ISE 2.0 およびアルバ WLC でゲスト フローを設定して下さい

目次

概要

このアルバ ワイヤレス LAN コントローラ (WLC) でゲスト ポータルを設定する資料 descrbies ステップ。 サード パーティ ネットワーク アクセスの Identity Services Engine （ ISE) バージョン 2.0 サポートからデバイス (NAD) はもたらされます。 ISE は現在ゲストのためのアルバ ワイヤレスとの統合を、ポスチャ サポートし、あなた自身のデバイス (BYOD) フローを持って来ます。

> **注:** Cisco は他の開発元からのデバイスの設定かサポートに責任がありません。

前提条件

要件

次の項目に関する知識が推奨されます。

- アルバ IAP 設定

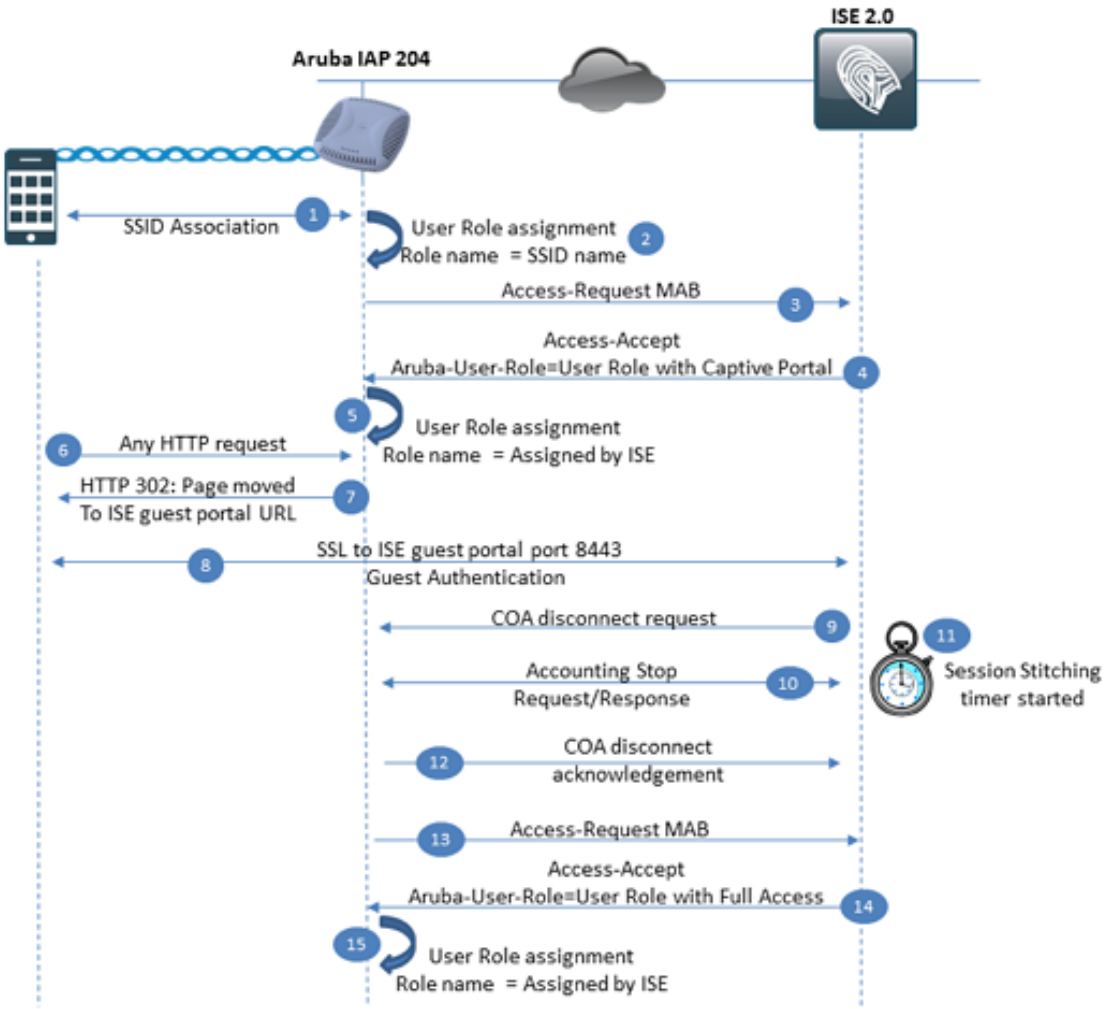
- ISE のゲスト フロー

使用するコンポーネント

- Aruba IAP 204 ソフトウェア 6.4.2.3
- Cisco Identity Services Engine 2.0

背景説明

ゲスト フロー



ステップ 1.ユーザはサービス セット識別子（SSID）に関連付けられます。 SSID は開いたでまたは事前共有キー 認証で設定することができます。

ステップ 2.アルバはこの接続にユーザの役割を適用します。 最初ユーザの役割は SSID 自体常にです。 ユーザの役割は VLAN、アクセス制御制限、捕虜門脈設定等々のような異なる設定が含まれています。 SSID に割り当てられる現在の例デフォルト ユーザの役割で許可すべての文だけ持っています。

ステップ 3. SSID は外部のRADIUSサーバにフィルタリングする MAC を提供するために設定されます。 Radius MAB（MAC 認証バイパス） access-request は ISE に送信 されます。

ステップ 4 ポリシー評価時に ISE はゲストに許可プロファイルを選択します。 この許可プロファ

イルは ACCESS_ACCEPT と等しい名前ユーザの役割のとアルバ WLC（ワイヤレス LAN コントローラ）でローカルで設定される等しいアクセス タイプおよびアルバ ユーザ ロールが含まれています。 このユーザの役割は捕虜門脈のために設定され、トラフィックは ISE の方にリダイレクトされます。

アルバ ユーザの役割

アルバ WLC によって使用する主要なコンポーネントはユーザの役割です。 ユーザの役割は接続の時にユーザに適当なアクセス制限を定義します。 アクセス制限は下記のものを含むことができます: 捕虜門脈リダイレクション、アクセス・コントロール・リスト、VLAN（バーチャル LAN）、帯域幅制限および他。 アルバ WLC の存在にユーザの役割が SSID 名前と等しいデフォルト ユーザの役割がある各 SSID は既定のロールから、仕様 SSID に接続されるすべてのユーザ最初に制限を得ます。 ユーザの役割は RADIUSサーバによってこの場合 Access-Accept はずですアルバ ベンダ別の属性アルバ ユーザ ロールが含まれている上書きすることができます。 WLC によってこの属性からの値がローカル ユーザの役割を見つけるのに使用されています。

ステップ 5 によって属性ローカルでアルバ ユーザ ロールの WLC チェック設定されたユーザの役割のために必須 1 つを適用し。

ステップ 6.ユーザはブラウザの HTTP 要求を始めます。

ステップ 7.捕虜ポータルのために設定されるユーザの役割が理由でアルバ WLC 切片要求。 この要求 WLC への応答が新しい場所として ISE ゲスト ポータルと移動する HTTP コード 302 ページを戻すように。

ステップ 8.ユーザはポート 8443 の ISE への SSL 接続を確立し、ゲスト ポータルの username/password を提供します。

ステップ 9. ISE はアルバ WLC に COA Disconnect 要求メッセージを送ります。

ステップ 10 接続は Radius アカウンティング要求（停止）メッセージを使用して終える必要があること COA 接続解除メッセージ WLC がユーザが付いている接続を破棄した、ISE を知らせる後。 ISE はこのメッセージがアカウンティングと受け取られたことを確認しなければなりません。

ステップ 11. ISE はセッション ステッチ タイマーを開始します。 このタイマーが COA の前後にセッションを一括してバインドするのに使用されています。 この時間の間に ISE はユーザ名、先祖などのようなすべてのセッション パラメータを覚えています 第 2 認証の試みはクライアントに正しい承認ポリシーを選択するためにこのタイマーが切れる前にする必要があります。 タイマーが切れれば、新しい Access-Request が全く新しいセッションとして解読され、ゲスト リダイレクトの承認ポリシーが再度適用されれば。

ステップ 12 アルバ WLC は COA 接続解除確認応答を用いる以前に受け取った COA Disconnect 要求を確認します。

ステップ 13 アルバ WLC は新しい MAB Radius Access-Request を送信 します。

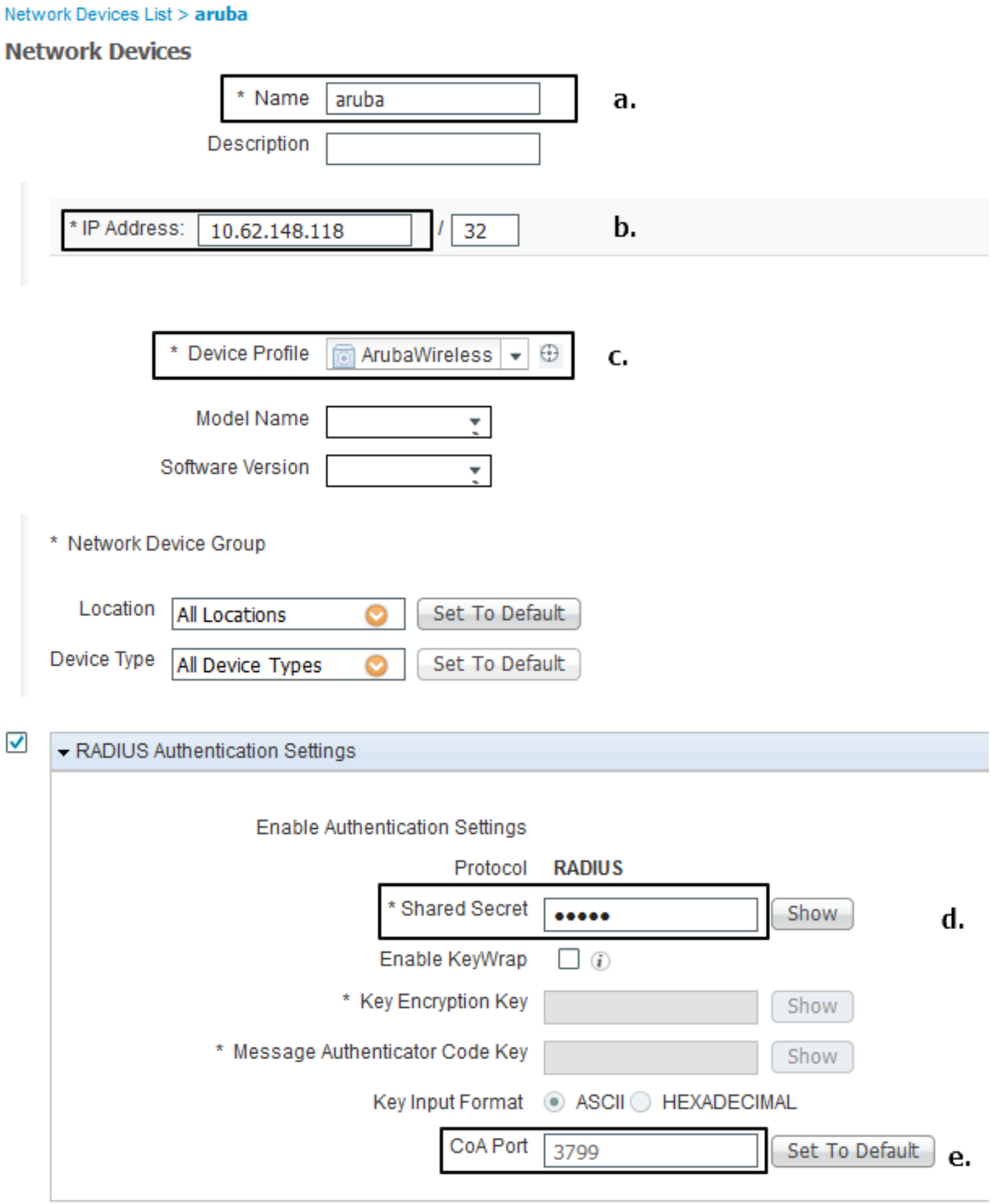
手順 14： ポリシー評価時に ISE は認証の後でゲストに許可プロファイルを選択します。 この許可プロファイルは ACCESS_ACCEPT と等しい名前ユーザの役割のとアルバ WLC でローカルで設定される等しいアクセス タイプおよびアルバ ユーザ ロールが含まれています。 割り当てに設定されるこのユーザの役割すべてのトラフィック。

手順 15： 属性アルバ ユーザ ロールは WLC によってローカルで設定されたユーザの役割をチェックし、必須 1 つを適用します。

設定

ステップ 1. ISE の NAD としてアルバ WLC を追加して下さい。

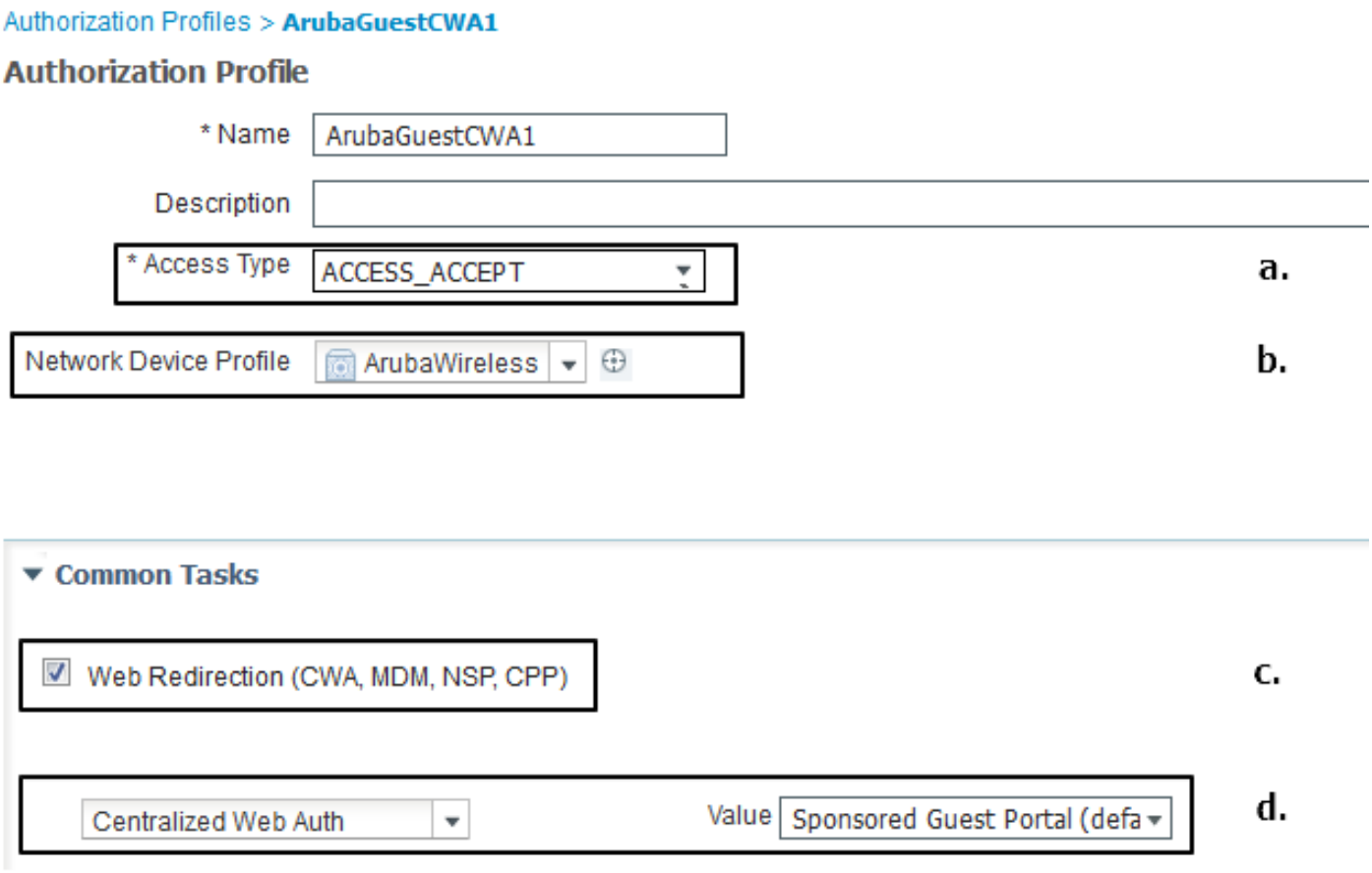
Administration > ネットワークリソース > ネットワークデバイスにナビゲート し、『Add』 をクリック して下さい

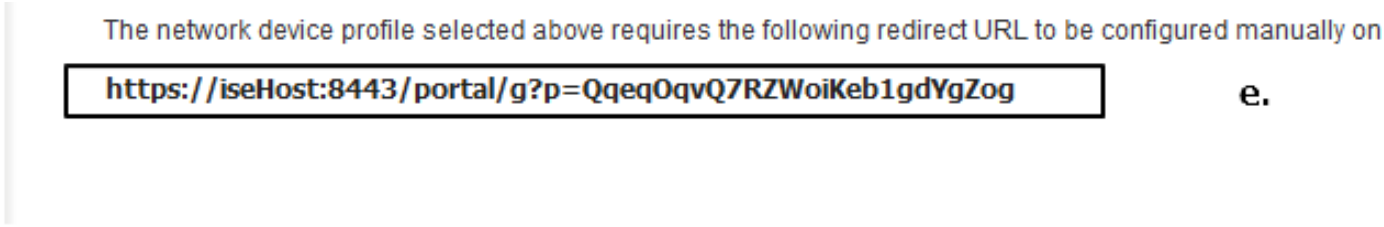


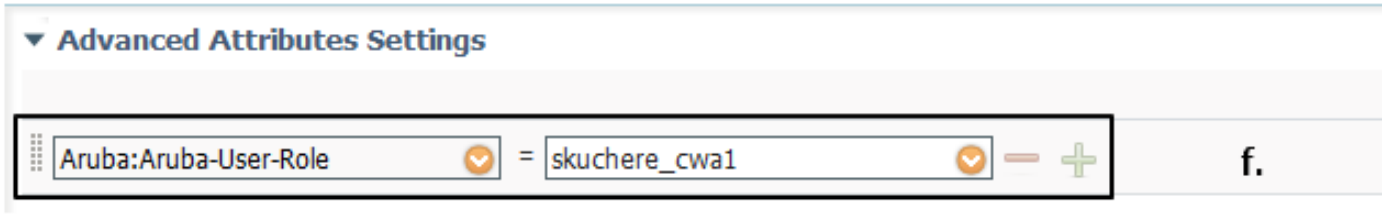
1. ネットワーク アクセス デバイス（NAD）名前をつけて下さい。
2. NAD IP アドレスを規定 して下さい。
3. ネットワークデバイス プロファイルを選択して下さい。 アルバ WLC に関しては組み込みプロファイル ArubaWireless を使用することができます。
4. 事前共有キーを提供します。
5. COA ポートを、Device 形式 COA のための現在の例使用 UDP ポート 3799 定義して下さい。

ステップ 2.許可プロファイルを設定して下さい。

ポリシー > ポリシー要素 > 結果 > 許可 > 許可プロファイルにナビゲート し、『Add』 をクリック して下さい。 最初にイメージに示すように中央 Web 認証（CWA）リダイレクトのための許可プロファイルを、作成しなければなりません。



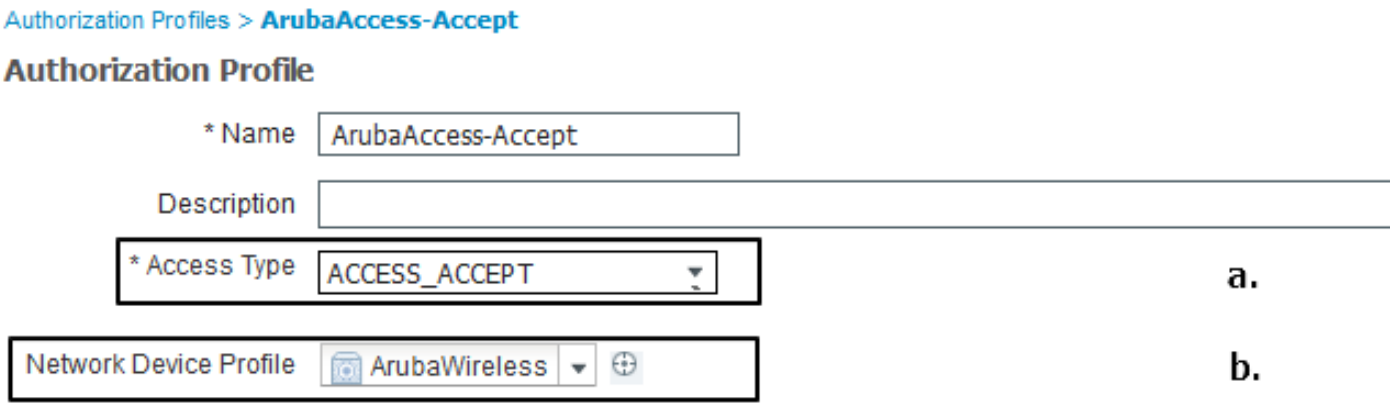


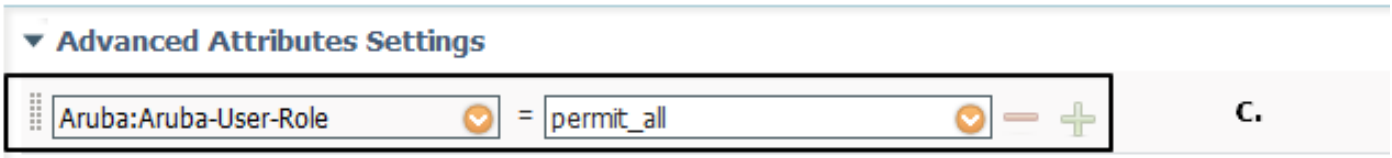


注: デフォルトですべての許可プロファイルに Cisco と等しいネットワークデバイス型があります。 NAD 自体が ArubaWireless で設定され、許可がその他のデバイス型のためにプロファイル作成されれば、このプロファイルはこのデバイスのために決して一致しません。

1. **Access-Accept** と**アクセス タイプを**定義して下さい。
2. ネットワークデバイス **プロファイル**で **ArubaWireless を**選択して下さい。
3. 一般的なタスク セクションでは、**Web リダイレクション** オプションを有効に して下さい。
4. リダイレクション型が**中央集中型 Web Auth を**選択し、リダイレクションのために使用するために望むポータルを『guest』 を選択 するので。
5. ISE 提供が外部捕虜ポータル URL とアルバ WLC で定義する必要があること URL。
6. **高度属性**では**設定は**アルバ属性値 ユーザの役割の区分しましたり、定義します。

第 2 許可プロファイルは門脈認証の後でゲストユーザ向けにアクセスを提供するために作成する必要があります:





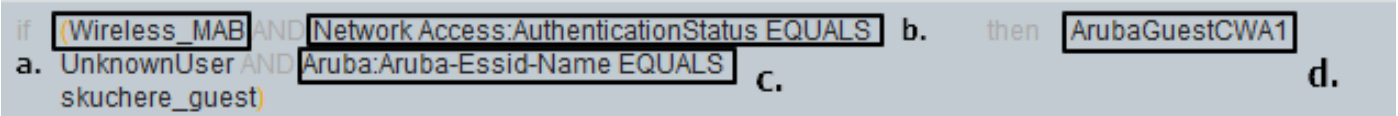
1. **Access-Accept** と**アクセス タイプを**定義して下さい。
2. **ネットワークデバイス プロファイル**で **ArubaWireless** を選択して下さい。
3. **高度属性設定**セクションでアルバ属性値 ユーザの役割の定義して下さい。 あとで同じ名前でアルバ WLC のローカル ユーザの役割を設定します。

ステップ 3.承認ポリシーを設定して下さい。

最初承認ポリシーはゲスト ポータルにユーザ リダイレクションに責任があります。 最も簡単なケースでは、複合条件（COBOL）で構築されて使用できます

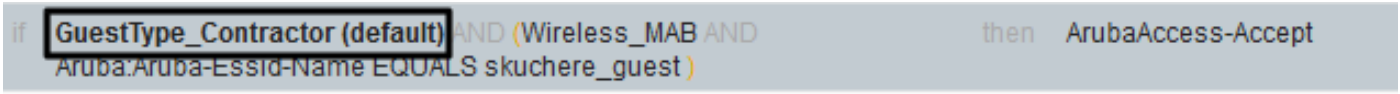
- Wireless_MAB （a.）
- 未知のユーザ（b.）へのネットワーク アクセス AuthenticationStatus 等号
- ゲスト SSID 名前（c.）と等しいアルバ アルバ Essid 名前。

このポリシーに関しては、その結果ゲスト ポータルにリダイレクトで許可プロファイルを設定して下さい（D.）

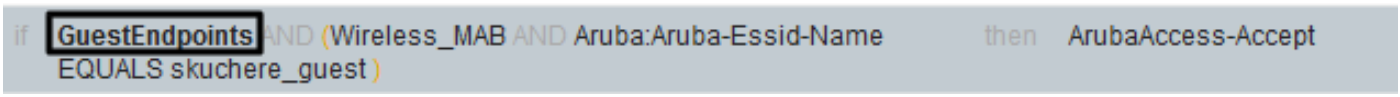


第 2 承認ポリシーはポータルによって認証の後でゲストユーザ向けにアクセスを提供する必要が

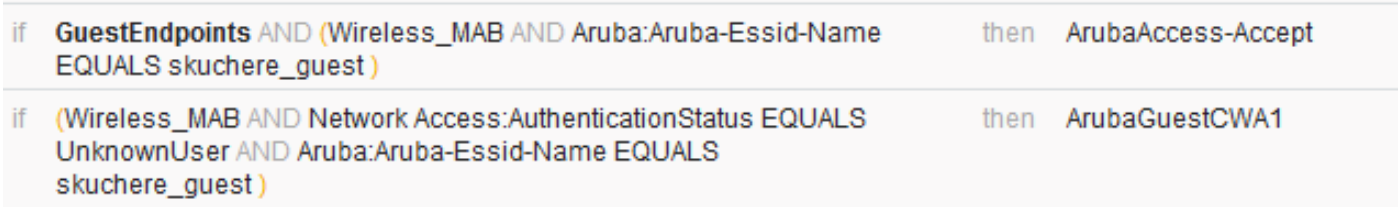
あります。 このポリシーはセッションデータ（ユーザ識別グループ/使用例ゲスト フロー等）に頼ることができます。 このシナリオでユーザはセッション ステッチ タイマーが切れる前に再接続する必要があります:



あなた自身をセッション ステッチ タイマー期限切れから保護するためにセッションデータの代りにエンド ポイント データに頼ることができます。 デフォルトで、ISE 2.0 の後援されたゲスト ポータルは自動ゲスト デバイス登録のために設定されます（ゲスト デバイスは Guest_Endpoints エンド ポイント識別グループで自動的に配置されます）。 このグループは状態として使用することができます:

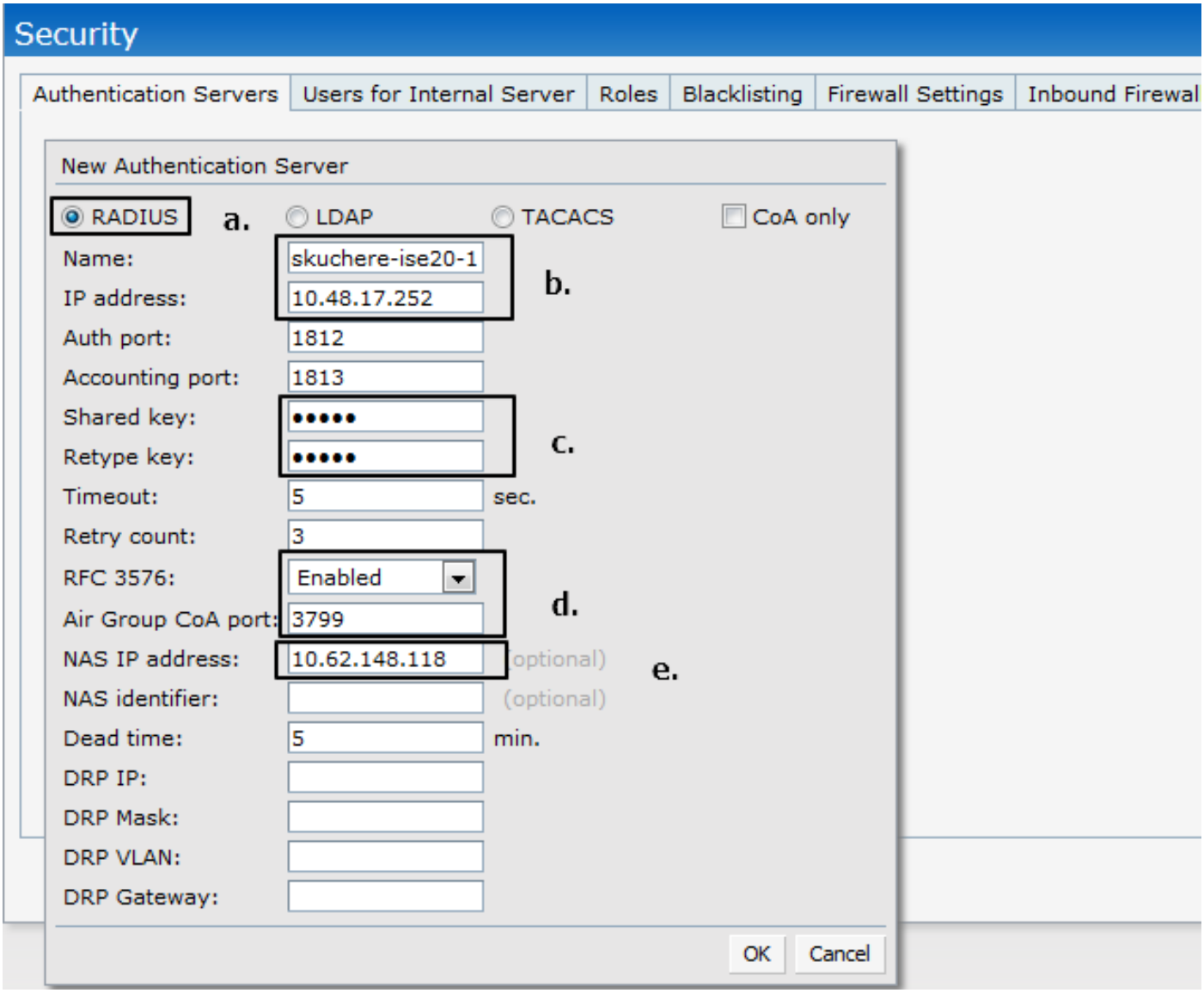


正しい順序で承認ポリシー:



ステップ 4.アルバの RADIUSサーバを設定して下さい。

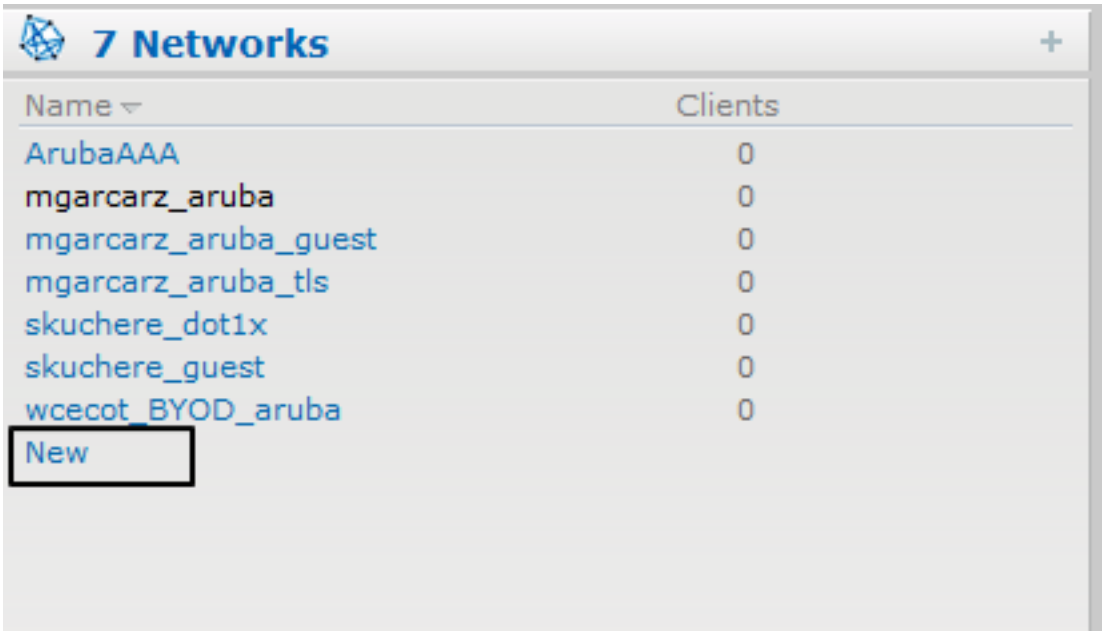
Security > Authentication サーバへのナビゲートは『New』 をクリック し、:



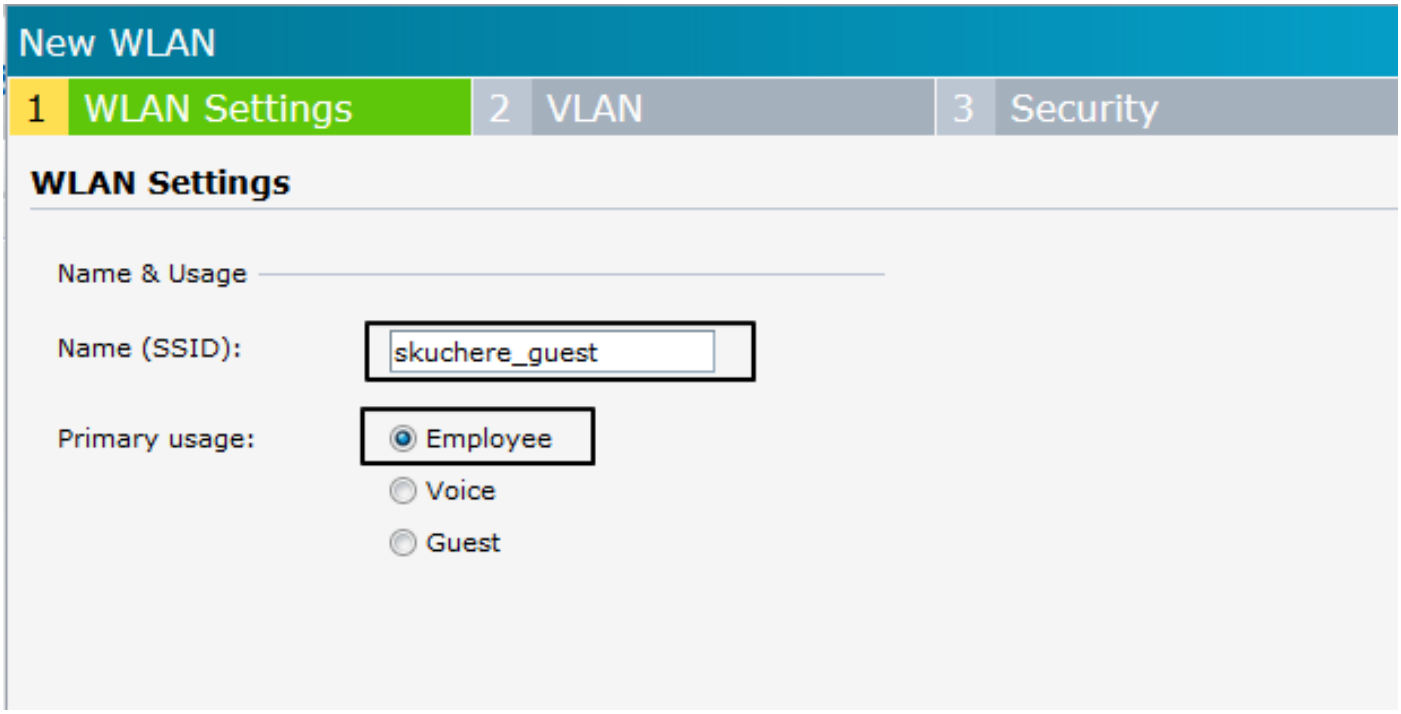
1. AAAプロトコルとして『RADIUS』 を選択 して下さい。
2. AAAサーバ名前および IP アドレスを定義して下さい。
3. 事前共有キーを規定 して下さい。
4. RFC 3576 サポートをイネーブルにし、COA ポートを定義して下さい。
5. NAS IP アドレスとしてアルバ WLC マネージメントインターフェイス IP を規定 して下さい。

ステップ 5.アルバのゲスト SSID を作成して下さい。

ダッシュボード ページでネットワークリストの端に『New』 を選択 して下さい。 SSID 作成ウィザードは開始する必要があります。 ウィザードの手順に従って下さい。

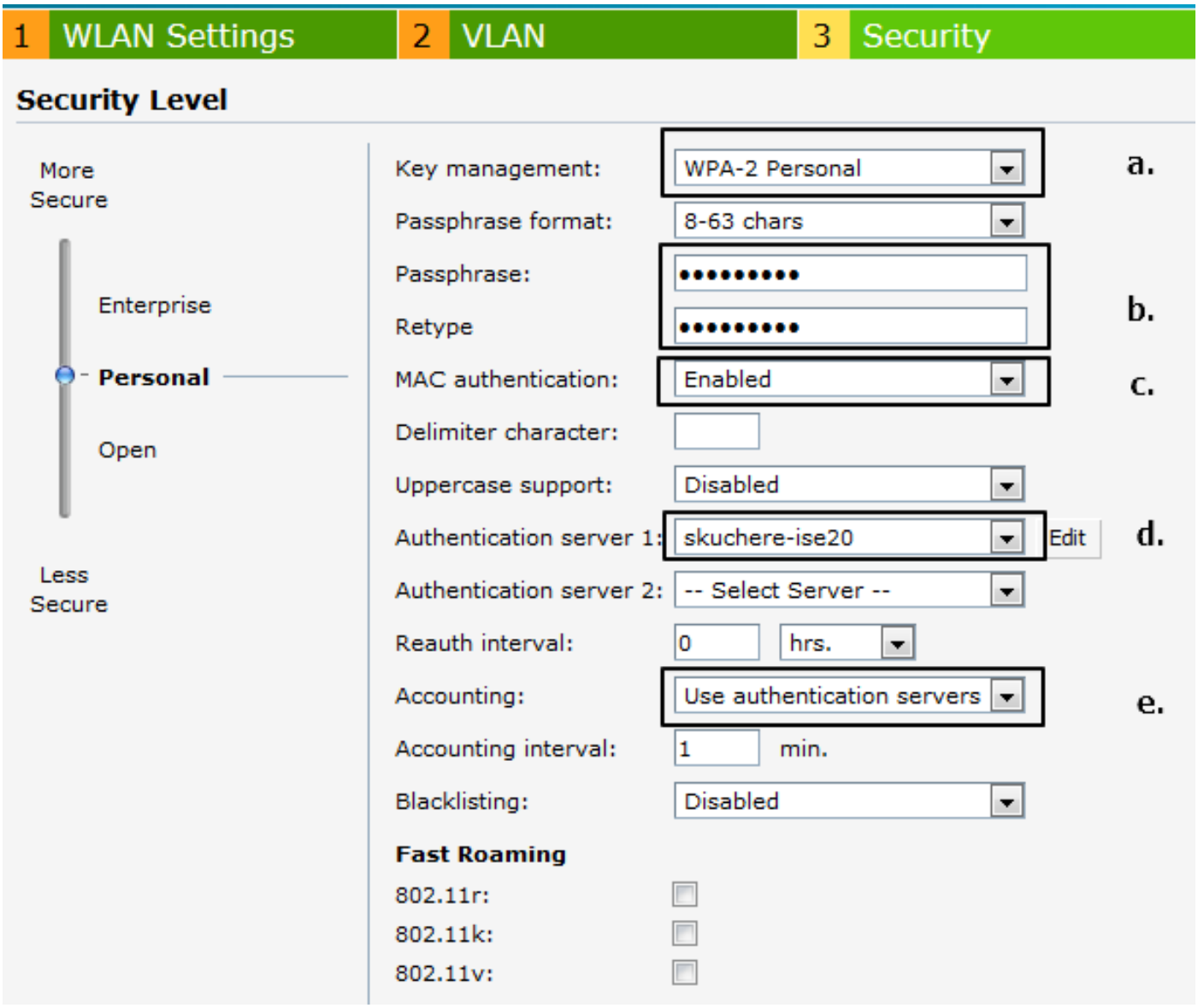


ステップ 1. SSID 名前を定義し、型を『SSID』 を選択 して下さい。 ここでは、SSID 型従業員は使用されます。 この SSID 型に割り当てとの既定のロールすべておよび捕虜門脈適用がありません。 また、ゲストを『Type』 を選択 することができます。 そのようなシナリオで SSID 設定の間に捕虜門脈設定を定義する必要があります。



ステップ 2. VLAN および IP アドレス割り当て。 ここでは、設定はイメージに示すようにデフォルトとして、残っています。

ステップ 3.セキュリティ設定。 ゲスト SSID の場合または個人的『Open』 を選択 することができます。 個人的前断片キーを必要とします。



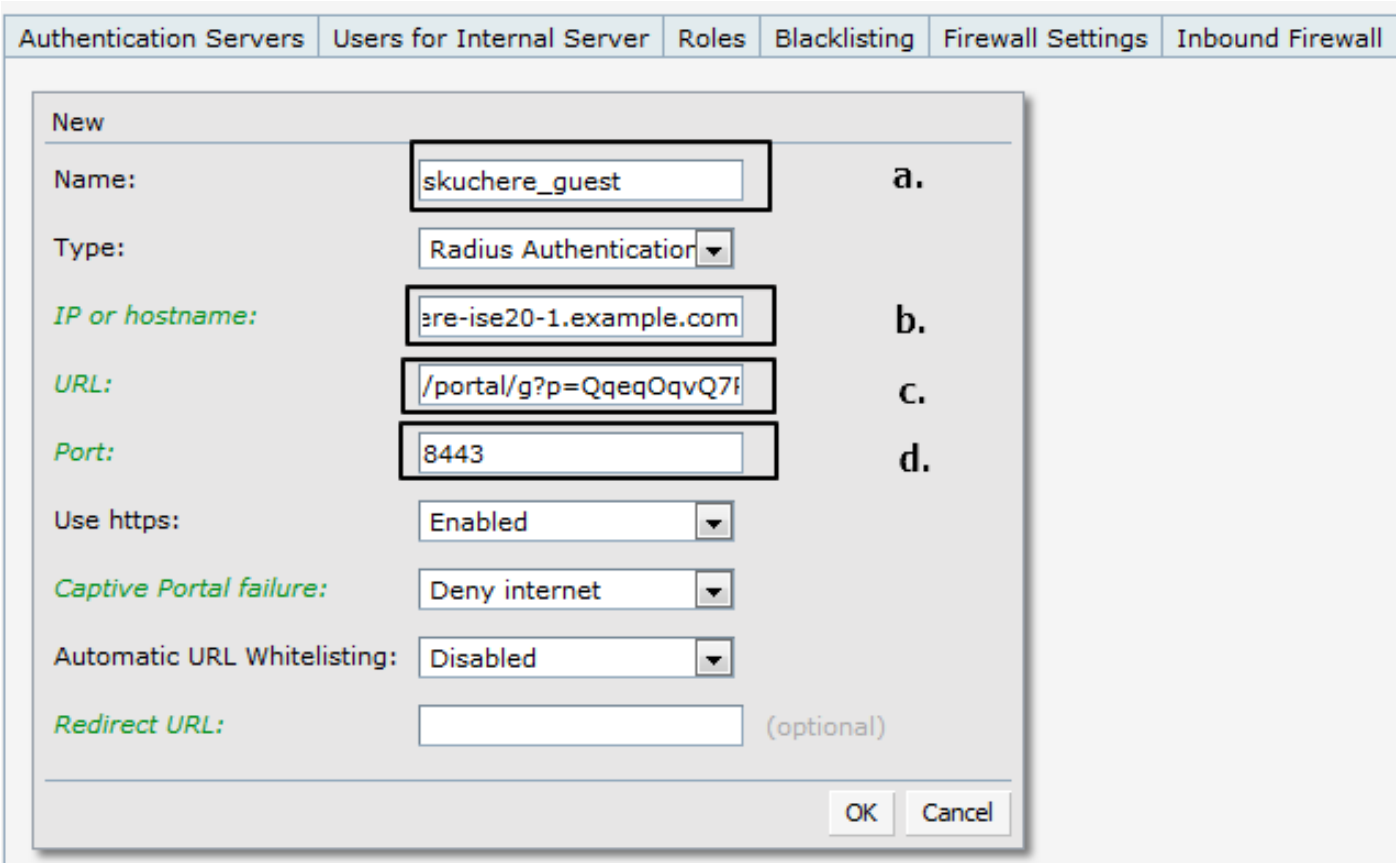
1. キー管理 メカニズムを選択して下さい。
2. 事前共有キーを定義して下さい。
3. ユーザをイネーブルになられている MAB MAC フィルタリング必要を使用して ISE に対して認証するため。
4. 認証サーバ リストで AAAサーバを選択して下さい。

5. 以前に定義された AAAサーバの方のアカウンティングをイネーブルにするためにドロップダウン リストの使用認証サーバを選択して下さい。

注: アカウンティングは三番目の一部 NADs と重大です。 ポリシー Service Node（PSN）が NAD からユーザ向けのアカウンティング停止を受け取らない場合、セッションは開始された状態にはまり込むかもしれません。

ステップ 6.捕虜ポータルを設定して下さい。

> 外部捕虜ポータルはセキュリティにナビゲート し、イメージに示すように新しいポータルを、作成します:



ステップ 1.捕虜門脈名前を規定 して下さい。

Steo 2.は ISE FQDN か IP アドレスを定義します。 IP アドレスを使用する場合、ようにゲストポータル証明書の Name（SAN）認証対象代替フィールドで定義されるこの IP して下さい。

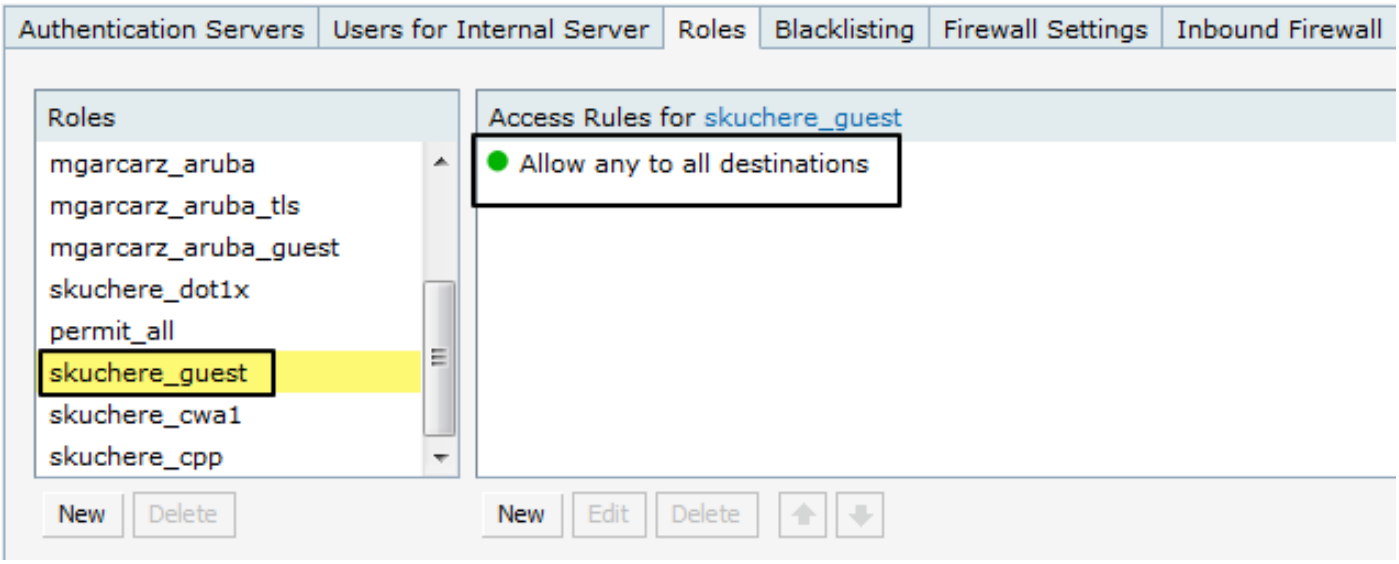
注: PSN サーバを使用するユーザは MAB が起こったサーバに常にリダイレクトする必要があります。 通常 SSID で設定された RADIUSサーバの FQDN を定義しなければなりません。

ステップ 3. ISE 許可プロファイルからのリダイレクトを提供します。 ポート番号の後に部品をここに置く必要があります

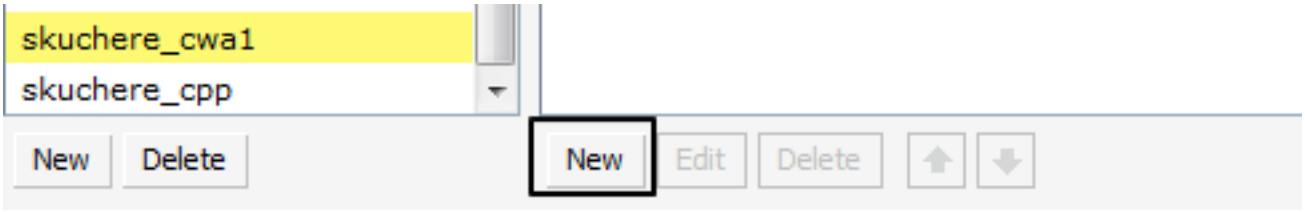
ステップ 4. ISE ゲスト ポータル ポートを定義して下さい。

ステップ 7.ユーザの役割を設定して下さい。

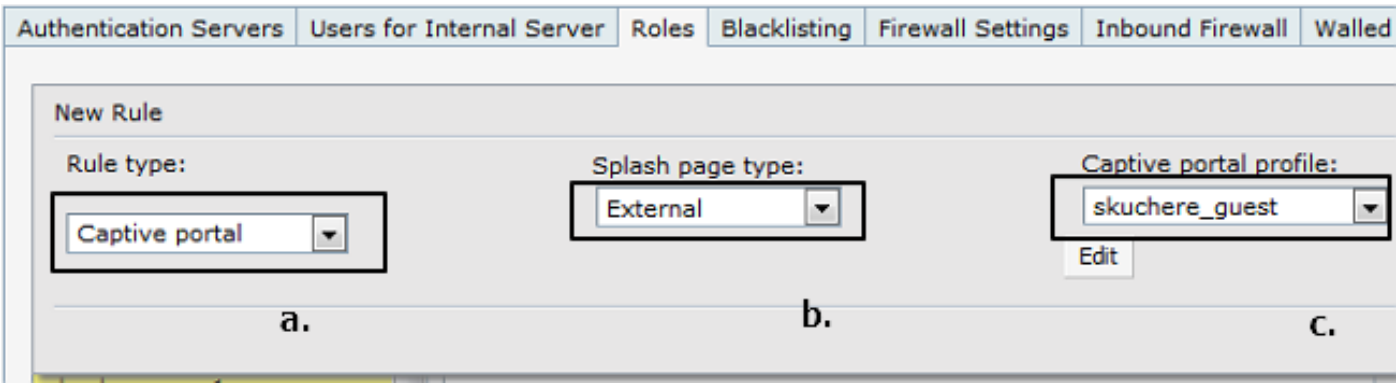
セキュリティ > ロールへのナビゲート。 SSID が作成された後、同じ名前の新しいロールはすべての宛先にアクセス規則割り当てが付いているリストにあることを確認して下さい。 さらに、2 つのロールを作成して下さい: CWA リダイレクトと二番目にゲスト ポータルの認証の後の割り当てアクセスのための 1 つ。 これらのロールの名前は ISE 許可プロファイルで定義されるアルバユーザの役割と同一であるはずです。



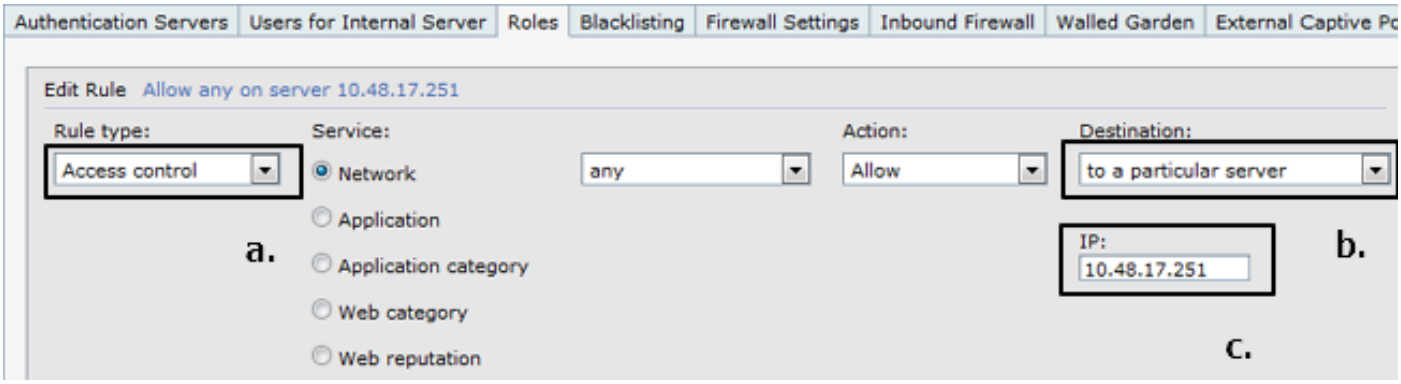
イメージに示すように、リダイレクトのための新規 ユーザ ロールを作成し、セキュリティ制限を追加して下さい。



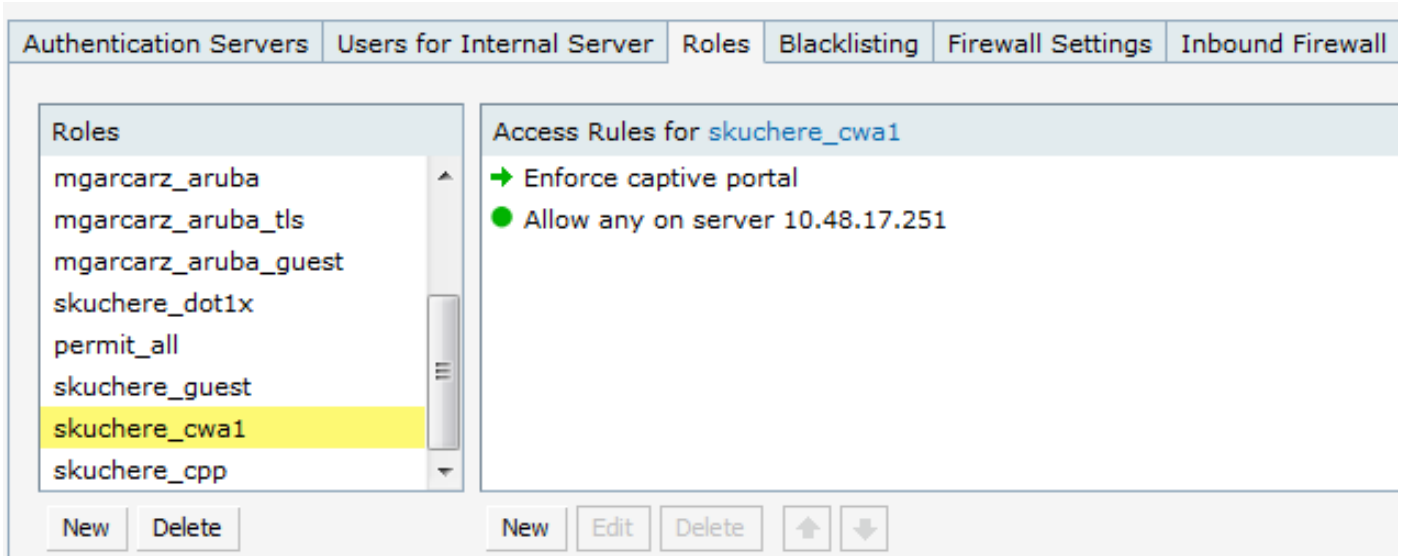
最初制限に関しては定義する必要があります:



第 2 制限に関しては定義する必要があります:

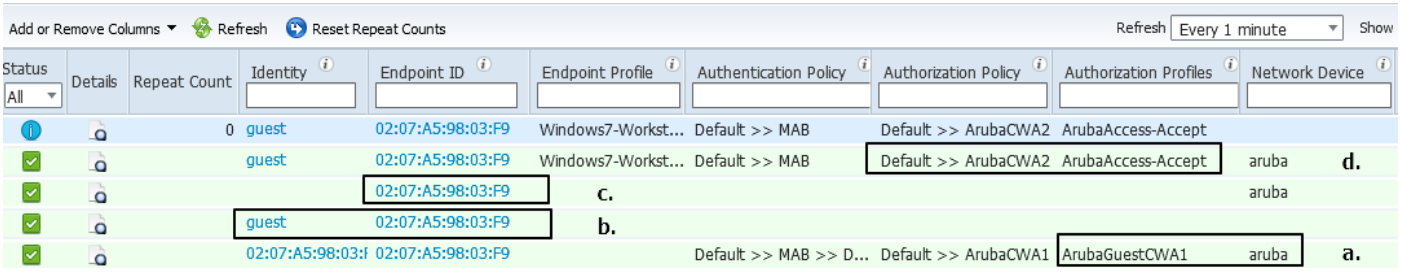


イメージに示すように、すべての宛先へのデフォルトのルール許可は削除することができます。これは設定ロールのの概要結果です。



確認

ISE **オペレーション > Radius Livelog** のゲスト フローの例。



1. 捕虜ポータルがあるユーザの役割および CWA リダイレクトの最初 MAB におよびその結果、許可プロファイル アルバ側で設定しました。
2. ゲスト認証。
3. 許可（CoA）の正常な変更。
4. 割り当てがアルバ側のすべてのルールある割り当てアクセスおよびユーザの役割の第 2 MAB およびその結果許可プロファイル。

アルバ側で認証の結果として**示しますクライアントに**ユーザが接続されるようにするコマンドを、IP アドレス割り当てられ、訂正しますユーザの役割を割り当てられます使用できます:

```
04:bd:88:c3:88:14# show clients

Client List
-----------
Name              IP Address    MAC Address        OS     Network        Access Point       Channel  Type  Role
----              ----------    -----------        --     -------        ------------       -------  ----  ----
02-07-A5-98-03-F9  10.62.148.77  02:07:a5:98:03:f9  Win 7  skuchere_guest  04:bd:88:c3:88:14  11       GN    skuchere_cwa1
Number of Clients   :1
Info timestamp      :92552
```

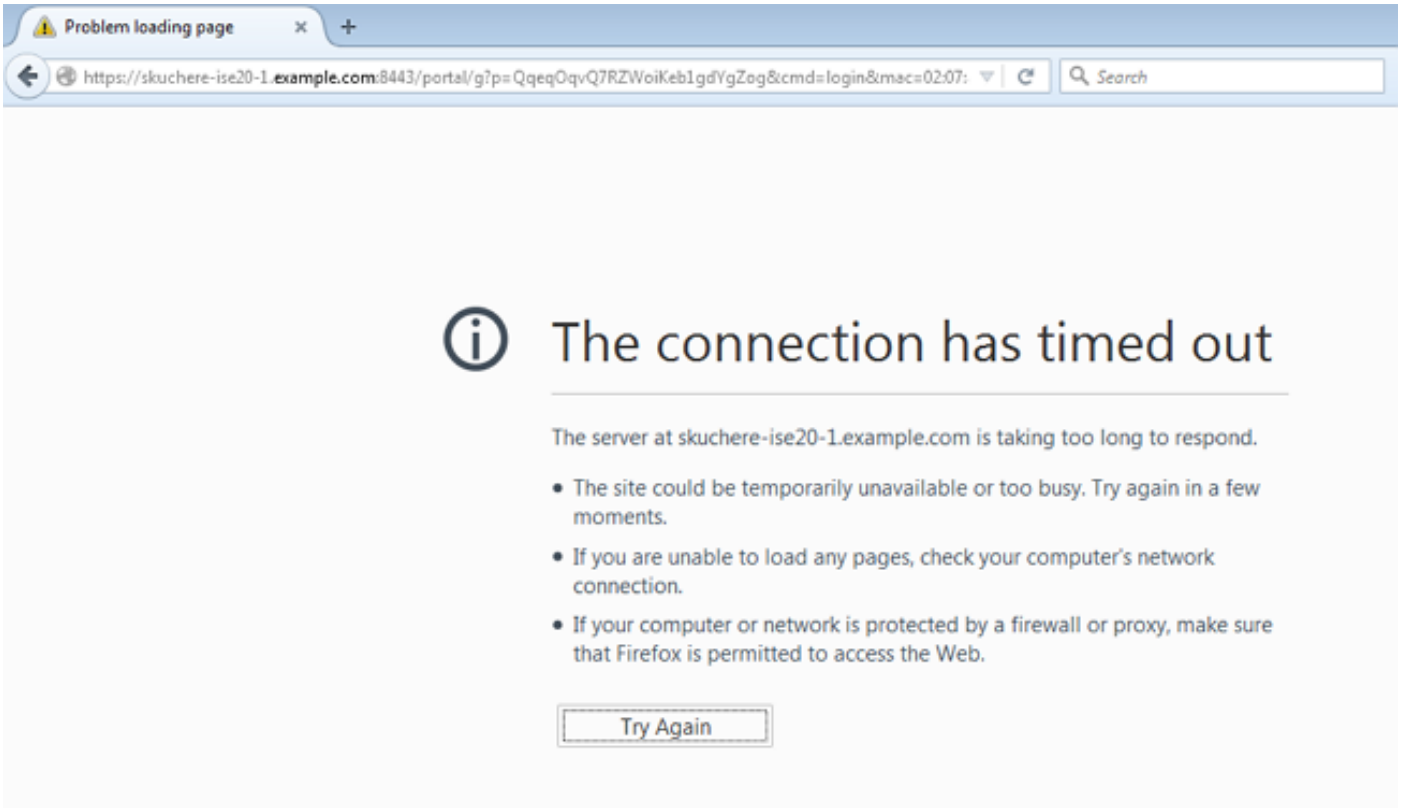
トラブルシューティング

壊れる COA

ISE 設定では、アルバ NAD が ISE 側の正しいネットワークデバイス型で設定され、COA が NAD 設定でポート正確に定義されるようにして下さい。 アルバ側面で RFC 3576 が認証サーバ設定でイネーブルになり、COA がポート正確に定義されるようにして下さい。 ネットワークの観点から UDP ポート 3799 が ISE とアルバ WLC の間で許可されることを確認して下さい。

問題をリダイレクトして下さい

ユーザはブラウザの ISE URL を見ますが、ISE ページはイメージに示すように、表示されません :

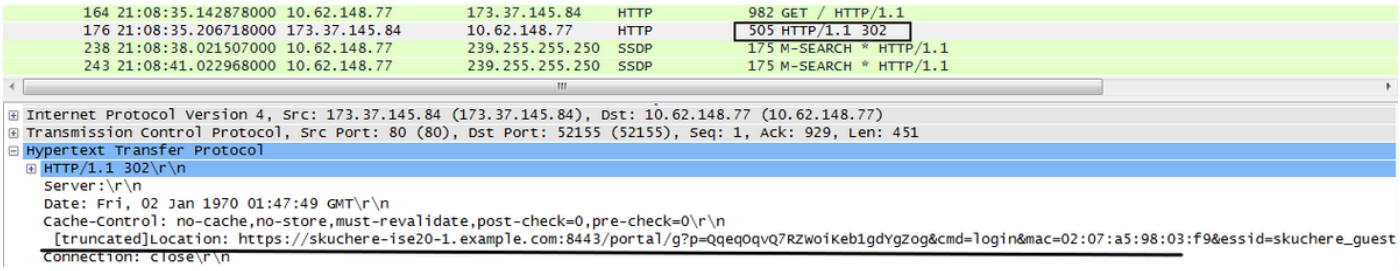


ユーザサイドで ISE FQDN が IP を訂正することを問題なく解決することができるようにして下さい。 アルバせき板 ISE URL がアクセス制限 ユーザの役割のので許可される ISE の方の捕虜門脈設定およびトラフィックで正確に定義されること。 また捕虜門脈設定の SSID および ISE PSN の RADIUSサーバが同じデバイスであることを確認して下さい。 ネットワークの観点から TCPポート 8443 がユーザ セグメントから ISE への許可されることを確認して下さい。

ユーザ ブラウザのリダイレクション URL 提供無し

ユーザサイドで各 HTTP 要求アルバ WLC の結果が ISE URL と移動する HTTP コード 302 ペー

ジを戻すようにようにして下さい。



切れるセッション ステッチ タイマー

この問題の一般的な症状はユーザがゲスト ポータルへの二回目の間リダイレクトされることです。 この場合 CWA の第 2 認証許可プロファイルのための COA が再度選択された後ことが ISE Radius Livelog でわかるはずです。 アルバ側で、実際のユーザの役割をの助けによって**示します クライアントに**コマンドをチェックして下さい。

この問題のための回避策が正常なゲスト認証の後で接続のために ISE のエンド ポイントによって基づく承認ポリシーを使用するかもしれないように。