ISE Guest tijdelijke en permanente toegang configureren

Inhoud

Inleiding

In dit document worden verschillende methoden beschreven voor de toegangsconfiguratie van de Identity Services Engine (ISE). Op grond van verschillende voorwaarden in de vergunningsregels:

- permanente toegang tot het net is mogelijk (geen vereiste voor latere echtheidscontroles)
- tijdelijke toegang tot het netwerk kan worden verleend (hiervoor is de verificatie van de gast na afloop van de sessie vereist)

Ook het specifieke WLC-gedrag (Wireless LAN Controller) voor sessieverwijdering wordt langs de impact op een tijdelijk toegangsscenario gepresenteerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ISE-implementaties en Guest-stromen
- Configuratie van draadloze LAN-controllers (WLC's)

Gebruikte componenten

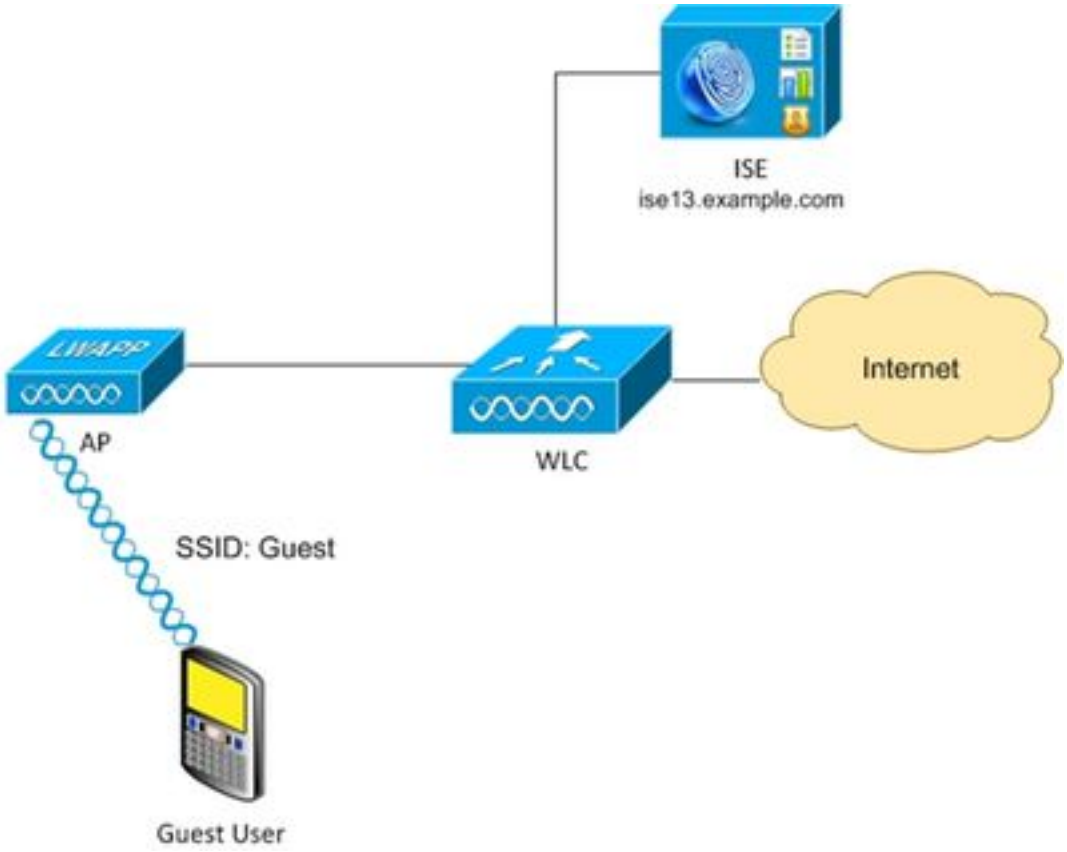
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 7
- Cisco WLC versie 7.6 en hoger
- ISE-software, versie 1.3 en hoger

Configureren

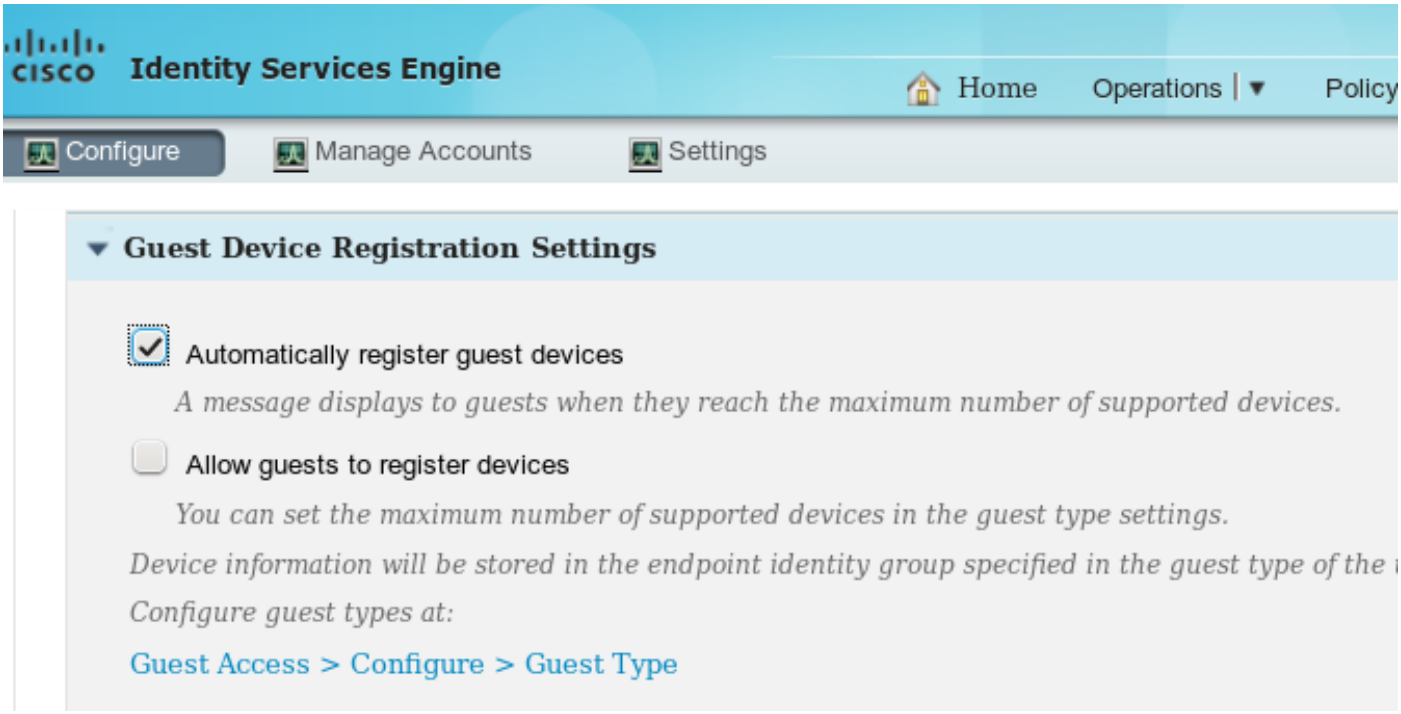
Voor basisconfiguratie van de toegang van een gast kunt u referenties met configuratievoorbeelden controleren. Dit artikel richt zich op de configuratie van de vergunningsregels en op verschillen in de vergunningsvoorwaarden.

Netwerkdiagram

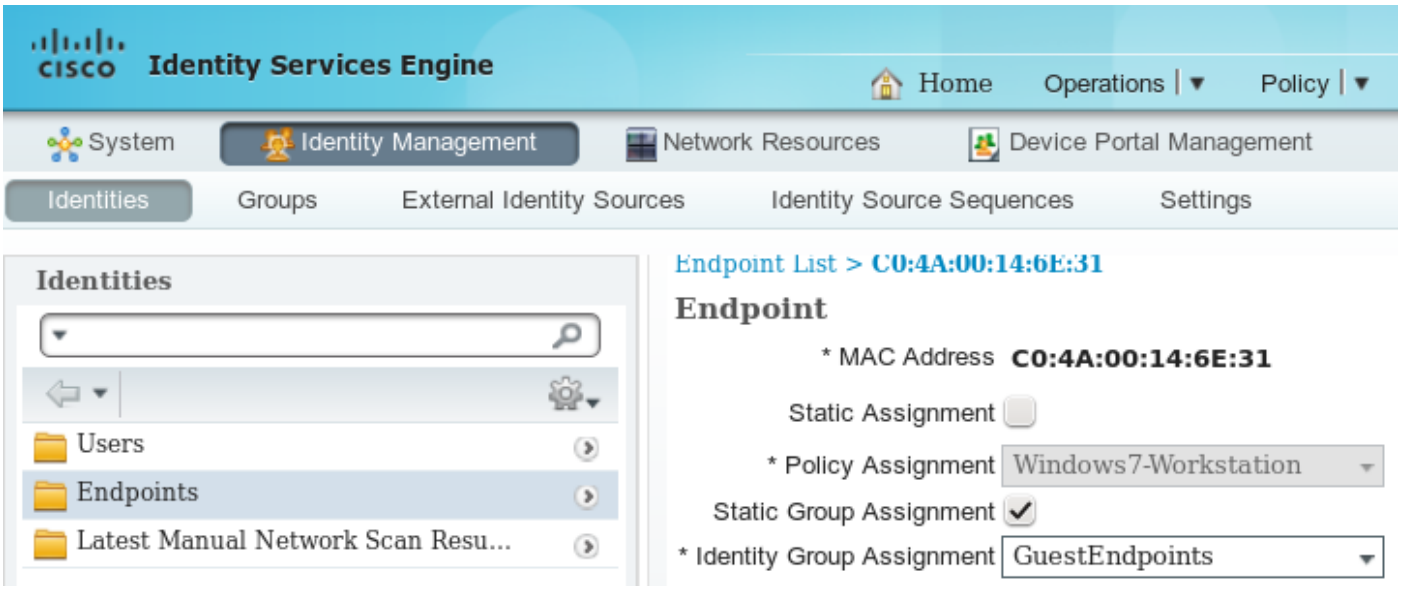


Permanente toegang

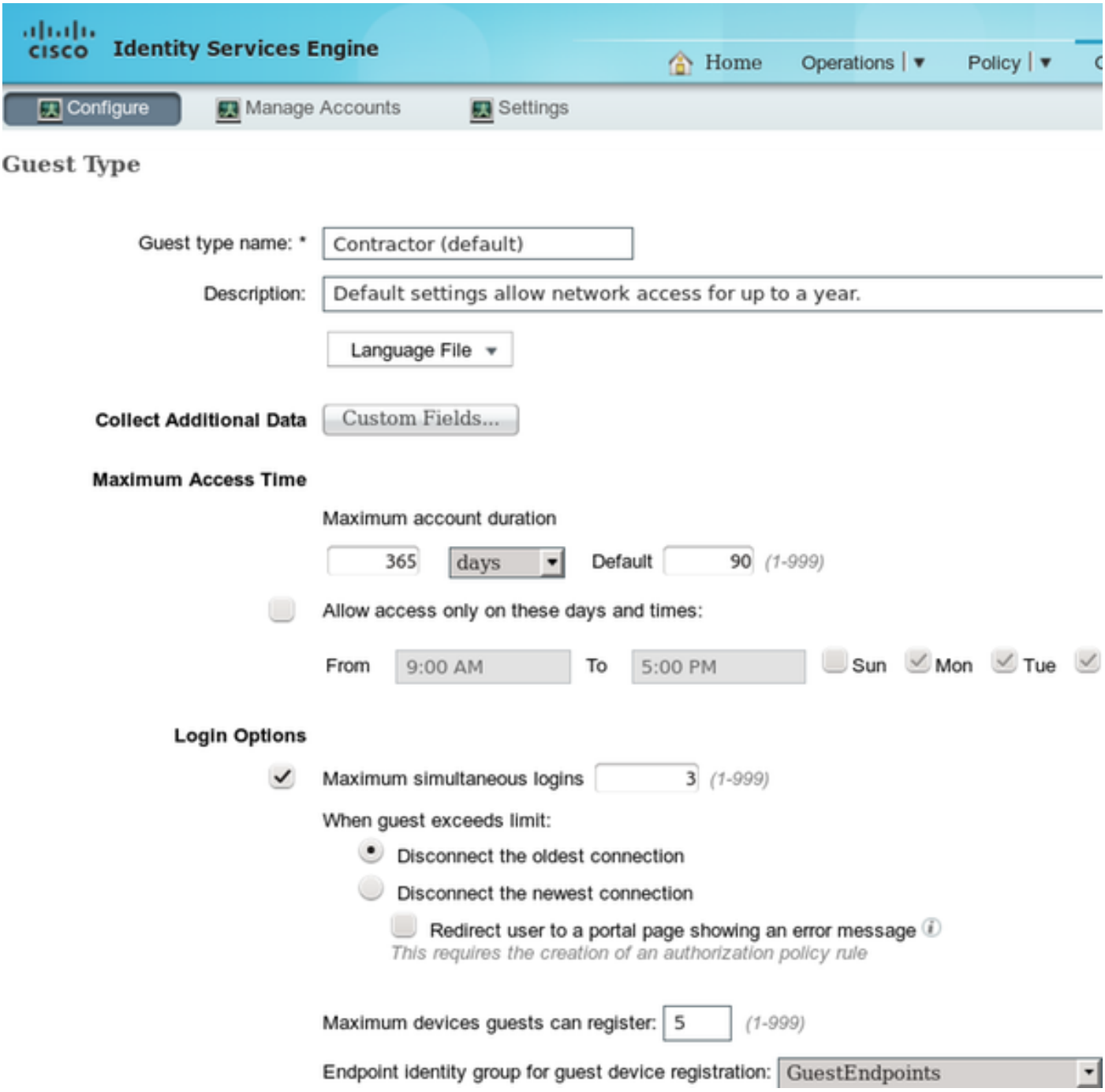
Voor ISE versie 1.3 en nieuwer na succesvolle authenticatie in het gastportaal met apparaatregistratie ingeschakeld.



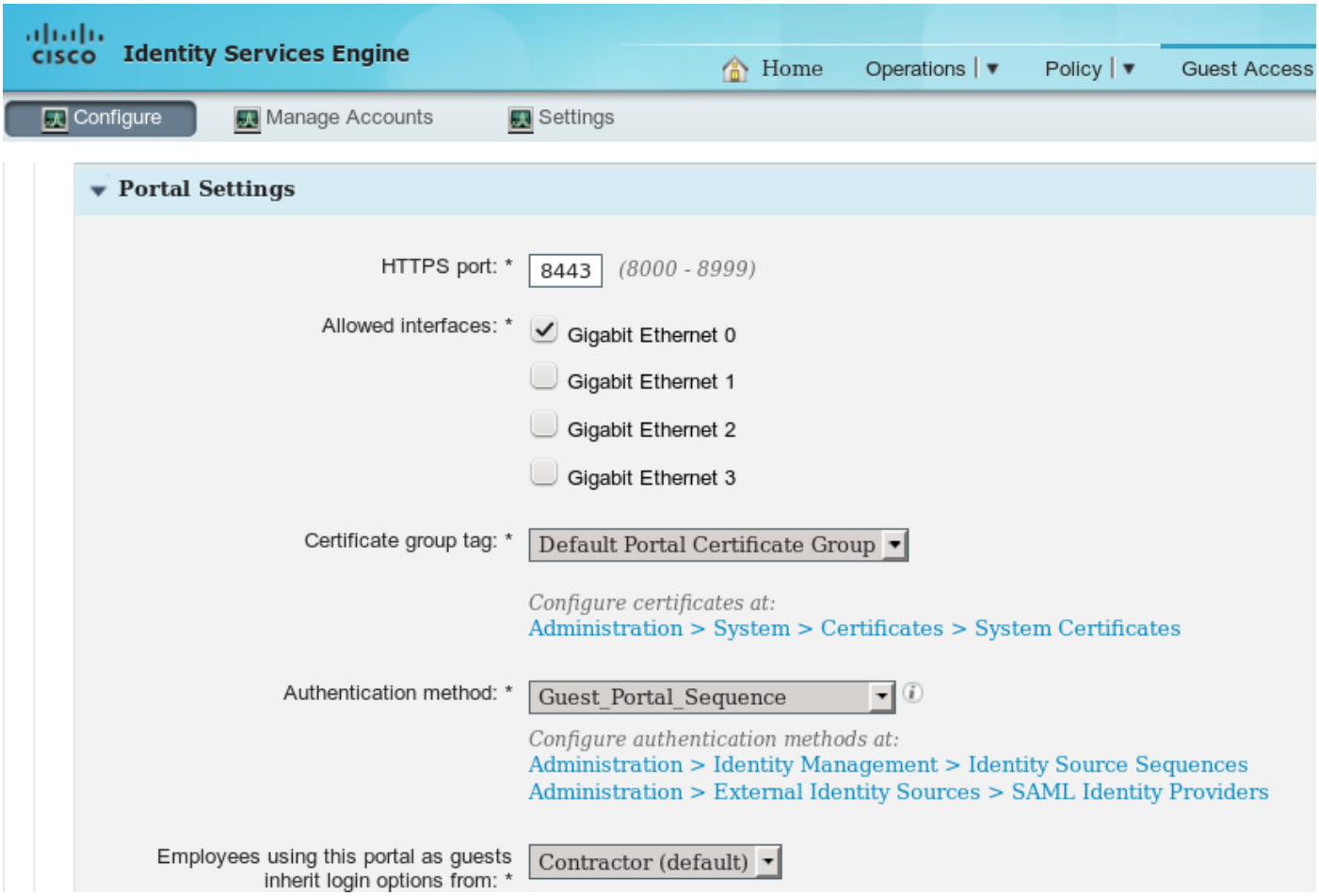
Endpoint device (mac-adres) is statistisch geregistreerd in specifieke endpointgroepen (GuestEndpoints in dit voorbeeld).



Deze groep is afgeleid van het gasttype van de gebruiker, zoals in deze afbeelding wordt getoond.



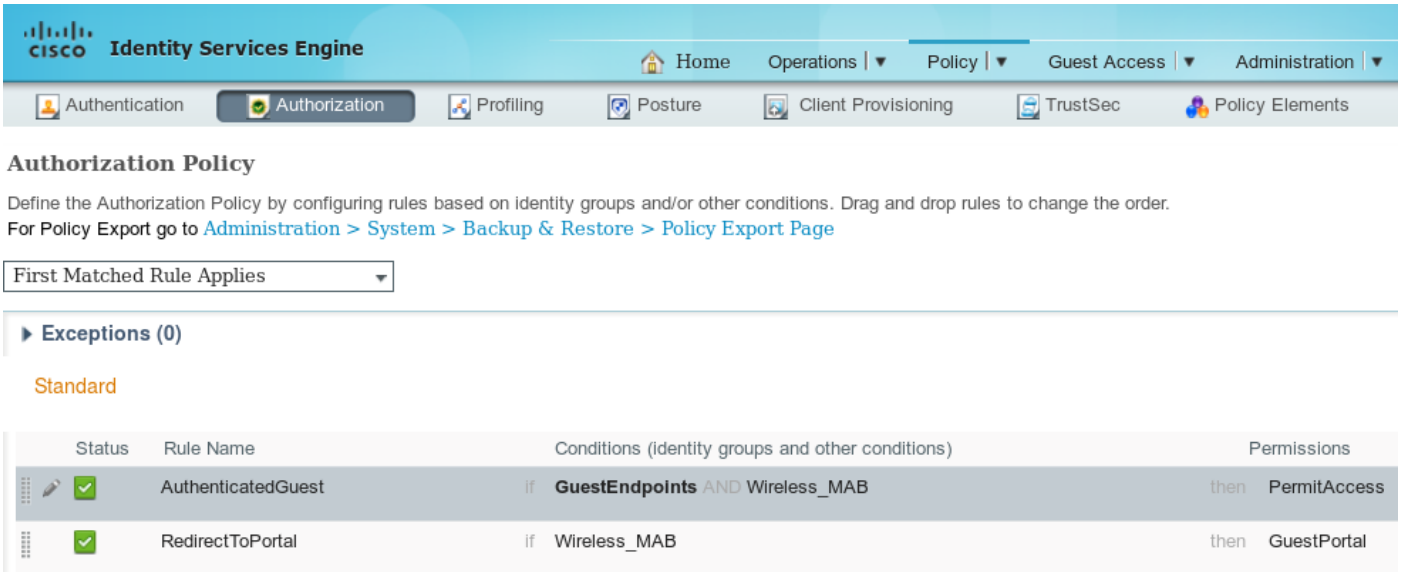
Als het een zakelijke gebruiker is (identiteitswinkel andere dan gast) die instelling is afgeleid van de portal instellingen.



Als gevolg daarvan behoort het met de gast verbonden hoofdadres altijd tot die specifieke identiteitsgroep. Dit kan niet automatisch worden gewijzigd (bijvoorbeeld door Profiler Service).

> Opmerking: Voor het toepassen van Profiler resultaten kan de voorwaarden van de EndPointPolicy autorisatie worden gebruikt.

Het weten dat het apparaat altijd deel uitmaakt van een specifieke eindpuntidentiteitsgroep is mogelijk om op basis daarvan goedkeuringsregels op te stellen, zoals in deze afbeelding wordt getoond.

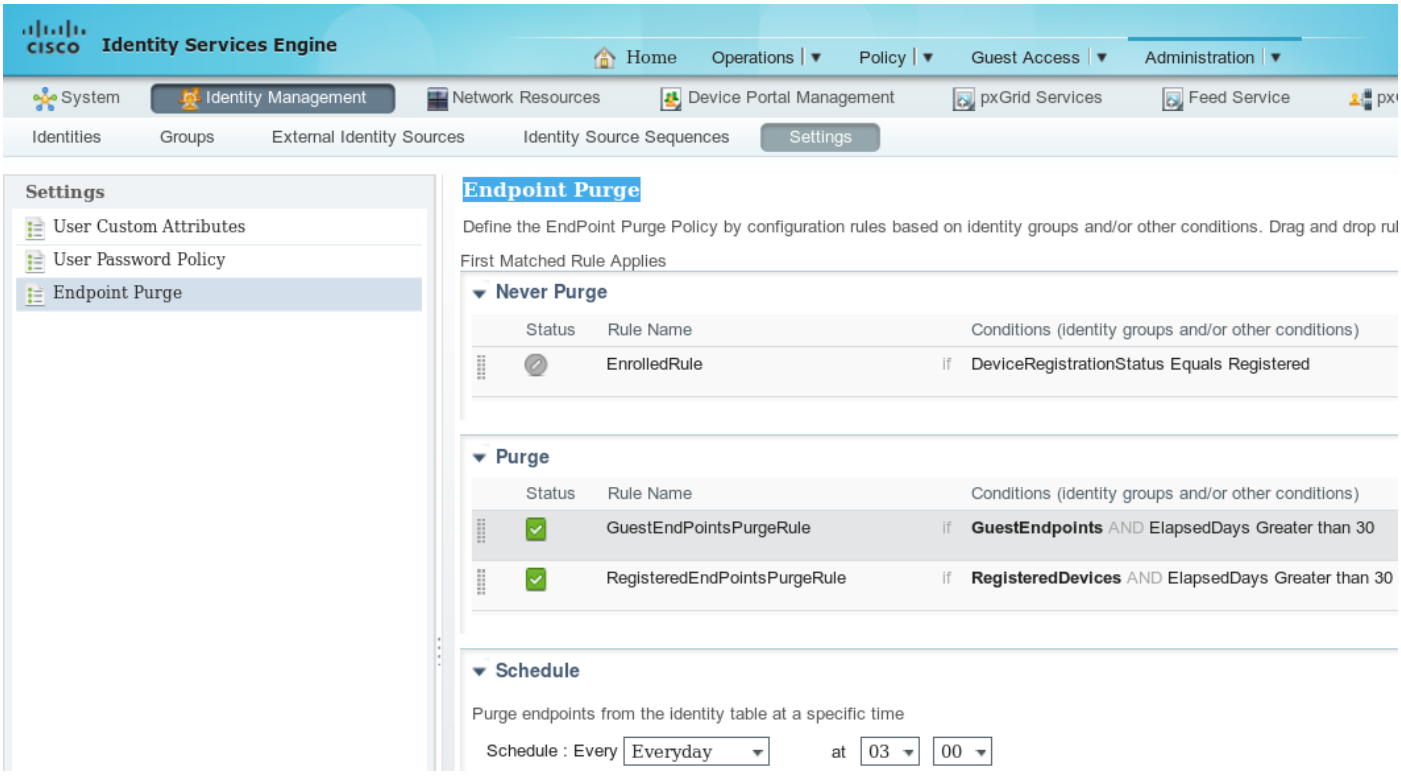


Zodra een gebruiker niet echt is bevonden, komt de autorisatie overeen met generieke regel

RedirectToPortal. Na omleiding naar het gastportal en verificatie wordt het eindpunt geplaatst in de specifieke eindpuntidentiteitsgroep. Dat wordt gebruikt door de eerste, specifiekere voorwaarde. Alle latere authenticaties van dat eindpunt bereiken de eerste machtigingsregel en de gebruiker wordt volledige netwerktoegang verleend zonder de noodzaak om op het gastportaal opnieuw te authentiseren.

Endpoint Purge voor Guest Account

Deze situatie kan eeuwig duren. Maar in ISE 1.3 is Purge Endpoint functionaliteit geïntroduceerd. Met de standaardconfiguratie.



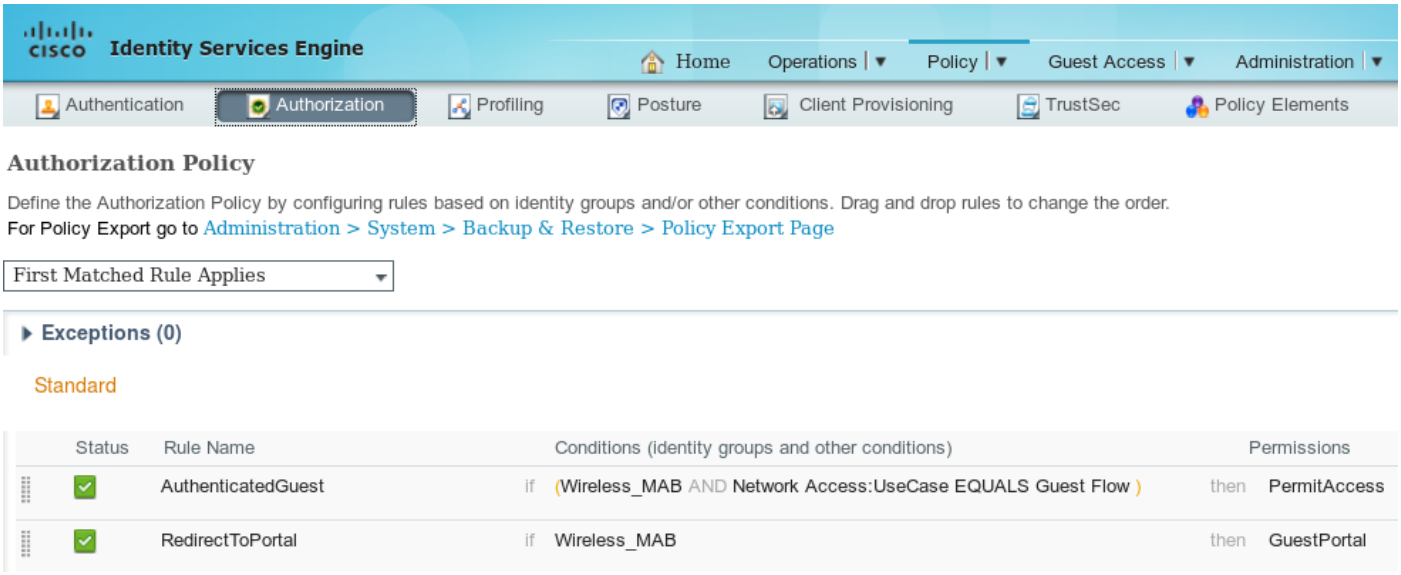
Alle eindpunten die gebruikt worden voor gastverificatie worden na 30 dagen verwijderd (na het maken van eindpunt). Het resultaat is gewoonlijk na 30 dagen dat de gastgebruiker probeert om toegang te krijgen tot de autorisatieregel van RedirectToPortal en wordt opnieuw gericht voor authenticatie.

> Opmerking: Endpoint Purge-functionaliteit is onafhankelijk van het beleid voor het zuiveren van uw account en het aflopen van uw account.

> Opmerking: In ISE 1.2 kunnen endpoints alleen automatisch worden verwijderd wanneer ze de limieten van de interne wachtrij voor profielen raken. Laatst gebruikte eindpunten worden dan verwijderd.

Tijdelijke toegang

Een andere methode voor gastentoegang is de Guest Flow conditie te gebruiken.



Die voorwaarde is het controleren van actieve sessies op ISE en het zijn eigenschappen. Als die sessie de eigenschap heeft die erop wijst dat de vorige gastgebruiker voor echt geauthentiseerd is voorwaarde wordt gematcht. Nadat ISE het bericht van de Voorbereiding van Radius van het Netwerk toegangsapparaat (NAD) ontvangt, wordt de sessie beëindigd en later verwijderd. In dat stadium is de conditie Network Access:UseCase = Guest Flow niet meer tevreden. Als resultaat hiervan bereikt alle verdere authenticaties van dat eindpunt generieke regel die omleiding voor gastauthenticatie.

> Opmerking: Guest Flow wordt niet ondersteund wanneer de gebruiker geauthentiseerd is via het Hot Folder-portal. Voor die scenario's is de eigenschap UseCase ingesteld op Host Lookup in plaats van Guest Flow.

WLC-gedrag van verbroken verbinding

Nadat klanten van draadloos netwerk losmaakt (bijvoorbeeld het gebruiken van losconnect knop in Windows) verstuurt het een authentificatiekader. Maar die is weggelaten door de WLC en kan worden bevestigd met behulp van "debug client xxxx" - WLC levert geen debugs op wanneer client wordt losgekoppeld van WLAN. Als resultaat bij Windows client:

- IP-adres wordt uit de interface verwijderd
- de interface staat in : media losgekoppeld

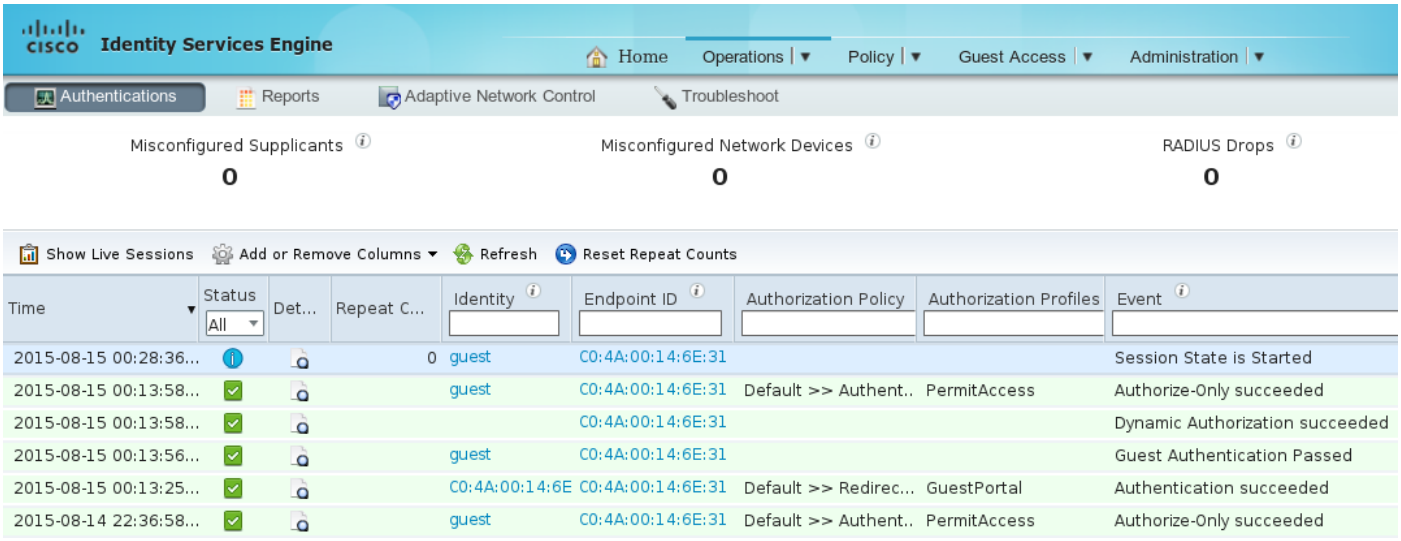
Maar op WLC is de status onveranderd (client nog steeds in RUN-status).

Dat is het geplande ontwerp voor WLC, de sessie wordt verwijderd wanneer

- hits als gebruikers die geen toegang tot de ether hebben
- hits in de sessie
- als L2-encryptie wordt gebruikt, dan wanneer het groep key interval bereikt
- iets anders veroorzaakt dat AP/WLC de client afschoppen (bijvoorbeeld AP-radio resets, iemand sluit de WLAN, enz.)

Met dat gedrag en de tijdelijke toegangsconfiguratie nadat gebruikers hun verbindingen hebben verbroken van WLAN-sessie, wordt niet verwijderd van ISE omdat WLC deze nooit heeft geklaard (en nooit Radius Accounting Stop heeft verzonden). Als de sessie niet wordt verwijderd, herinnert ISE zich nog steeds oude sessie en is de toestand van de gastenstroom bevredigend. Na het afsluiten en opnieuw verbinden heeft de gebruiker volledige netwerktoegang zonder vereiste om

opnieuw te bevestigen.



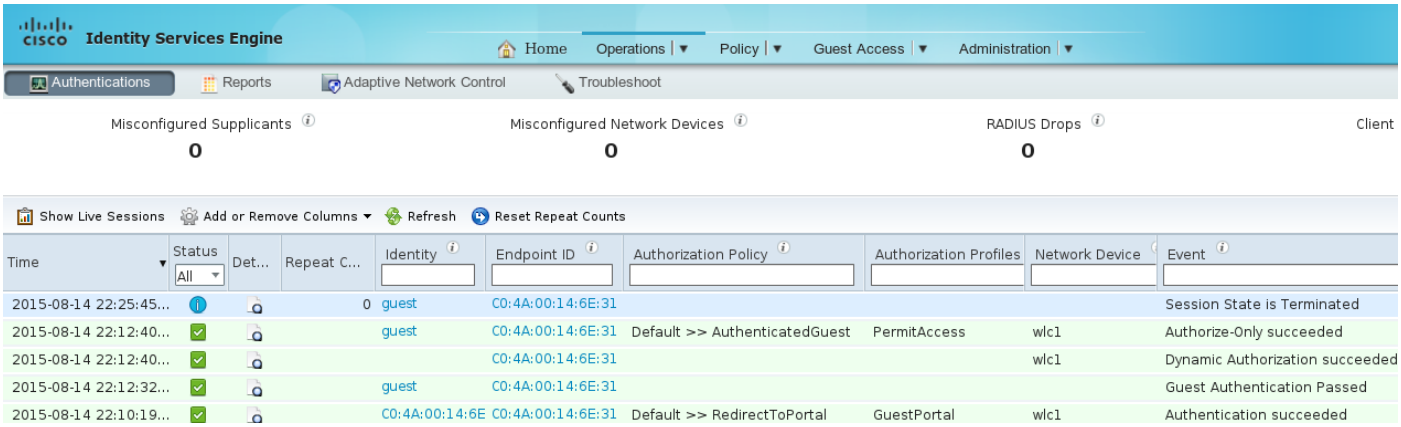
Maar als een gebruiker die de verbinding met een ander WLAN heeft verbroken, beslist WLC om de oude sessie te wissen. Radius accounting Stop wordt verzonden en ISE verwijdert de sessie. Als de client probeert verbinding te maken met de oorspronkelijke WLAN-status is de gebruiker niet tevreden en wordt de gebruiker opnieuw gericht op verificatie.

> Opmerking: WLC ingesteld met Management Frame Protection (MFP) accepteert versleuteld verificatiekader van CCXv5 MFP-client.

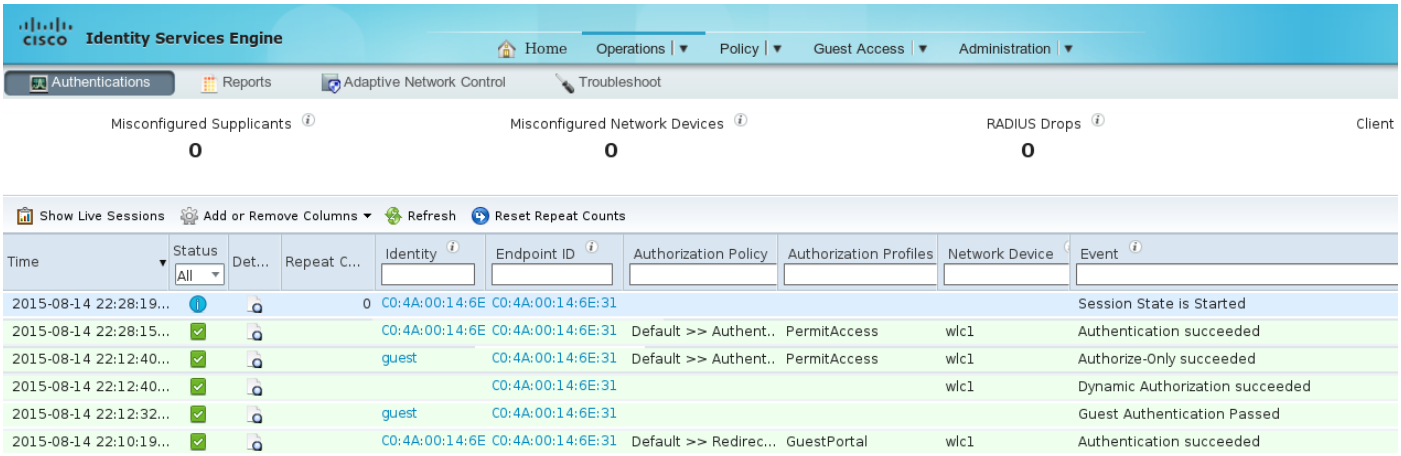
Verifiëren

Permanente toegang

Na omleiding naar het gastportaal en succesvolle authenticatie stuurt ISE een wijziging van de vergunning (CoA) om verificatie te starten. Als resultaat hiervan wordt er een nieuwe MAC Verificatie Bypass (MAB)-sessie gebouwd. Dit tijd-eindpunt behoort tot de identiteitsgroep van GuestEndpoints en de wedstrijdregel die volledige toegang verleent.

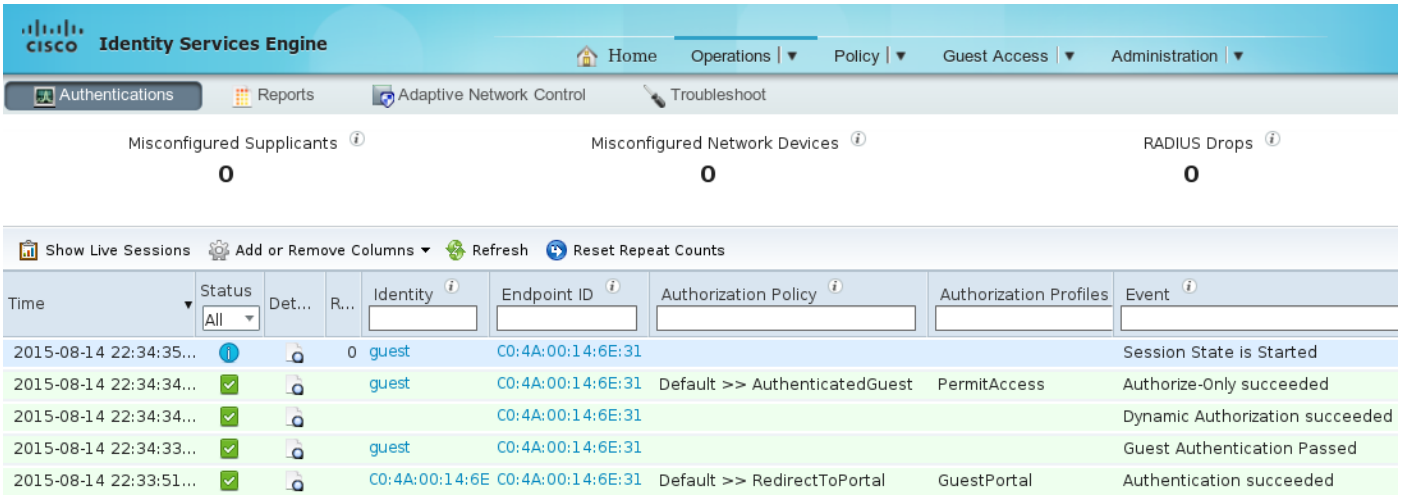


In dat stadium kan de draadloze gebruiker de verbinding verbroken, verbinding maken met verschillende WLAN's en vervolgens opnieuw aansluiten. Al die latere authenticaties gebruiken een identiteit gebaseerd op het mac-adres, maar slaan de eerste regel aan vanwege het eindpunt dat tot een specifieke identiteitsgroep behoort. Volledige netwerktoegang wordt geboden zonder gastverificatie.

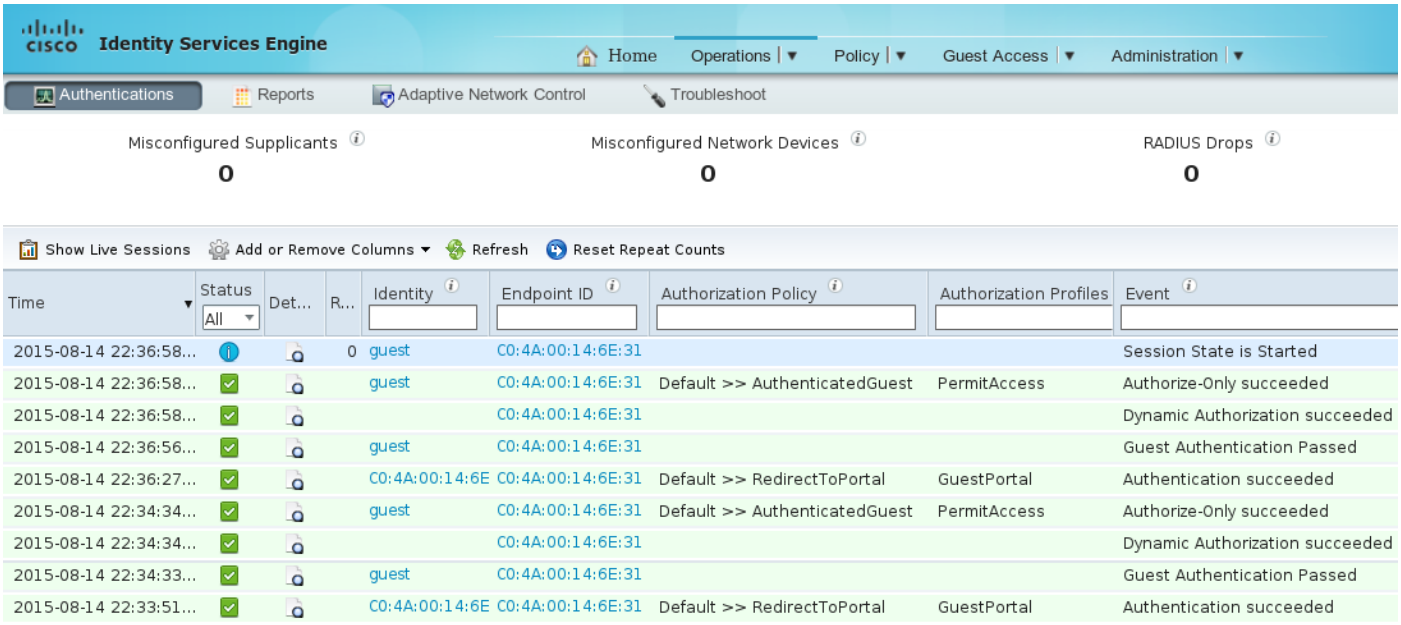


Tijdelijke toegang

Voor het tweede scenario (met conditie gebaseerd op Guest Flow) is het begin hetzelfde.

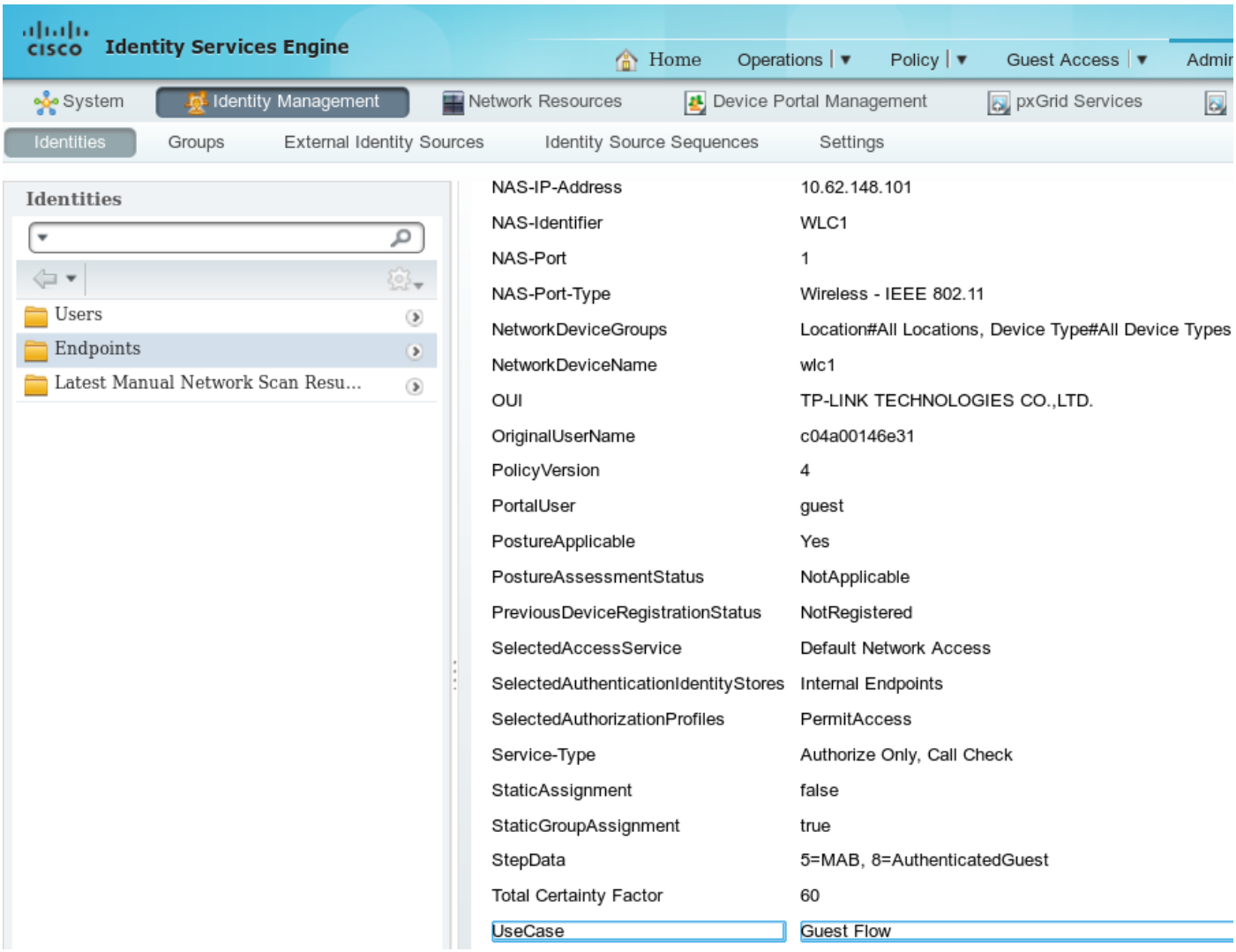


Maar nadat de sessie voor alle latere authenticaties is verwijderd, slaat gast algemene regels op en wordt opnieuw gericht voor gastauthenticatie.



De voorwaarde van de stroom van de gast is tevreden wanneer de juiste eigenschappen voor de zitting bestaan. Dat kan worden geverifieerd door te kijken naar de eigenschappen van het

eindpunt. Het resultaat van geslaagde verificatie van gasten wordt aangegeven.




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

Bugs

CSCuu41157 ISE ENH CoA beëindigen de verzending van een gastaccount of het verlopen van het account.

(verzoek om versterking om gastsessies te beëindigen na verwijdering of beëindiging van de gastaccount)

Referenties

- Cisco ISE 1.3 beheerdershandleiding
- Cisco ISE 1000 1000 1000 1000000000 SERIES BEHEERDERS
- ISE versie 1.3 Configuratievoorbeeld voor hotspotjes
- Configuratievoorbeeld van ISE versie 1.3, zelfgeregistreerd Guest Portal
- Central-webverificatie in het configuratievoorbeeld van WLC en ISE
- Central-webverificatie met FlexConnect APs op een WLC met ISE-configuratievoorbeeld

- Technische ondersteuning en documentatie – Cisco Systems