Acceso temporal y permanente del invitado de la configuración ISE

Contenido

Introducción

Este documento describe los métodos distintos para la configuración del acceso de invitado del Identity Services Engine (ISE). De acuerdo con diversas condiciones en las reglas de la autorización:

- el acceso permanente a la red puede ser proporcionado (ningún requisito para las autenticaciones subsiguientes)
- el Acceso temporario a la red puede ser proporcionado (requiriendo la autenticación del invitado después de que expire la sesión)

También el comportamiento específico del regulador del Wireless LAN (WLC) para el retiro de la sesión se presenta a lo largo del impacto en el escenario del Acceso temporario.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Implementaciones ISE y flujos del invitado
- Configuración de los reguladores del Wireless LAN (WLCs)

Componentes Utilizados

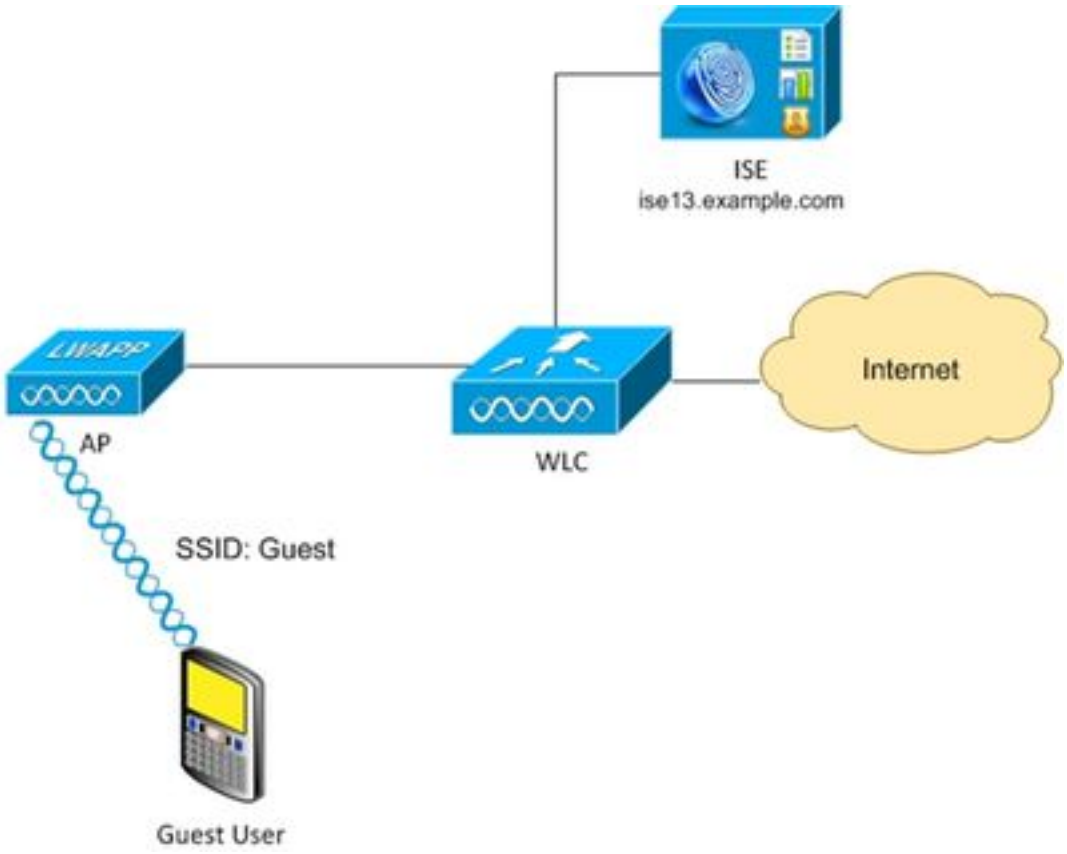
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows 7
- Versión 7.6 y posterior del WLC de Cisco
- Software ISE, versión 1.3 y posterior

Configurar

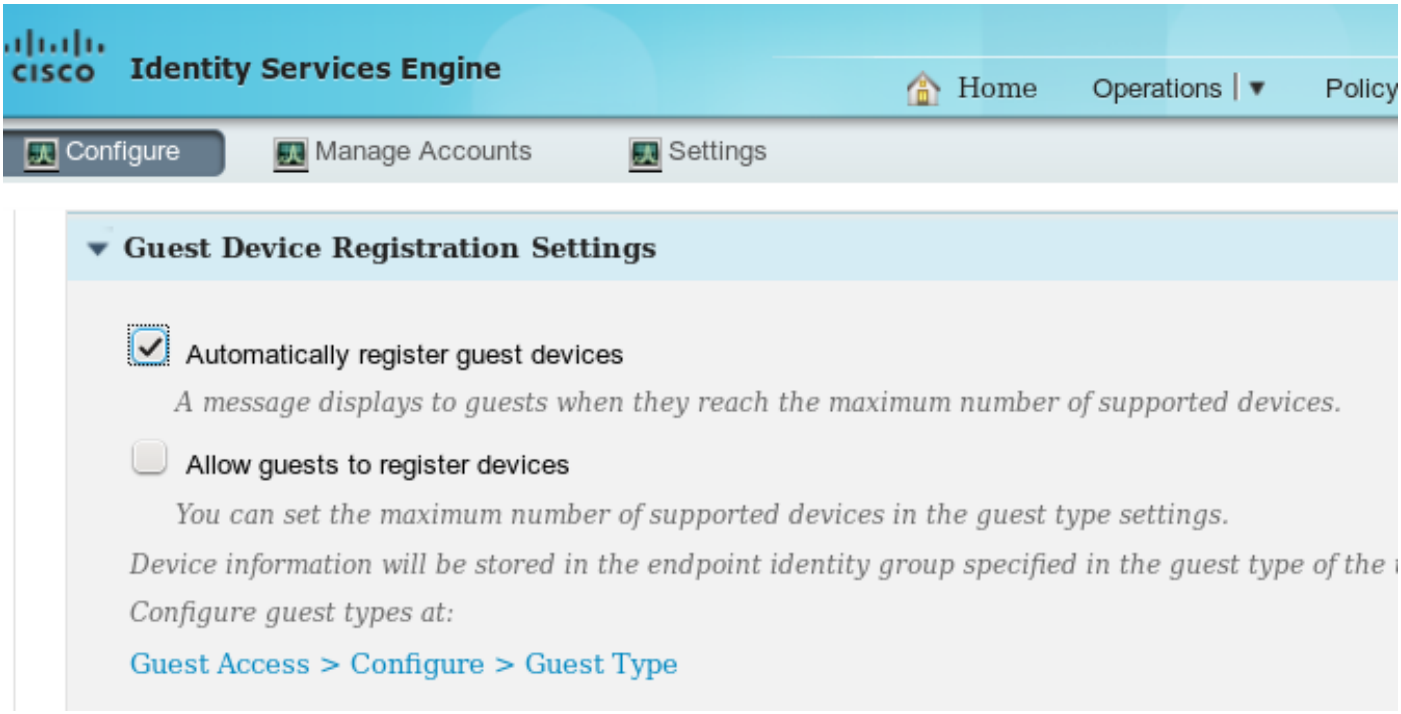
Para la configuración básica del acceso de invitado marque por favor las referencias con los ejemplos de configuración. Este artículo se centra en las reglas configuración y diferencias de la autorización en las condiciones de la autorización.

Diagrama de la red

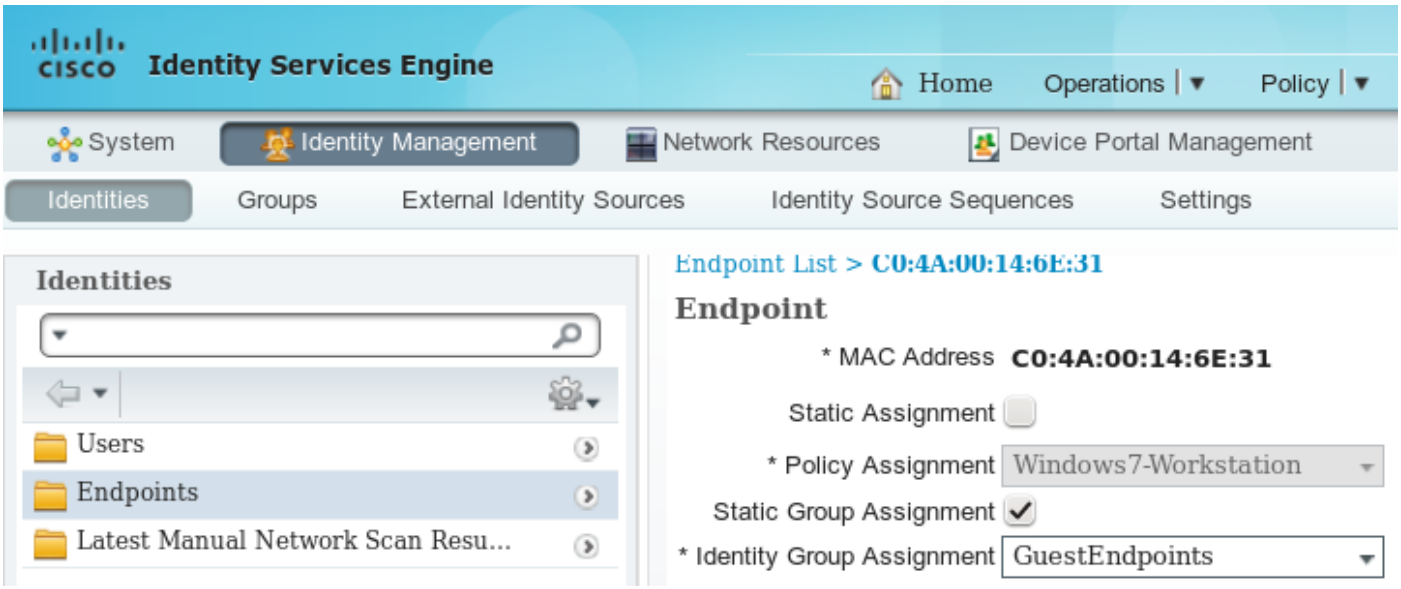


Acceso permanente

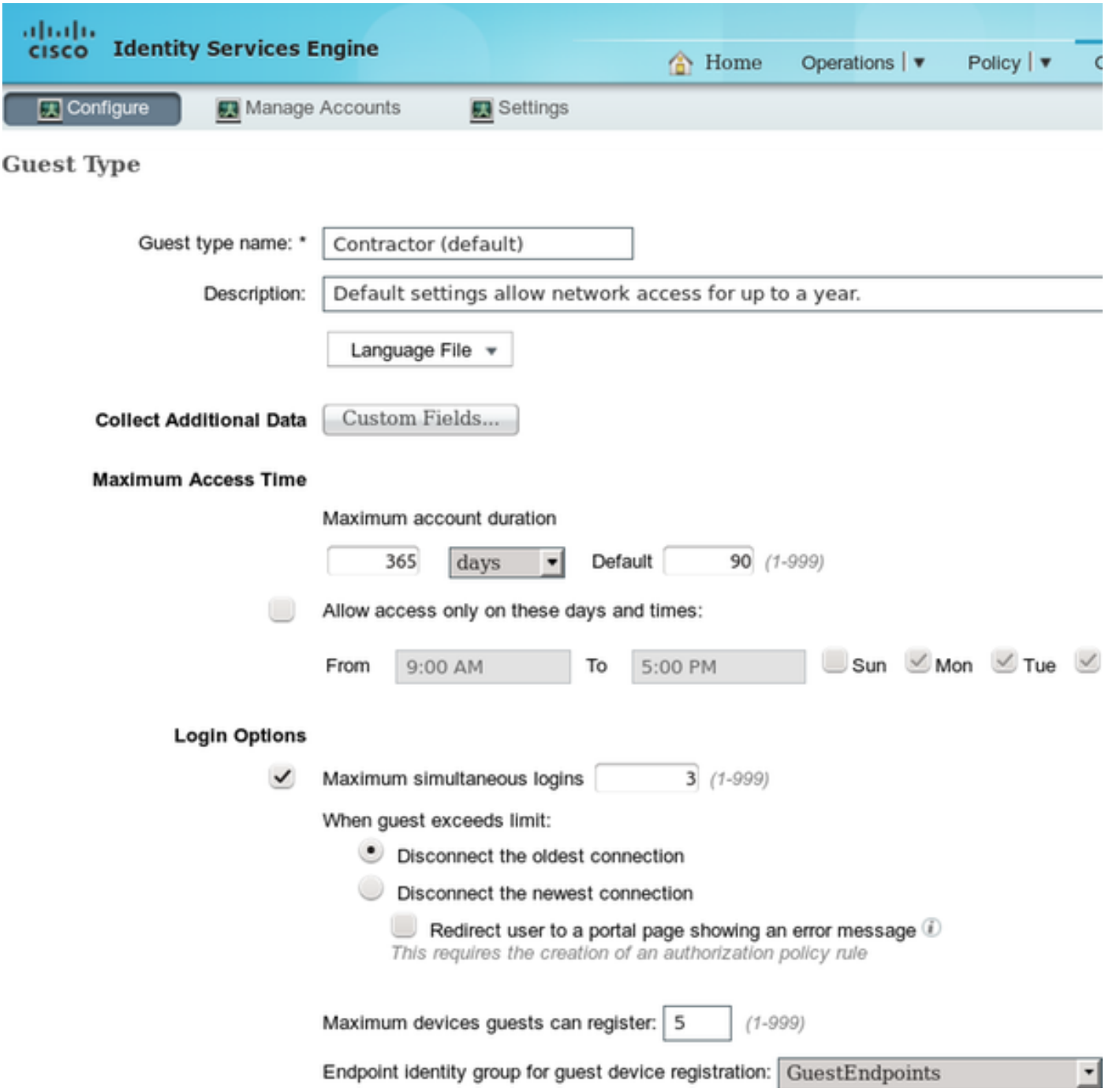
Para la versión 1.3 posterior ISE después de la autenticación satisfactoria en el portal del invitado con el registro del dispositivo habilitado.



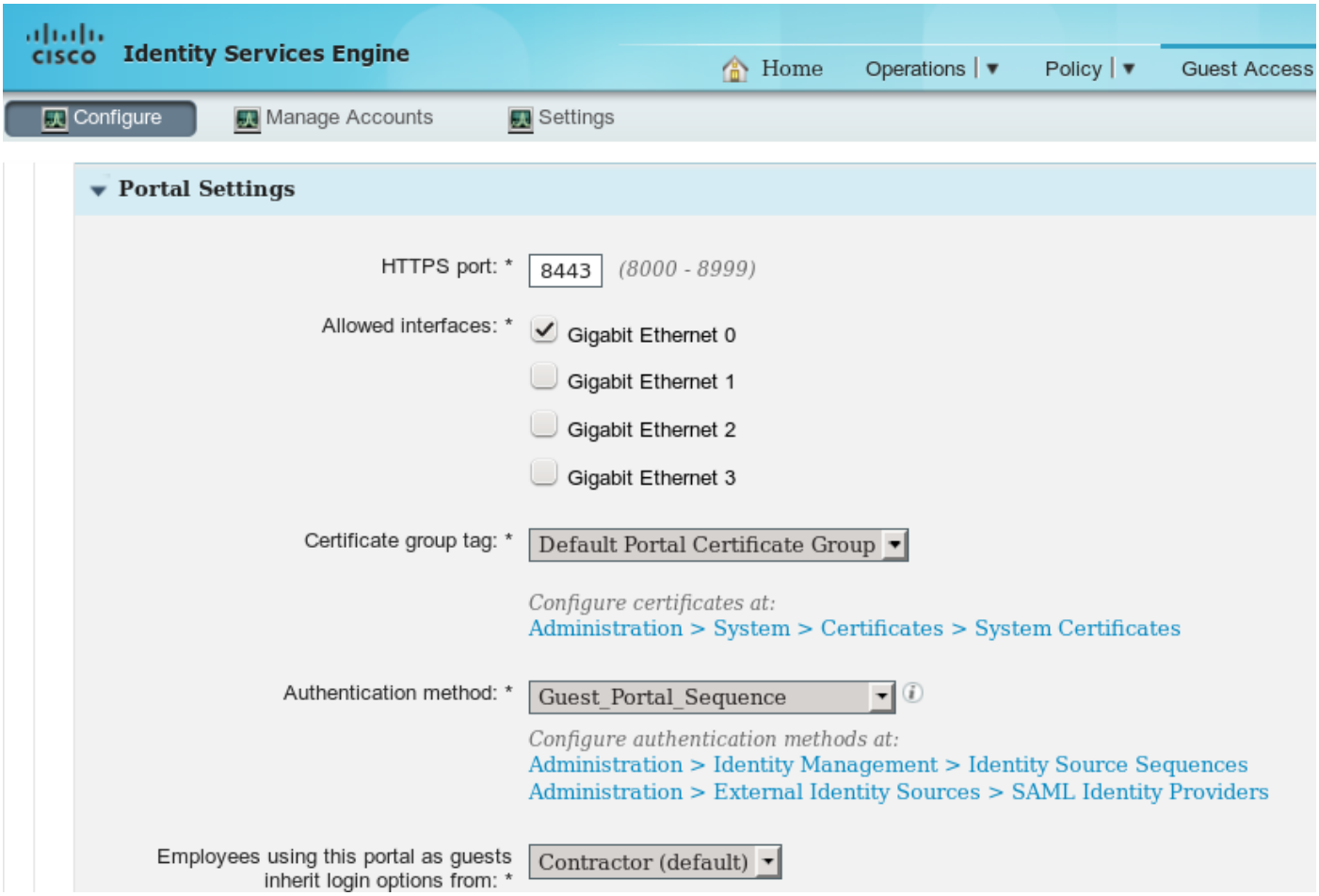
El dispositivo de punto final (MAC address) se registra estáticamente en el grupo específico del punto final (GuestEndpoints en este ejemplo).



Derivan a ese grupo del tipo del invitado del usuario, tal y como se muestra en de esta imagen.



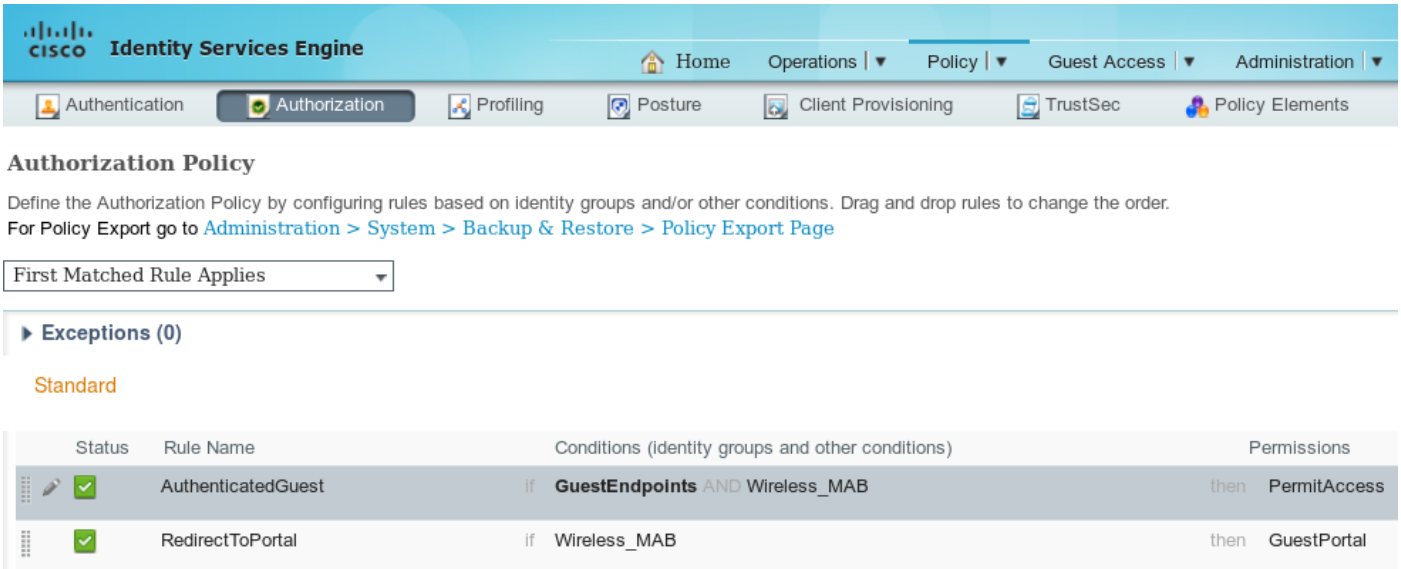
Si es usuario corporativo (almacén de la identidad el otro entonces invitado) esa configuración se deriva de las configuraciones porta.



Como consecuencia el MAC address asociado al invitado pertenece siempre a ese grupo específico de la identidad. Eso no puede ser cambiada automáticamente (por ejemplo por el servicio del Profiler).

> **Note**: Para aplicar la condición de la autorización de EndPointPolicy de los resultados del Profiler puede ser utilizada.

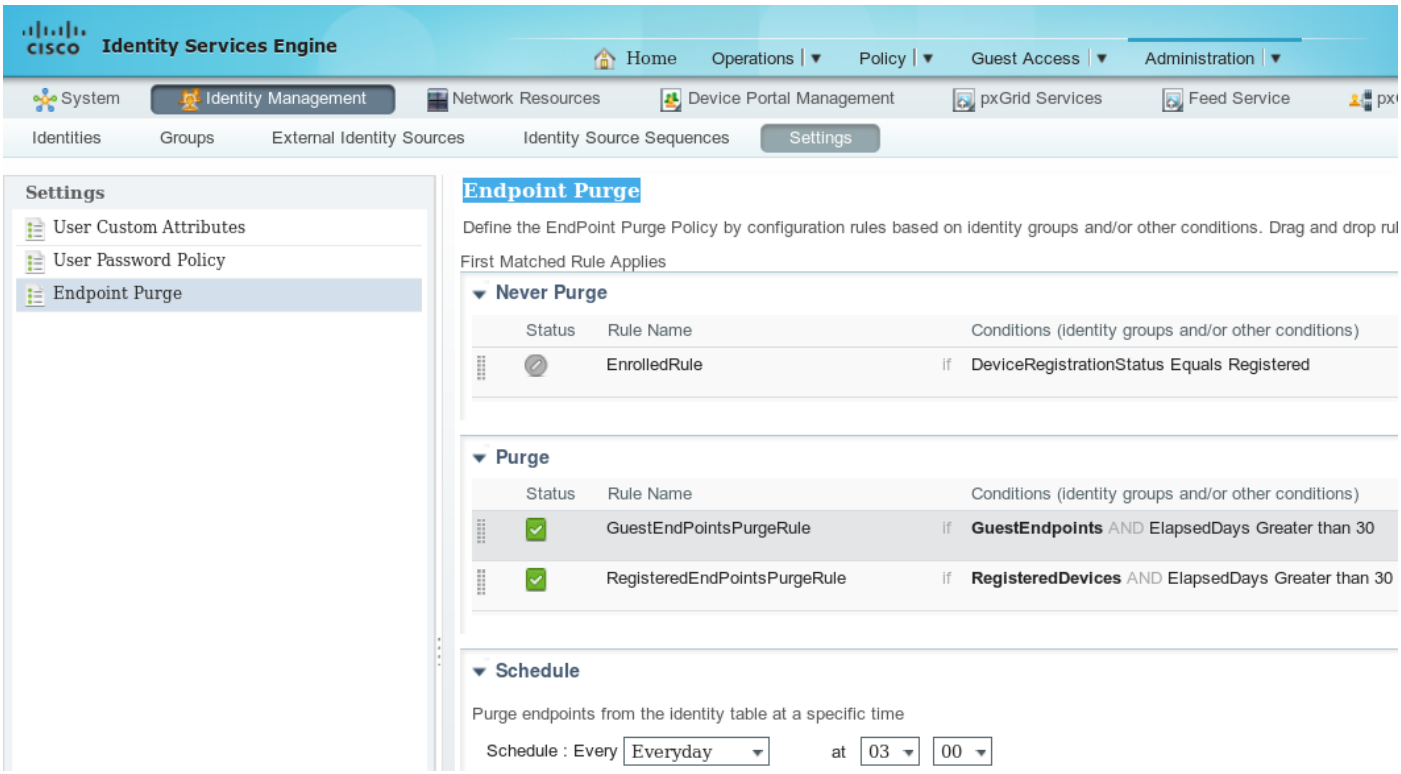
Sabiendo que el dispositivo pertenece siempre al grupo específico de la identidad del punto final que es posible construir las reglas de la autorización basadas en ésa, tal y como se muestra en de esta imagen.



Una vez que no autentican a un usuario, la autorización hace juego la regla genérica RedirectToPortal. Después del cambio de dirección al portal y a la autenticación del invitado, el punto final se pone en el grupo específico de la identidad del punto final. Eso es utilizada por el primer, una condición más específica. Todas las autenticaciones subsiguientes de ese punto final golpean la primera regla de la autorización y el usuario es acceso a la red completo proporcionado sin la necesidad de reautentificar en el portal del invitado.

Purgación del punto final para las cuentas de invitado

Esta situación podía durar para siempre. Pero en el punto final de la purgación ISE 1.3 se han introducido las funciones. Con la configuración predeterminada.



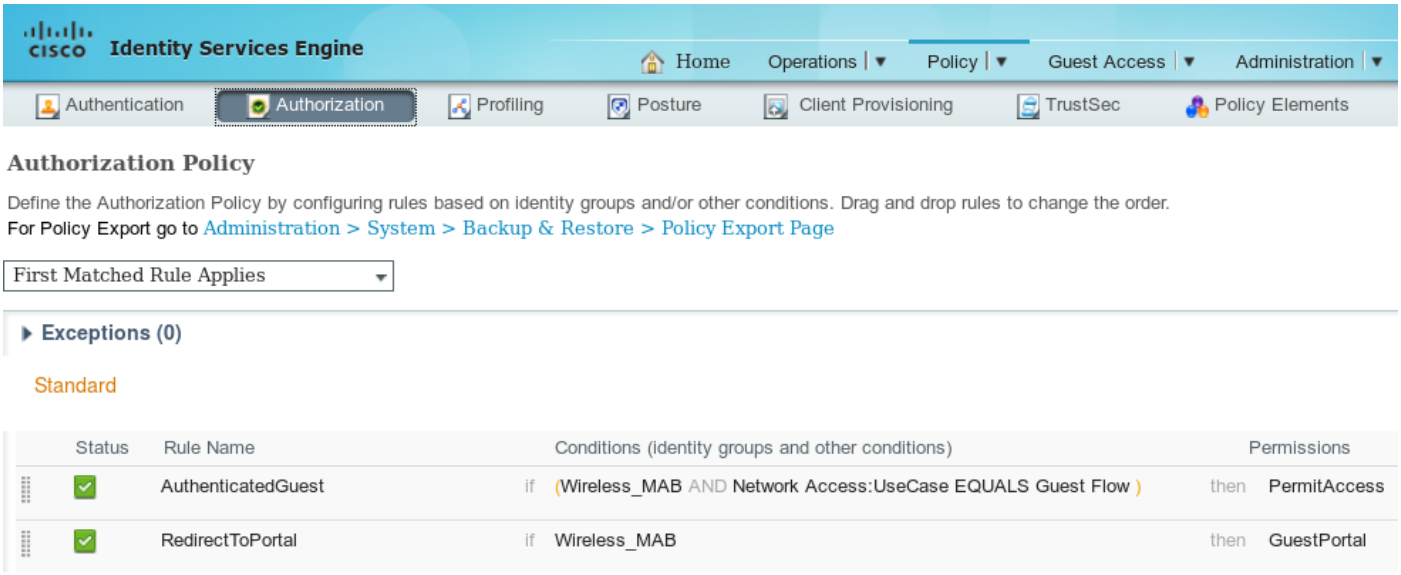
Todos los puntos finales usados para la autenticación del invitado se quitan después de 30 días (de la creación del punto final). Como consecuencia después de 30 días el Usuario invitado que intenta a la red de acceso golpea la regla de la autorización de RedirectToPortal y se reorienta generalmente para la autenticación.

> **Note**: Las funciones de la purgación del punto final son independiente de la expiración de la directiva y de la cuenta de invitado de la purgación de la cuenta de invitado.

> **Note**: En ISE 1.2 los puntos finales podían ser quitados automáticamente solamente al golpear los límites de cola internos del profiler. Entonces menos puntos finales usados recientemente se están quitando.

Acceso temporario

Otro método para el acceso de invitado es utilizar la condición de flujo del invitado.



Que la condición está marcando a las sesiones activas en el ISE y ella es atributos. Si esa sesión tiene el atributo que indica que el Usuario invitado ha autenticado previamente con éxito condicione se corresponde con. Después de que el ISE reciba el mensaje de la parada de las estadísticas del radio del dispositivo de acceso a la red (NAD), la sesión se termina y posterior quitó. En esa etapa el acceso a la red de la condición: UseCase = el flujo del invitado no se satisface más. Como consecuencia todas las autenticaciones subsiguientes de ese punto final golpean la regla genérica que reorienta para la autenticación del invitado.

> **Note**: Flujo del invitado no soportado cuando autentican al usuario vía el portal del hotspot. Para esos escenarios el atributo de UseCase se fija a las operaciones de búsqueda del host en vez del flujo del invitado.

Comportamiento de la desconexión del WLC

Después de que las desconexiones de los clientes de la red inalámbrica (por ejemplo usando el botón disconnect en Windows) él envíen la trama del deauthentication. Pero eso es omitida por el WLC y se puede confirmar usando “el xxxx del cliente del debug” - el WLC no presenta ningún debug cuando el cliente está desconectando de la red inalámbrica (WLAN). Como consecuencia en el cliente de Windows:

- el IP Address se quita de la interfaz
- la interfaz está en el estado: media desconectados

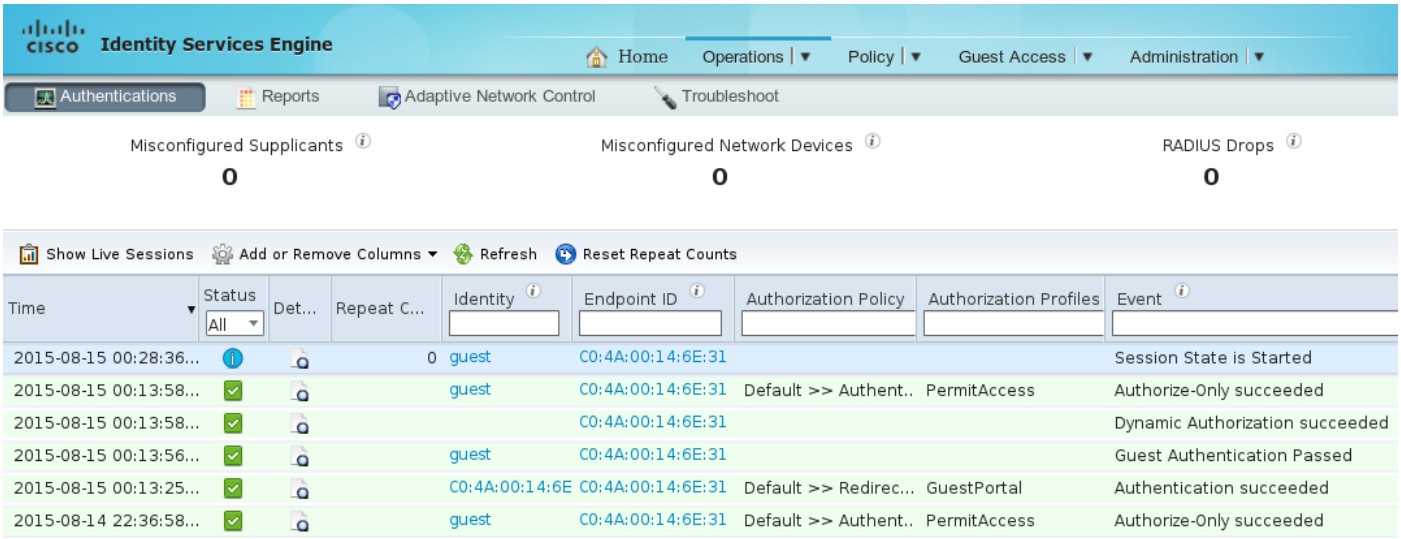
Pero en el WLC el estatus es sin cambios (todavía cliente en el estado de FUNCIONAMIENTO).

Se quita ése es diseño previsto para el WLC, la sesión cuando

- golpes del tiempo de inactividad del usuario
- golpes del sesión-descanso
- si usa el cifrado L2, entonces cuando el intervalo de la rotación de la clave del grupo golpea
- el algo más hace el AP/WLC golpear al cliente con el pie de (e.g. las restauraciones de la radio AP, alguien apagan el WLAN, el etc.)

Con esa configuración del comportamiento y del Acceso temporario después de que las desconexiones del usuario de la sesión de la red inalámbrica (WLAN) no se quiten del ISE porque el WLC nunca ha borrado lo (y la parada nunca enviada de las estadísticas del radio). Si la sesión no se quita, el ISE todavía recuerda que la vieja condición de flujo de la sesión y del invitado está

satisfecha. Después del usuario de la desconexión y de la reconexión tenga acceso a la red completo sin el requisito de reautenticate.



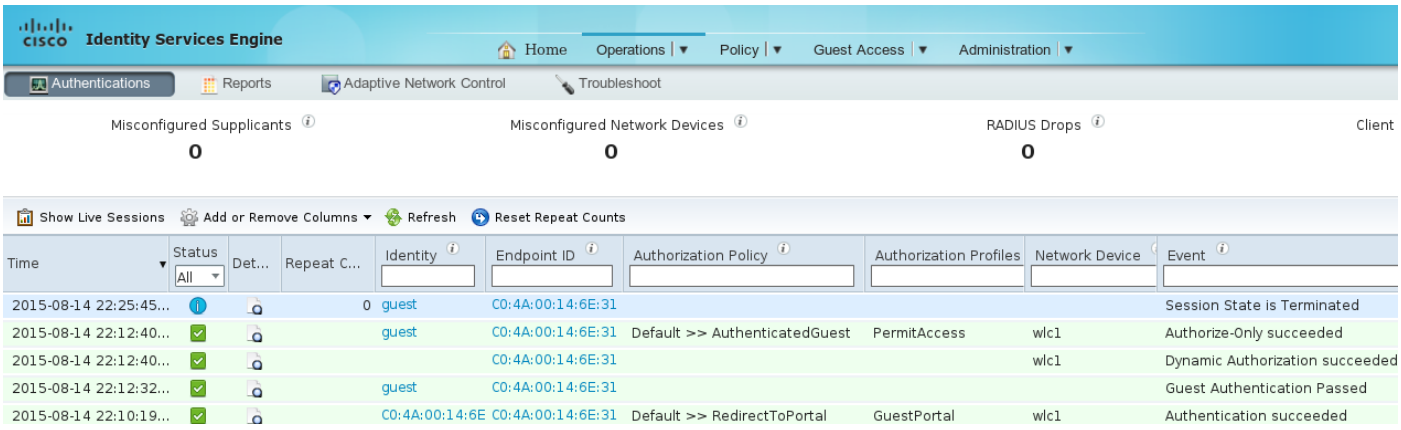
Pero si después de que el usuario de la desconexión conecte con diversa red inalámbrica (WLAN), después el WLC decide a borrar la vieja sesión. Se envía la parada de las estadísticas del radio y el ISE quita la sesión. Si los intentos del cliente a conectar con la condición de flujo original del invitado de la red inalámbrica (WLAN) no se satisfacen y reorientan al usuario para la autenticación.

> **Note**: El WLC configurado con la protección del capítulo de la Administración (MFP) valida la trama cifrada del deauthentication del cliente CCXv5 MFP.

Verificación

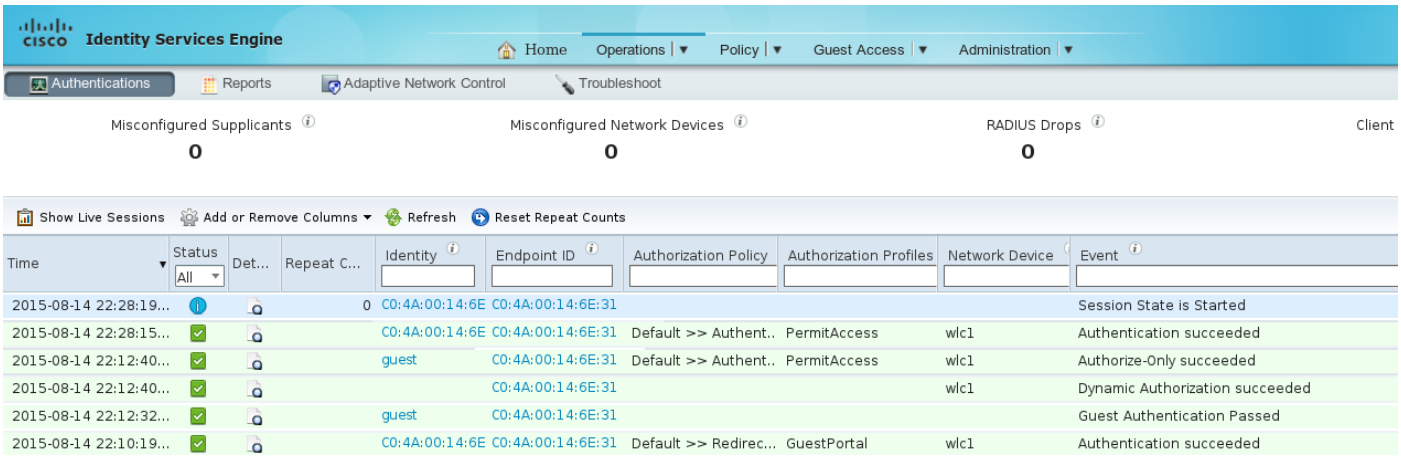
Acceso permanente

Después del cambio de dirección al portal y a la autenticación satisfactoria del invitado el ISE envía el cambio de la autorización (CoA) de accionar el reauthentication. Como consecuencia la nueva sesión de puente de la autenticación de MAC (MAB) se está construyendo. Este punto final del tiempo pertenece al grupo de la identidad de GuestEndpoints y hace juego la regla que proporciona al acceso total.



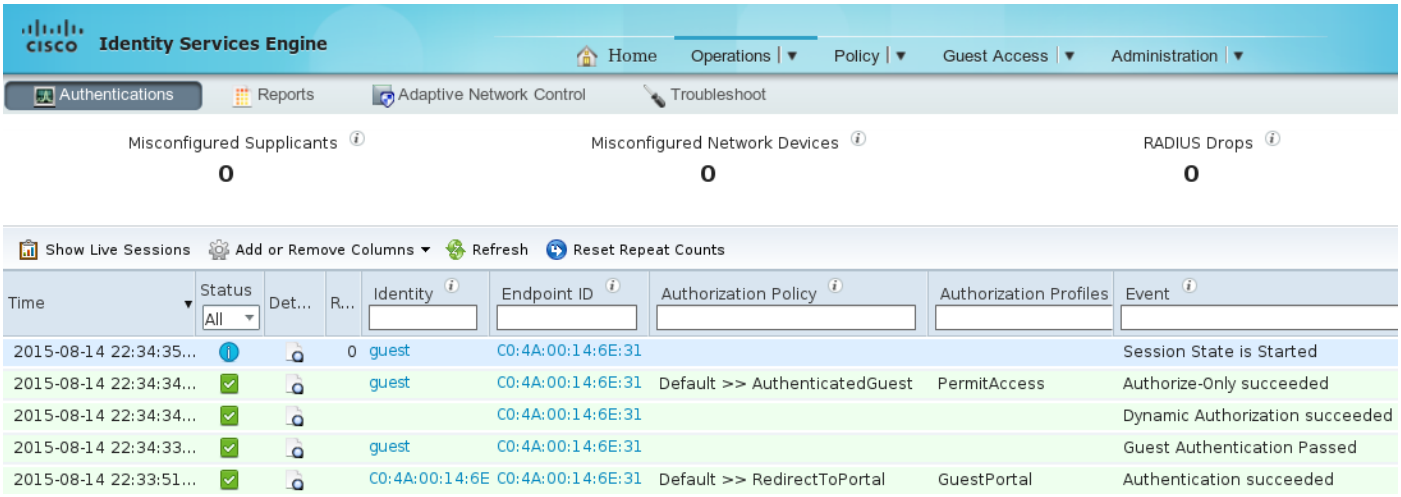
En ese usuario de red inalámbrica de la etapa puede desconectar, conectar con diversos WLAN, después volver a conectar. Todas esas autenticaciones subsiguientes utilizan la identidad basada

en el MAC address, pero golpean la primera regla debido al punto final que pertenece al grupo específico de la identidad. El acceso a la red completo se proporciona sin la autenticación del invitado.

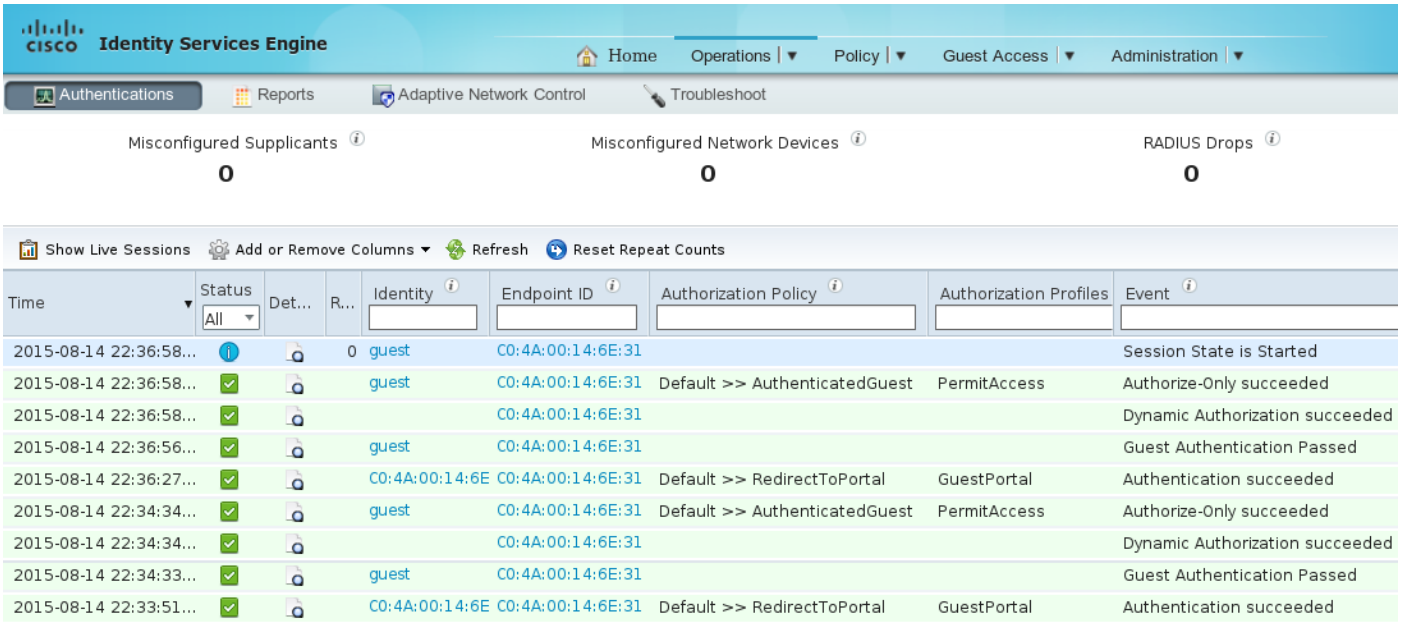


Acceso temporario

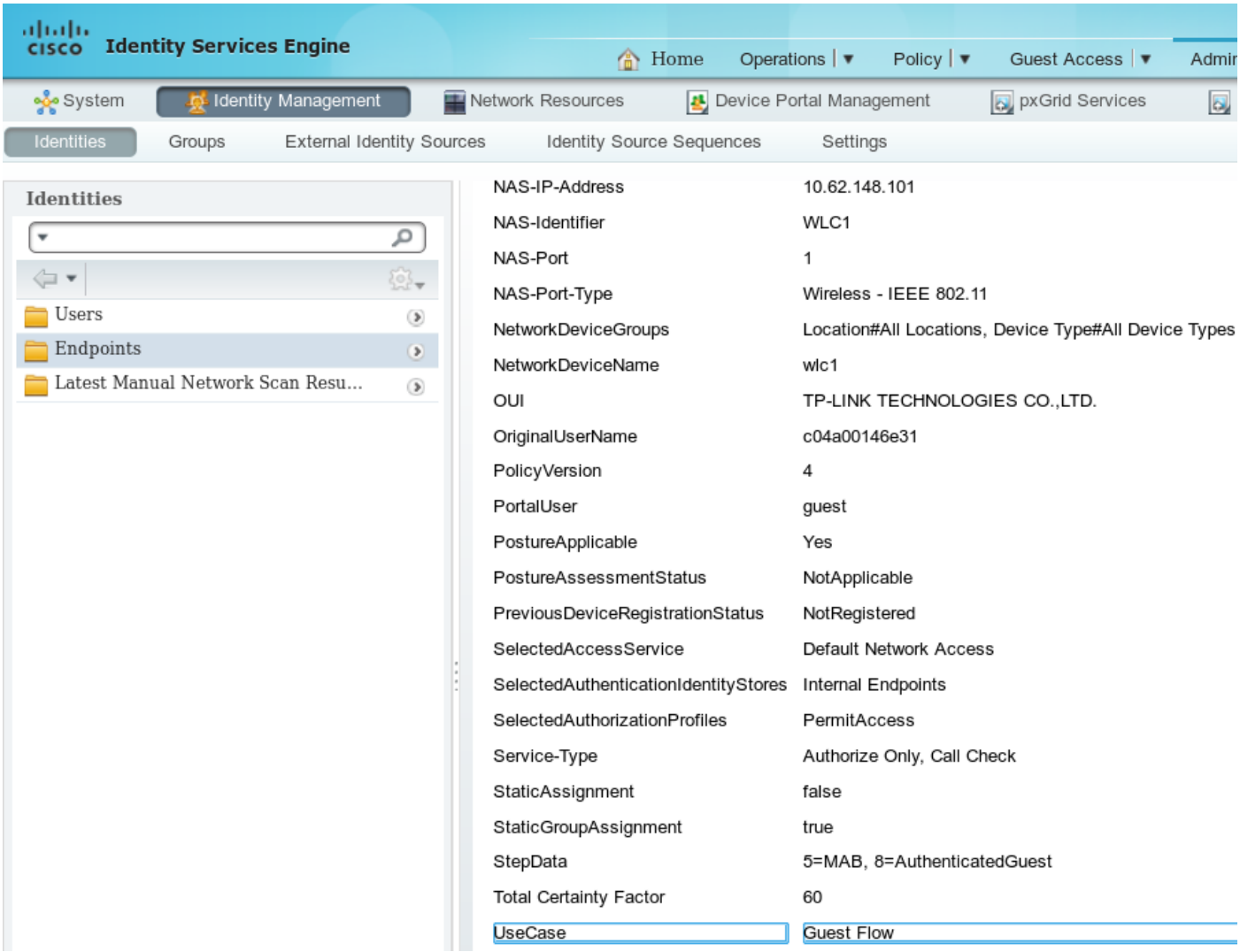
Para el segundo principio del escenario (con la condición basada en el flujo del invitado) es lo mismo.



Pero después de que la sesión se quite para todas las autenticaciones subsiguientes, el invitado golpeó la regla genérica y se reorienta otra vez para la autenticación del invitado.



Satisfagan al invitado que es la condición de flujo cuando los atributos correctos son existentes para la sesión. Eso puede ser verificada mirando los atributos del punto final. El resultado de la autenticación acertada del invitado se indica.




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

Bug

El CoA CSCuu41157 ISE ENH termina envía encendido el retiro o el vencimiento de la cuenta de invitado.

(pedido de mejora de terminar las sesiones del invitado después del retiro o del vencimiento de la cuenta de invitado)

Referencias

- Guía de administradores de Cisco ISE 1.3
- Guía de administradores de Cisco ISE 1.4
- Ejemplo de configuración del hotspot de la versión 1.3 ISE
- Ejemplo de configuración registrado uno mismo del portal del invitado de la versión 1.3 ISE
- Autenticación Web central en el ejemplo de configuración del WLC y ISE
- Autenticación Web central con FlexConnect AP en un WLC con el ejemplo de configuración ISE
- Soporte Técnico y Documentación - Cisco Systems