ISE ゲストの一時および永続的なアクセスの設定

目次

概要

この資料は Identity Services Engine （ISE）ゲスト アクセス設定用の異った方法を記述したものです。 承認規則の異なる条件に基づく:

- ネットワークへの常置アクセスは提供することができます（それに続く認証のための要件無し）
- ネットワークへの一時アクセスは提供することができま（セッションが切れた後ゲスト認証を必要とします）

またセッション削除のための特定のワイヤレス LAN コントローラ（WLC）動作は一時アクセスシナリオの影響に沿って示されます。

前提条件

要件

次の項目に関する知識が推奨されます。

- ISE の導入およびゲスト フロー
- ワイヤレス LAN コントローラ（WLC）の設定

使用するコンポーネント

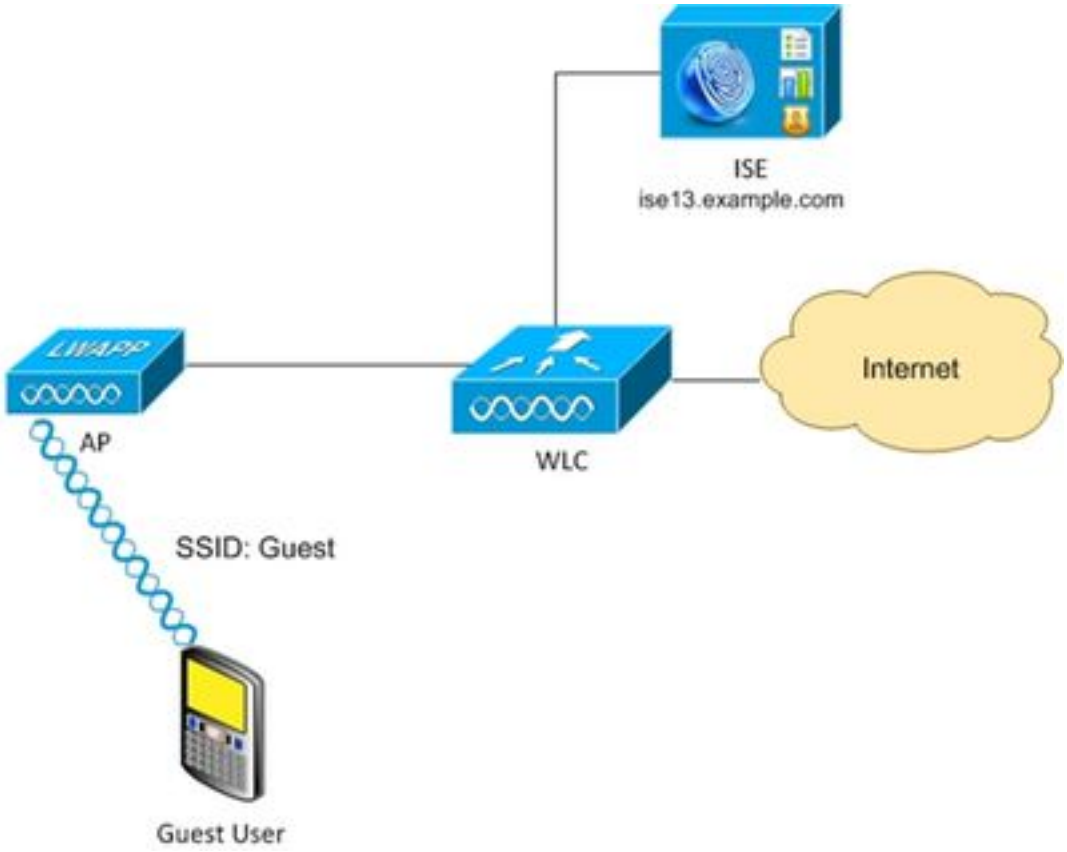
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Microsoft Windows 7
- Cisco WLC バージョン 7.6 以降
- ISE ソフトウェア バージョン 1.3 以降

設定

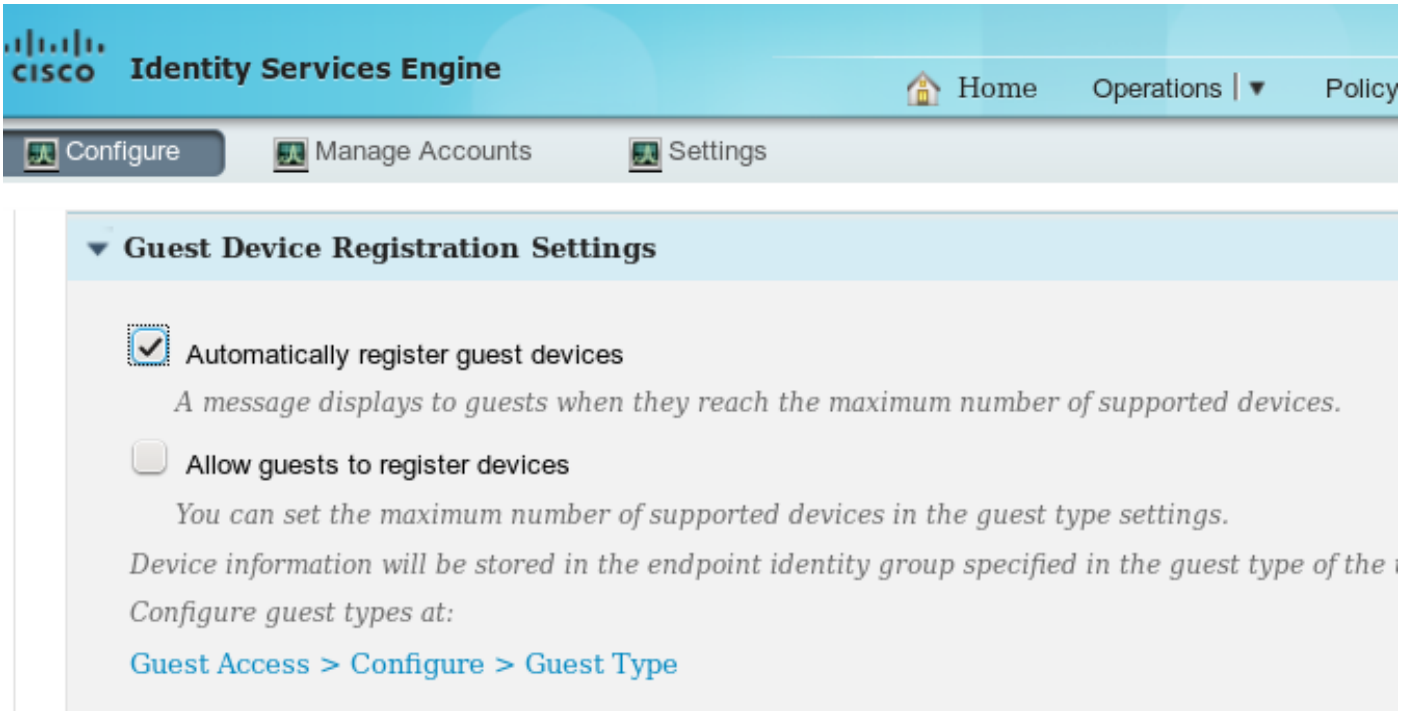
基本的なゲスト アクセス設定に関しては設定例と参照をチェックして下さい。 この技術情報は許可状態の承認規則設定および違いに焦点を合わせます。

ネットワーク図

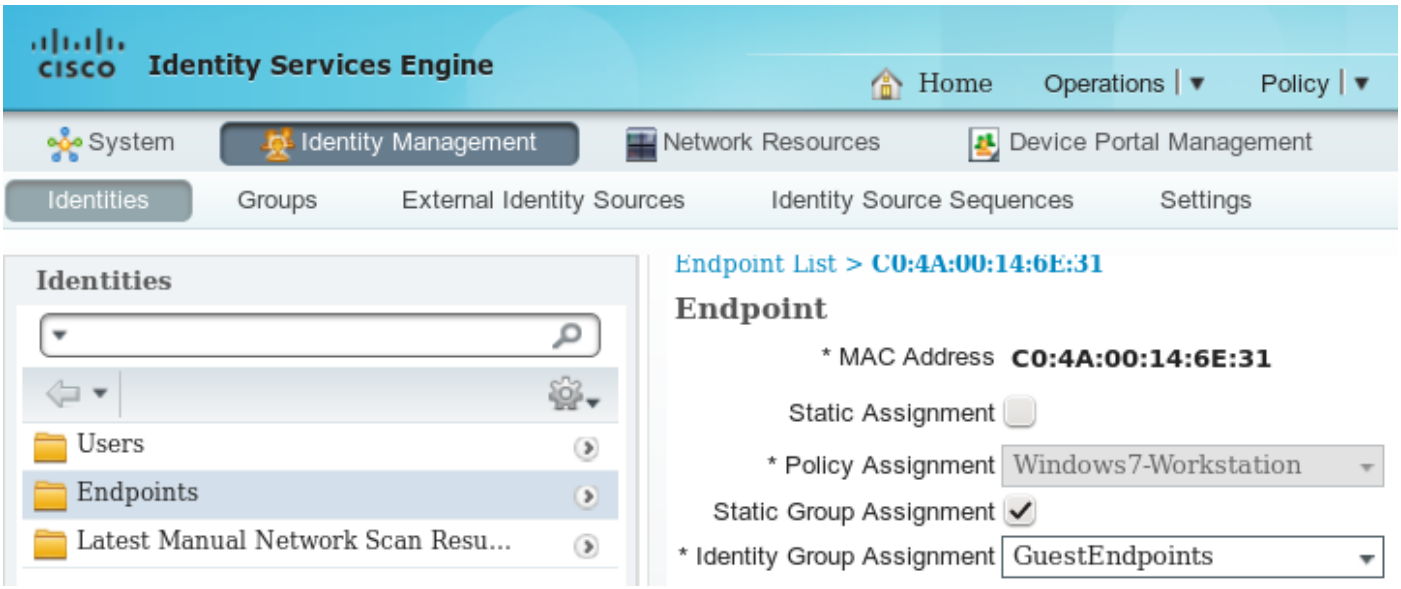


常置アクセス

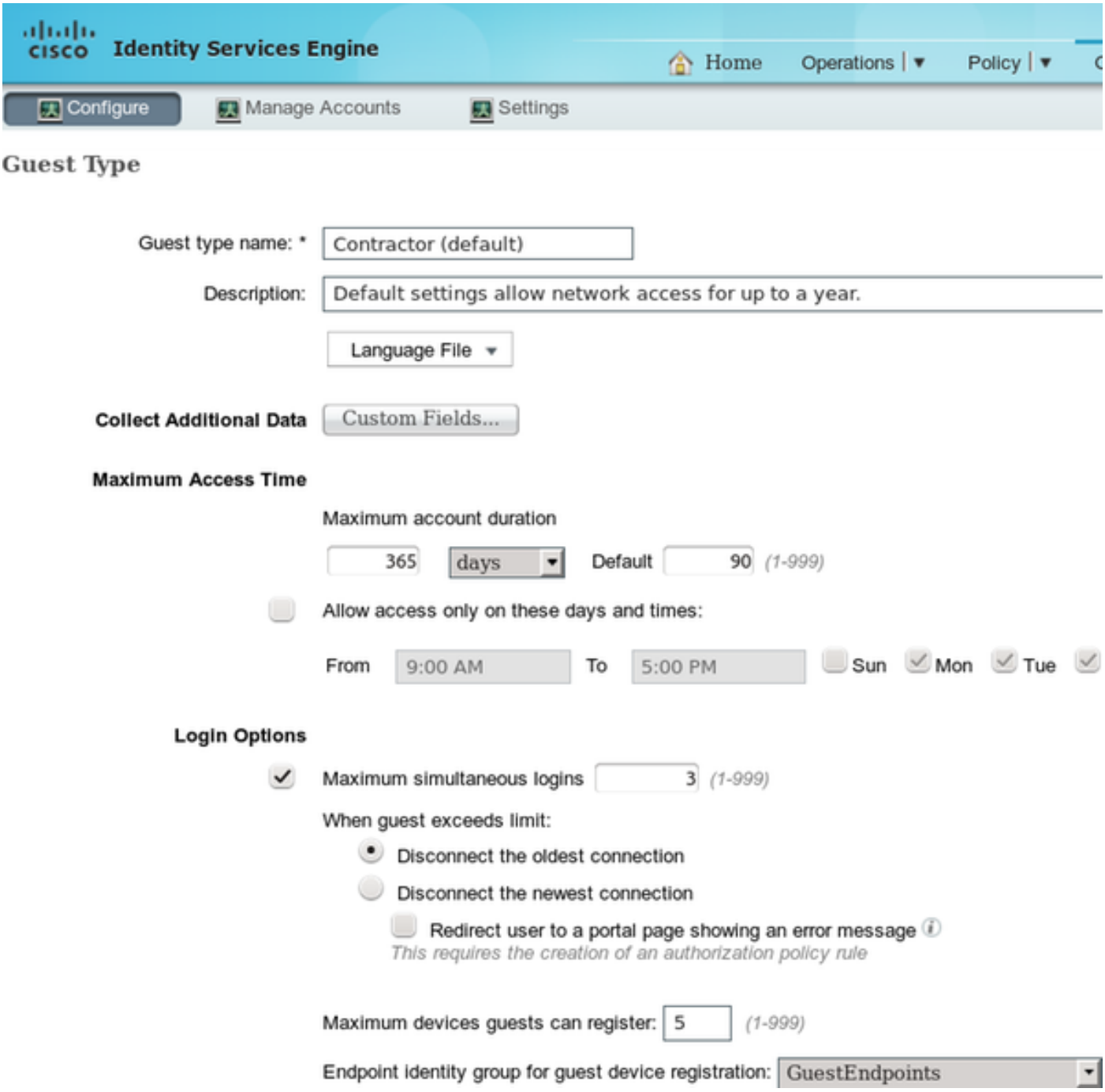
デバイス登録がイネーブルの状態でゲスト ポータルの認証の成功の後の ISE バージョン 1.3 および それ 以降に関しては。



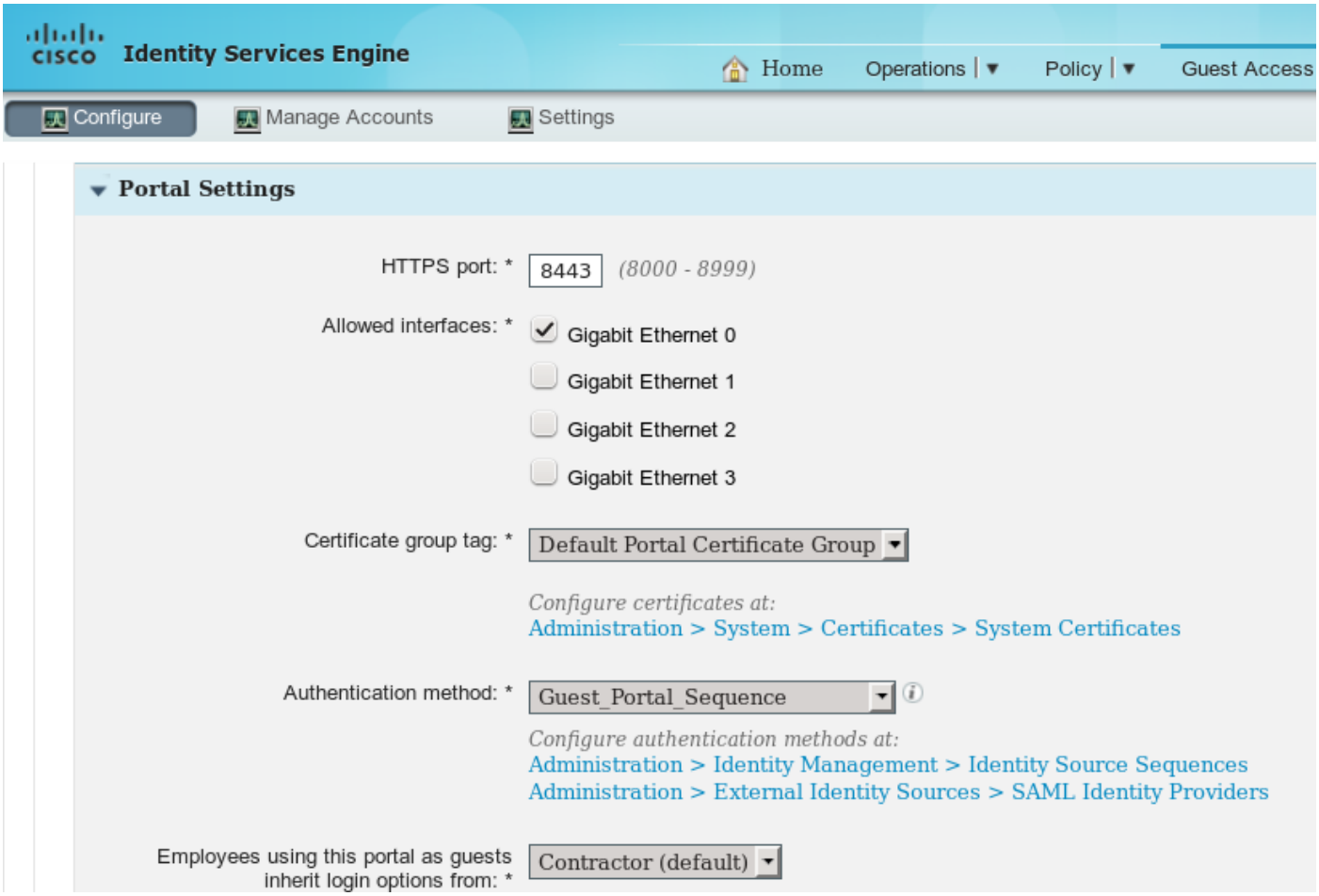
エンドポイント デバイス (MAC アドレス) は特定のエンド ポイント グループ (この例の GuestEndpoints) で静的に登録されています。



そのグループはこのイメージに示すようにユーザのゲスト型から、得られます。



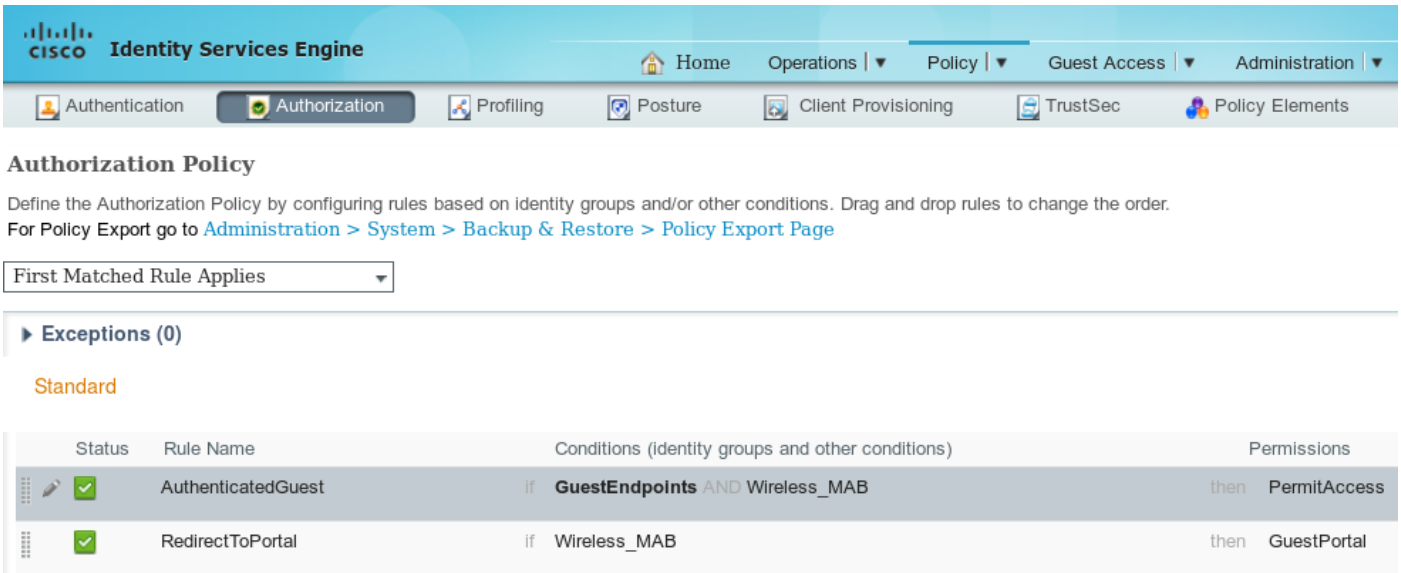
それが企業ユーザ（識別ストア他のそしてゲスト）ならその設定は門脈設定から得られます。



その結果ゲストと関連付けられる MAC アドレスはその特定の識別グループに常に属します。 それは自動的に変更することができません（たとえばプロファイラー サービスによって）。

> **注:** プロファイラー結果 EndPointPolicy 許可状態を適用することは使用することができます。

デバイスがによってそれに基づいて承認規則を構築することは可能性のあるである特定のエンドポイント識別グループに常に属することをこのイメージに示すように確認します。

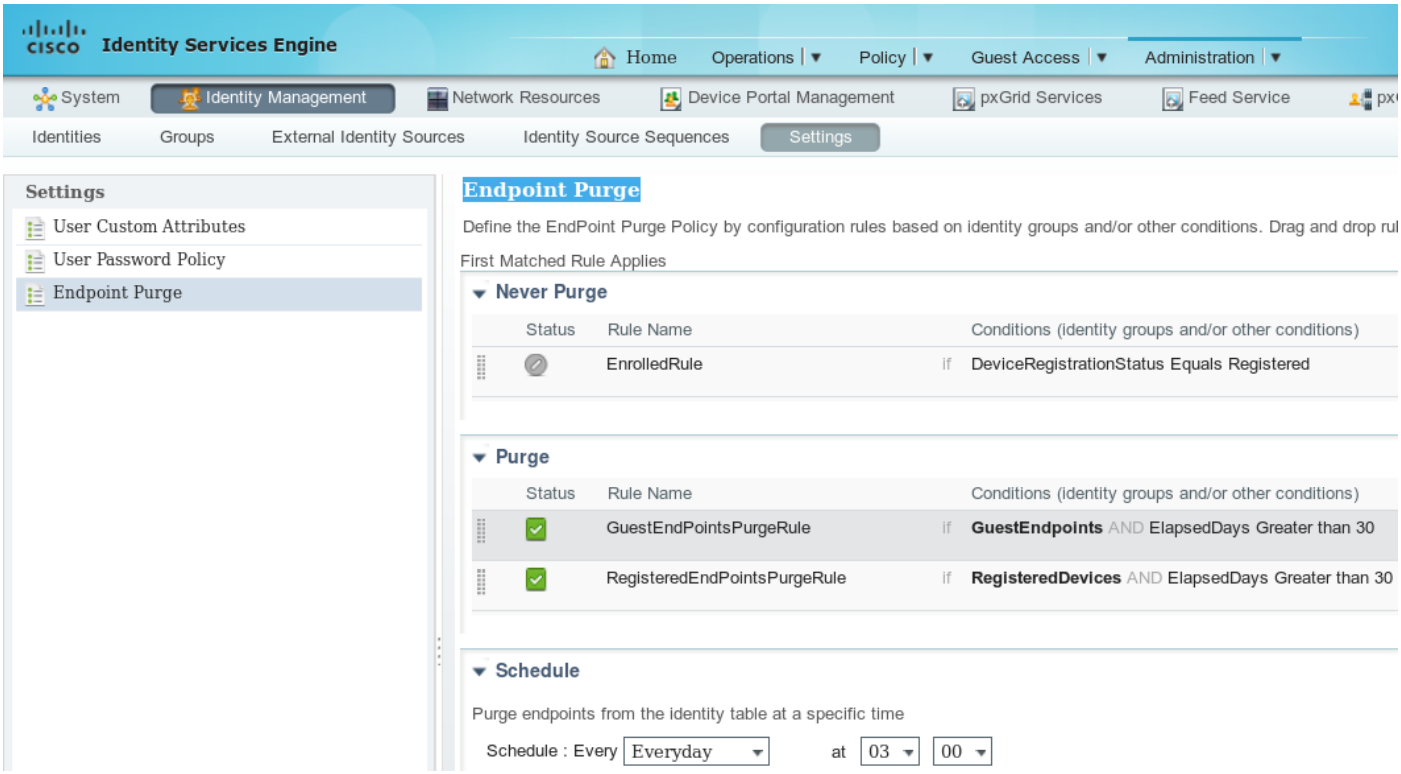


ユーザが認証されなければ、許可は汎用ルール RedirectToPortal と一致します。 ゲスト ポータルおよび認証へのリダイレクションの後で、エンド ポイントは特定のエンド ポイント識別グルー

プに置かれます。 それは第 1 によって、特定の状態使用されます。 そのエンド ポイントのすべてのそれに続く認証は最初の承認規則を見つけ、ユーザはゲスト ポータルで再認証する必要なしに提供された完全なネットワーク アクセスです。

ゲスト アカウントのためのエンド ポイント パージ

この状況は永久に持続する可能性があります。 しかし ISE 1.3 パージ エンド ポイントで機能性はもたらされました。 デフォルト 設定を使って。



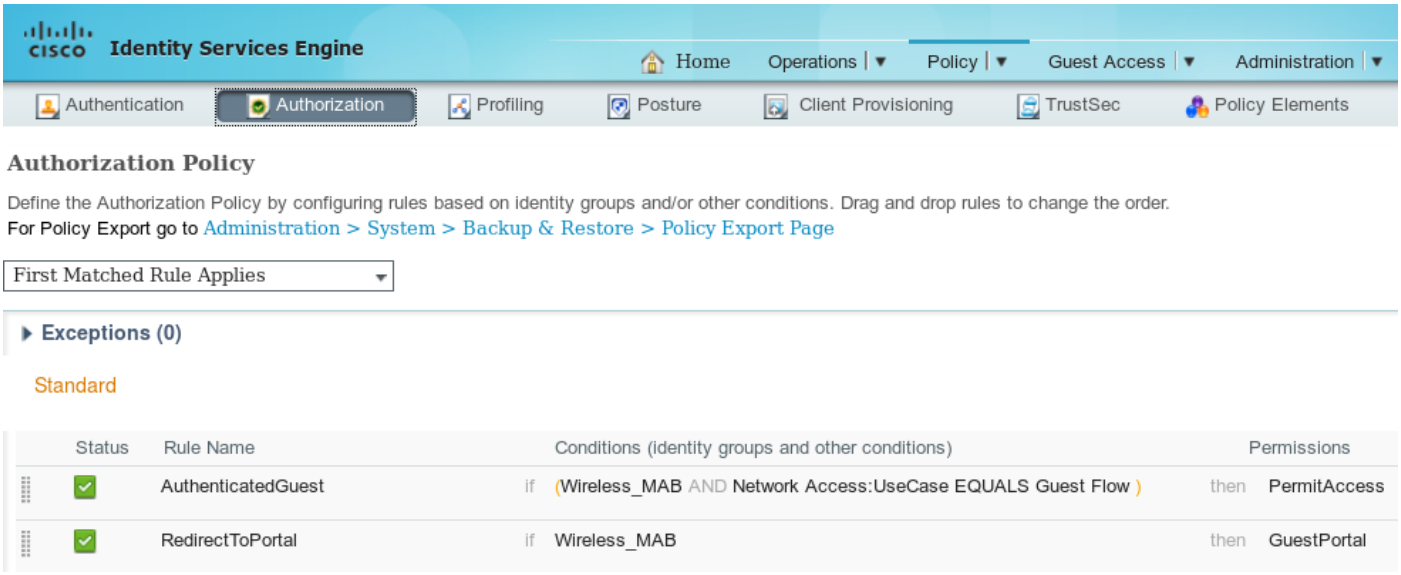
ゲスト認証に使用するすべてのエンド ポイントは 30 日以降に取除かれます (エンド ポイント作成から)。 その結果通常 30 日ゲストユーザの後でネットワーク ヒット RedirectToPortal 承認規則にアクセスすることを試みることは認証のためにリダイレクトされ。

> **注:** エンド ポイント パージ機能性はゲスト アカウント パージ ポリシーおよびゲスト アカウント有効期限の依存しないです。

> **注:** ISE 1.2 でエンド ポイントは内部プロファイラー キュー制限を見つけるときだけだけ自動的に取除くことができます。 それから最も少なく最近使用されたエンド ポイントは取除かれています。

一時アクセス

ゲスト アクセスにおけるもう一つの方式はゲスト フロー条件を使用することです。



条件は ISE およびそれのアクティブセッションをチェックしていること属性です。 以前に ゲストユーザは認証に成功したことをそのセッションに示す属性があったら一致されます調節して下さい。 ISE がネットワーク アクセス デバイス（NAD）から Radius アカウンティング停止メッセージを受け取った後、セッションは取除かれる終えられたおよびそれ以降です。 それステージ条件ネットワーク アクセス: UseCase = ゲスト フローはもう満たされません。 その結果そのエンド ポイントのすべてのそれに続く認証はゲスト認証のためにリダイレクトする汎用ルールを見つけます。

> **注:** ユーザがホットスポット ポータルによって認証される時サポートされないゲスト フロー。 それらのシナリオに関しては UseCase 属性はゲスト フローの代りにホスト ルックアップに設定されます。

WLC 接続解除動作

クライアントが無線ネットワークから切断された後（たとえば Windows の Disconnect ボタンを使用して）deauthentication フレームを送信 します。 しかしそれは WLC で省略され、「デバッグ クライアントを使用して xxxx」確認することができます-クライアントが WLAN から切断されているとき WLC はデバッグを示しません。 その結果 Windows クライアントで:

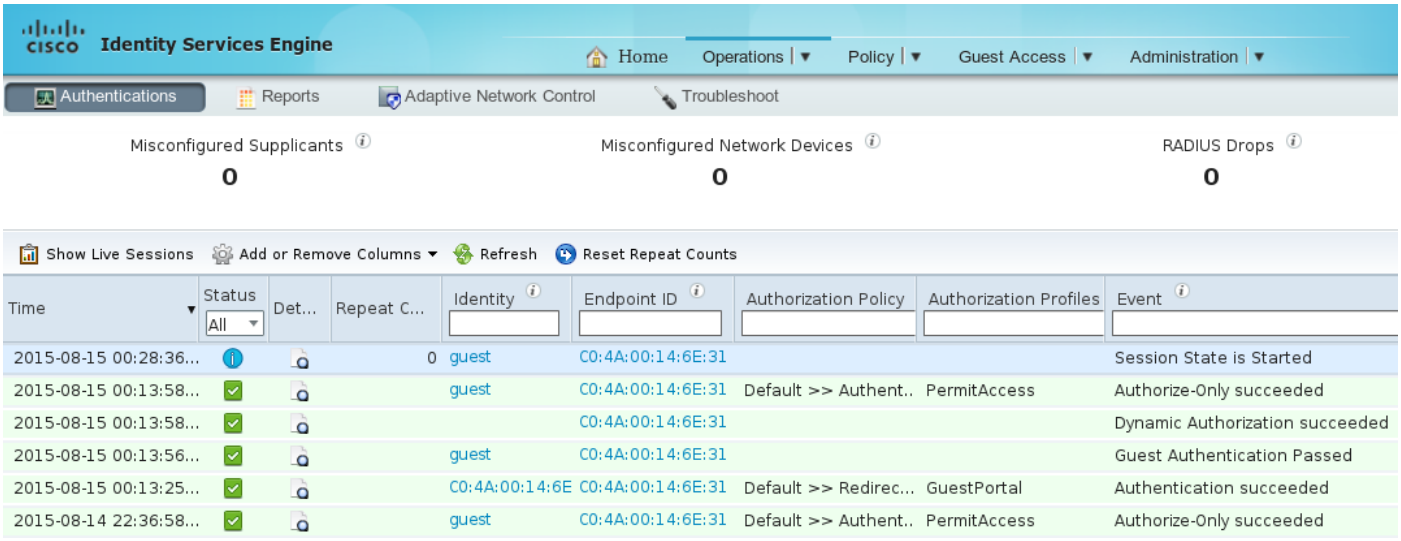
- IP アドレスはインターフェイスから削除されます
- インターフェイスは状態にあります: 切られるメディア

しかし WLC でステータスは不変です（走行状態のまだクライアント）。

それは WLC のための計画設計、セッション取除かれます時です

- ユーザ アイドルタイムアウト ヒット
- セッション タイムアウト ヒット
- L2 暗号化を使用している、場合 Group 鍵回転間隔が見つかる時
- 何か他のものにより AP/WLC はクライアントをを離れて蹴ります（例えば AP Radio リセットは、誰か WLAN、等をシャットダウンします）

その動作および一時アクセス設定を使ってずっと WLC が決してそれクリアしていないので WLAN セッションからのユーザ切断が ISE から取除かれなかった後（および決して送信 された Radius アカウンティング停止を）。 セッションが取除かれない場合、ISE はまだ古いセッションおよびゲスト フロー条件が満足することを覚えています。 切断および再接続ユーザの後で再認証するべき要件なしで完全なネットワーク アクセスを持って下さい。



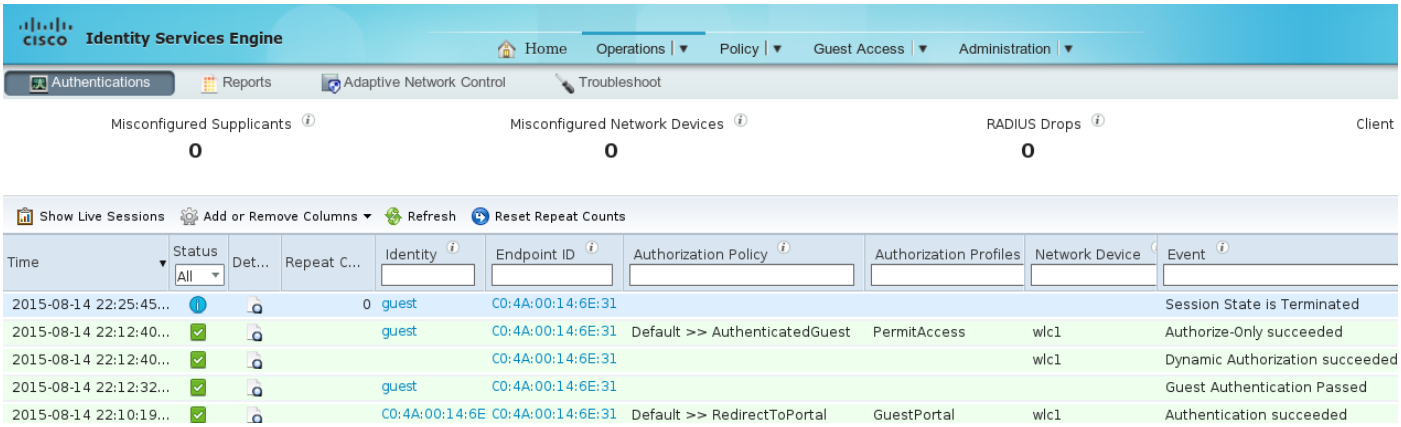
しかし切断ユーザが別の WLAN に接続した後、そして WLC は古いセッションを解決することにします。 Radius アカウンティング停止は送信 され、ISE はセッションを取除きます。 によってフロー条件満足しないおよびクライアントがオリジナル WLAN ゲストに接続することを試みればユーザは認証のためにリダイレクトされます。

> **注:** 管理フレーム保護（MFP）で設定される WLC は CCXv5 MFP クライアントからの暗号化された deauthentication フレームを受け入れます。

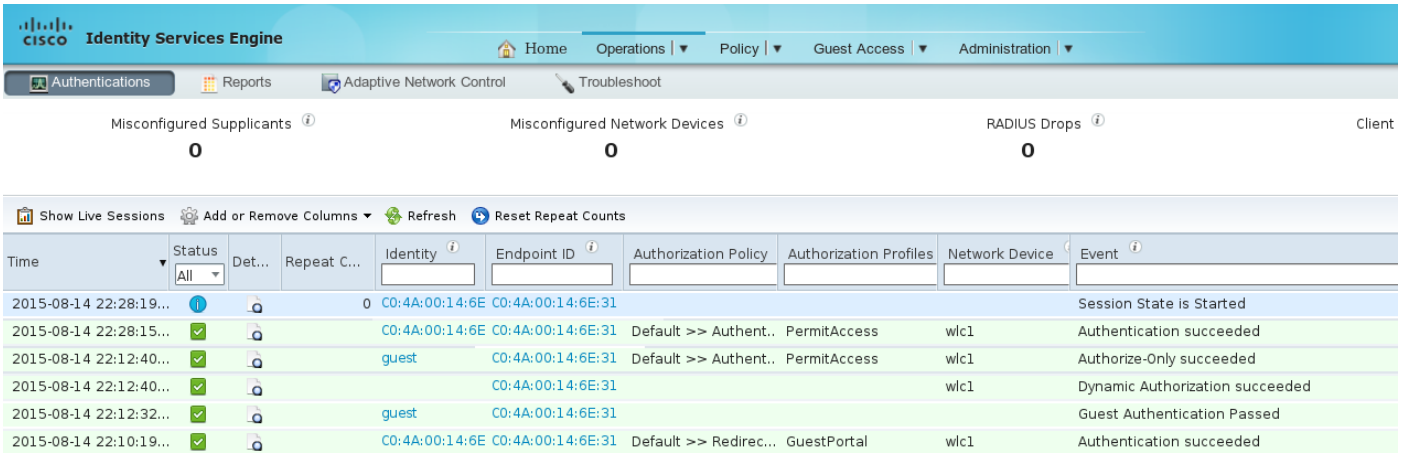
確認

常置アクセス

再認証を誘発する許可（CoA）のゲスト ポータルおよび認証の成功 ISE 送信変更へのリダイレクションの後。 その結果新しい MAC 認証バイパス（MAB）セッションは構築されています。 今回エンド ポイントは GuestEndpoints 識別グループに属し、一致はフルアクセスの提供を支配します。

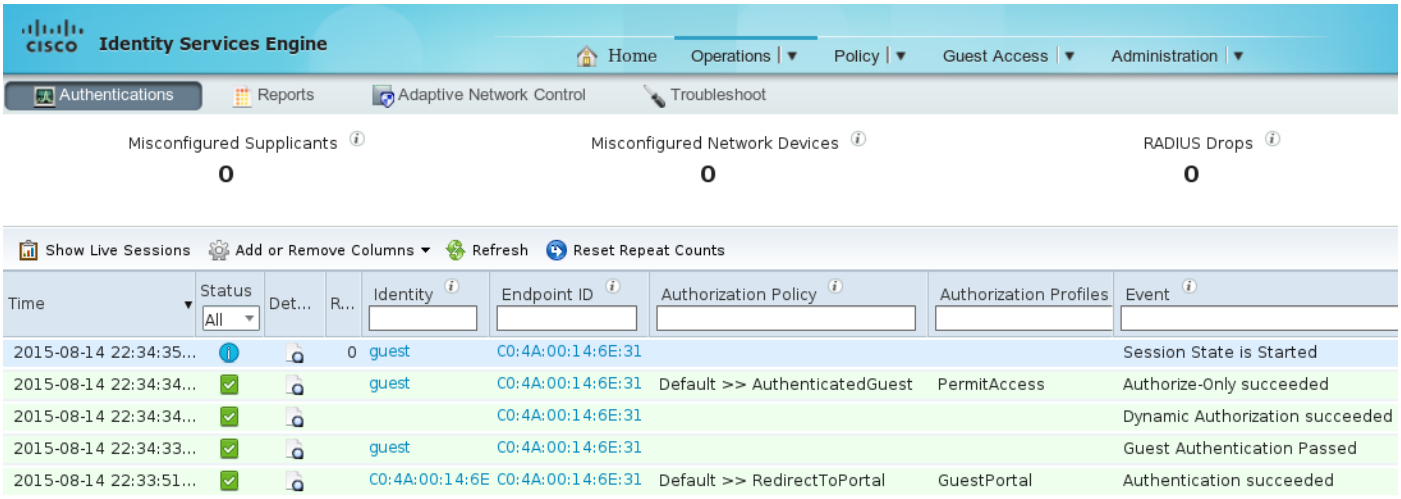


そのステージ無線ユーザで切り、異なる WLAN に接続し、そして再接続できます。 それらのそれに続く認証はすべて MAC アドレスに基づいて識別を使用しますが特定の識別グループに属するエンド ポイントが理由で最初のルールを見つけます。 完全なネットワーク アクセスはゲスト認証なしで提供されます。

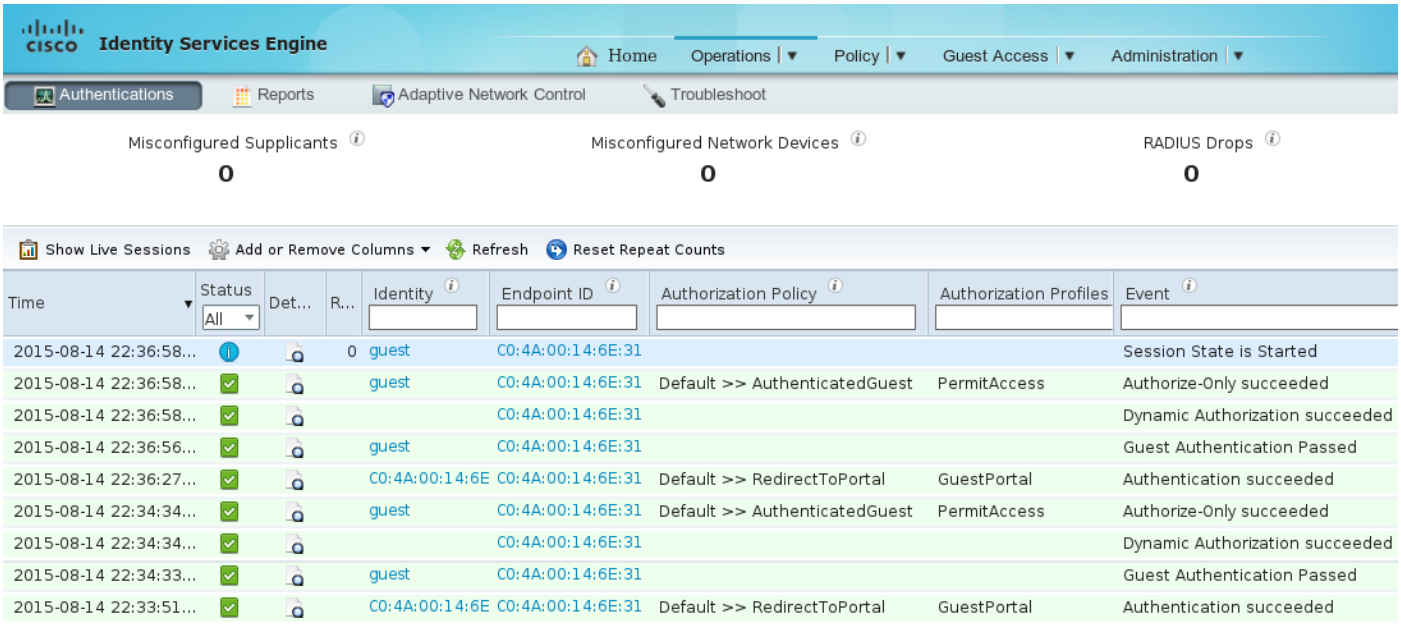


一時アクセス

第 2 シナリオ (ゲスト フローに基づく条件が) 始まりに関しては同じはあります。

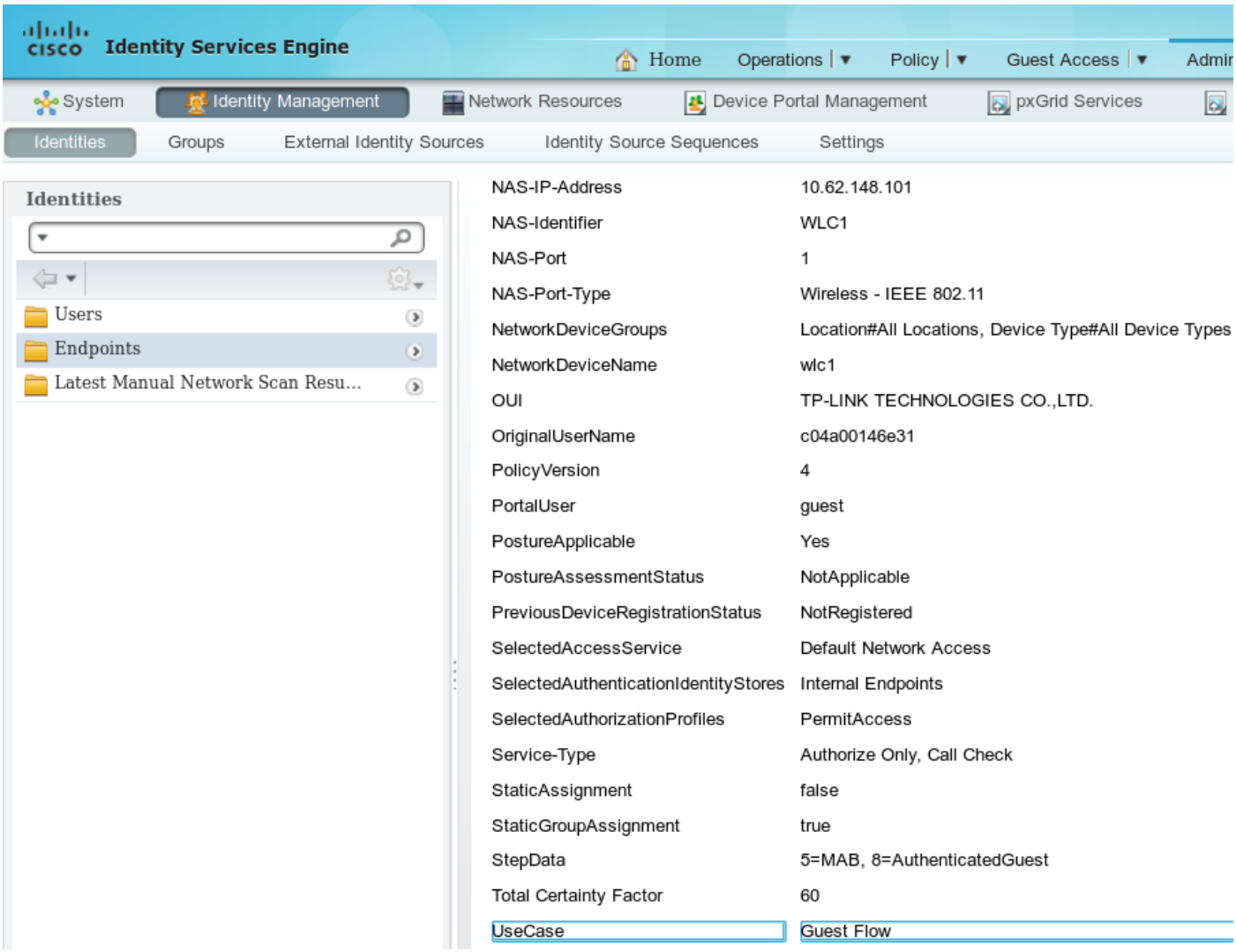


しかしセッションがすべてのそれに続く認証のために取除かれた後、ゲストは汎用ルールを見つけ、ゲスト認証のために再度リダイレクトされます。



ゲストはフロー条件によってがある正しい属性がセッションのために存在 して いるとき満足します。 それはエンド ポイント属性を検知 することによって確認することができます。 正常なゲス

ト認証の結果は示されます。




```
PortalUser guest
StepData 5=MAB, 8=AuthenticatedGuest
UseCase Guest Flow
```

バグ

CSCuu41157 ISE ENH CoA はゲスト アカウント削除または終止の送信を終えます。

（ゲスト アカウント削除か終止の後でゲスト セッションを終了する機能拡張要求）

参考資料

- Cisco ISE 1.3 アドミニストレータ ガイド
- Cisco ISE 1.4 管理者ガイド
- ISE バージョン 1.3 ホットスポットの設定例
- ISE バージョン 1.3 の自己登録したゲスト ポータルの設定例
- WLC と ISE での中央 Web 認証の設定例
- ISE を搭載した WLC 上で FlexConnect AP を使用した中央 Web 認証の設定例
- テクニカル サポートとドキュメント – Cisco Systems