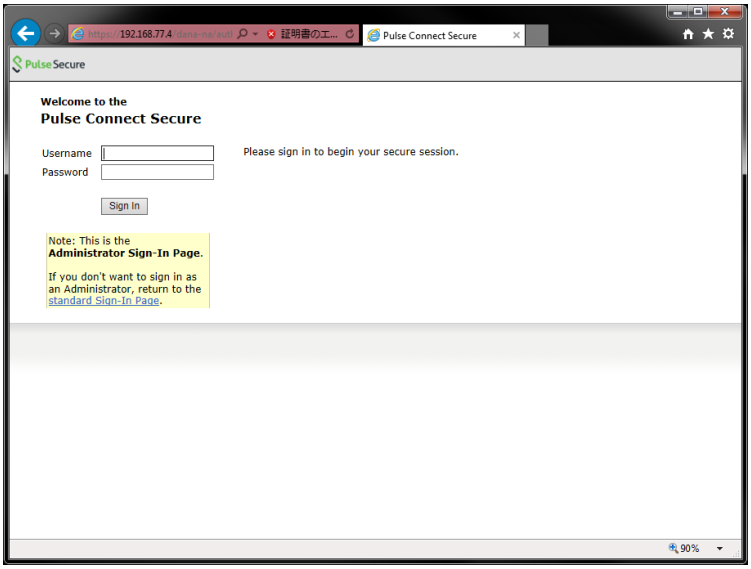
■Pulse Connect Secure（PSA300）のクライアント証明書認証の設定手順

1. Pulse Connect Secure（PSA300）の管理画面へブラウザからアクセス
   https://<Pulse Connect Secure の IP、または FQDN>/admin
   ※IP、または FQDN に対してサーバ証明書が設定されていない場合、
   以下の警告メッセージが出力されますが、”このサイトの閲覧を続行する”をクリックする。

2. Username/Password を入力してログイン

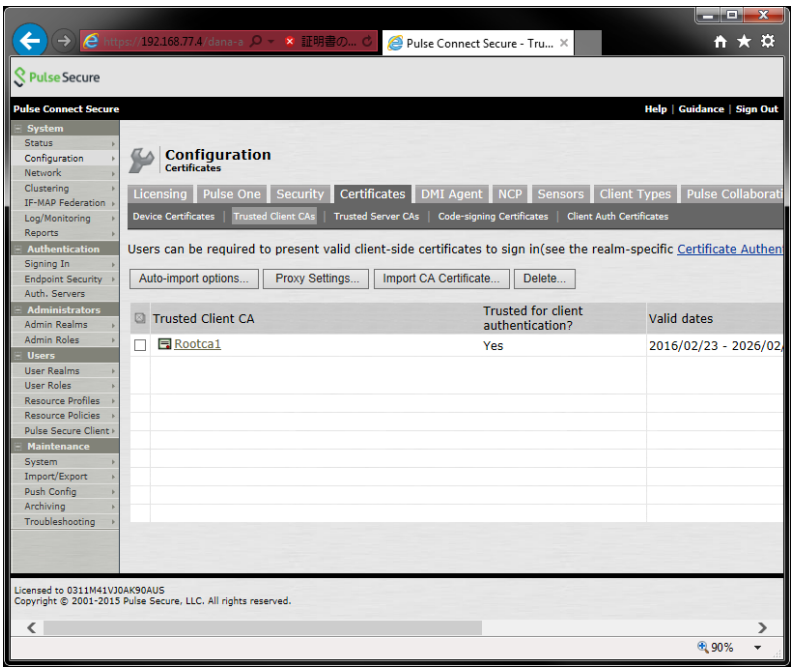


3. NRA のルート証明書、中間証明書の設定
ルート証明書と利用中の中間認証局の証明書を下記 URL からダウンロード。

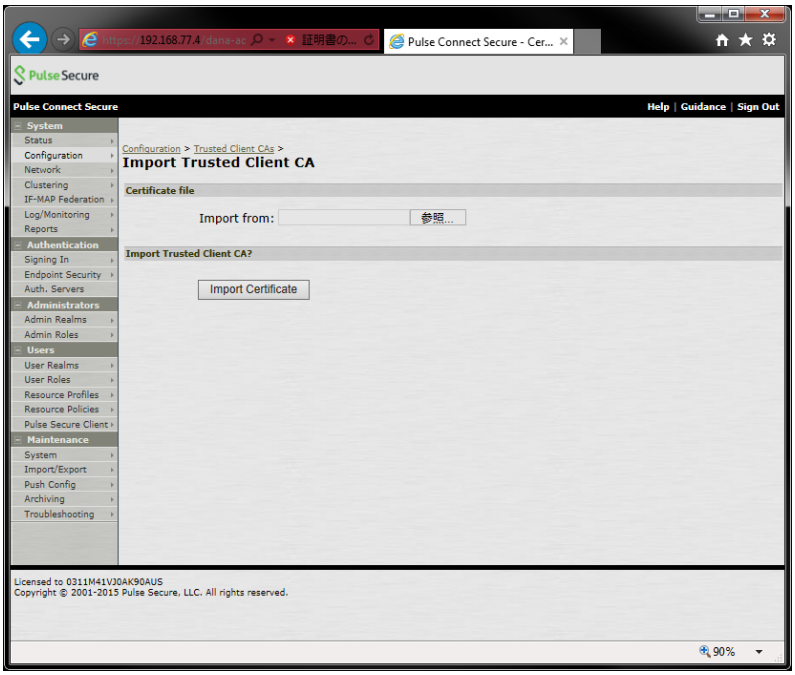
・中間証明書(CA3)
https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority3.crt
・中間証明書(CA4)
https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority4.crt
・ルート証明書
https://www.nrapki.jp/nrawp/cert/NipponRARootCertificationAuthority.crt

下図の NRA-PKI システム管理画面にて、[利用者メンテナンス]をクリックすると、適用されているサービス名が表示される。サービス名の後に（CA4）という表記があれば CA4、なければ CA3 を利用している。

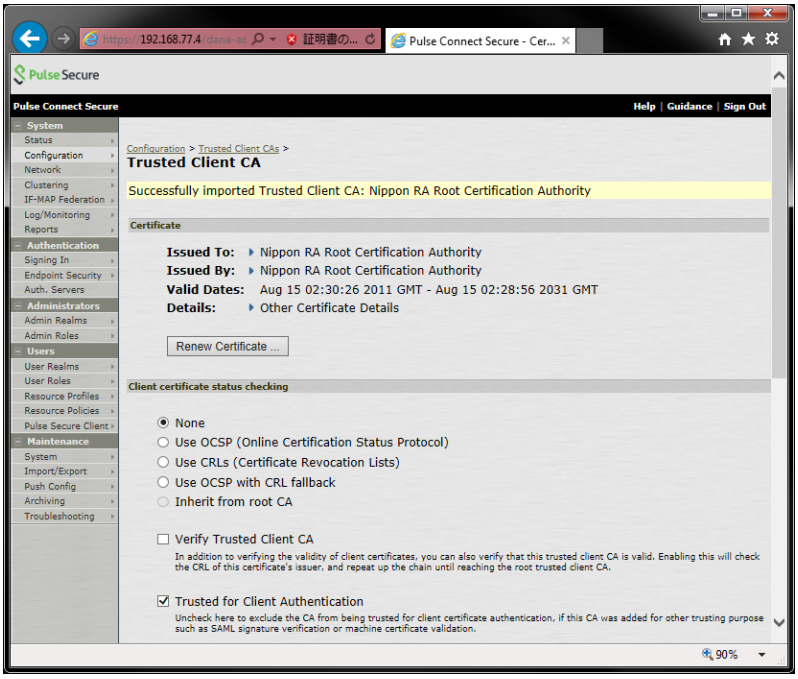
トップ画面の左ペイン、”System”→”Configuration”→”Certificates”→”Trusted Client CAs”を選択し、Configration 画面を表示させ“Import CA Certificate”ボタンをクリックする。



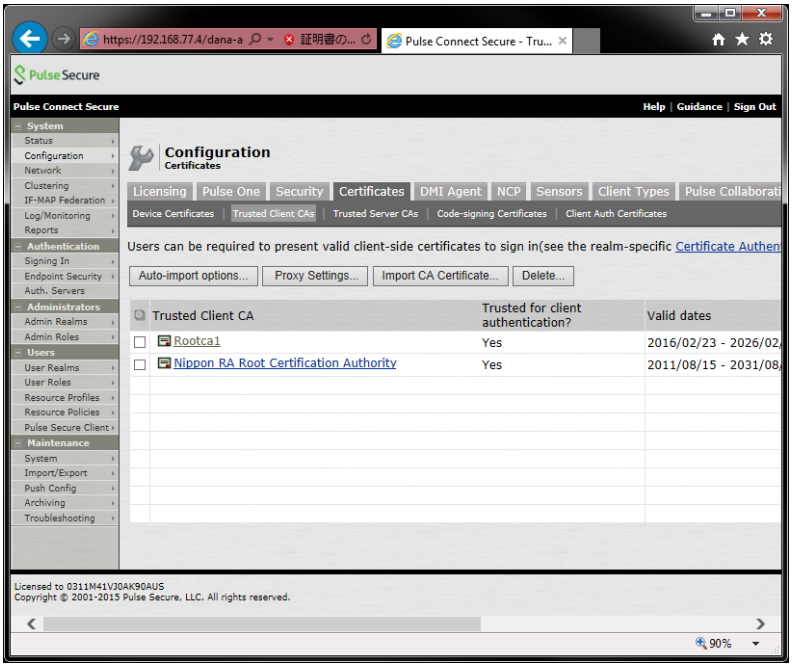
“参照”ボタンをクリックする。ダウンロードしたルート証明書のファイルを選択し”開く”をクリックし、続けて”Import Certificate”をクリック。



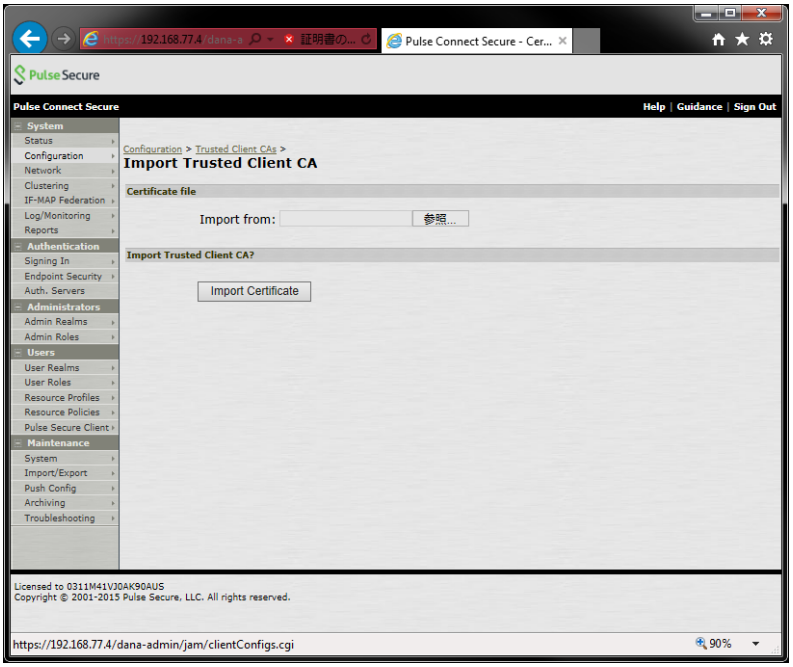
“Successfully～”と表示され正常にインポートされたことを確認し、上部の”Trusted Client CAs”をクリック。



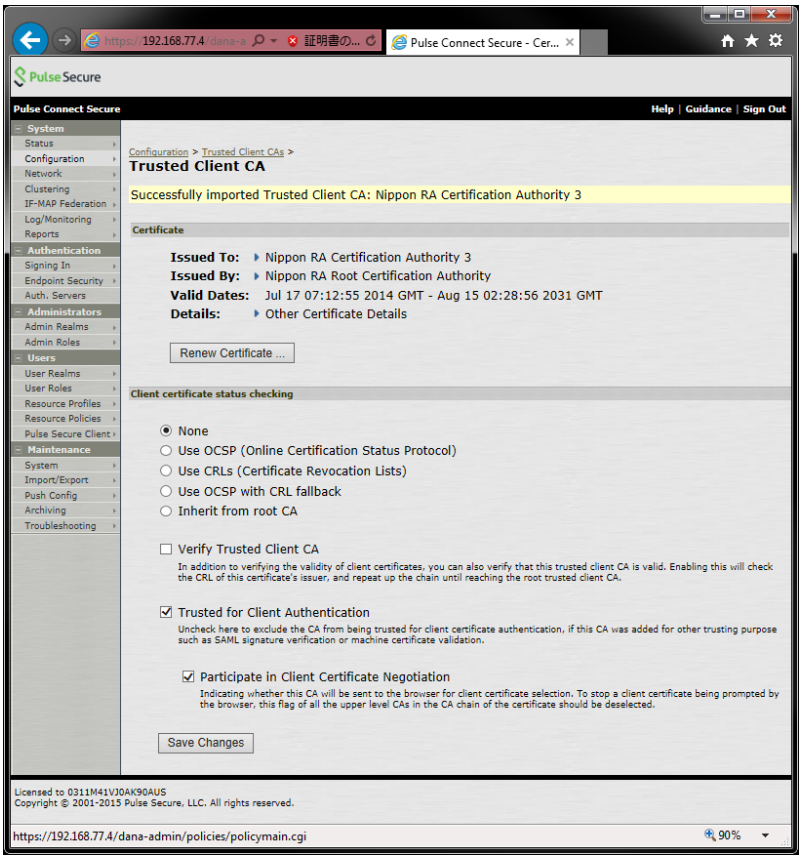
次に中間証明書をインポートするために“Import CA Certificate”ボタンをクリックする。



“参照”ボタンをクリックする。

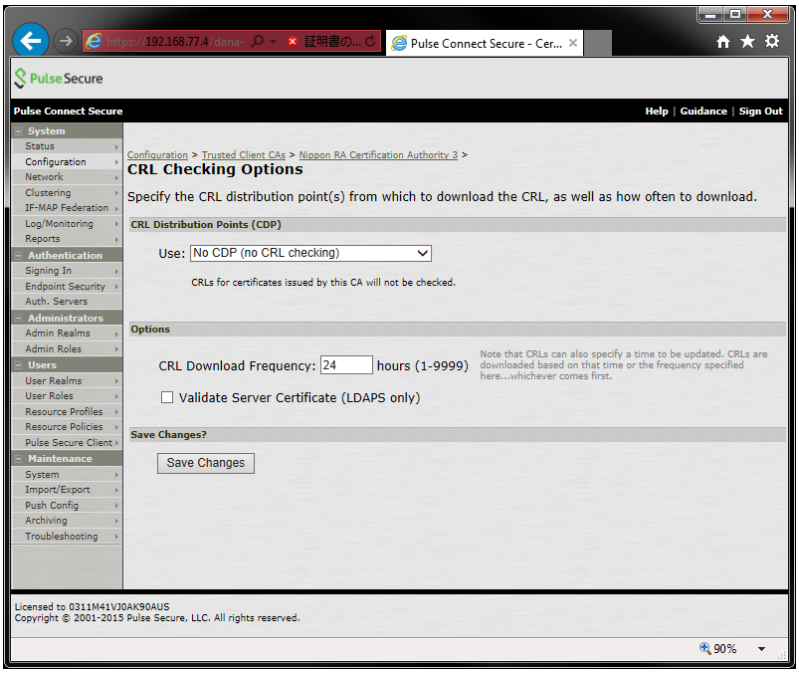


ダウンロードした中間証明書のファイルを選択し”開く”をクリックし、続けて”Import Certificate”をクリック。



続けて、失効リスト（CRL）の設定する。
“Client certificate status checking”のラジオボタンメニューから” Use CRLs（Certificate Revocation Lists)”を選択し、”Save Changes”をクリックする。

下部、” CRL Settings”の”CRL Checking Options…”ボタンをクリックする。



下記、3 項目を設定し、”Save Changes”をクリックする。

① 失効リストの設定選択

“CRL Checking Options”→” CRL Distribution Points (CDP)”→”Use:” リストボックスから、”Manually configured CDP”を選択する。

② 失効リストの配布ポイントの設定

“Primary CDP”に、失効リスト（CRL）の URL を入力する。

※ご利用中の中間認証局に合わせてどちらかを入力。

中間認証局(CA3):

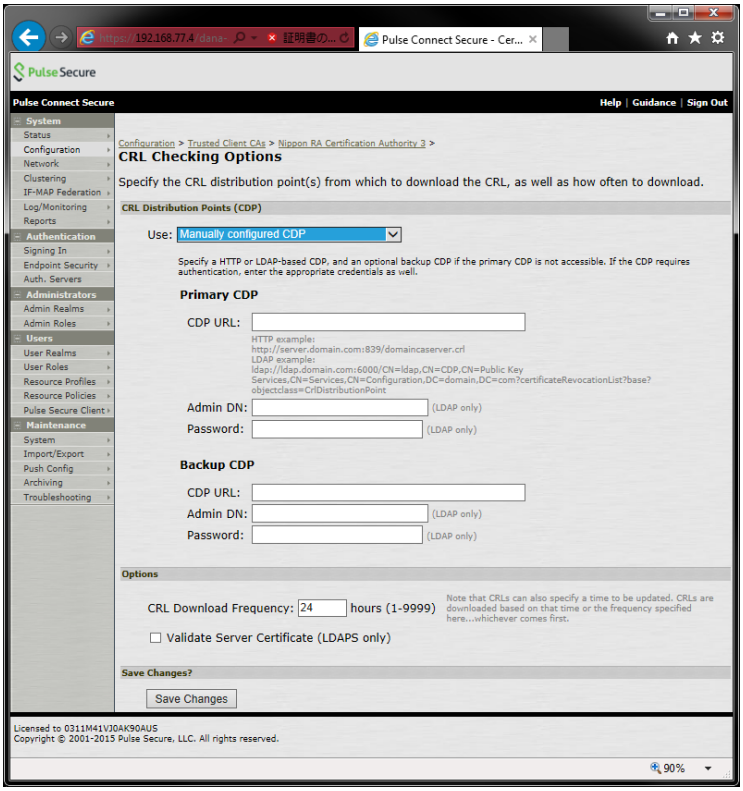
http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3/cdp.crl

中間認証局(CA4):

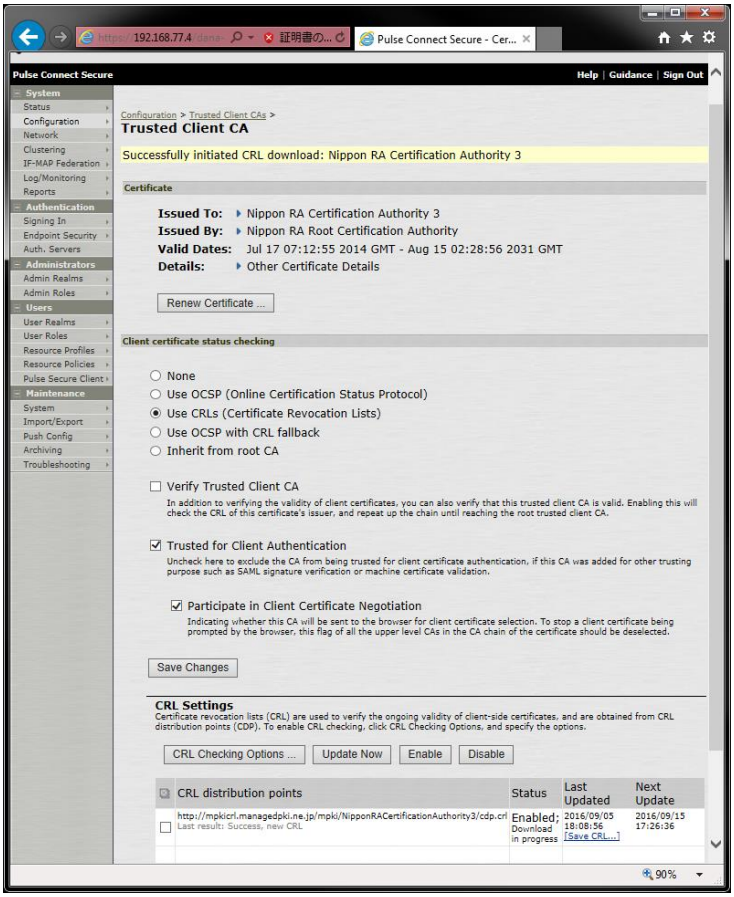
http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4/cdp.crl

③ 失効リスト（CRL）のリフレッシュ間隔

初期値の 24 時間から1時間に変更する。



“Update Now”をクリックし、CRLのダウンロードが成功したかを確認する。



4. “User Role”の作成

トップ画面の左ペイン、”Users”→”User Roles”→”New User Role”を選択し、New Role 画面を表示させ各種設定をする。

任意の Role 名（例：xxx_role）を入力し、以下の設定をする。

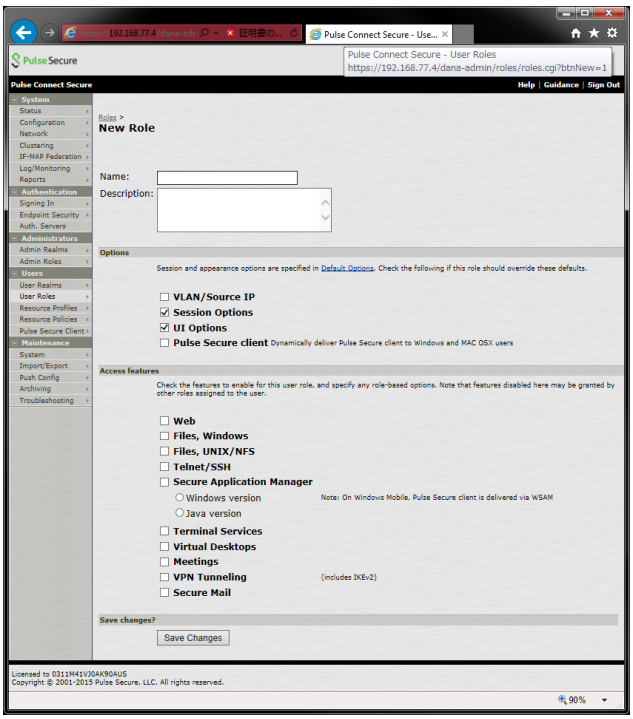
“Option”パート

Session Options、UI Options にチェックを入れる。

“Access features”パート

Network Connect にチェックを入れ、Network Connect ラジオボタンを選択する。

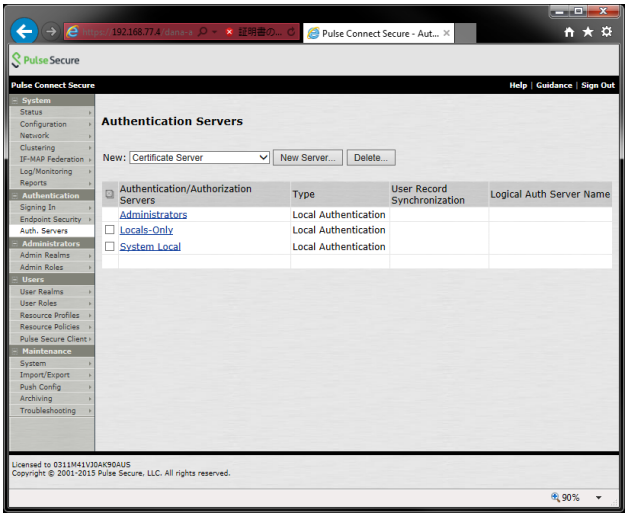
最後部の”Save Changes”をクリックして設定を保存する。



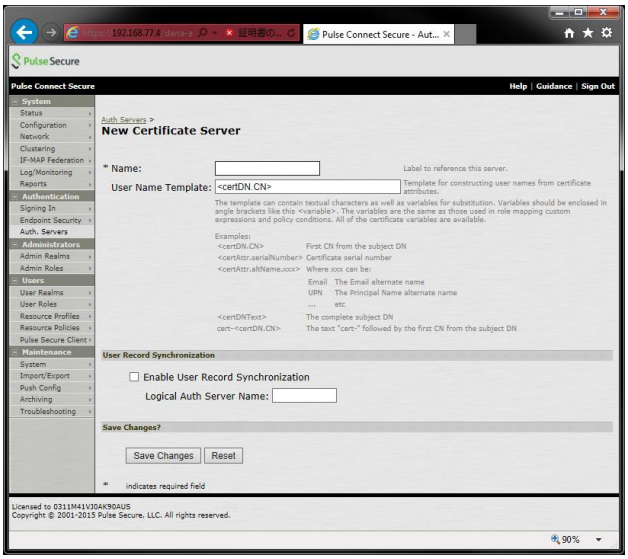
5. “Authentication Servers”の設定。

トップ画面の左ペイン、“Authentications”→”Auth, Servers”を選択し、Authetication Servers 画面を表示させ各種設定をする。

（Select server type）のリストボックスの”Certificate Server”を選択して、“New Server”をクリックする。



任意の Certification Server 名を入力しデフォルトのまま、”Save Changes”をクリックする。



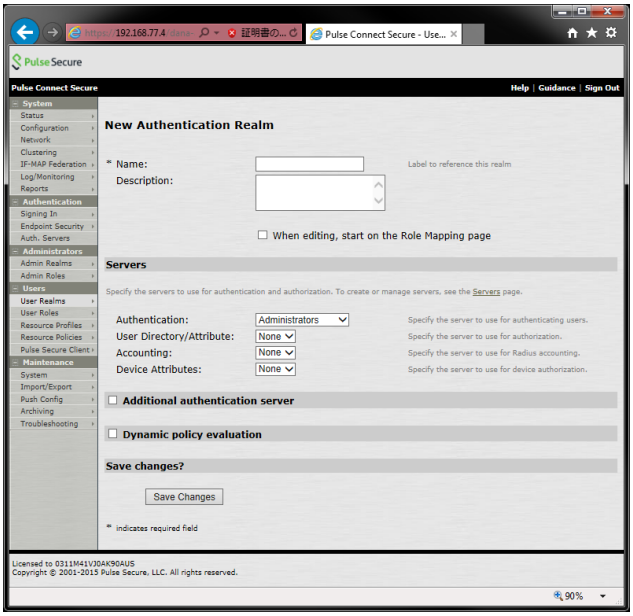
6. “User Realm”の作成

トップ画面の左ペイン、”Users”→”User Realms”→”New User Realms”を選択し、New Authentication Realms 画面を表示させ各種設定をする。

任意の Realm 名（例：xxx）を入力し、以下の設定をする。

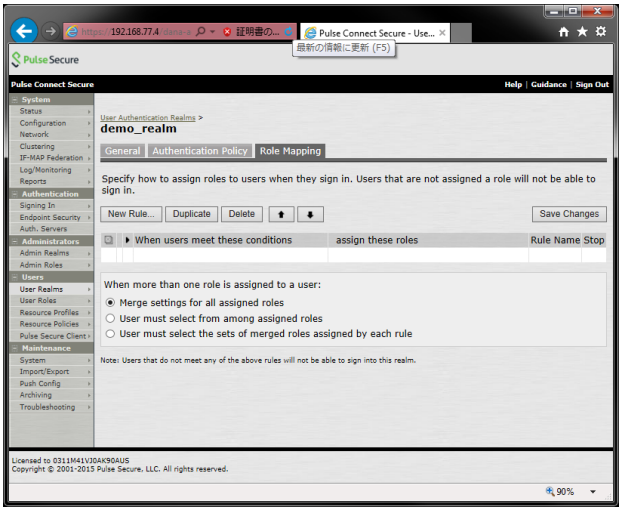
“Servers”パート→Authentication のリストボックスから、6.で作成した Certificate Server を指定する。

上記を確認し、“Save Changes”をクリックする。

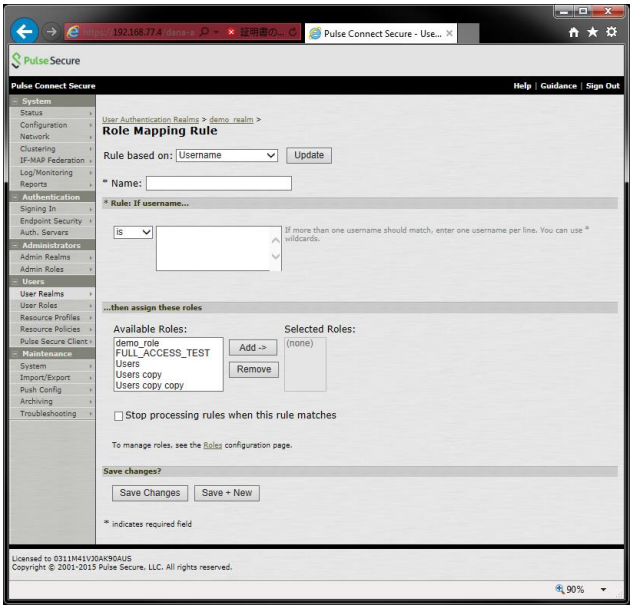


7. 作成した Realm と Role のマッピング

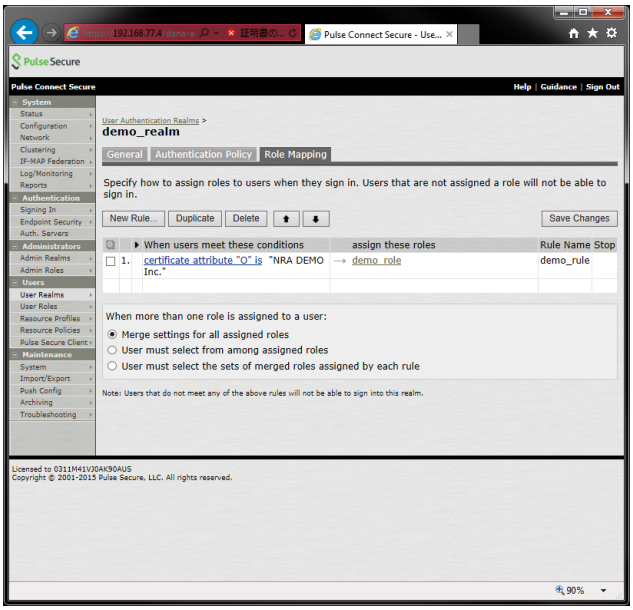
トップ画面の左ペイン、”Users”→”User Realms”→”任意で作成した Realm”→”Role Maping”を選択し、”New Rule”をクリックして Rule を設定する。



“Rule based on”：リストボックスから”Certificate”を指定し、”Update”をクリック
“Name”→任意の Role Maping Rule 名を入力（例：XXX_Rule_）“Rule If certificate has・・”
→”Attribute”に”O”と入力する。
続けてリストボックスから ”is” を選択して任意の文字列（法人名）を指定
“…then assign these roles ”の一覧から作成した Role を選択し、”Add”をクリックして”Selected Roles”に移動した事を確認する。
上記を確認し、“Save Changes”をクリックする。



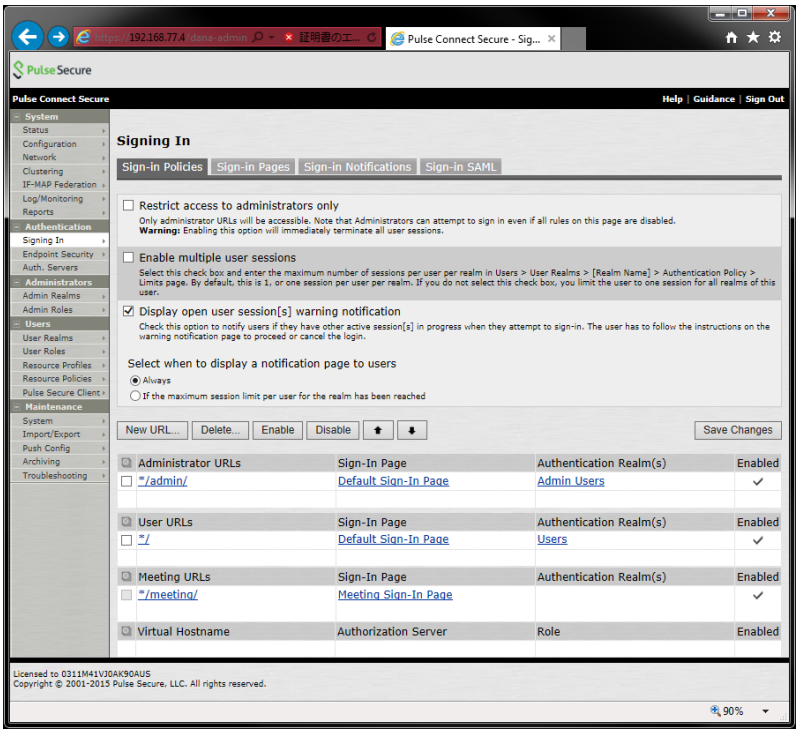
作成した”Realm”と”Role”のマッピング設定を確認する。



8. SSL-VPN 接続時にクライアント証明書認証をする設定

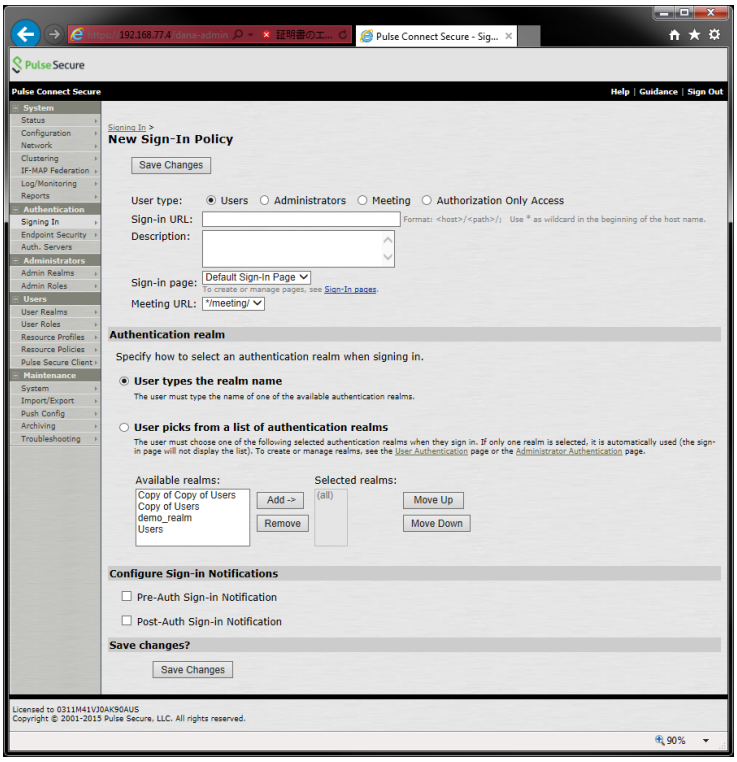
トップ画面の左ペイン、”Authentication”→” Signing In”→” Sign-in Policies”を選択する。

“New URL…”ボタンをクリックします。



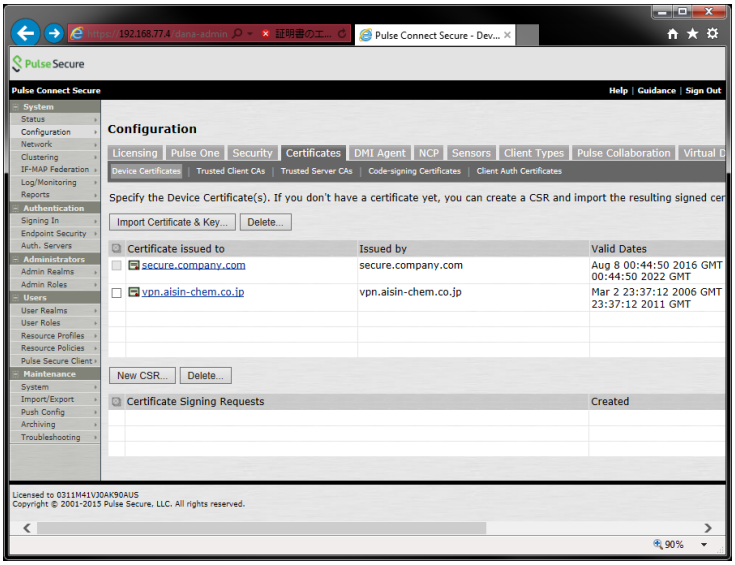
下記、項目を設定し”Save Changes”をクリックします。

① “Sign-in URL:”にクライアント証明書認証を有効にする任意の URL を指定
② “Authentication realm”に作成した Realm を指定して”ADD”をクリック

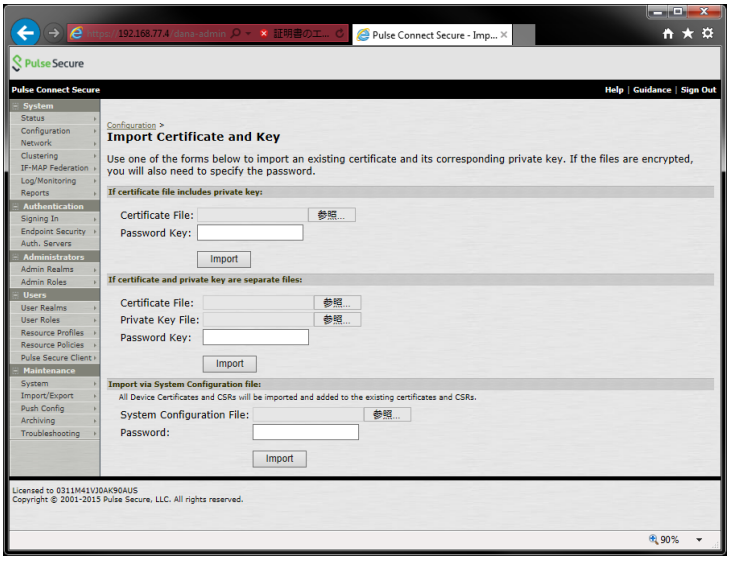


9. SSL 通信用のサーバ証明書の設定

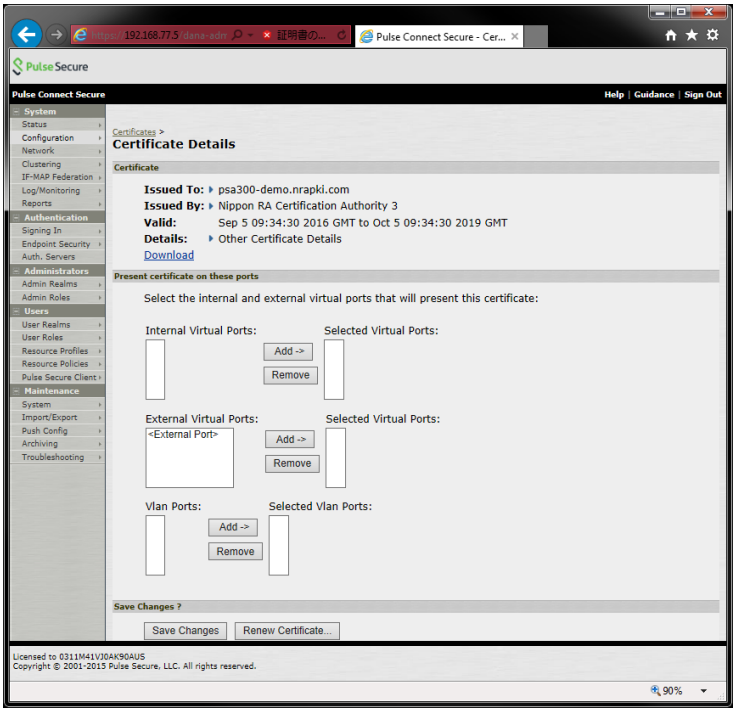
トップ画面の左ペイン、”System”→”Configuration”→”Certificates”→” Device Certificates”を選択し、Configration 画面を表示させ“Import Certificate & Key”ボタンをクリックする。



NRA から提供するイントラ用 SSL サーバ証明書は P12 形式で提供する為、” If certificate file includes private key:”メニューの”参照”をクリックする。



SSL サーバ証明書と紐づけるポートは、“Internal Port”、”External Port”の設計に合わせて設定し、”Save Changes”をクリックして



SSL サーバ証明書がインポートされたことを確認する。