ISE 2.x に対してプライム記号 3.1 TACACS認証を設定して下さい

目次

概要

この資料に Prime Infrastructure を ISE 2.x の TACACS によって認証するために設定する方法を記述されています。

要件

次の項目に関する基本的な知識があることが推奨されます。

- Identity Services Engine (ISE)
- Prime Infrastructure

設定

Cisco Prime Network Control System 3.1

Cisco 識別 サービス エンジン 2.0 またはそれ以降。

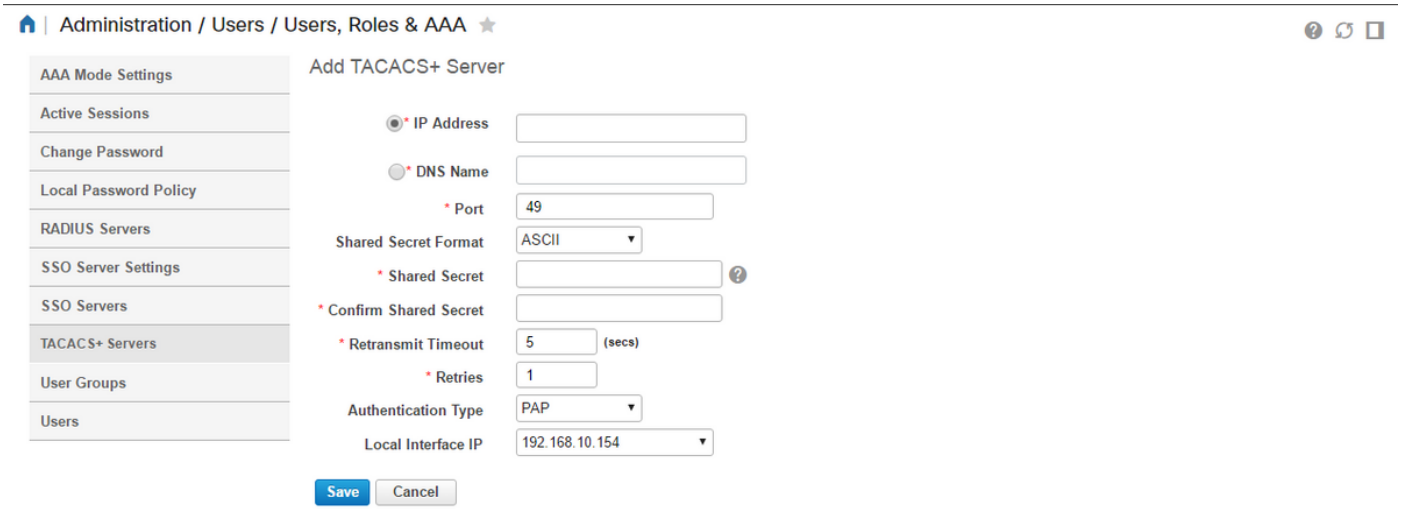
(注： ISE はバージョン 2.0 から開始する TACACS だけをサポートしますが Radius を使用するためにプライム記号を設定することは可能性のあるです。 プライム記号は ISE またはサード パーティ ソリューションのより古いバージョンの TACACS に加えて Radius を使用するために好んだら RADIUS特性のリストが含まれています。)

主な設定

次の画面への Navigiate: 次を見られる管理/ユーザ ユーザ、ロール及び AAA。

そこに、TACACS+ サーバ タブを選択したら、そして上部右上隅の追加 TACACS+ サーバオプションを選択し、『Go』 を選択 して下さい。

Next 画面で TACACSサーバ エントリの設定は利用できます (これは各々の個々の TACACSサーバのためにされなければなりません)



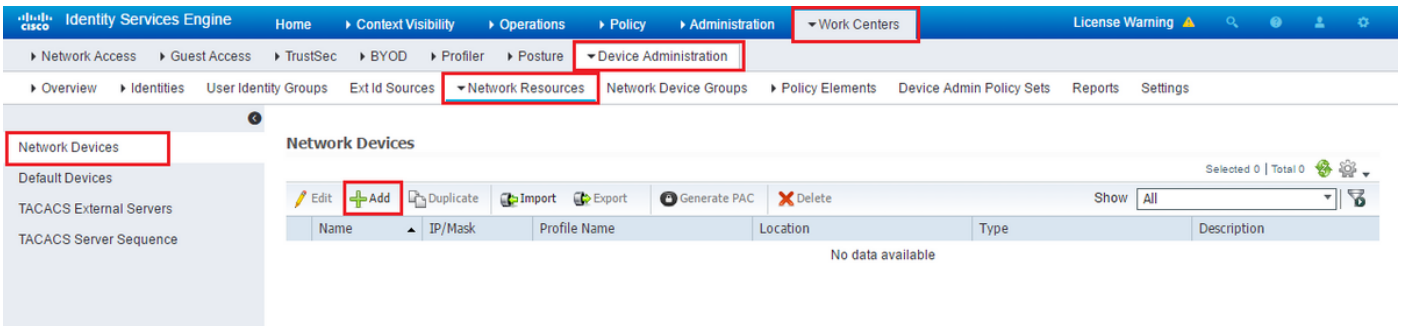
サーバの IP アドレスか DNS アドレス、また共有秘密キーを入力する必要があります。 またこの同じ IP アドレスが ISE で AAA クライアントにあとで使用する必要があるように、使用するために望む以下の事項に注意して下さい:ローカルインターフェイス IP。

プライム記号の設定を完了するため。 AAA モード設定タブの下で管理/ユーザ/ユーザ、役割及び AAA の下で TACACS をイネーブルにする必要があります。

（注： 特に設定をテストしている間）無応答または失敗オプションまたはとサーバレスポンスのだけローカル オプションにイネーブル フォールバックを、チェックすることを推奨します、

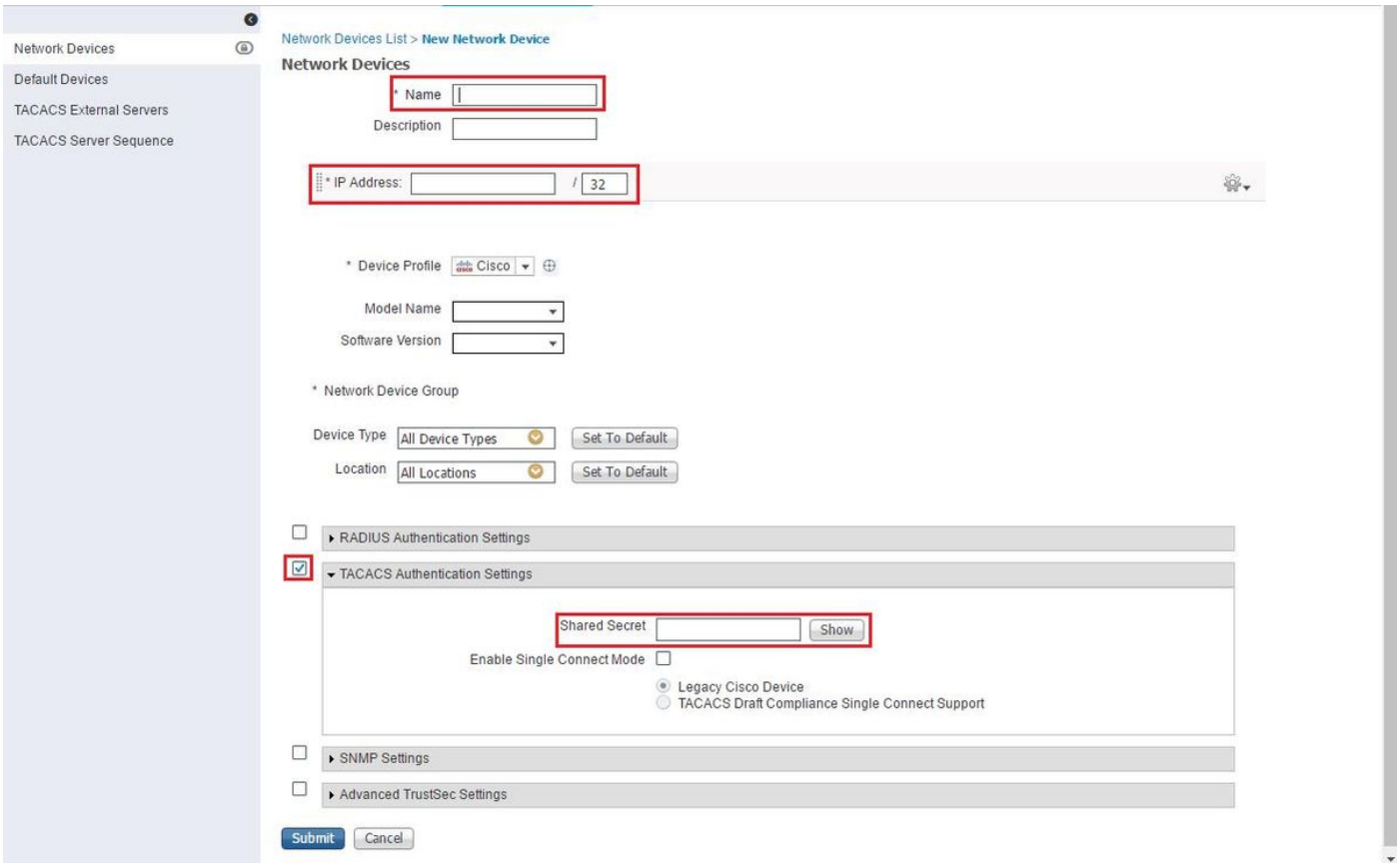
ISE 設定

プライム記号を ISE の AAA クライアントで作業センター/デバイス 管理/ネットワークリソース/ネットワークデバイスで設定して下さい/追加して下さい

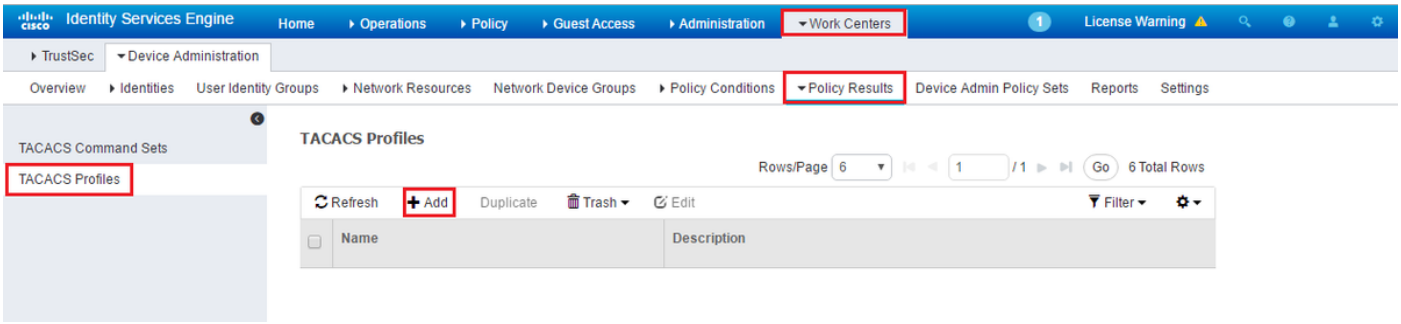


主なサーバのための情報を入力して下さい。 含む必要がある必須 属性はネーム、IP アドレスで

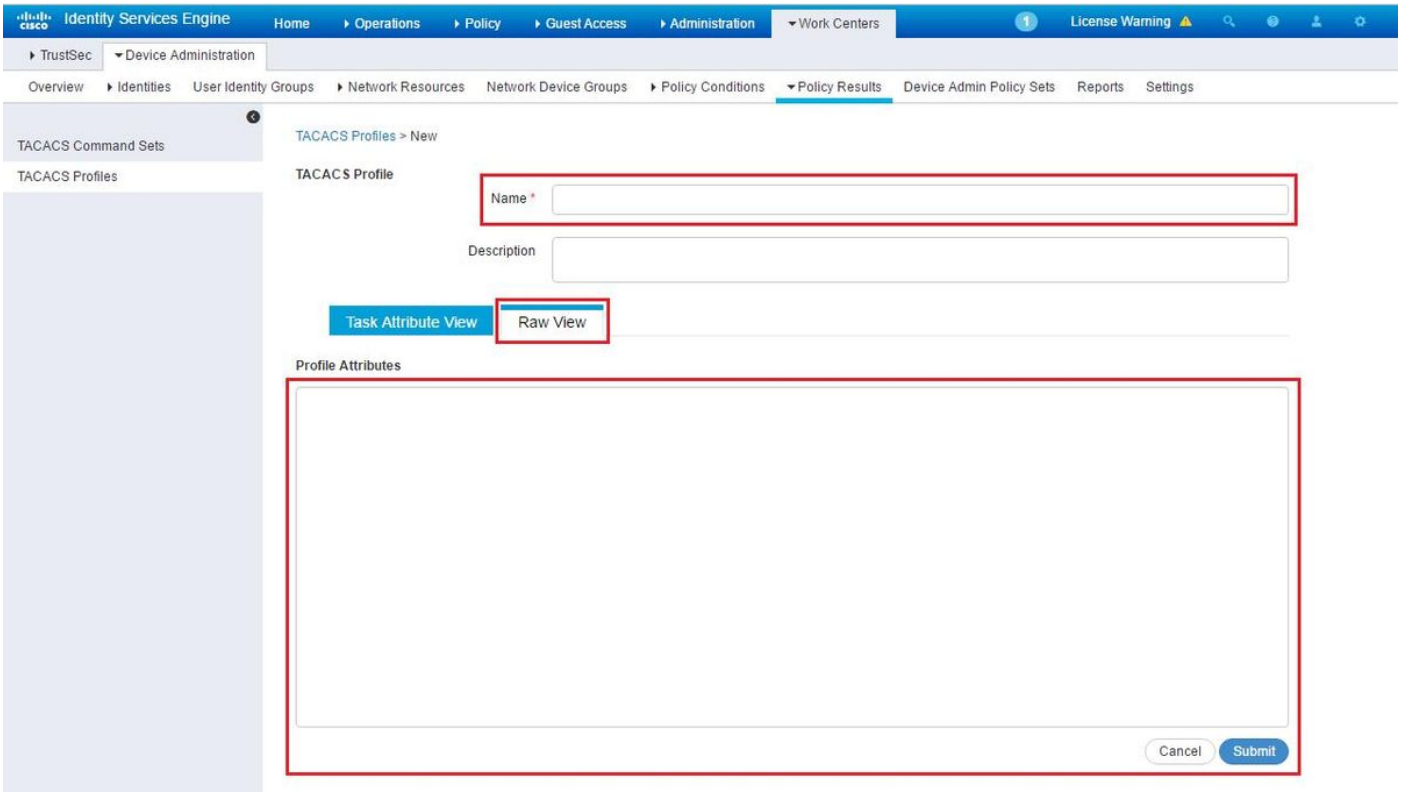
、TACACS および共有秘密にオプションを選択します。 これがオプションであるどんなに承認規則か他の情報を条件としてあとで使用するためにその上にプライム記号に対するデバイスの種類を、とりわけ、追加したい場合もあります。



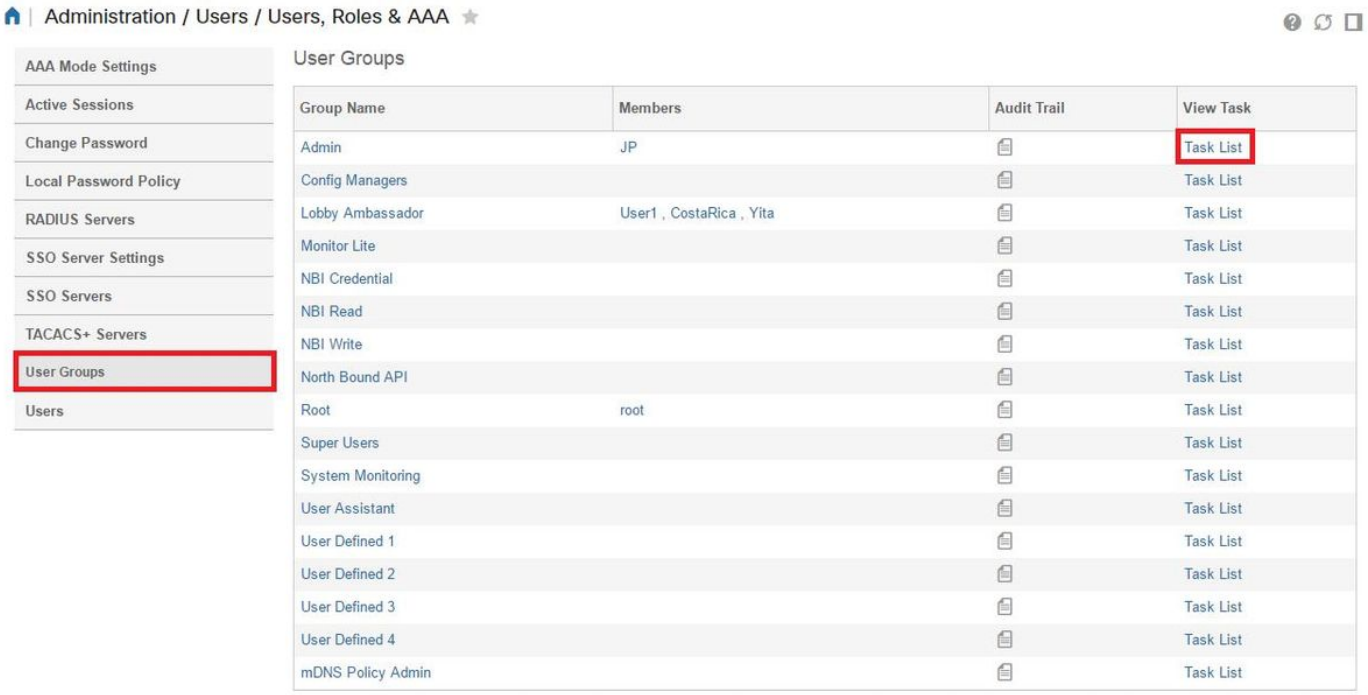
それから ISE からの必須 属性を発動を促すために送信 するように TACACS プロファイルの結果をアクセスの正しいレベルを提供するために作成して下さい。 作業センター/ポリシーへのナビゲートは/Tacacs プロファイル生じ、追加オプションを選択します。



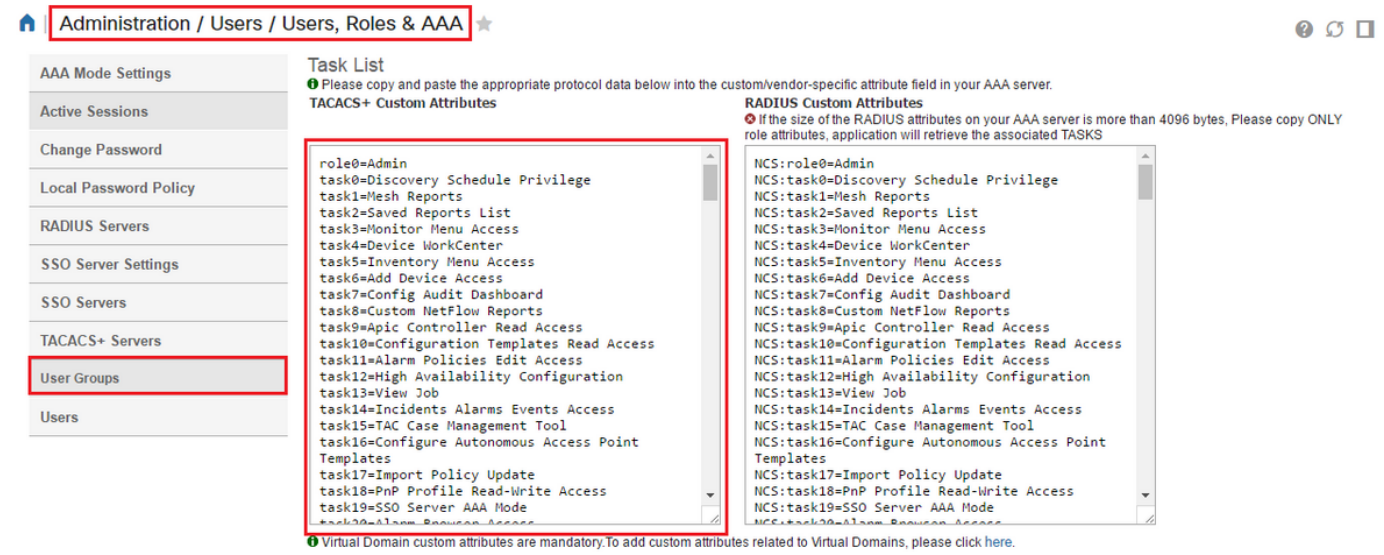
名前を設定し、プロファイル属性ボックスの下で属性を入力するために未加工ビューのオプションを使用して下さい。 属性は概要サーバ自体から来ます。



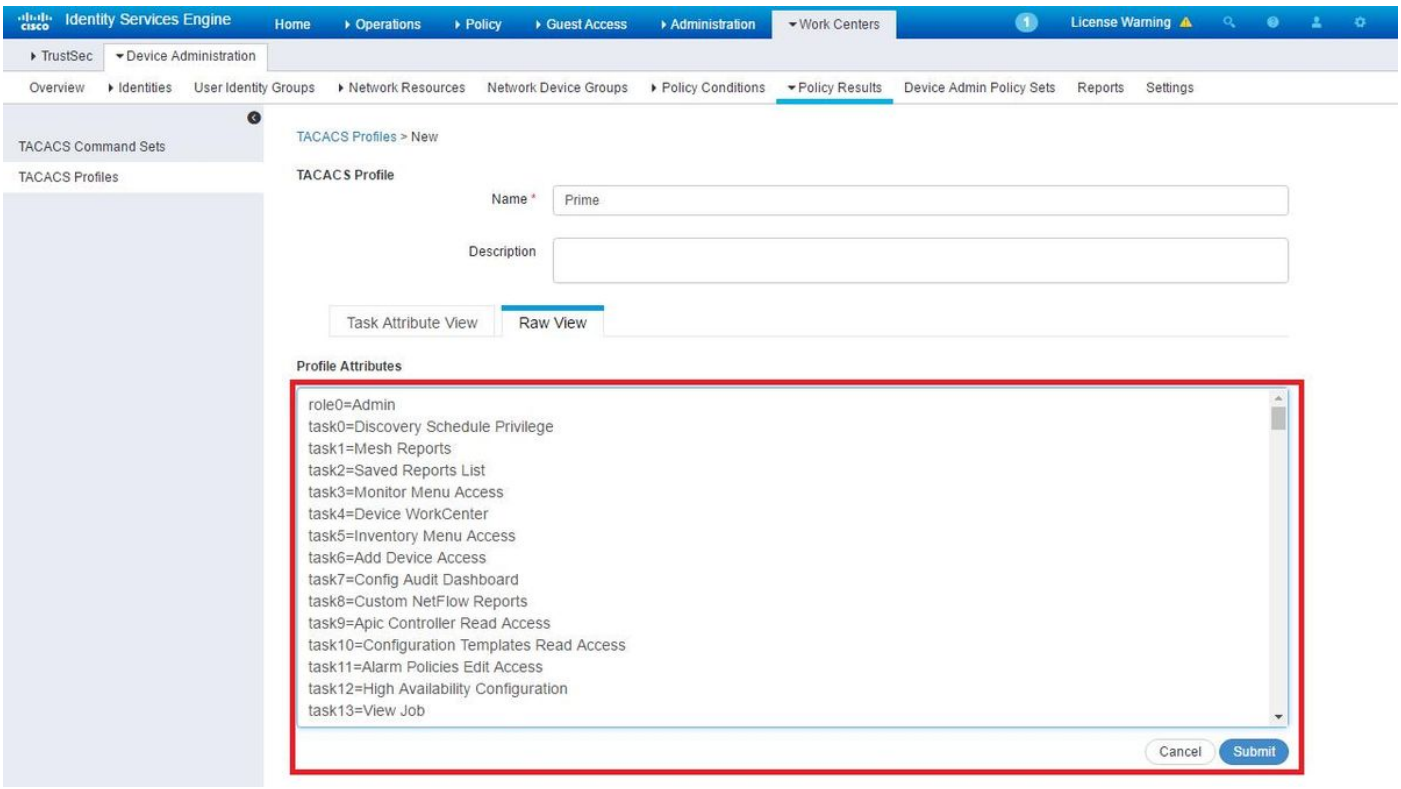
属性を管理/ユーザ ユーザ、役割及び AAA 画面の下で得、ユーザグループ タブを選択して下さい。 提供したいアクセスのグループ レベルを選択します。 この Admin 例で提供されます左側で適切な課業 表の選択によってアクセスして下さい。



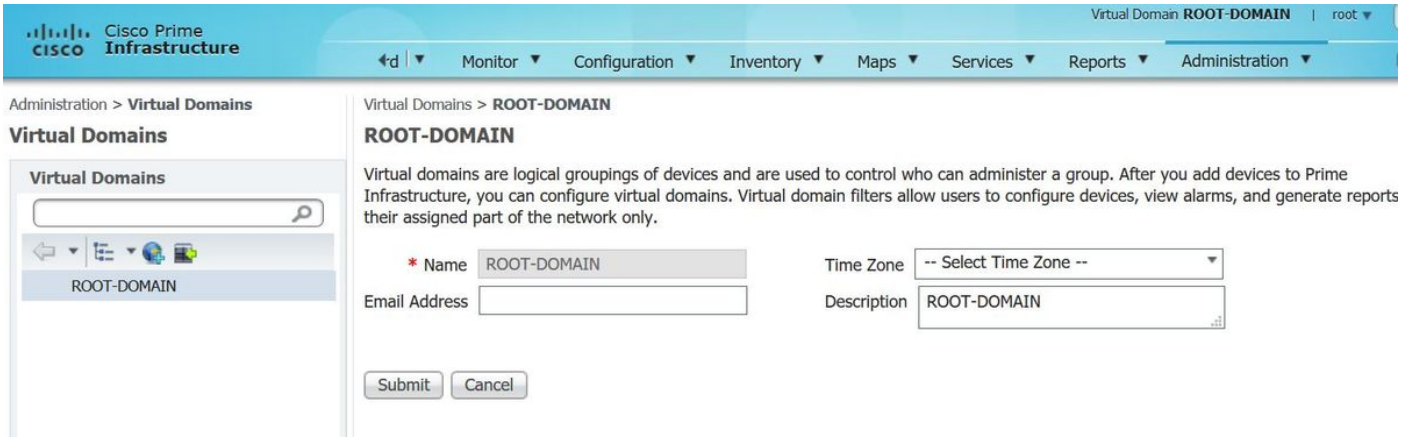
TACACS カスタム属性すべてをコピーして下さい。



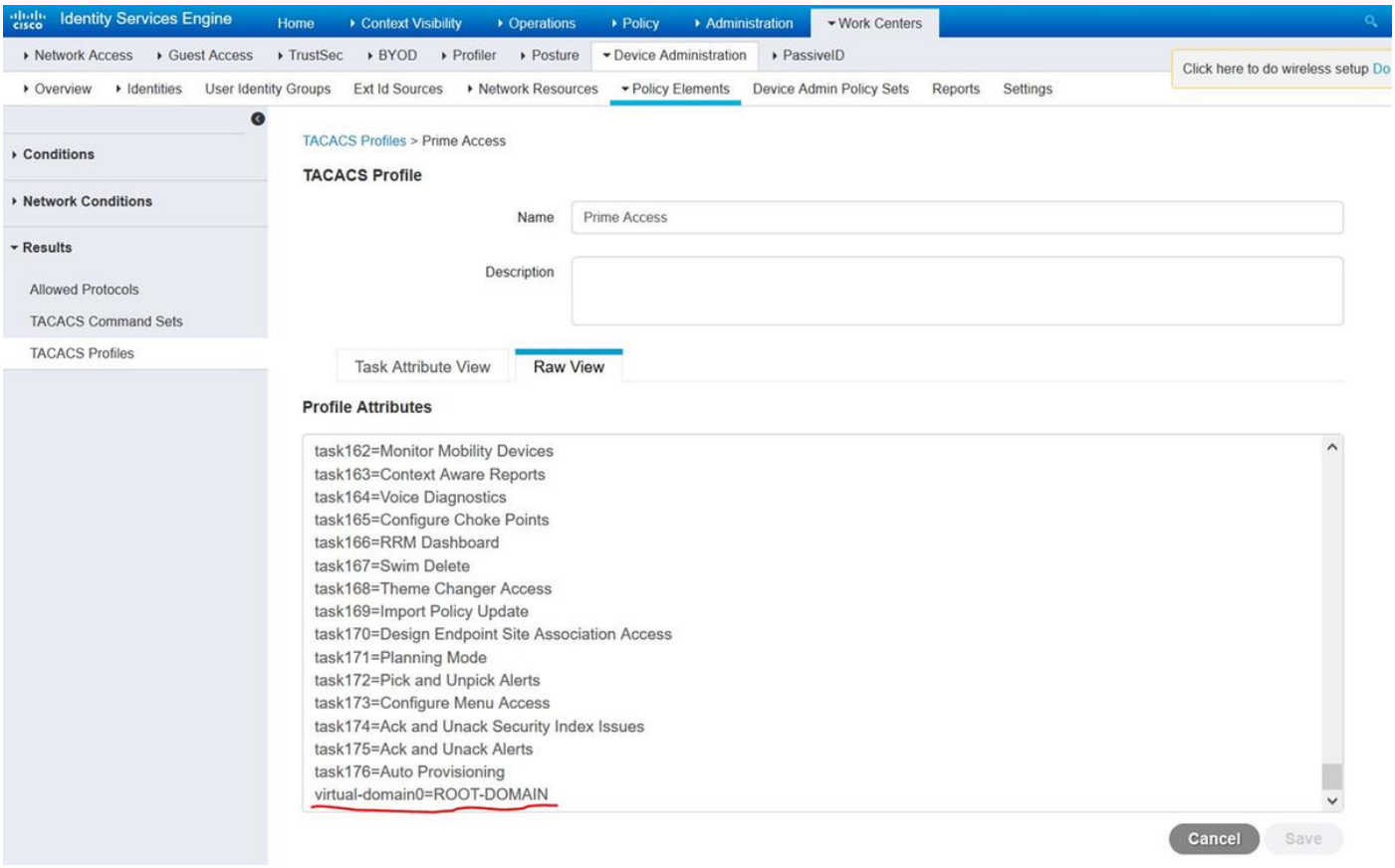
それから ISE のプロファイルの未加エビュー セクションにそれらを貼り付けて下さい。



バーチャル ドメイン カスタム属性は必須です。 ルート ドメイン情報は主な管理の下で- > バーチャル ドメイン見つけることができます。

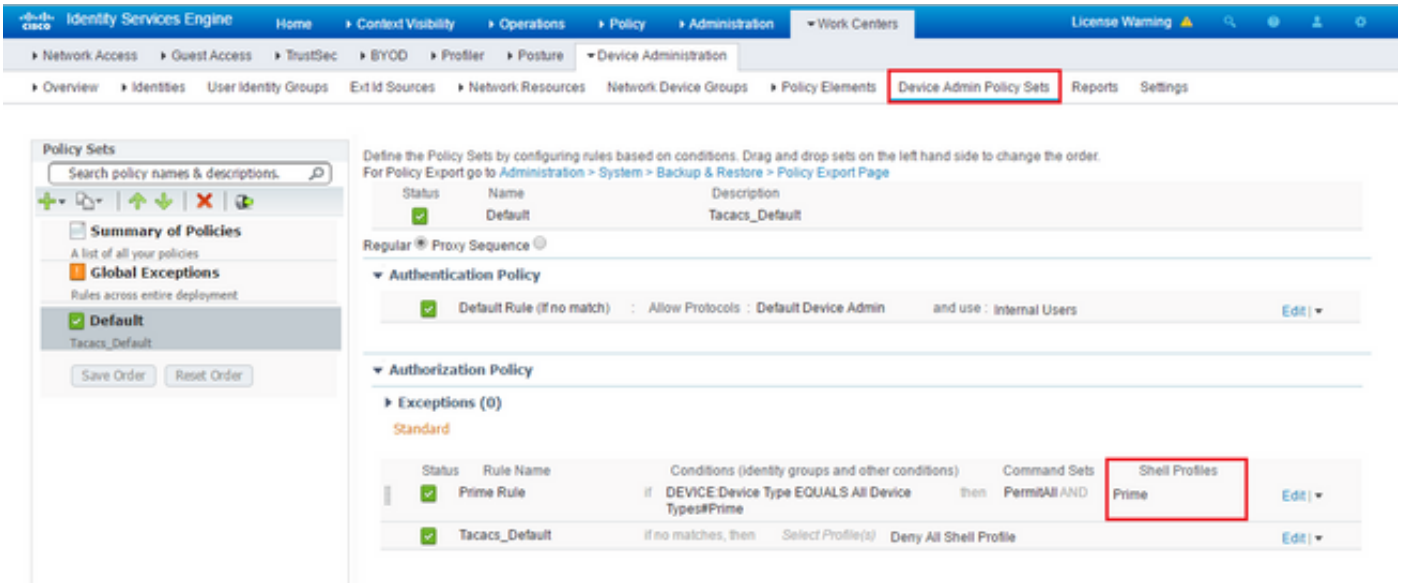


主なバーチャル ドメインの名前は属性 virtual-domain0="virtual ドメイン名として」追加されなければなりません



それがすべてされれば作業センター/デバイス 管理/デバイス Admin ポリシー セットの下で前の手順で、作成されるシェル プロファイルを割り当てるルールを作成するべきですする必要があります

（注：「きちんとこのルール Filters 要求ようにプライム記号の IP アドレスのようなフィルタのプライム記号か別のタイプのために「デバイスの種類」を特に使用することができるどんなに条件」は配置によっての 1 として「調節します」変わります）



この時点で設定は完了したはずです。

トラブルシューティング

この設定が不成功なら、そしてローカル フォール バック オプションがプライム記号のイネーブル、ISE からプライム記号の IP アドレスの削除によって失敗を、強制できます。 これにより ISE は応答し、ローカル信任状の使用を強制します。 ローカル フォールバックがリジェクトで実行されたために設定される場合ローカルアカウントはまだ顧客へのアクセスをはたらかせ、提供します。

ISE が認証の成功を示し、しかし正しいルールを一致すればプライム記号はまだプロファイルで正しく設定される属性を慎重に検査したい場合もある追加属性は送信 されて いません要求を拒否して。