2) しばらく待つと、コンフィグ同期が完了し、各ステータスがグリーンになります。

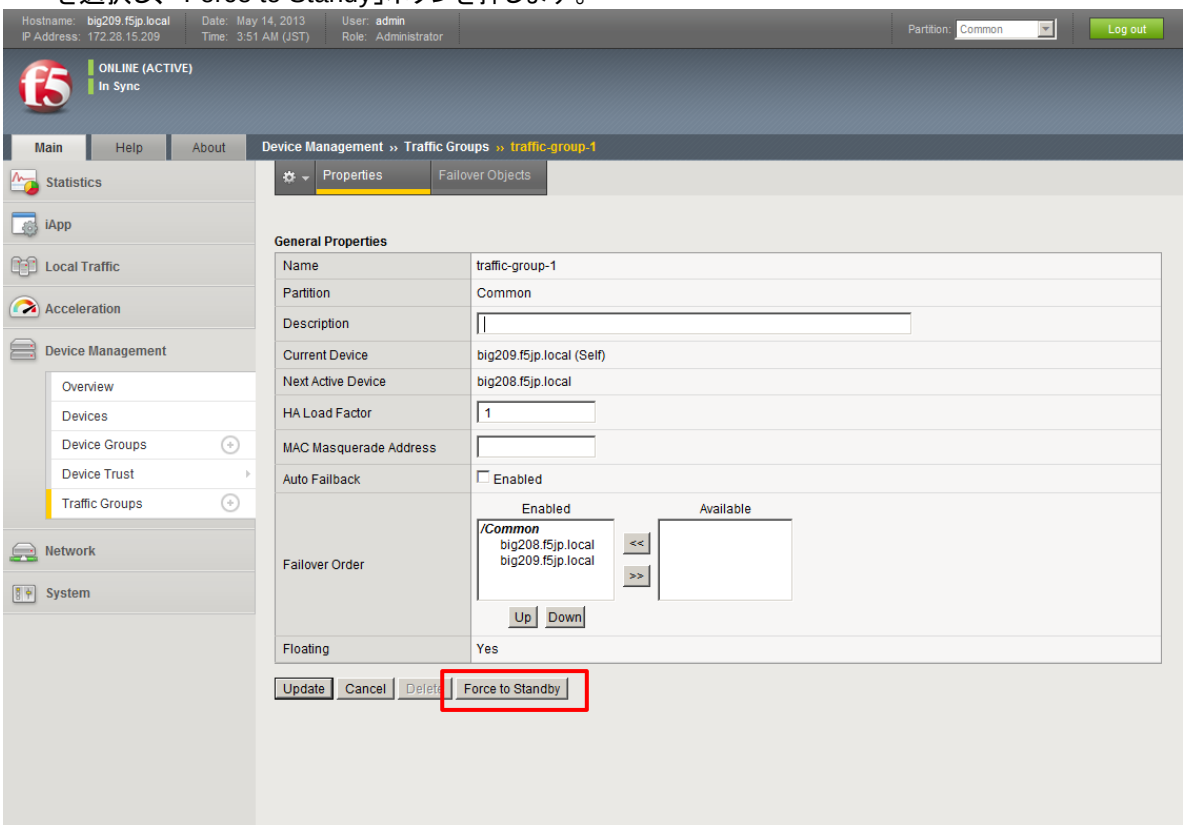


7.9. Traffic-group-1 の優先度設定

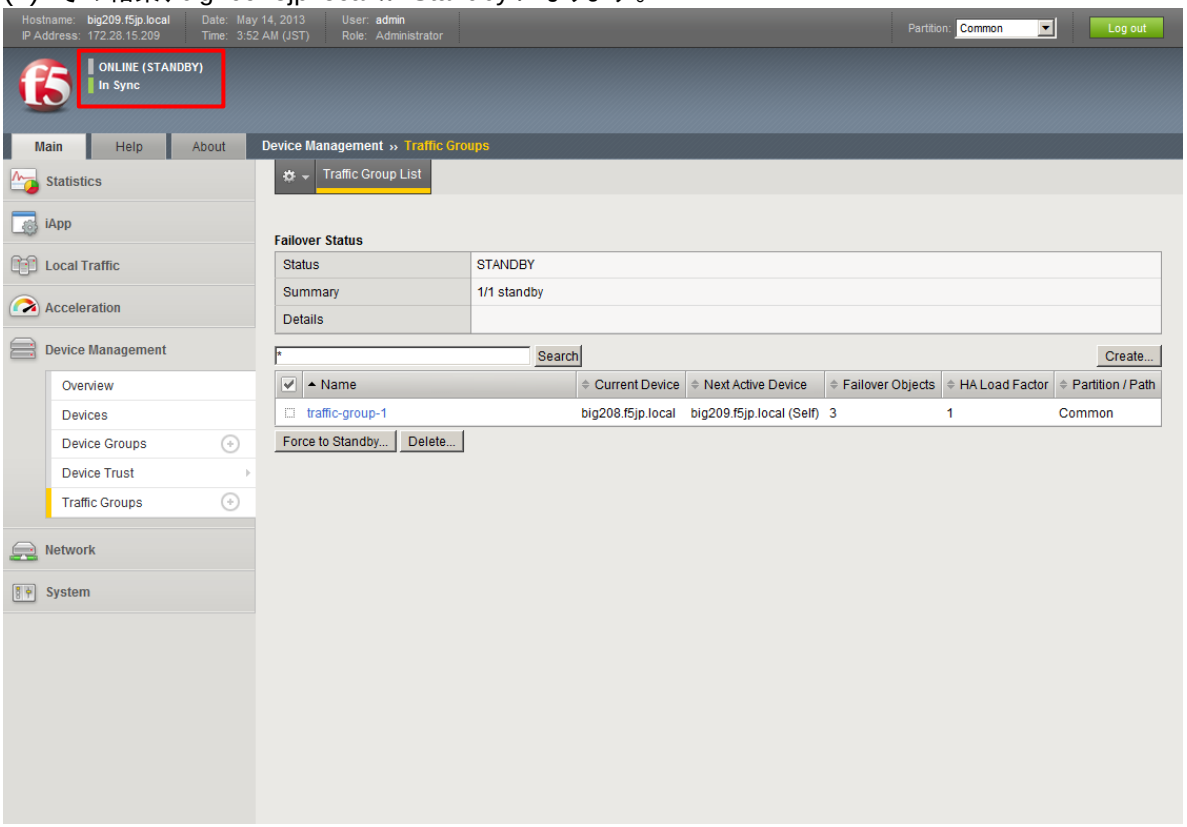
デフォルトでは、管理 IP アドレス設定の大きい値を持つものが Traffic-group-1 の Active 機になります。
したがって、本構成では、Standby にしたい機器：big209.f5jp.local がこの Traffic-group-1 の Active となっています。

以降、Active 機にしたい機器：big208.f5jp.local が Traffic-group-1 の Active になるように設定します。

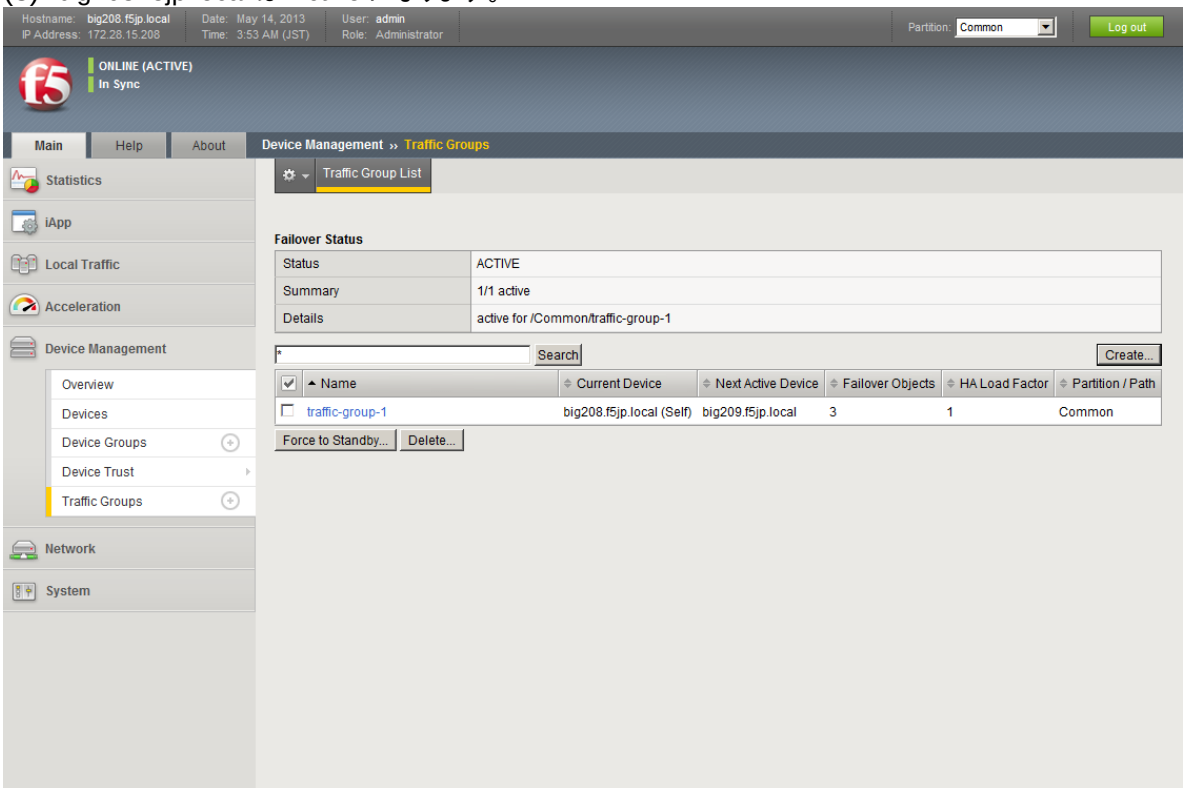
(1) big209.f5jp.local へ移動し、「Main」メニュー→「Device Management」→「Traffic Groups」から Traffic-group-1 を選択し、「Force to Standy」ボタンを押します。



(2) その結果、big209.f5jp.local が Standby になります。



(3) big208.f5jp.local は Active になります。



以上で冗長化設定は終わりです。

7.10. クライアント PC からのアクセス

クライアント PC から、設定した Virtual Server へのネットワークアクセスが完了することを確認します。

8. おわりに

基本的な APM セットアップに関しては以上で終了となります。

BIG-IP シリーズ製品ラインナップにおいては、ソフトウェアモジュールライセンスを追加することで、サーバ負荷分散はもちろんのこと、広域負荷分散やネットワークファイアウォール機能、Web アプリケーションファイアウォール機能など、アプリケーションアクセスを最適化する為の多彩な機能が使用できるようになります。
詳細は各種 WEB サイトにてご確認いただくか、購入元にお問い合わせください。

＜F5 ネットワークス WEB サイトの紹介＞

F5 ネットワークスジャパン総合サイト
http://www.f5networks.co.jp/

F5 Tech Depot：エンジニア向け製品関連情報サイト
http://www.f5networks.co.jp/depot/

AskF5：ナレッジベース総合サイト（英語）
http://support.f5.com/kb/en-us.html

DevCentral：F5 ユーザコミュニティサイト（英語：アカウント登録が必要です）
https://devcentral.f5.com/

以上