

■ 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

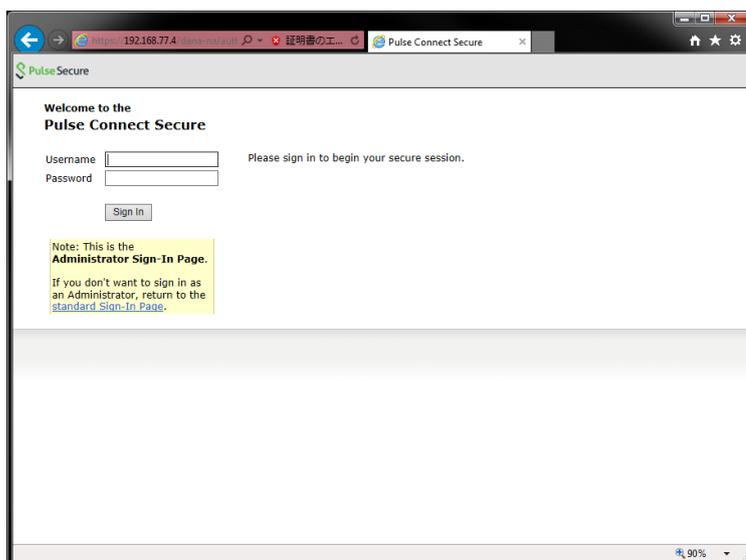
https://<Pulse Connect Secure の IP、または FQDN>/admin

※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。

統合認証基盤システム

利用法人テスト 担当者1 様 ログイン中

サービス情報メンテナンス

利用法人 詳細設定

利用者 メンテナンス

利用者 削除

データ

ファイル送信

ヘルプ

チャットで お問い合わせ

このサイトの実在証明

www1.nrapki.co.jp

cybertrust

利用者メンテナンス

利用法人組織の選択

利用者のメンテナンス

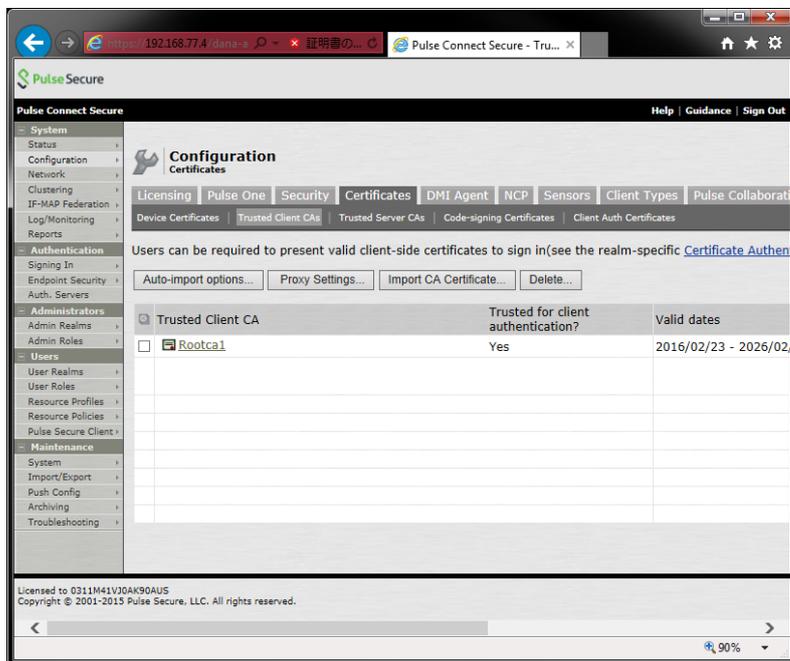
利用法人テスト 加入組織情報

以下のサービスを選択しています。

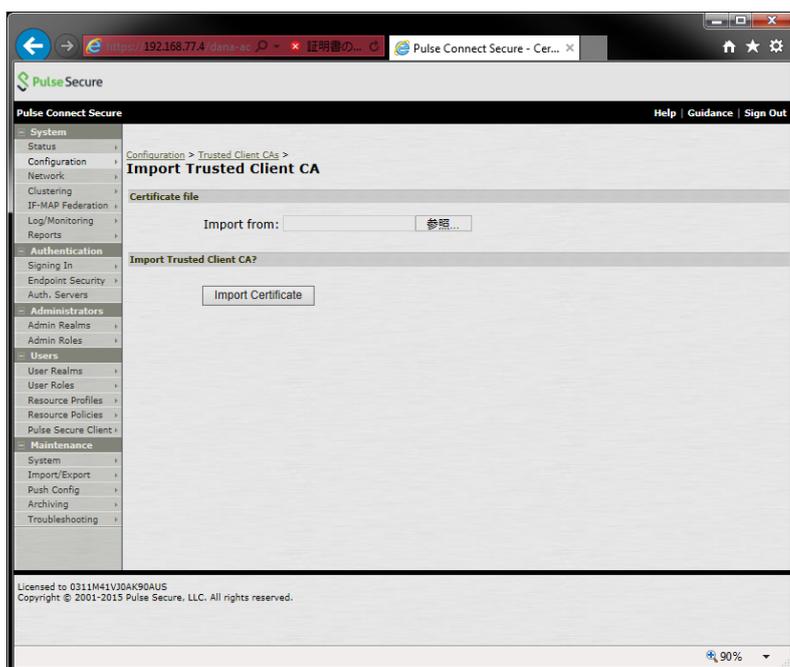
テストサービス (CA4)

組織名	部門	住所
本社		北海道 test test

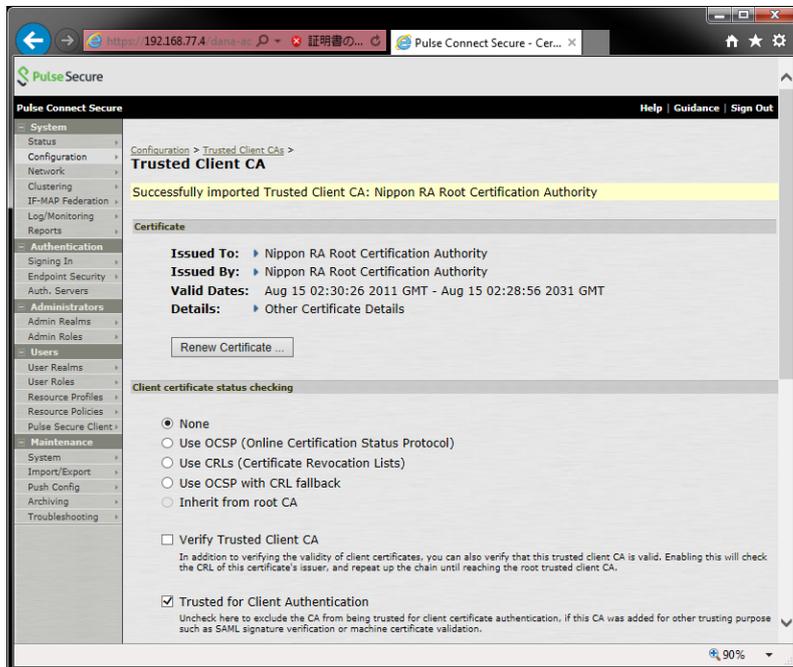
トップ画面の左ペイン、”System”→”Configuration”→”Certificates”→”Trusted Client CAs”を選択し、Configuration 画面を表示させ”Import CA Certificate”ボタンをクリックする。



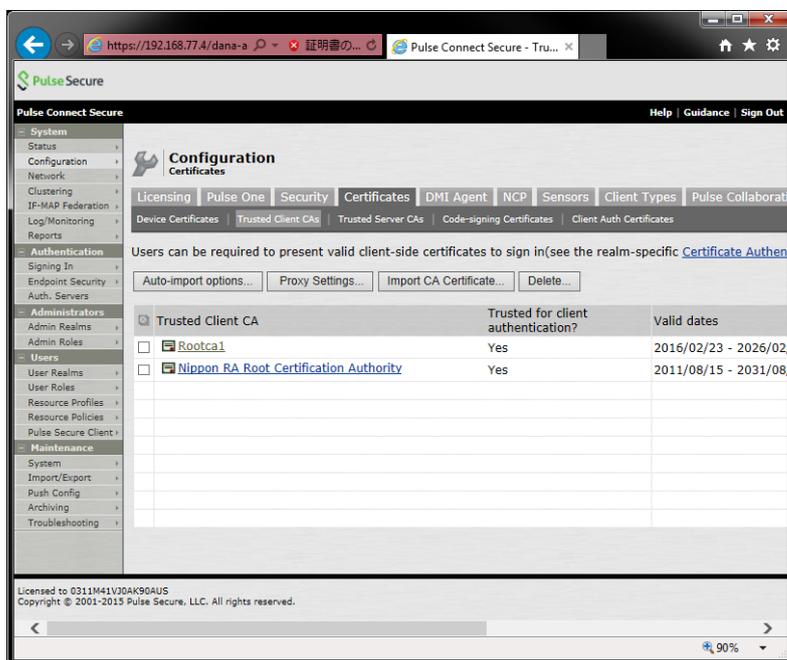
“参照”ボタンをクリックする。ダウンロードしたルート証明書のファイルを選択し”開く”をクリックし、続けて”Import Certificate”をクリック。



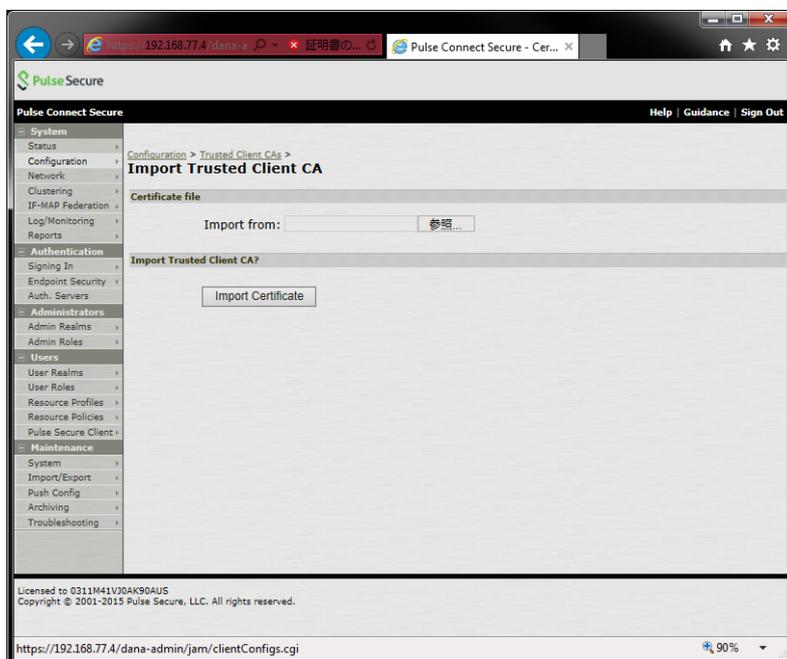
“Successfully〜”と表示され正常にインポートされたことを確認し、上部の” Trusted Client CAs” をクリック。



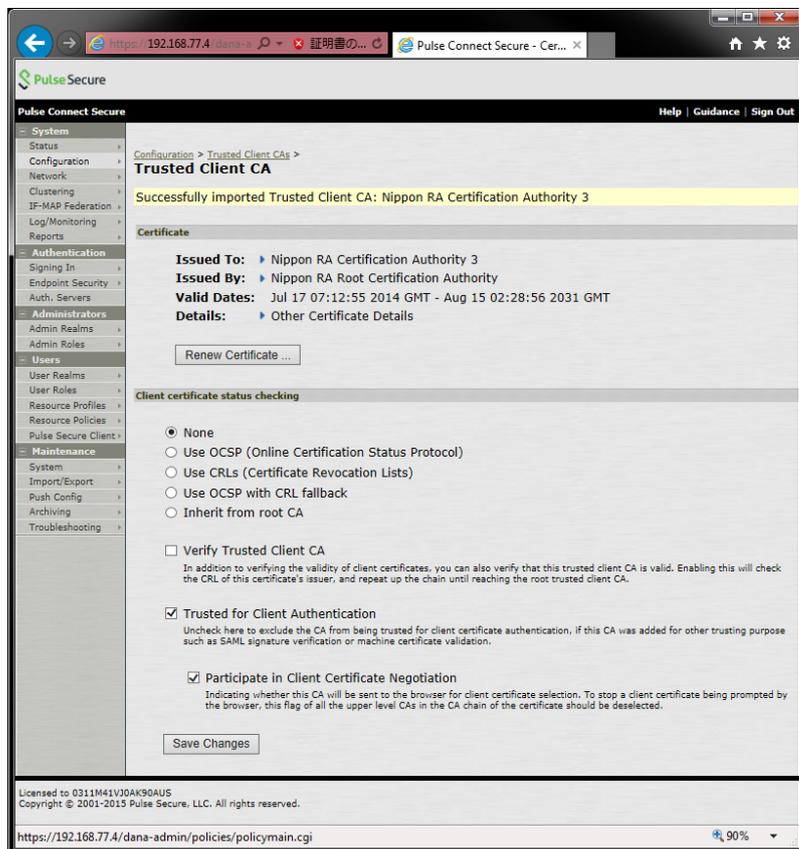
次に中間証明書をインポートするために“Import CA Certificate” ボタンをクリックする。



“参照”ボタンをクリックする。



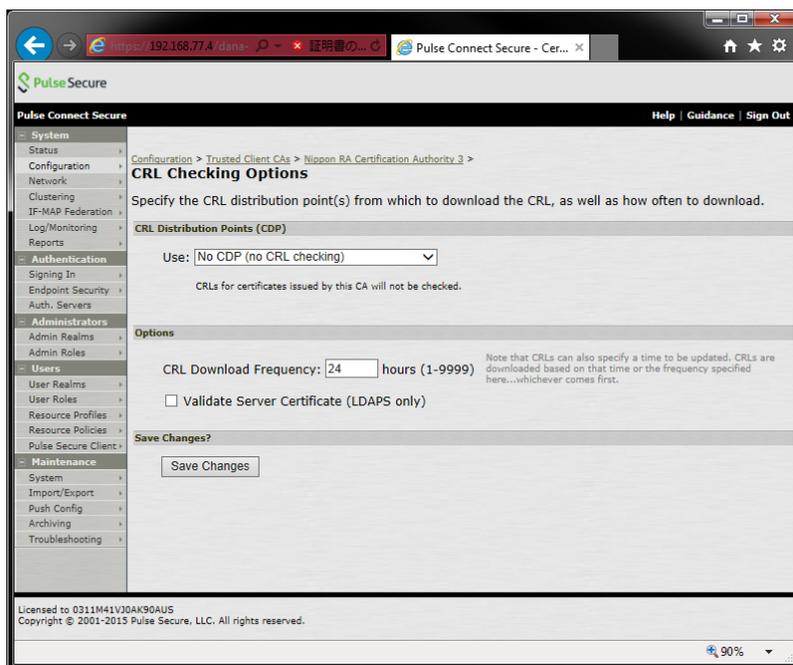
ダウンロードした中間証明書のファイルを選択し”開く”をクリックし、続けて”Import Certificate”をクリック。



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。

Pulse Connect Secure

Configuration > Trusted Client CAs > Nippon RA Certification Authority 3 >

CRL Checking Options

Specify the CRL distribution point(s) from which to download the CRL, as well as how often to download.

CRL Distribution Points (CDP)

Use: **Manually configured CDP**

Specify a HTTP or LDAP-based CDP, and an optional backup CDP if the primary CDP is not accessible. If the CDP requires authentication, enter the appropriate credentials as well.

Primary CDP

CDP URL:

HTTP example:
http://server.domain.com:839/domaincaserver.crl
LDAP example:
ldap://ldap.domain.com:6000/CN=ldap,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=domain,DC=com?certificateRevocationList?base?objectclass=CrlDistributionPoint

Admin DN: (LDAP only)

Password: (LDAP only)

Backup CDP

CDP URL:

Admin DN: (LDAP only)

Password: (LDAP only)

Options

CRL Download Frequency: hours (1-9999) Note that CRLs can also specify a time to be updated. CRLs are downloaded based on that time or the frequency specified here...whichever comes first.

Validate Server Certificate (LDAPS only)

Save Changes?

Licensed to 0311M41VJ0AK90AUS
Copyright © 2001-2015 Pulse Secure, LLC. All rights reserved.

90%

“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。

The screenshot shows the Pulse Connect Secure web interface. The left sidebar contains navigation menus for System, Authentication, Administrators, Users, Maintenance, and Troubleshooting. The main content area is titled 'Trusted Client CA' and shows a success message: 'Successfully initiated CRL download: Nippon RA Certification Authority 3'. Below this, certificate details are listed: Issued To: Nippon RA Certification Authority 3, Issued By: Nippon RA Root Certification Authority, Valid Dates: Jul 17 07:12:55 2014 GMT - Aug 15 02:28:56 2031 GMT, and Details: Other Certificate Details. A 'Renew Certificate ...' button is visible. The 'Client certificate status checking' section has radio buttons for 'None', 'Use OSCP (Online Certification Status Protocol)', 'Use CRLs (Certificate Revocation Lists)' (selected), 'Use OSCP with CRL fallback', and 'Inherit from root CA'. There are also checkboxes for 'Verify Trusted Client CA', 'Trusted for Client Authentication', and 'Participate in Client Certificate Negotiation'. A 'Save Changes' button is at the bottom of this section. The 'CRL Settings' section includes a 'CRL Checking Options ...' button and 'Update Now', 'Enable', and 'Disable' buttons. A table below shows CRL distribution points:

CRL distribution points	Status	Last Updated	Next Update
<input checked="" type="checkbox"/> http://mpkicrl.managedki.ne.jp/mpk/NipponRACertificationAuthority3/cdp.crl	Enabled	2016/09/05 18:08:56	2016/09/15 17:26:36
<input type="checkbox"/> Last result: Success, new CRL	Download in progress		[Save CRL...]

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。

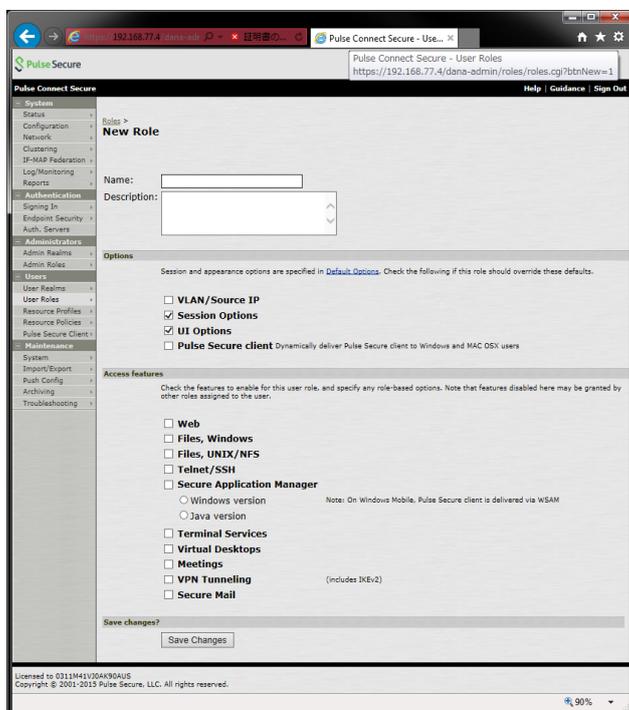
“Option”パート

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。

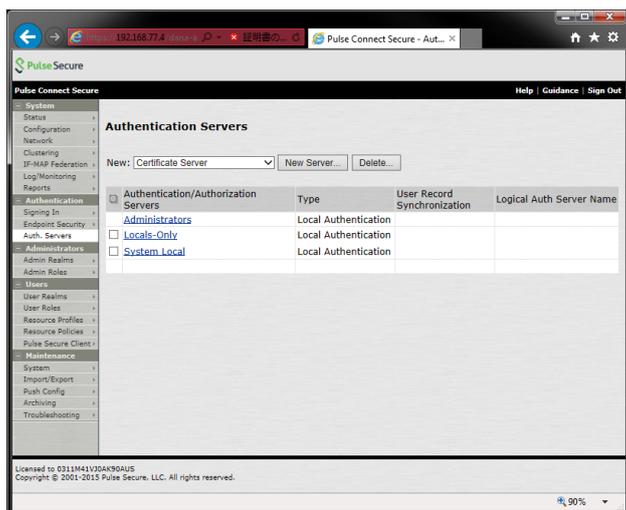
最後部の”Save Changes”をクリックして設定を保存する。



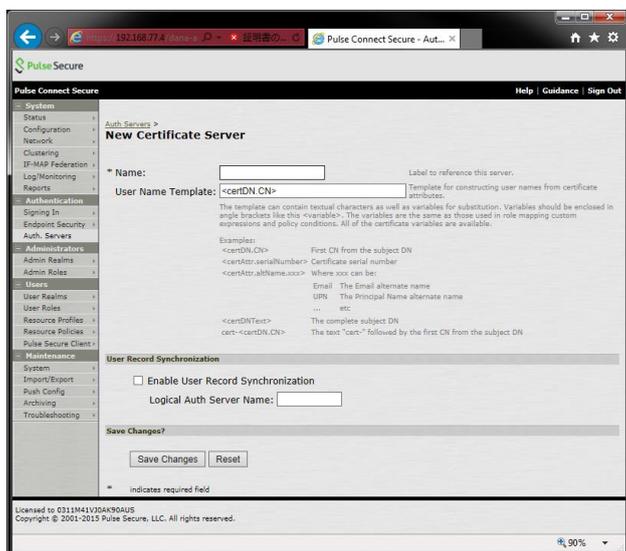
5. “Authentication Servers”の設定。

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。



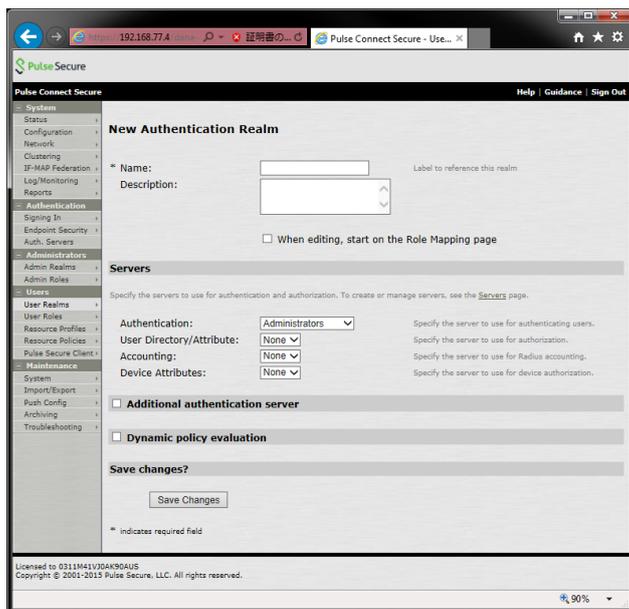
6. “User Realm”の作成

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。

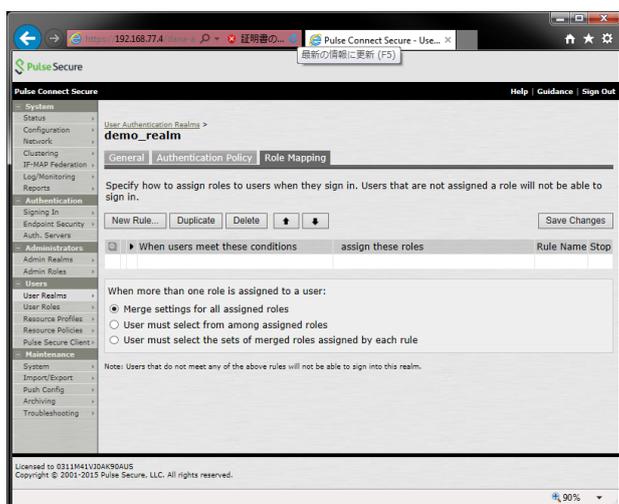
“Servers”パート→Authentication のリストボックスから、6.で作成した Certificate Server を指定する。

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 Mapping”を選択し、“New Rule”をクリックして Rule を設定する。



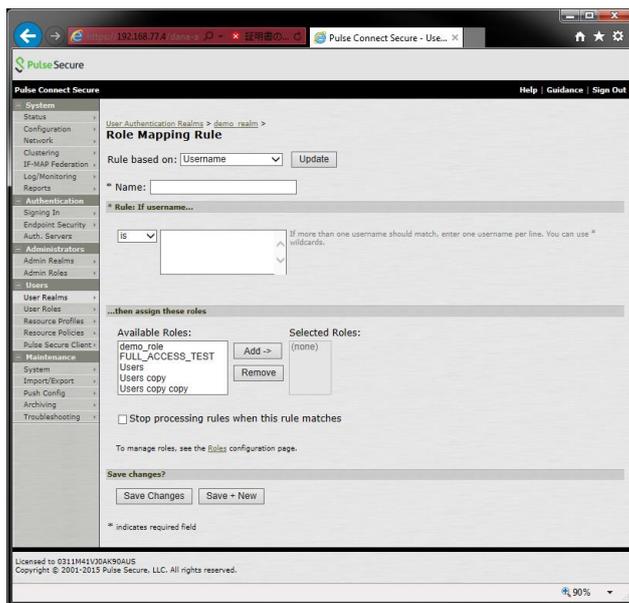
“Rule based on”：リストボックスから”Certificate”を指定し、”Update”をクリック

“Name”→任意の Role Mapping Rule 名を入力（例：XXX_Rule_） “Rule If certificate has . . .”
→”Attribute”に”O”と入力する。

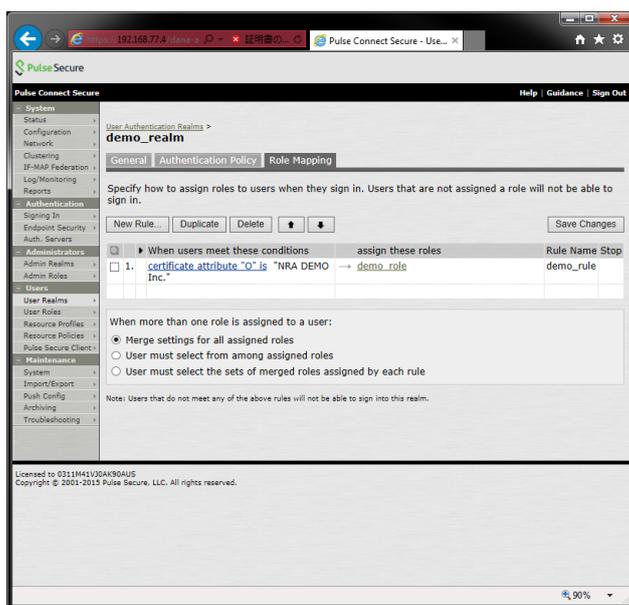
続けてリストボックスから ”is” を選択して任意の文字列（法人名）を指定

“...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。

The screenshot shows the Pulse Connect Secure web interface. The left navigation menu is expanded to 'Authentication' > 'Signing In' > 'Sign-in Policies'. The main content area displays the 'Sign-in Policies' configuration page. The page includes a 'New URL...' button and a table of URL rules.

Sign-in Policies Configuration:

- Restrict access to administrators only
Only administrator URLs will be accessible. Note that Administrators can attempt to sign in even if all rules on this page are disabled.
Warning: Enabling this option will immediately terminate all user sessions.
- Enable multiple user sessions
Select this check box and enter the maximum number of sessions per user per realm in Users > User Realms > [Realm Name] > Authentication Policy > Limits page. By default, this is 1, or one session per user per realm. If you do not select this check box, you limit the user to one session for all realms of this user.
- Display open user session[s] warning notification
Check this option to notify users if they have other active session[s] in progress when they attempt to sign-in. The user has to follow the instructions on the warning notification page to proceed or cancel the login.

Select when to display a notification page to users

Always
 If the maximum session limit per user for the realm has been reached

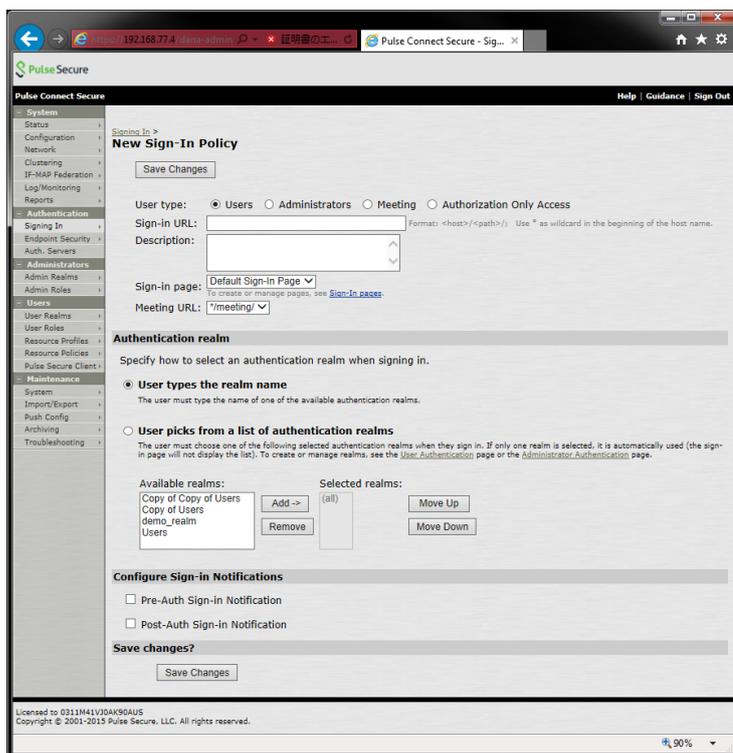
URL Rules Table:

URL	Sign-In Page	Authentication Realm(s)	Enabled
<input checked="" type="checkbox"/> */admin/	Default Sign-In Page	Admin Users	Enabled
<input type="checkbox"/> */	Default Sign-In Page	Users	Enabled
<input checked="" type="checkbox"/> */meeting/	Meeting Sign-In Page		Enabled
<input checked="" type="checkbox"/> Virtual Hostname	Authorization Server	Role	Enabled

Licensed to 0311M41V3DAK9GAUS
Copyright © 2001-2015 Pulse Secure, LLC. All rights reserved.

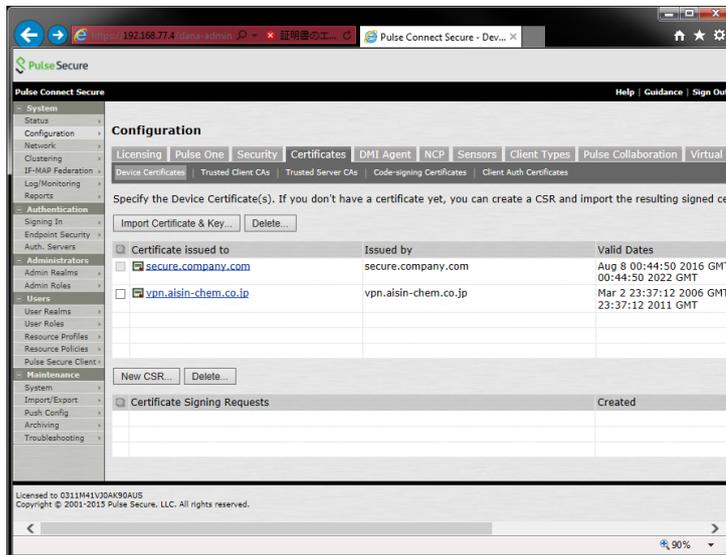
下記、項目を設定し”Save Changes”をクリックします。

- 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

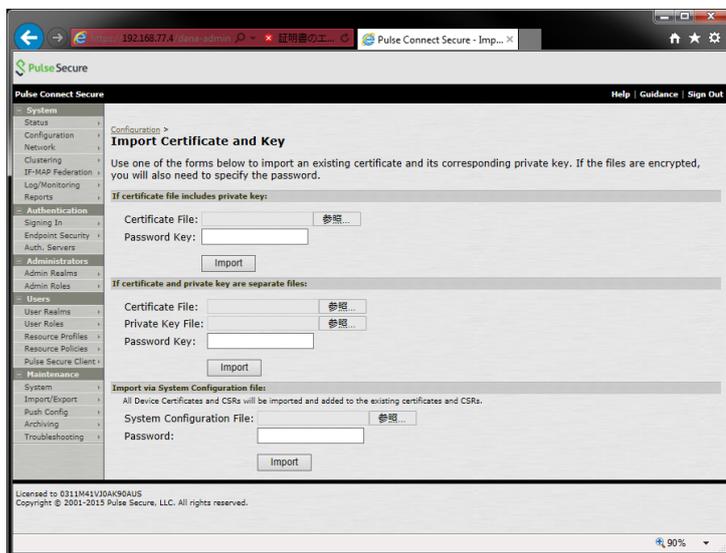


9. SSL 通信用のサーバ証明書の設定

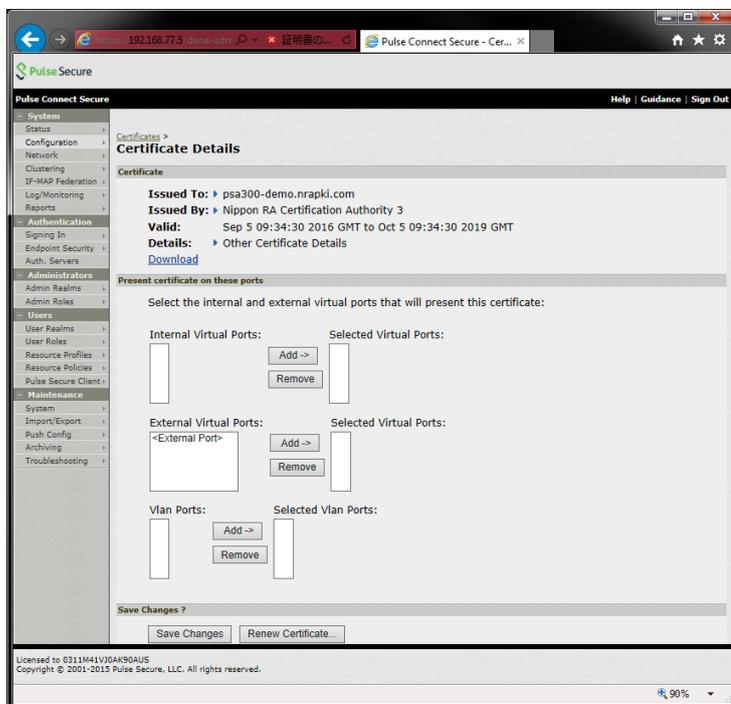
トップ画面の左ペイン、”System”→”Configuration”→”Certificates”→” Device Certificates”を選択し、 Configuration 画面を表示させ”Import Certificate & Key”ボタンをクリックする。



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。

