Konfigurieren des temporären und permanenten ISE-Gastzugriffs

Inhalt

Einführung

In diesem Dokument werden verschiedene Methoden für die Identity Services Engine (ISE)-Gastzugriffskonfiguration beschrieben. Basierend auf unterschiedlichen Bedingungen in Autorisierungsregeln:

- permanenter Netzwerkzugriff ist möglich (keine nachträgliche Authentifizierung erforderlich)
- temporärer Zugriff auf das Netzwerk möglich ist (Gastauthentifizierung nach Ablauf der Sitzung erforderlich)

Neben den Auswirkungen auf das Szenario des temporären Zugriffs wird auch ein bestimmtes Verhalten des Wireless LAN Controller (WLC) für die Sitzungsentfernung dargestellt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ISE-Bereitstellungen und Gastdatenströme
- Konfiguration der Wireless LAN Controller (WLCs)

Verwendete Komponenten

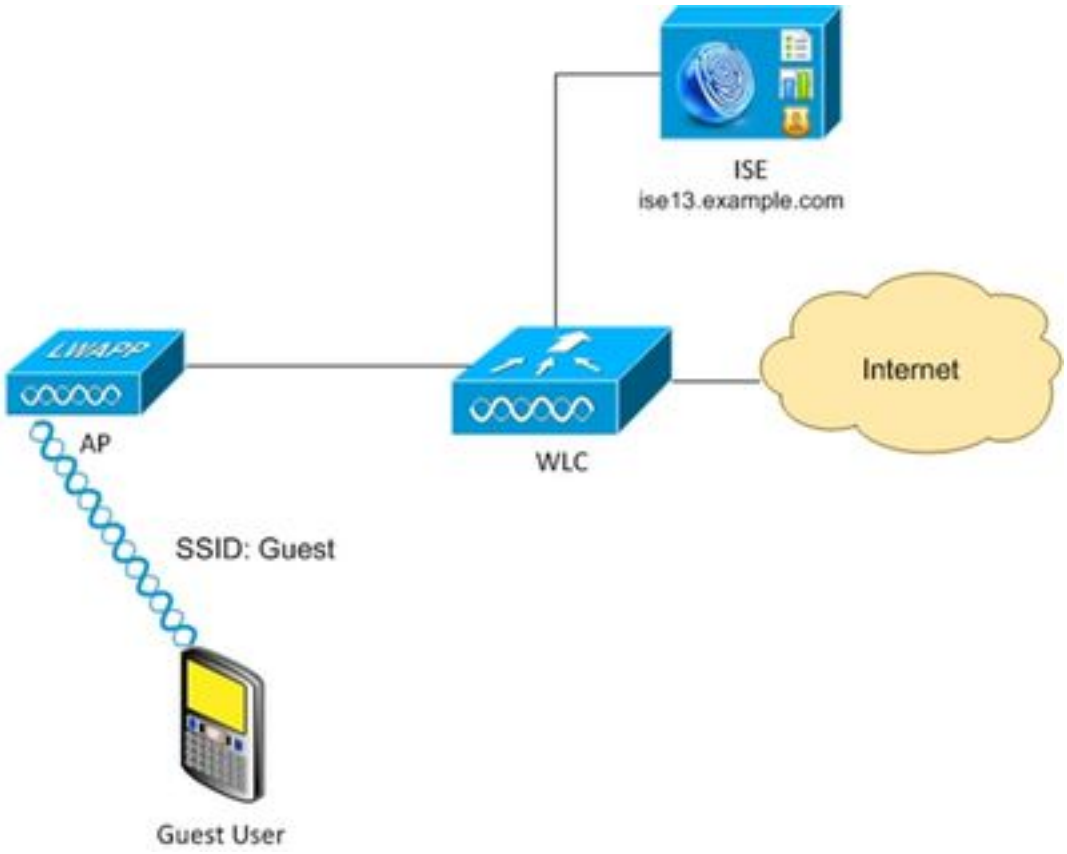
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Microsoft Windows 7
- Cisco WLC 7.6 oder höher
- ISE Software, Version 1.3 und höher

Konfigurieren

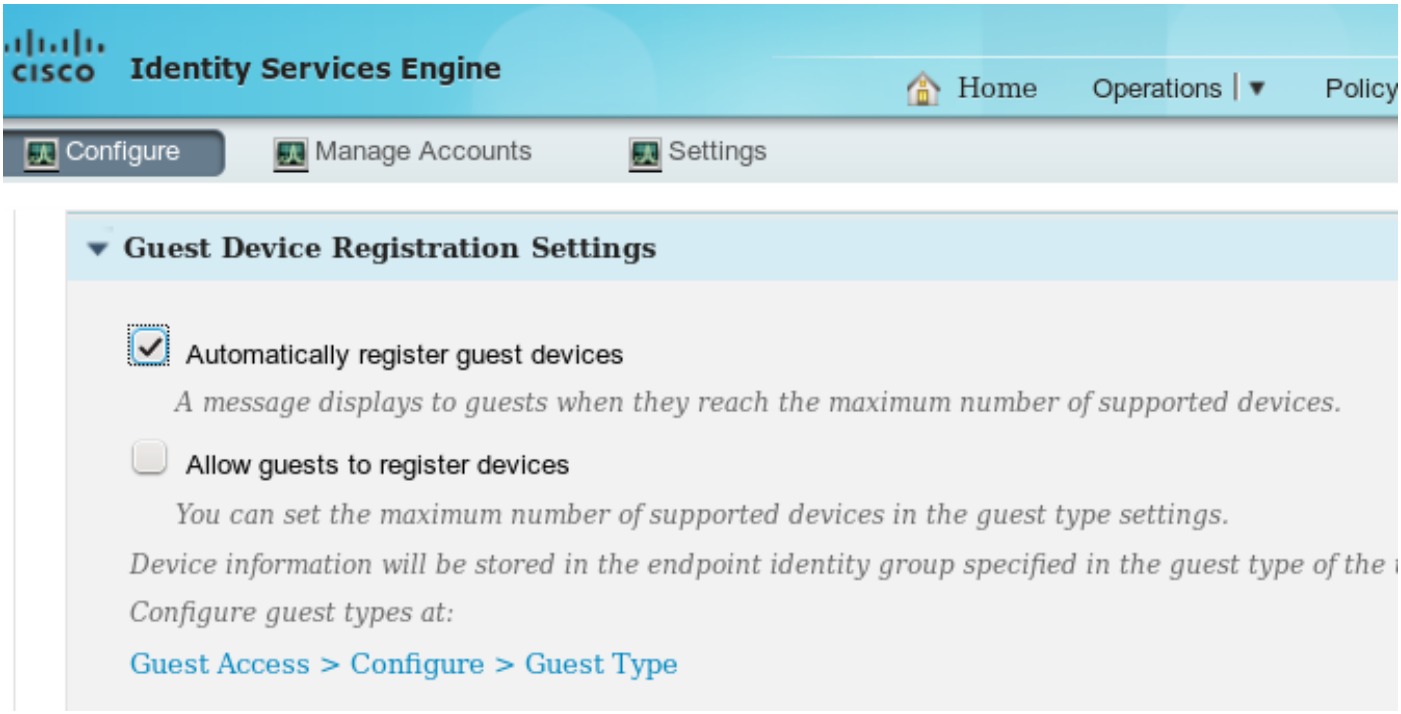
Eine grundlegende Konfiguration für den Gastzugriff finden Sie in den Referenzen mit Konfigurationsbeispielen. Dieser Artikel behandelt die Konfiguration von Autorisierungsregeln und Unterschiede in den Autorisierungsbedingungen.

Netzwerkdiagramm

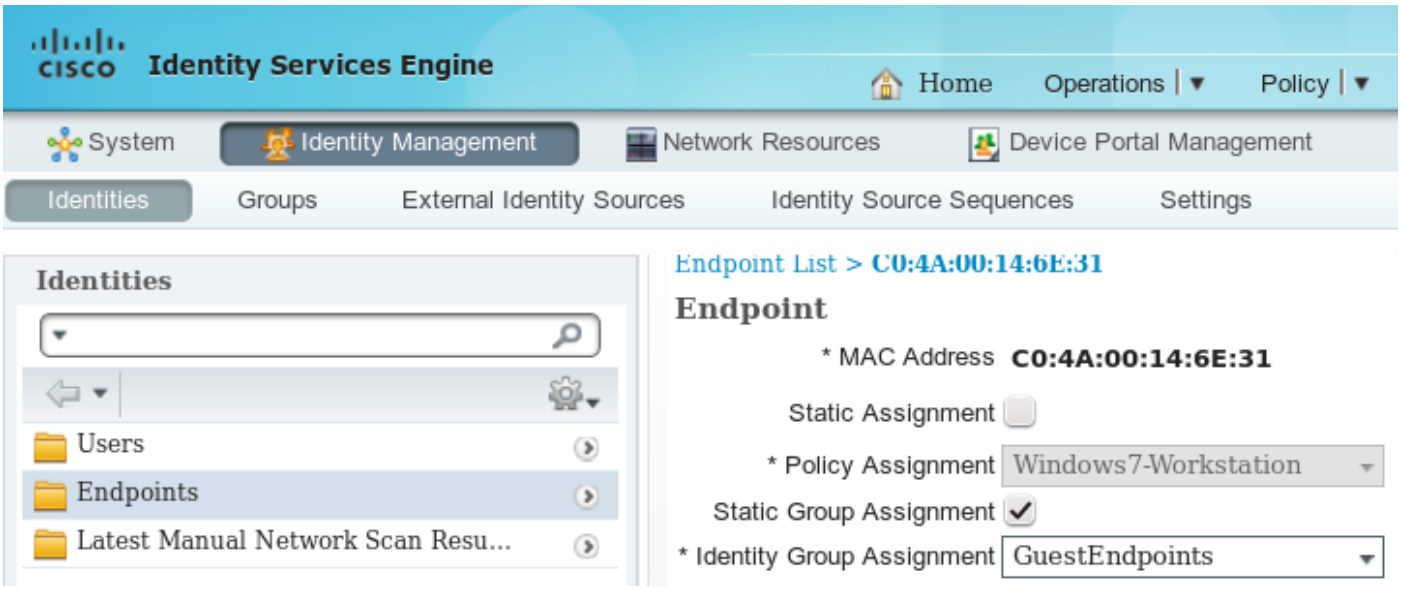


Permanenter Zugriff

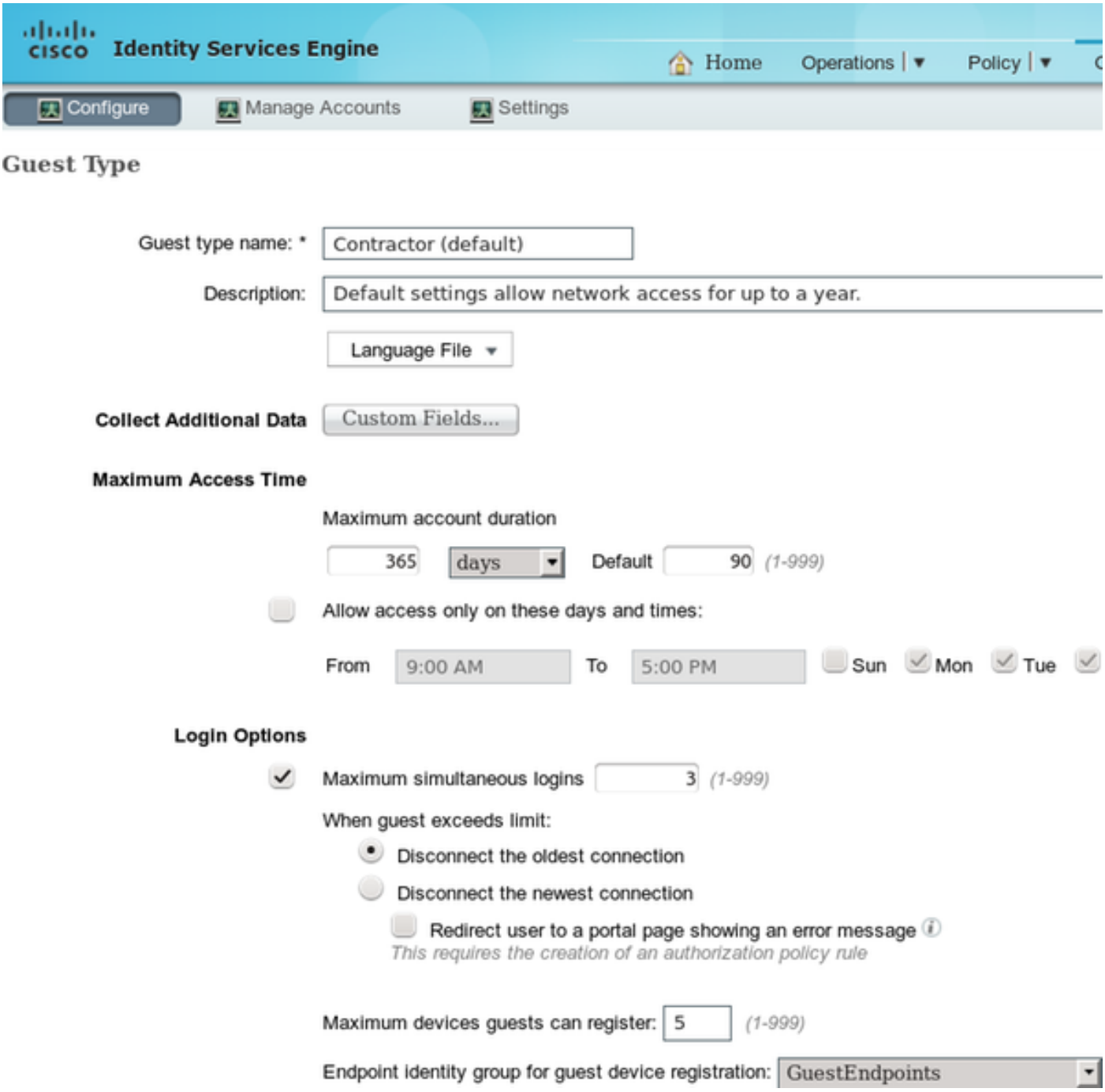
Für ISE Version 1.3 und höher nach erfolgreicher Authentifizierung auf dem Gastportal mit aktivierter Geräteregistrierung.



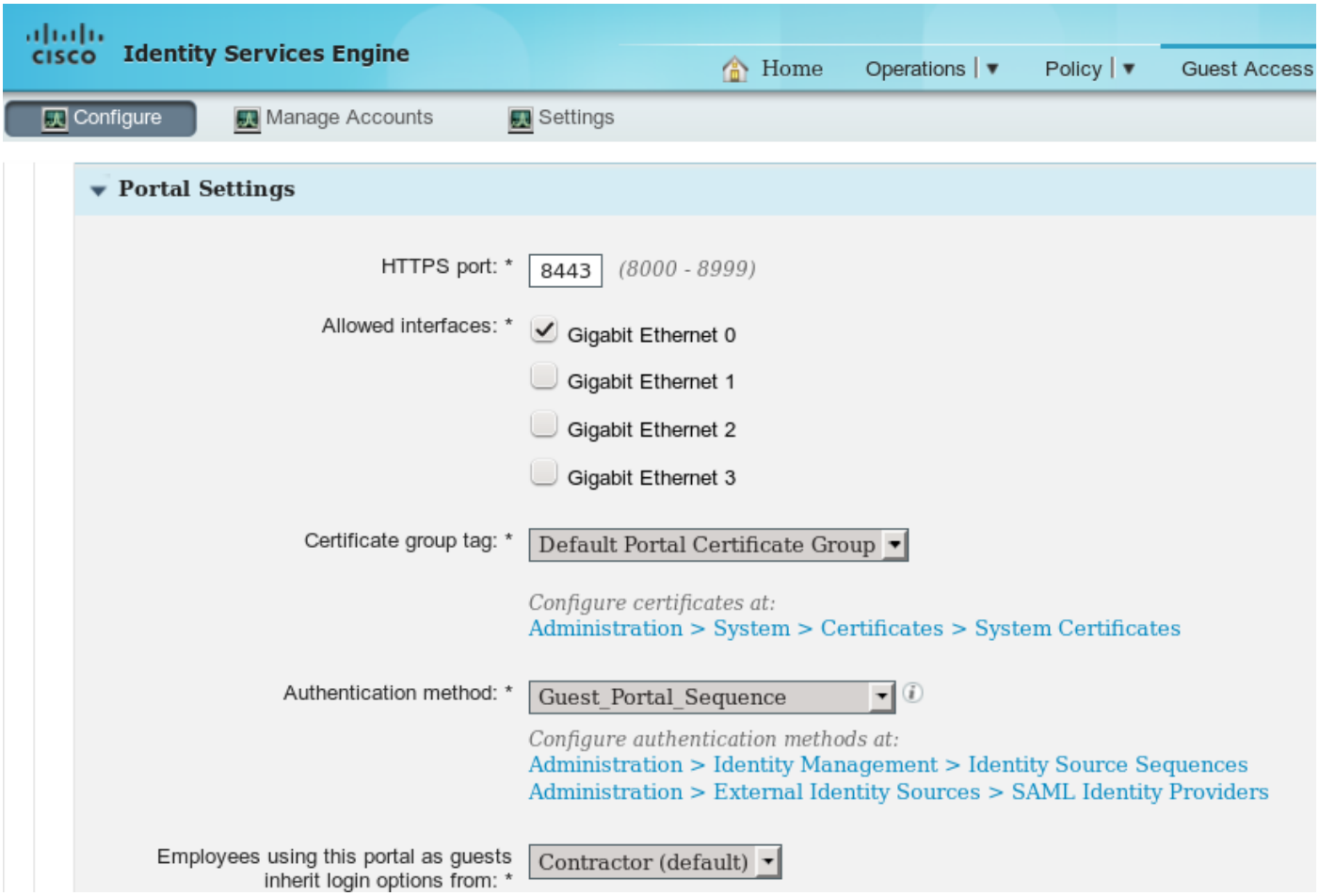
Endgerät (MAC-Adresse) ist statisch in einer bestimmten Endpunktgruppe registriert (in diesem Beispiel GuestEndpoints).



Diese Gruppe wird vom Gasttyp des Benutzers abgeleitet, wie in diesem Bild gezeigt.



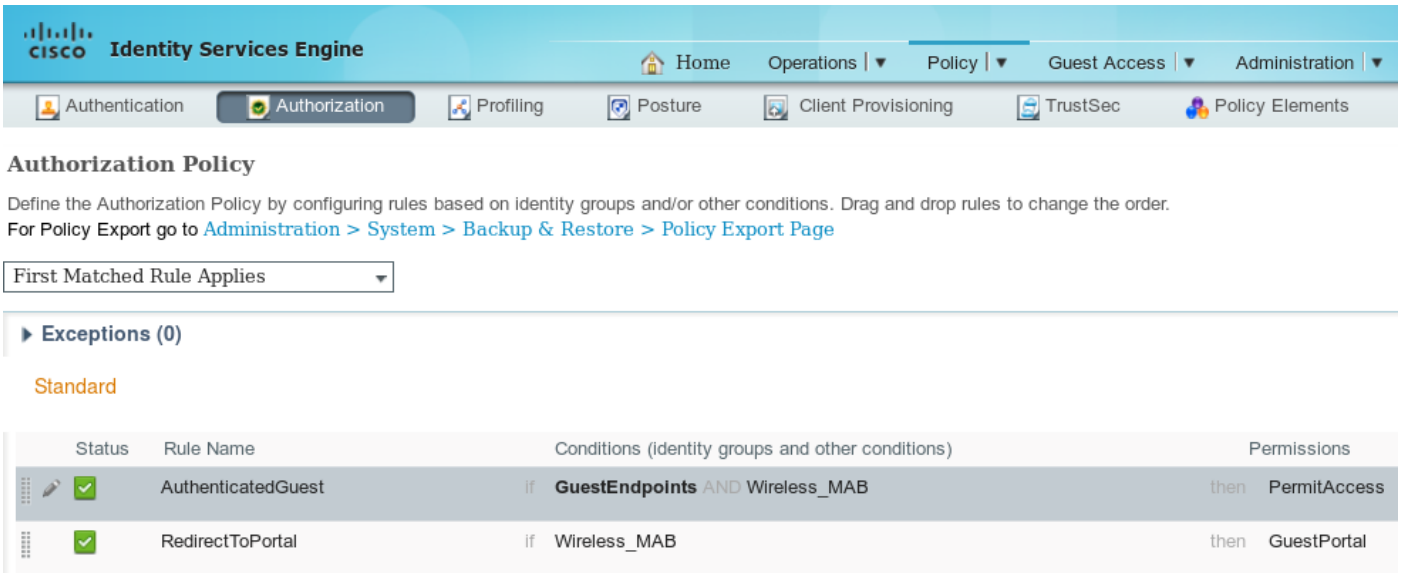
Wenn es sich um einen Firmenbenutzer (Identitätsspeicher mit Ausnahme von Gast) handelt, wird diese Einstellung von den Portaleinstellungen abgeleitet.



Folglich gehört die dem Gast zugeordnete MAC-Adresse immer zu dieser spezifischen Identitätsgruppe. Das kann nicht automatisch geändert werden (z.B. durch Profiler Service).

> **Hinweis**: Zum Anwenden von Profilerergebnissen kann eine EndPointPolicy-Autorisierungsbedingung verwendet werden.

Da das Gerät immer zu einer bestimmten Endpunkt-Identitätsgruppe gehört, können auf dieser Grundlage Autorisierungsregeln erstellt werden, wie in diesem Bild gezeigt.

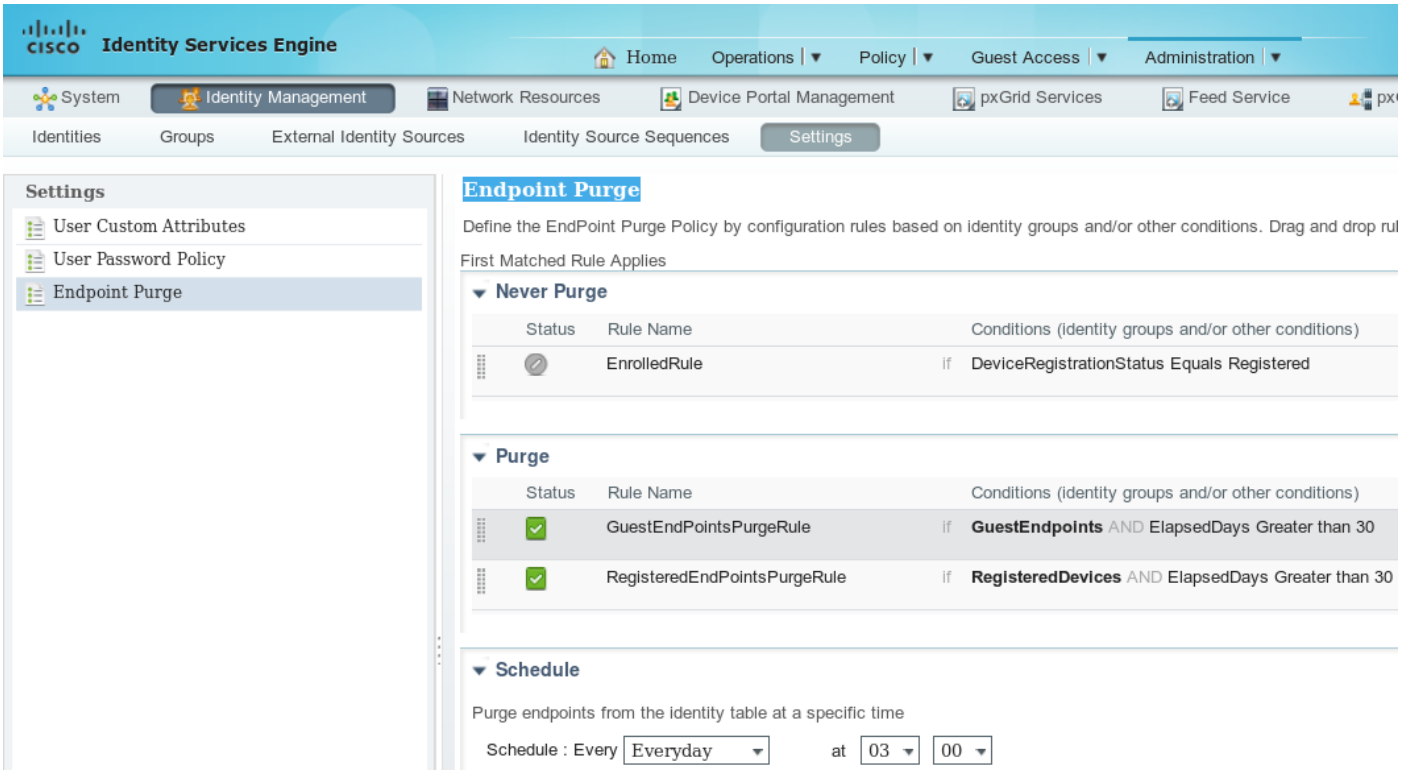


Wenn ein Benutzer nicht authentifiziert wurde, stimmt die Autorisierung mit der generischen Regel RedirectToPortal überein. Nach der Umleitung zum Gastportal und der Authentifizierung wird der

Endpunkt in der spezifischen Endpunkt-Identitätsgruppe platziert. Das wird von der ersten, spezifischeren Bedingung verwendet. Alle nachfolgenden Authentifizierungen dieses Endpunkts treffen auf die erste Autorisierungsregel, und der Benutzer erhält vollständigen Netzwerkzugriff, ohne dass eine erneute Authentifizierung im Gastportal erforderlich ist.

Endpunktlöschung für Gastkonten

Diese Situation könnte ewig andauern. In ISE 1.3 wurde jedoch die Funktion "Endgeräte entfernen" eingeführt. Mit der Standardkonfiguration.



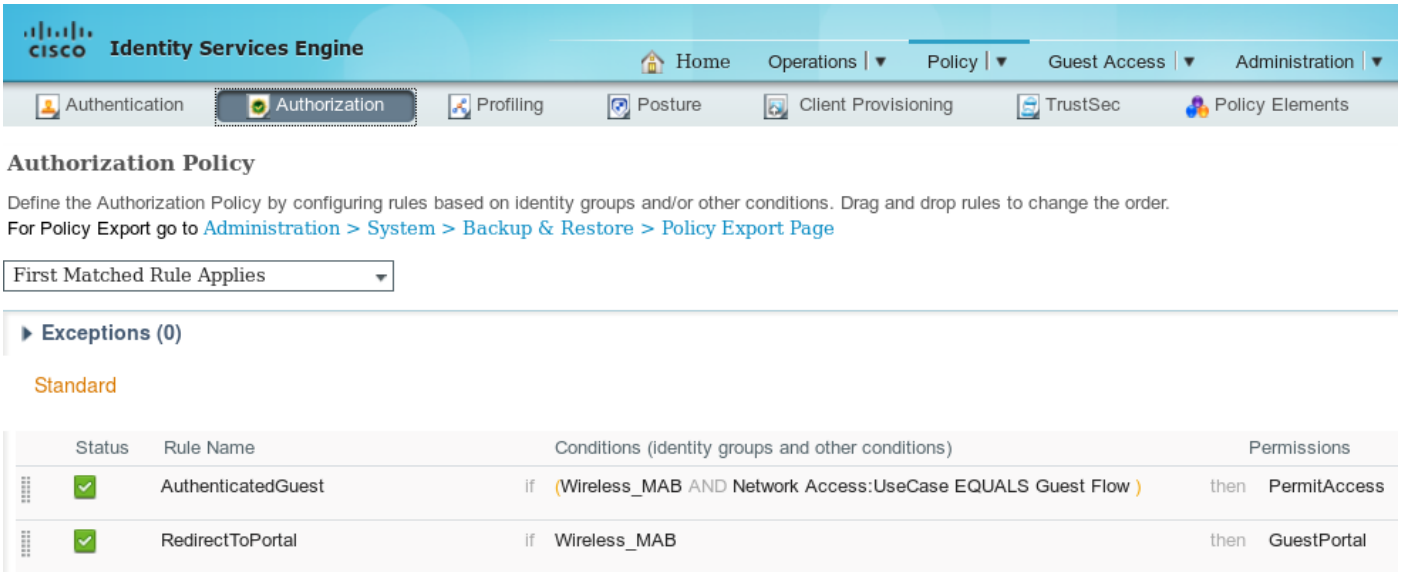
Alle Endpunkte, die für die Gastauthentifizierung verwendet werden, werden nach 30 Tagen (von der Erstellung des Endpunkts an) entfernt. Daher trifft ein Gastbenutzer, der versucht, auf das Netzwerk zuzugreifen, in der Regel nach 30 Tagen auf die RedirectToPortal-Autorisierungsregel und wird zur Authentifizierung umgeleitet.

> **Hinweis**: Die Funktion zum Zurücksetzen von Endpunkten ist unabhängig von der Richtlinie zum Zurücksetzen von Gastkonten und dem Ablauf von Gastkonten.

> **Hinweis**: In der ISE 1.2 konnten Endpunkte nur dann automatisch entfernt werden, wenn die internen Warteschlangenbeschränkungen für Profiler eingehalten wurden. Dann werden die zuletzt verwendeten Endgeräte entfernt.

Temporärer Zugriff

Eine weitere Methode für den Gastzugriff ist die Verwendung des Gastdatenflusszustands.



Diese Bedingung besteht darin, aktive Sitzungen auf der ISE und deren Attribute zu überprüfen. Wenn diese Sitzung über das Attribut verfügt, das angibt, dass der zuvor erfolgreich authentifizierte Gastbenutzer zugeordnet wurde. Nachdem die ISE die RADIUS Accounting Stopp-Nachricht vom Network Access Device (NAD) erhält, wird die Sitzung beendet und später entfernt. In dieser Phase ist die Bedingung Netzwerkzugriff:UseCase = Guest Flow nicht mehr erfüllt. Infolgedessen treffen alle nachfolgenden Authentifizierungen dieses Endpunkts auf die generische Regelumleitung für die Gastauthentifizierung.

> **Hinweis**: Guest Flow wird nicht unterstützt, wenn der Benutzer über das HotSpot-Portal authentifiziert wird. In diesen Szenarien ist das UseCase-Attribut auf Host Lookup anstatt auf Guest Flow festgelegt.

WLC-Trennungsverhalten

Nachdem Clients die Verbindung zum Wireless-Netzwerk getrennt haben (z. B. über die Trenntaste in Windows) sendet sie einen deauthentifizierten Frame. Dies wird vom WLC jedoch weggelassen und kann mit dem Befehl "debug client xxxx" bestätigt werden. WLC zeigt keine Debugging-Meldungen an, wenn der Client die Verbindung zum WLAN trennt. Als Ergebnis auf Windows-Client:

- IP-Adresse wird von der Schnittstelle entfernt
- Schnittstelle ist in Status: Medien getrennt

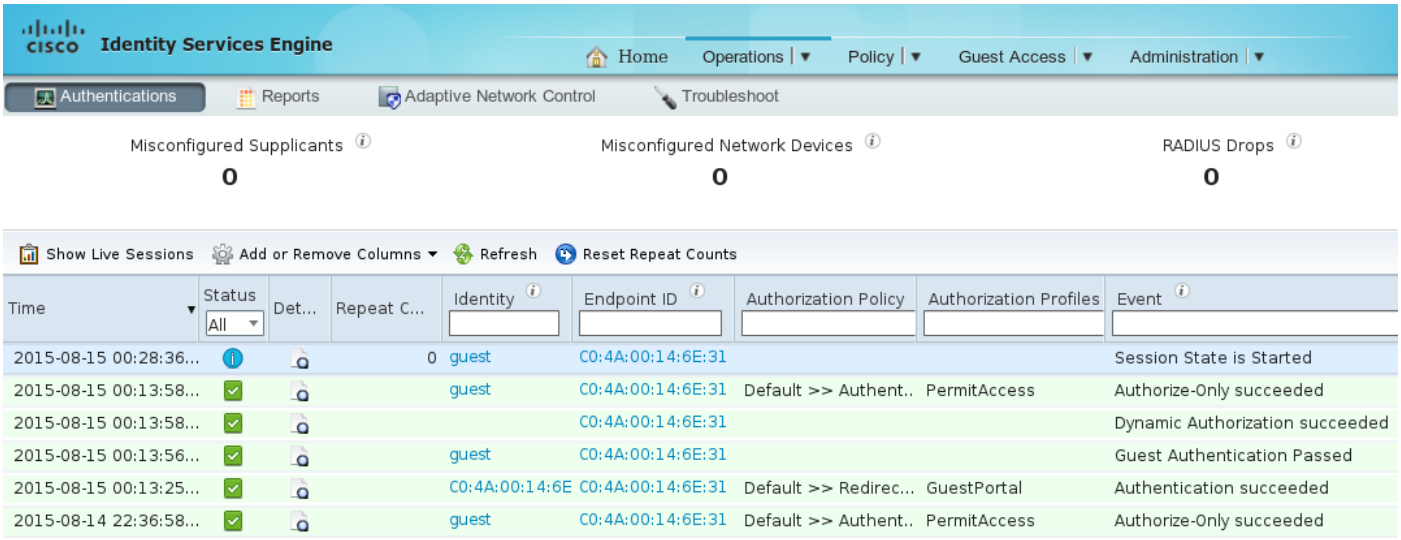
Auf dem WLC ist der Status jedoch unverändert (der Client befindet sich noch im RUN-Status).

Das geplante Design für WLC sieht vor, dass die Sitzung entfernt wird, wenn

- Timeout-Treffer im Leerlauf
- Sitzungs-Timeout-Treffer
- Wenn L2-Verschlüsselung verwendet wird, dann wenn das Rotationsintervall für die Gruppenschlüssel erreicht wird
- Ein anderer Grund führt dazu, dass der Access Point/WLC den Client ausschaltet (z. B. Zurücksetzen der AP-Funkverbindung, Herunterfahren des WLAN usw.)

Mit diesem Verhalten und der Konfiguration des temporären Zugriffs, nachdem der Benutzer die Verbindung von der WLAN-Sitzung getrennt hat, wird diese nicht aus der ISE entfernt, da der

WLC diesen Vorgang nie gelöscht hat (und keinen Radius Accounting Stopp gesendet hat). Wenn die Sitzung nicht entfernt wird, speichert die ISE weiterhin die alte Sitzung und die Bedingung für den Gastfluss ist erfüllt. Nach dem Trennen der Verbindung und der erneuten Verbindung hat der Benutzer uneingeschränkten Netzwerkzugriff, ohne dass eine erneute Authentifizierung erforderlich ist.



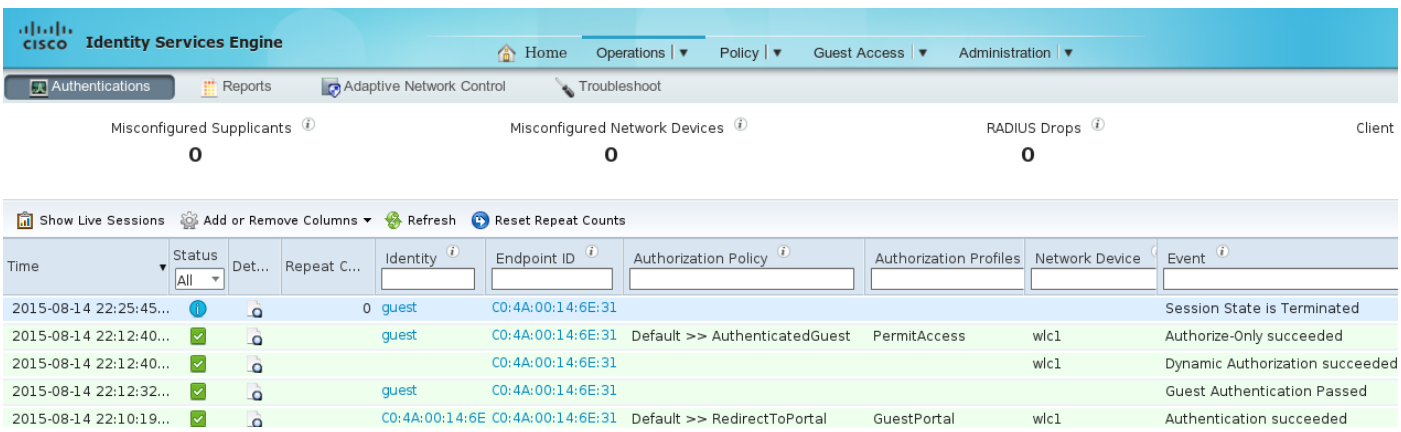
Wenn der Benutzer nach dem Trennen der Verbindung jedoch eine Verbindung zu einem anderen WLAN herstellt, entscheidet der WLC, die alte Sitzung zu löschen. Radius Accounting Stopp wird gesendet, und die ISE entfernt die Sitzung. Wenn der Client versucht, eine Verbindung zum ursprünglichen Zustand des WLAN-Gastdatenflusses herzustellen, ist dieser nicht zufrieden und der Benutzer wird zur Authentifizierung umgeleitet.

> **Hinweis**: WLC, konfiguriert mit Management Frame Protection (MFP), akzeptiert verschlüsselte deauthentifizierte Frames vom CCXv5 MFP-Client.

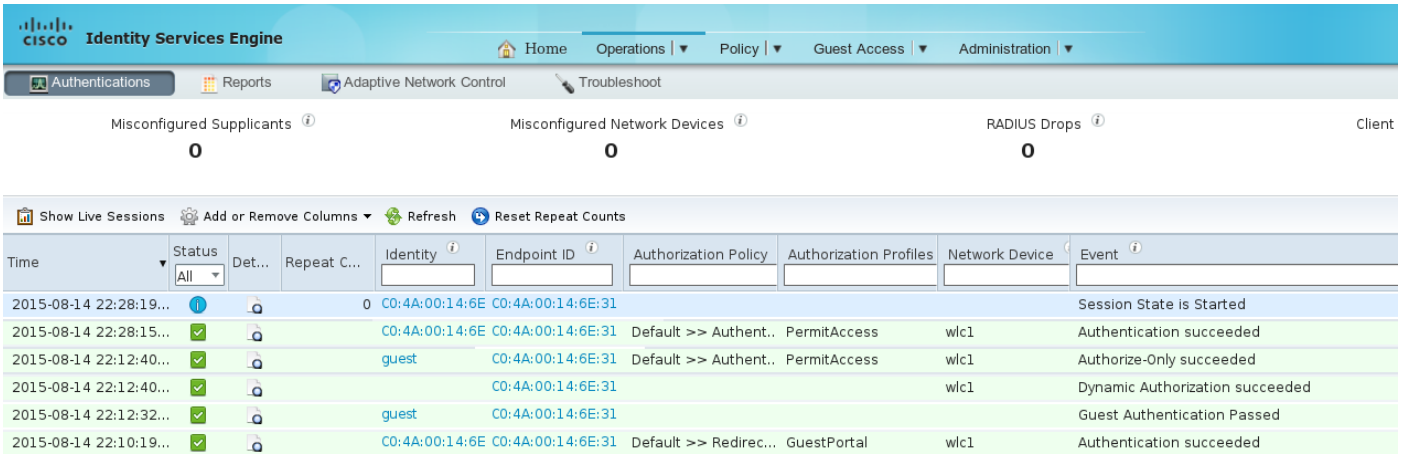
Überprüfen

Permanenter Zugriff

Nach der Umleitung zum Gastportal und erfolgreicher Authentifizierung sendet die ISE CoA (Change of Authorization), um eine erneute Authentifizierung auszulösen. Infolgedessen wird eine neue MAB-Sitzung (MAC Authentication Bypass) erstellt. Dieser Zeitendpunkt gehört zur Identitätsgruppe GuestEndpoints und stimmt mit einer Regel überein, die vollständigen Zugriff bereitstellt.

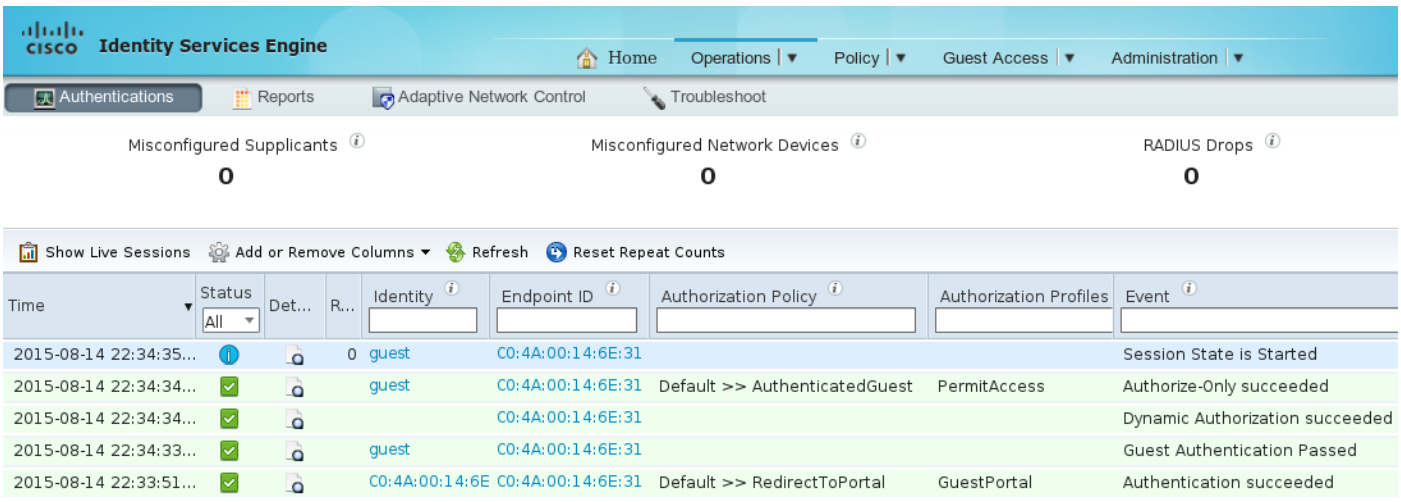


In dieser Phase kann der Wireless-Benutzer die Verbindung trennen, eine Verbindung zu verschiedenen WLANs herstellen und dann die Verbindung wieder herstellen. Alle diese nachfolgenden Authentifizierungen verwenden die Identität basierend auf der MAC-Adresse, treffen aber die erste Regel, weil der Endpunkt zu einer bestimmten Identitätsgruppe gehört. Der vollständige Netzwerkzugriff wird ohne Gastauthentifizierung bereitgestellt.

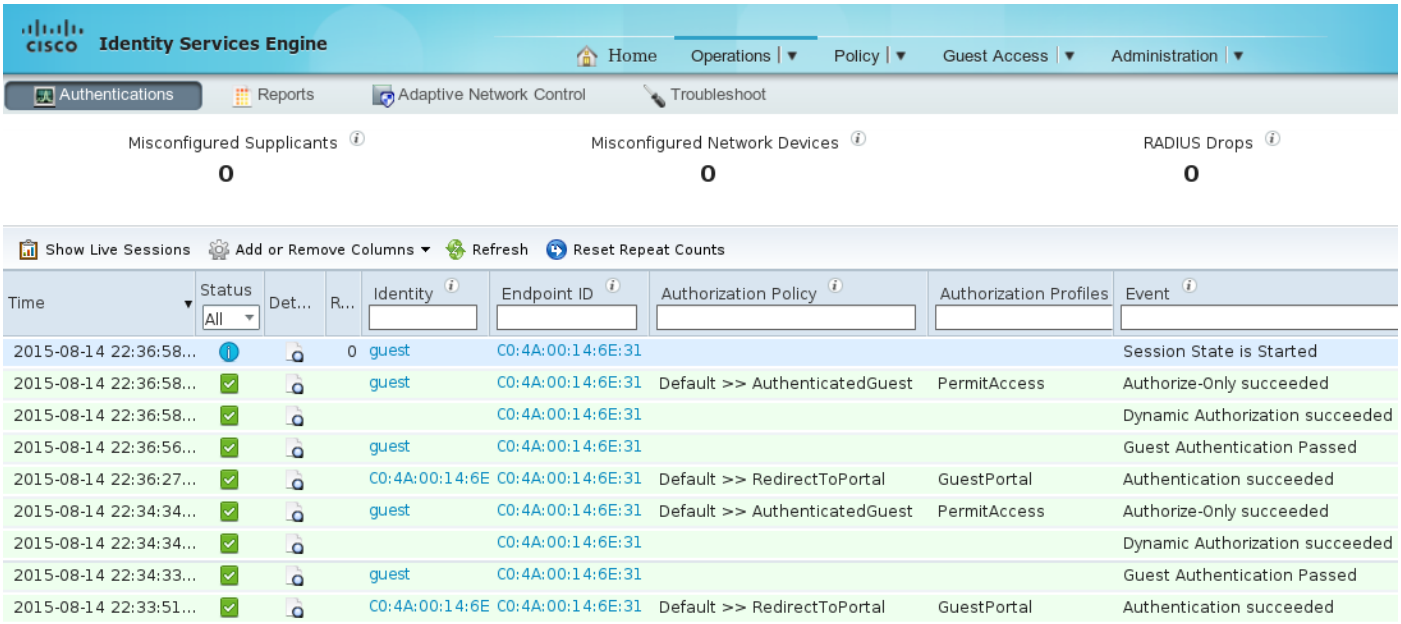


Temporärer Zugriff

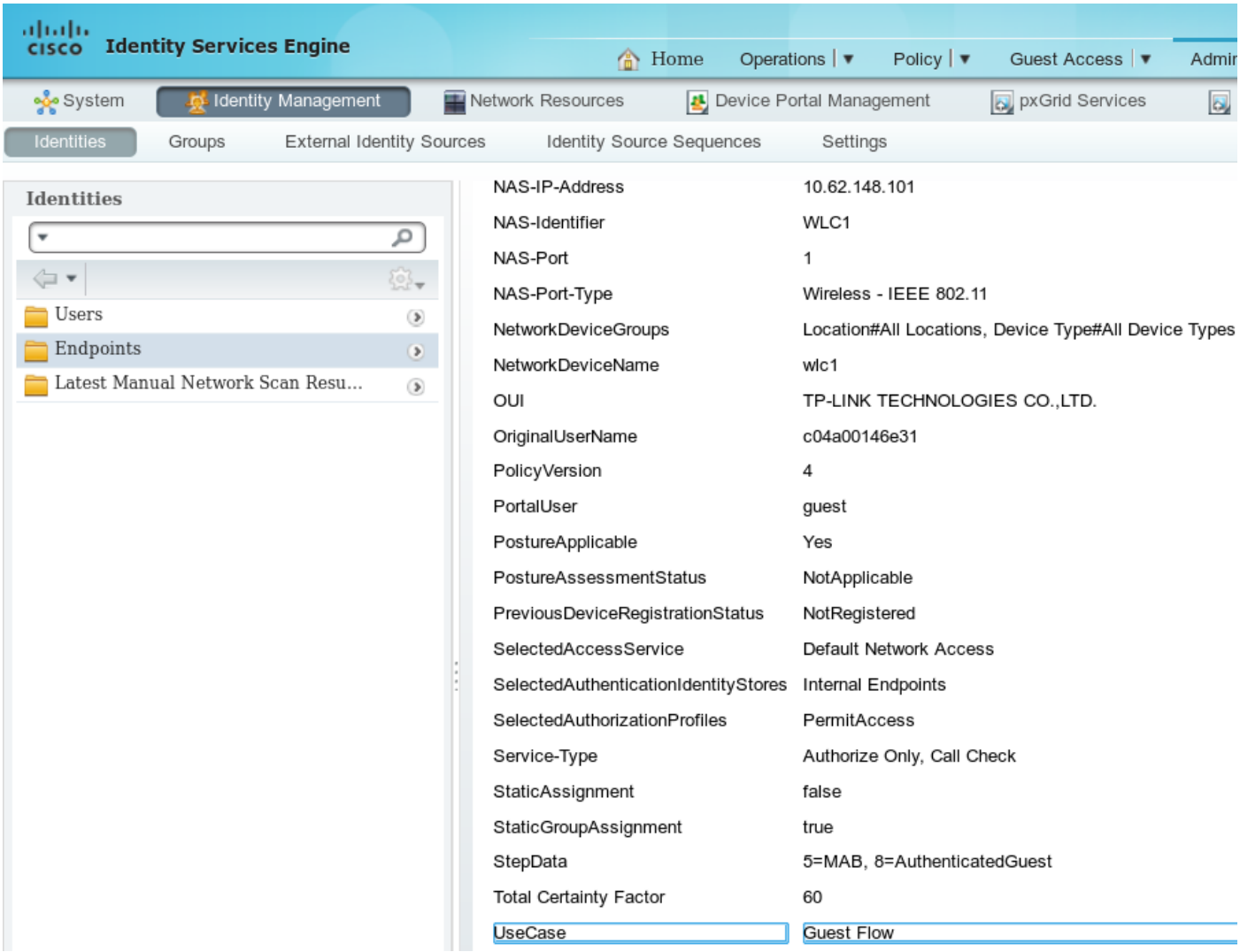
Für das zweite Szenario (mit einer Bedingung, die auf Guest Flow basiert) ist der Beginn identisch.



Nachdem die Sitzung jedoch für alle nachfolgenden Authentifizierungen entfernt wurde, trifft der Gast die generische Regel und wird erneut zur Gastauthentifizierung umgeleitet.



Die Bedingung für den Gastfluss ist erfüllt, wenn die richtigen Attribute für die Sitzung vorhanden sind. Dies lässt sich durch die Betrachtung von Endgeräteattributen überprüfen. Das Ergebnis der erfolgreichen Gastauthentifizierung wird angezeigt.




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

Bug

CSCuu41157 ISE ENH CoA wird bei Entfernung oder Ablauf eines Gastkontos beendet.

(Erweiterungsanfrage zur Beendigung von Gastsitzungen nach Entfernung oder Ablauf eines Gastkontos)

Referenzen

- Cisco ISE 1.3 Administratorhandbuch
- Cisco ISE 1.4 Administratorhandbuch
- Konfigurationsbeispiel für ISE-Version 1.3 Hotspot
- Konfigurationsbeispiel für das selbst registrierte Gastportal der ISE-Version 1.3
- Zentrale Webauthentifizierung im Konfigurationsbeispiel für WLC und ISE
- Zentrale Webauthentifizierung mit FlexConnect-APs auf einem WLC mit ISE-Konfigurationsbeispiel
- Technischer Support und Dokumentation - Cisco Systems