Configurar o acesso provisório e permanente do convidado ISE

Índice

Introdução

Este documento descreve métodos diferentes para a configuração do acesso do convidado do Identity Services Engine (ISE). Baseado em condições diferentes em regras da autorização:

- o acesso permanente à rede pode ser fornecido (nenhuma exigência para autenticações subsequente)
- o acesso temporário à rede pode ser fornecido (exigindo a autenticação do convidado depois que a sessão expira)

O comportamento específico do controlador do Wireless LAN (WLC) para a remoção da sessão é apresentado igualmente ao longo do impacto na encenação do acesso temporário.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Disposições ISE e fluxos do convidado
- Configuração dos controladores do Wireless LAN (WLC)

Componentes Utilizados

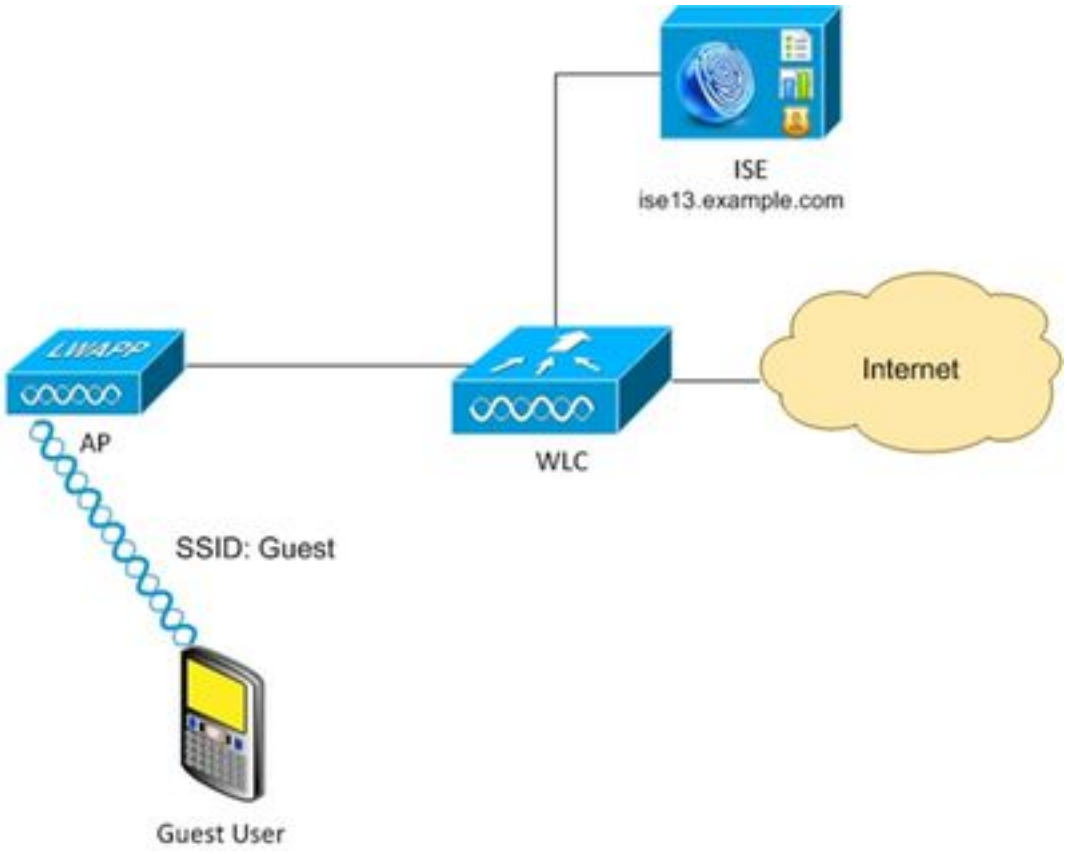
As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7
- Versão 7.6 e mais recente de Cisco WLC
- Software ISE, versão 1.3 e mais recente

Configurar

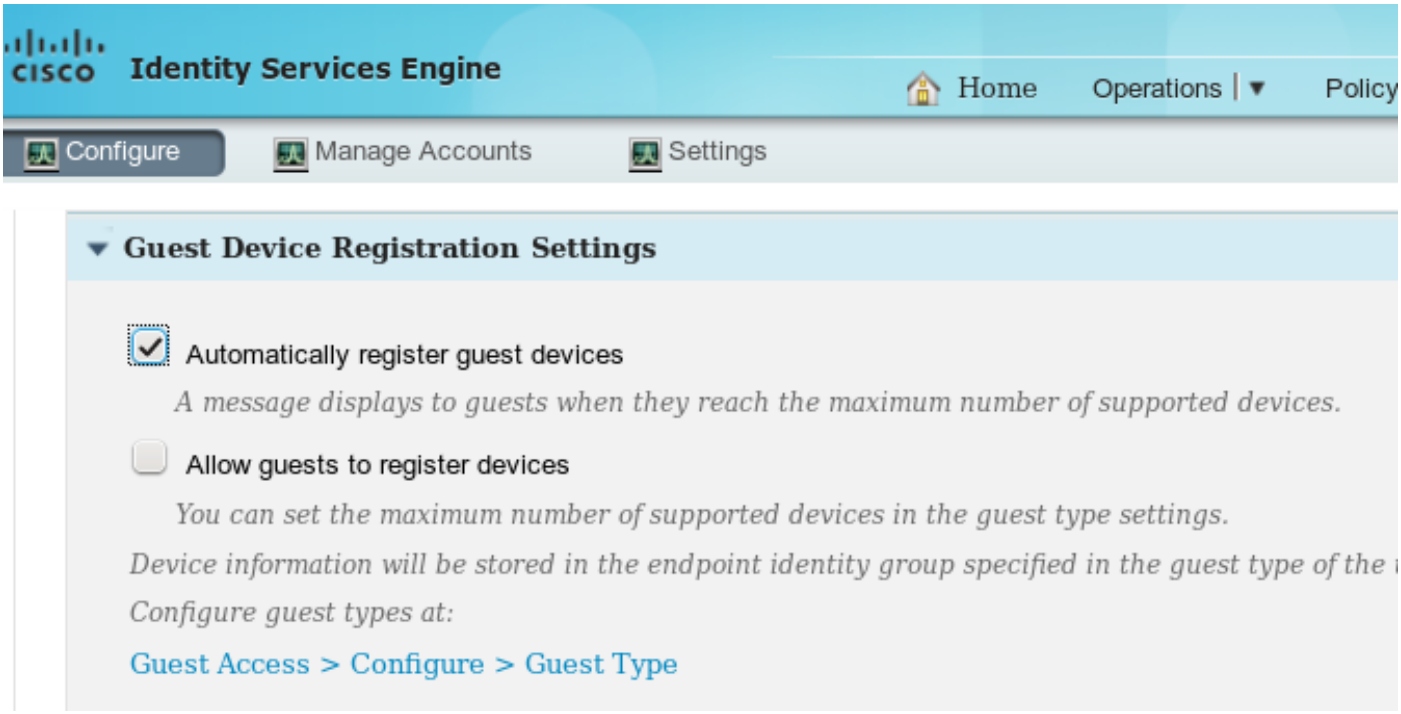
Para a configuração básica do acesso do convidado verifique por favor referências com os exemplos de configuração. Este artigo centra-se sobre regras configuração e diferenças da autorização nas condições da autorização.

Diagrama de Rede

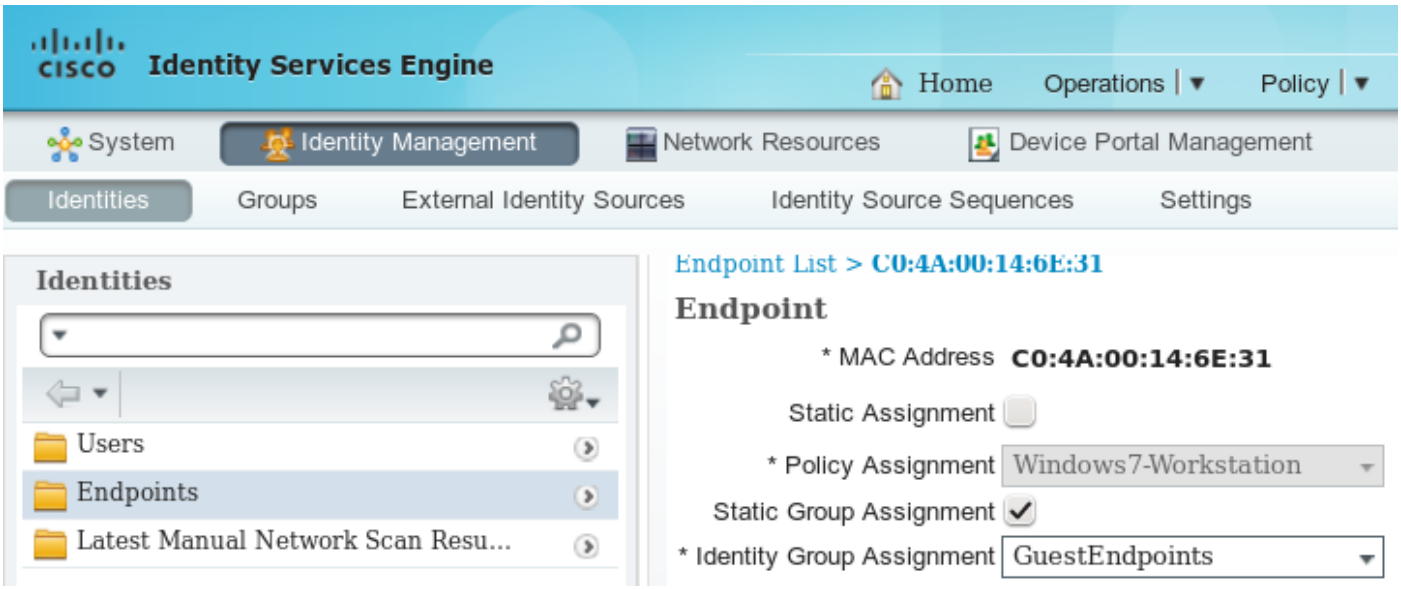


Acesso permanente

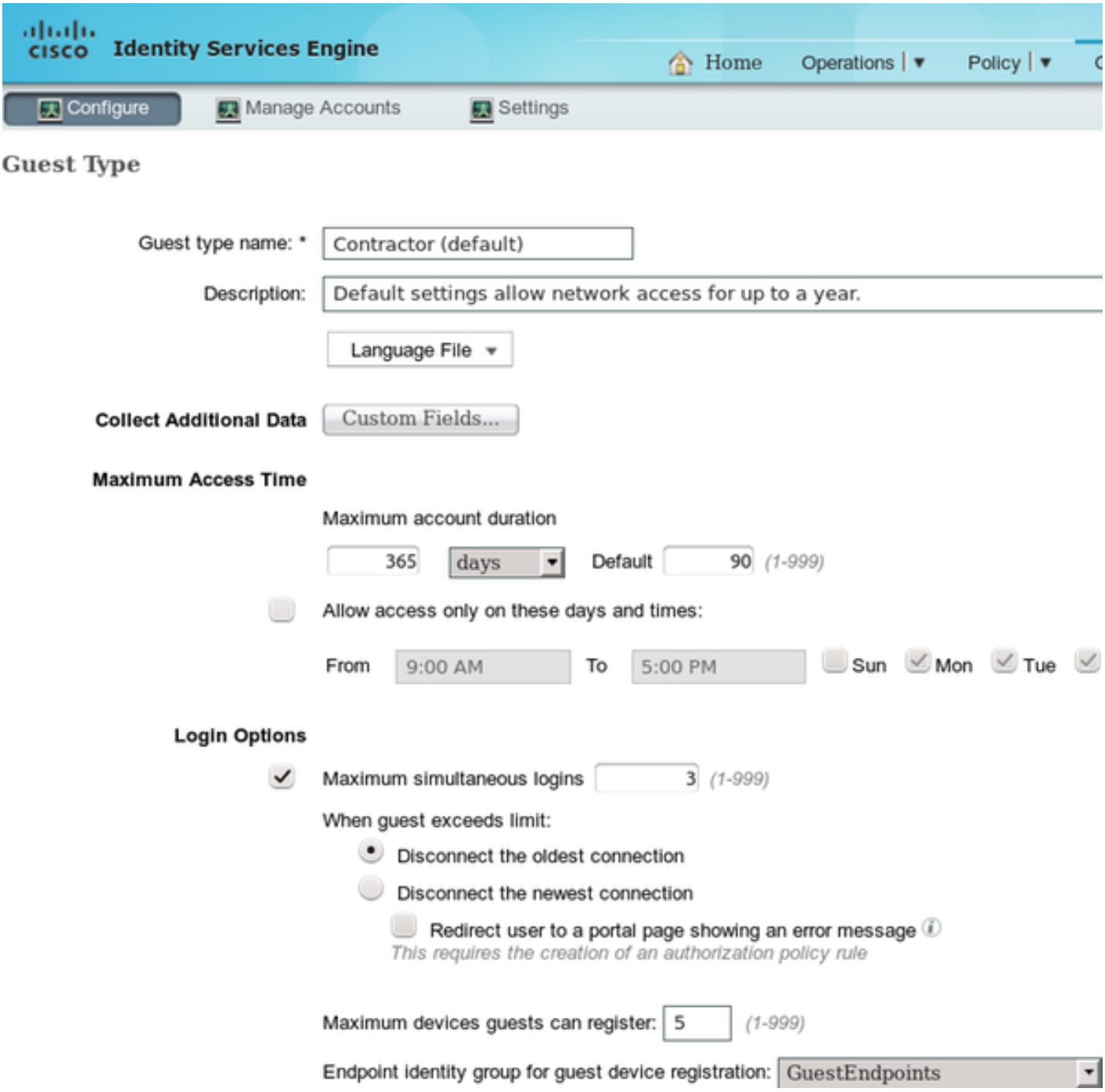
Para a versão 1.3 mais recente ISE após a autenticação bem sucedida no portal do convidado com o registro do dispositivo permitido.



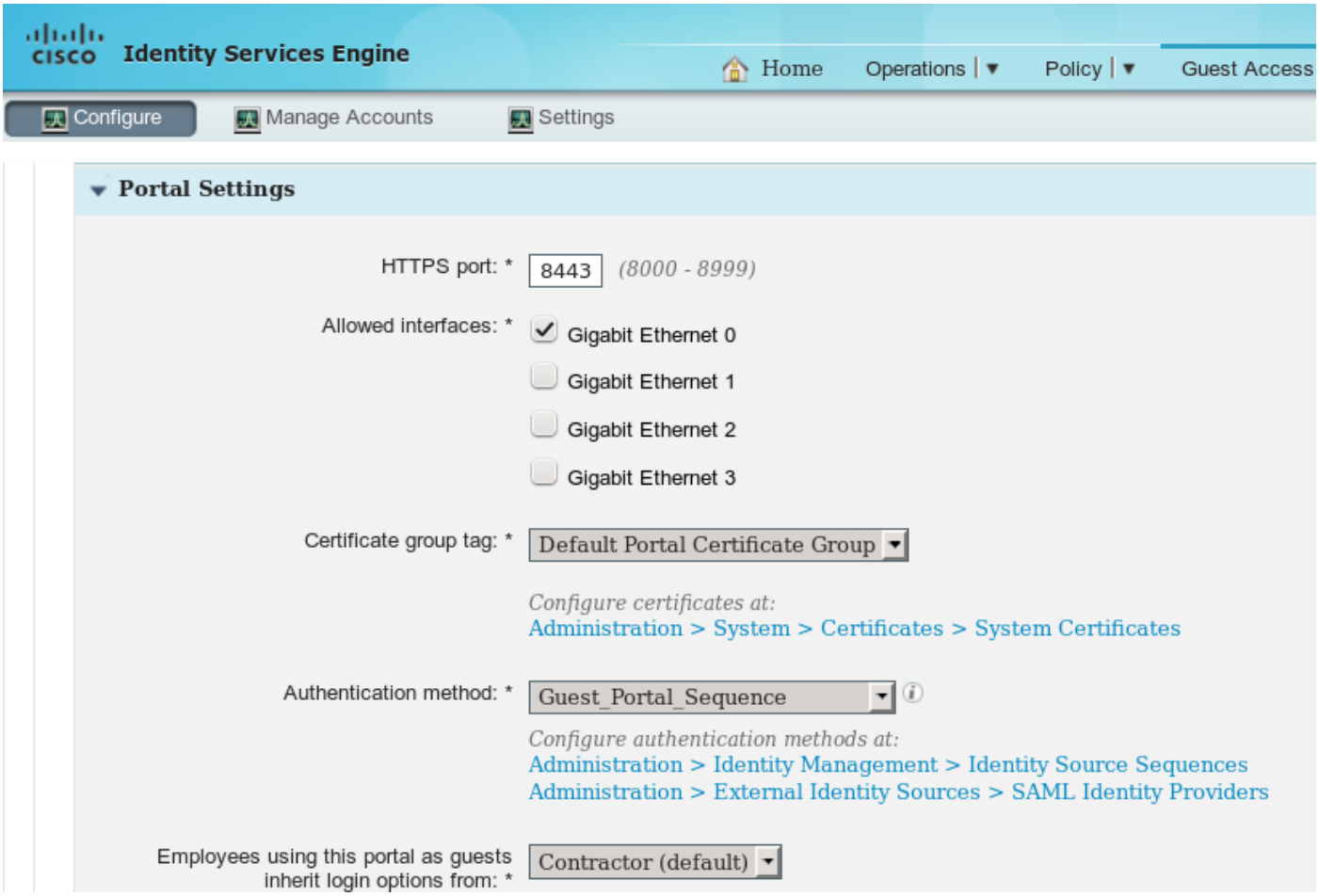
O dispositivo de ponto final (MAC address) é registrado estaticamente no grupo específico do valor-limite (GuestEndpoints neste exemplo).



Esse grupo é derivado do tipo do convidado do usuário, segundo as indicações desta imagem.



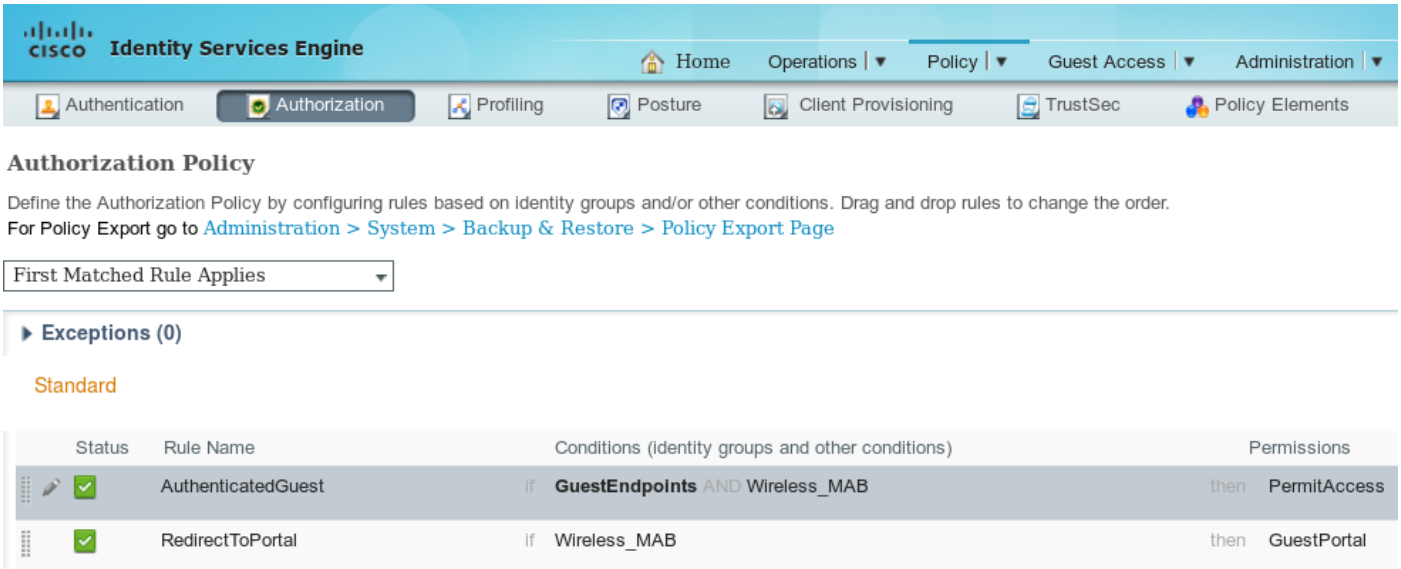
Se é um usuário corporativo (loja da identidade o outro então convidado) esse ajuste é derivado dos ajustes portais.



Em consequência o MAC address associado com o convidado pertence sempre a esse grupo específico da identidade. Isso não pode ser mudado automaticamente (por exemplo pelo serviço do perfilador).

> **Note**: Para aplicar a condição da autorização de EndPointPolicy dos resultados do perfilador pode ser usada.

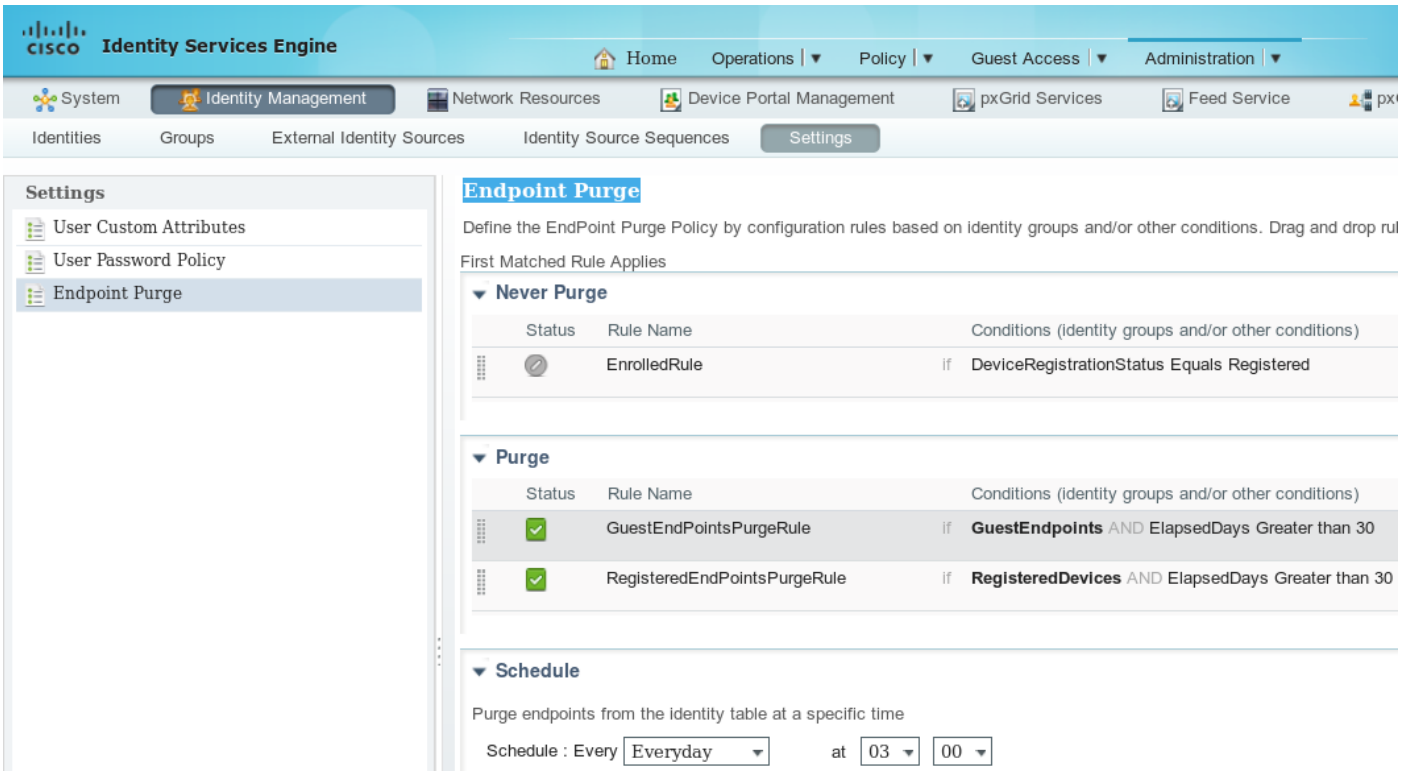
Sabendo que o dispositivo pertence sempre ao grupo que específico da identidade do valor-limite é possível construir as regras da autorização baseadas naquela, segundo as indicações desta imagem.



Uma vez que um usuário não é autenticado, a autorização combina a regra genérica RedirectToPortal. Após a reorientação ao portal e à autenticação do convidado, o valor-limite é colocado no grupo específico da identidade do valor-limite. Isso é usado pelo primeiro, uma circunstância mais específica. Todas as autenticações subsequente desse valor-limite batem a primeira regra da autorização e o usuário é acesso de rede completo fornecido sem a necessidade de autenticar novamente no portal do convidado.

Remoção do valor-limite para contas do convidado

Esta situação podia durar para sempre. Mas no valor-limite da remoção ISE 1.3 a funcionalidade foi introduzida. Com a configuração padrão.



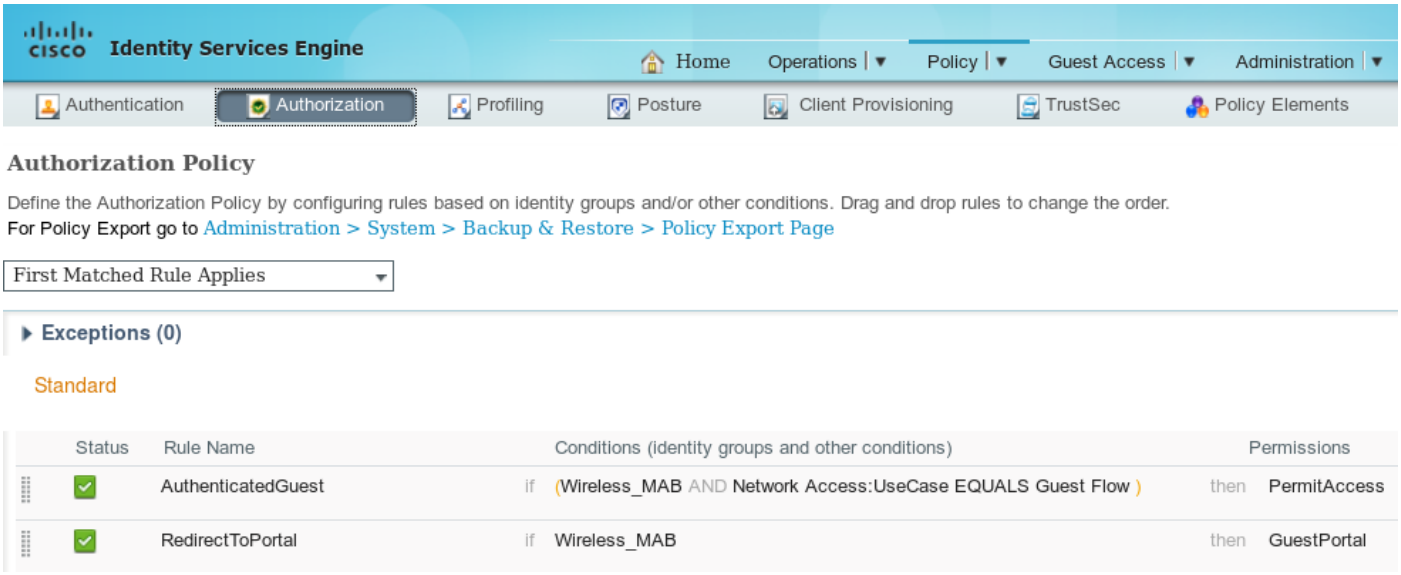
Todos os valores-limite usados para a autenticação do convidado são removidos após 30 dias (da criação do valor-limite). Em consequência após 30 dias o usuário convidado que tenta à rede de acesso bate a regra da autorização de RedirectToPortal e é reorientado geralmente para a autenticação.

> **Note**: A funcionalidade da remoção do valor-limite é independente da expiração da política da remoção da conta do convidado e da conta do convidado.

> **Note**: Em ISE 1.2 os valores-limite podiam ser removidos automaticamente somente ao bater limites de fila internos do perfilador. Os valores-limite o mais menos recentemente usados estão sendo removidos então.

Acesso temporário

Um outro método para o acesso do convidado é usar a condição de fluxo do convidado.



Que a circunstância está verificando sessões ativa no ISE e nela é atributos. Se essa sessão tem o atributo que indica que previamente o usuário convidado autenticou com sucesso condicione é combinado. Depois que o ISE recebe a mensagem da parada da contabilidade do raio do dispositivo do acesso de rede (NAD), a sessão está terminada e removida mais tarde. Nessa fase o acesso de rede da circunstância: UseCase = o fluxo do convidado não são satisfeitos anymore. Em consequência todas as autenticações subsequente desse valor-limite batem a regra genérica que reorienta para a autenticação do convidado.

> **Note**: Fluxo do convidado não apoiado quando o usuário for autenticado através do portal do ponto quente. Para aquelas encenações o atributo de UseCase é ajustado à consulta do host em vez do fluxo do convidado.

O WLC desliga o comportamento

Depois que as disconexões dos clientes da rede Wireless (por exemplo usando o botão disconnect em Windows) ele enviam o quadro do deauthentication. Mas isso é omitido pelo WLC e pode ser utilização confirmada “debuga o cliente xxxx” - o WLC apresenta o nenhum debuga quando o cliente está desligando do WLAN. Em consequência no cliente do Windows:

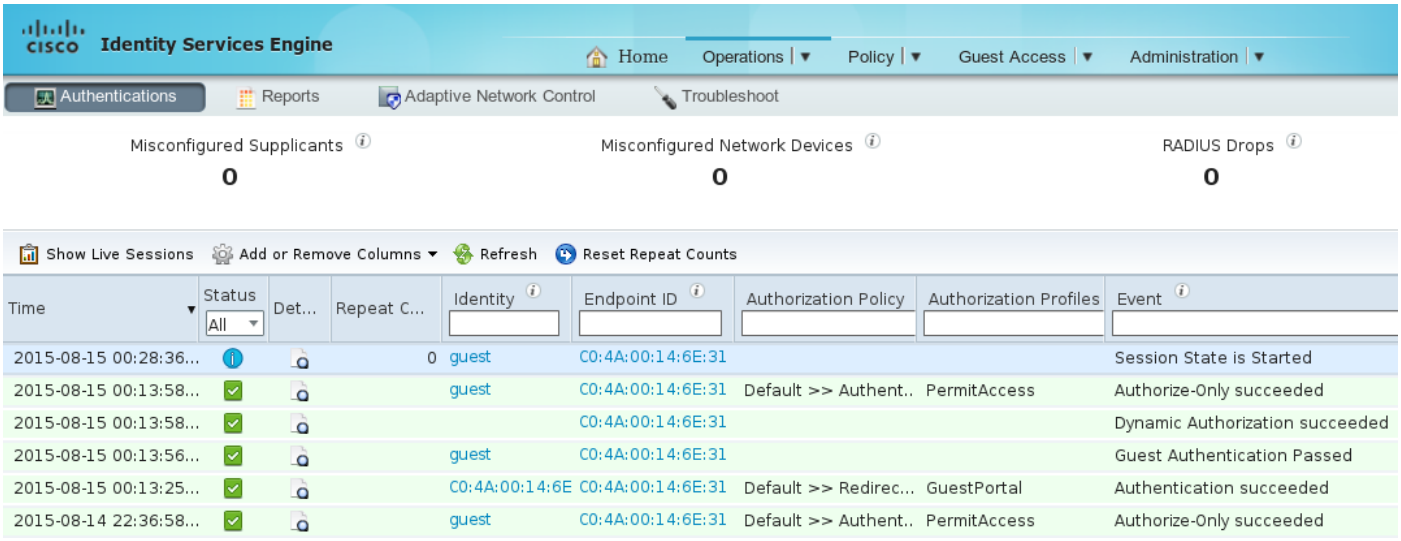
- o endereço IP de Um ou Mais Servidores Cisco ICM NT é removido da relação
- a relação está no estado: media desligados

Mas no WLC o estado é inalterado (cliente ainda no estado de CORRIDA).

Aquele for projeto de planeamento para o WLC, a sessão é removido quando

- batidas do idle timeout do usuário
- batidas do sessão-intervalo
- se usando a criptografia L2, então quando o intervalo da rotação da chave do grupo bater
- algo faz com mais que o AP/WLC retroceda o cliente fora de (por exemplo as restaurações do rádio AP, alguém fecham o WLAN, etc.)

Com essa configuração do comportamento e do acesso temporário depois que as disconexões do usuário da sessão WLAN não são removidas do ISE porque o WLC nunca cancelou o (e a parada nunca enviada da contabilidade do raio). Se a sessão não é removida, o ISE ainda recorda que a condição de fluxo velha da sessão e do convidado está satisfeita. Após o usuário da desconexão e da reconexão tenha o acesso de rede completo sem exigência reauthenticate.



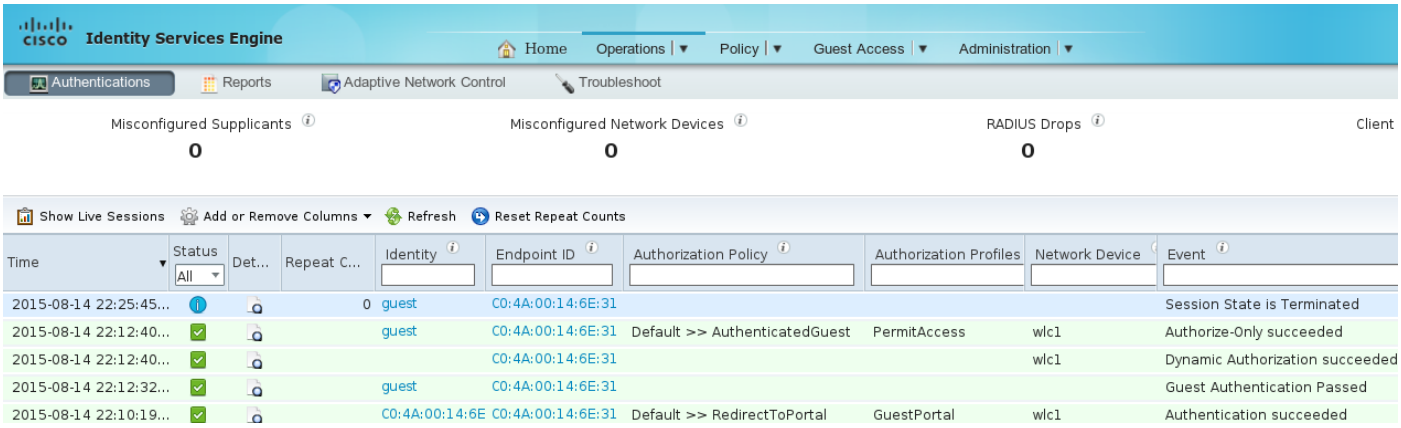
Mas se depois que o usuário da desconexão conecta ao WLAN diferente, a seguir o WLC decide cancelar a sessão velha. A parada da contabilidade do raio é enviada e o ISE remove a sessão. Se as tentativas do cliente a conectar à condição de fluxo original do convidado WLAN não são satisfeitas e o usuário está reorientado para a autenticação.

> **Note**: O WLC configurado com proteção do quadro do Gerenciamento (MFP) aceita o quadro cifrado do deauthentication do cliente CCXv5 MFP.

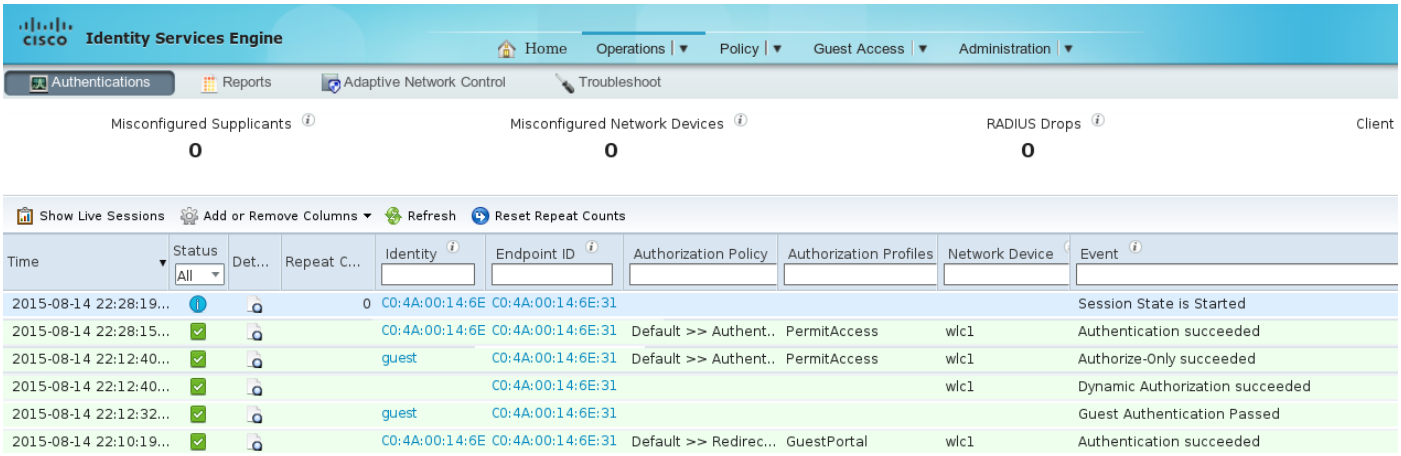
Verificar

Acesso permanente

Após a reorientação ao portal e à autenticação bem sucedida do convidado o ISE envia a mudança da autorização (CoA) provocar o reauthentication. Em consequência a sessão nova do desvio da autenticação de MAC (MAB) está sendo construída. Este valor-limite do tempo pertence ao grupo da identidade de GuestEndpoints e os fósforos ordenam o fornecimento do acesso direto.

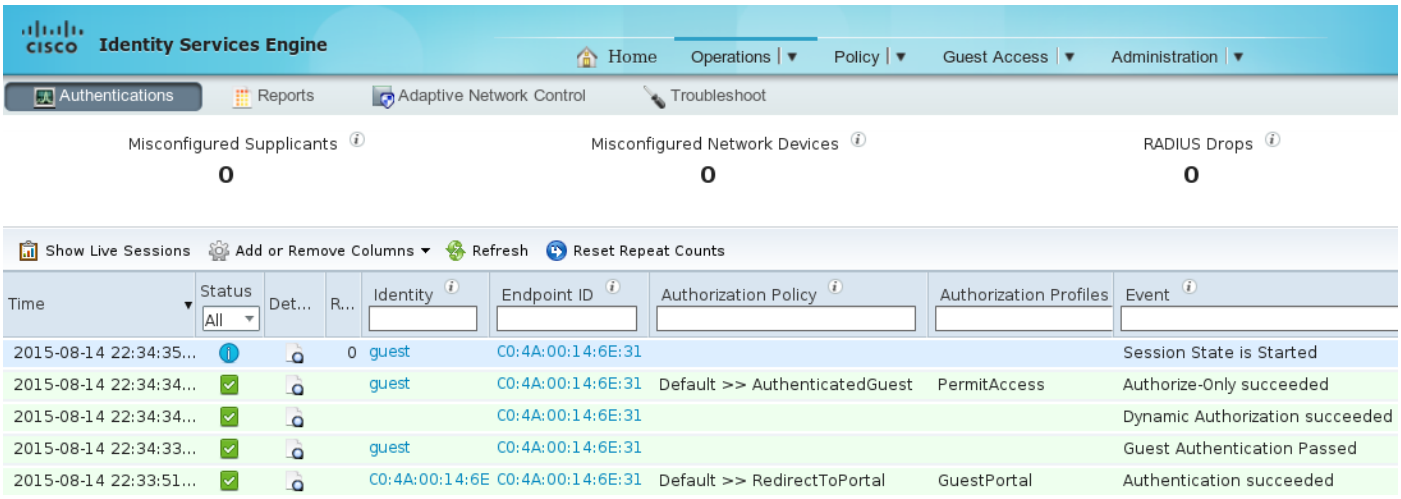


Nesse usuário Wireless da fase pode desligar, conectar aos WLAN diferentes, a seguir reconectar. Todas aquelas autenticações subsequente usam a identidade baseada no MAC address, mas batem a primeira regra devido ao valor-limite que pertence ao grupo específico da identidade. O acesso de rede completo é fornecido sem a autenticação do convidado.

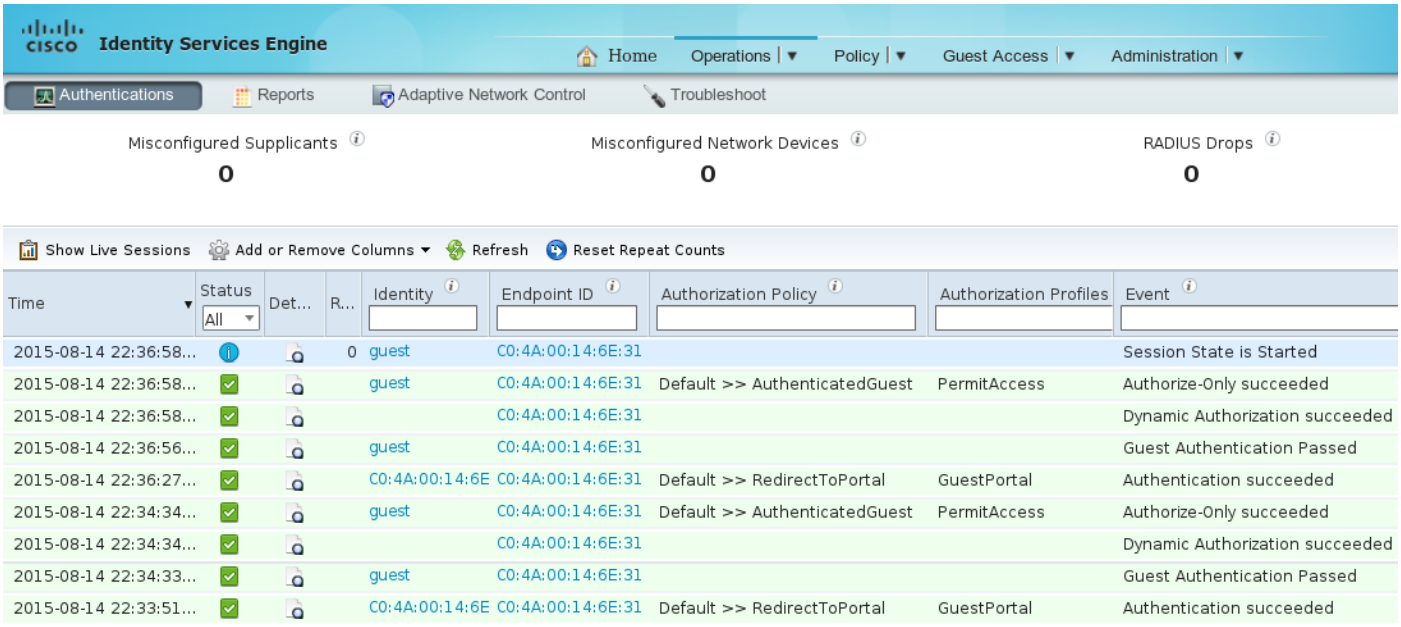


Acesso temporário

Para o segundo começo da encenação (com a circunstância baseada no fluxo do convidado) é o mesmo.

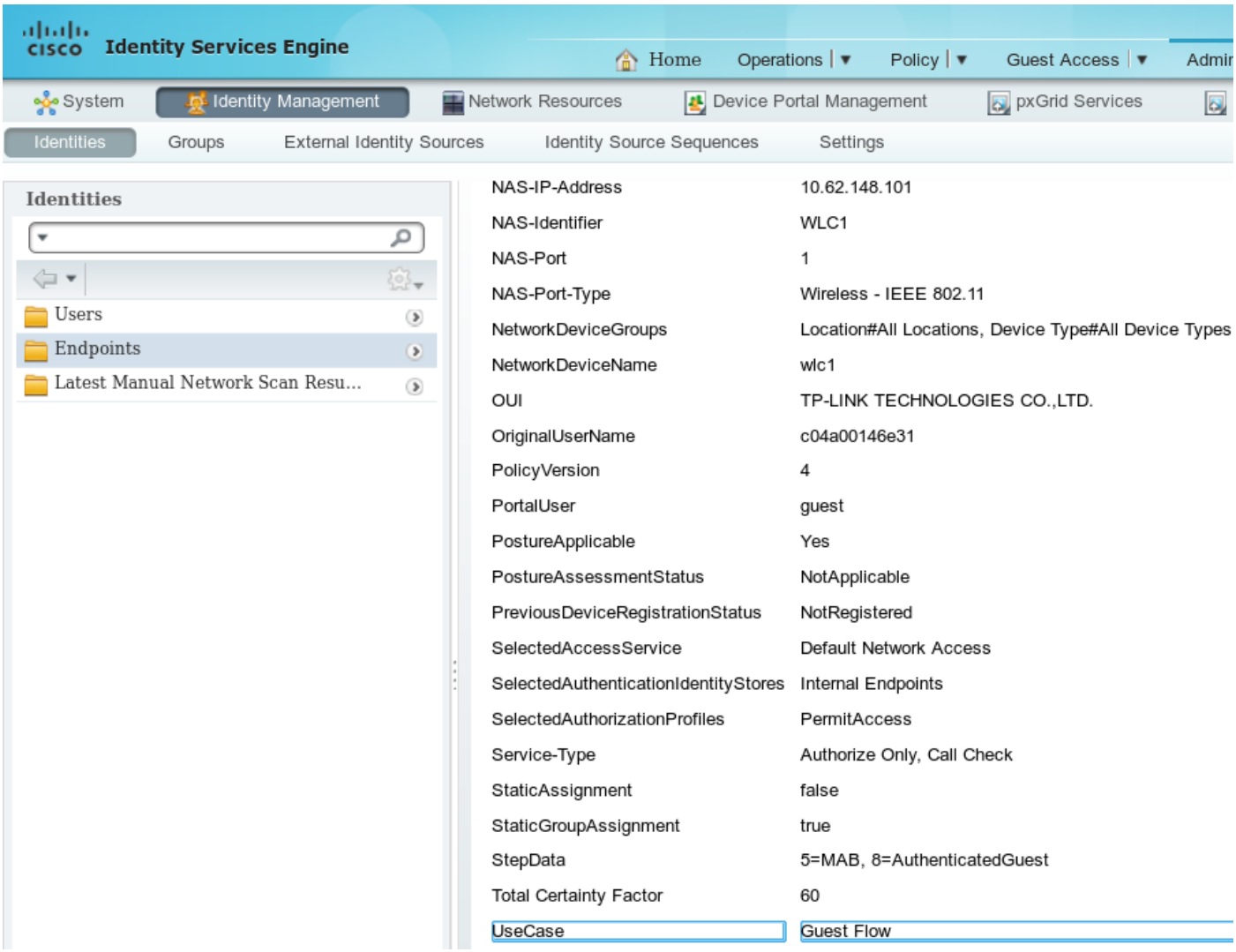


Mas depois que a sessão é removida para todas as autenticações subsequente, o convidado bateu a regra genérica e foi reorientado outra vez para a autenticação do convidado.



O convidado a condição de fluxo que é seja satisfeito quando os atributos corretos são existentes

para a sessão. Isso pode ser verificado olhando atributos do valor-limite. O resultado da autenticação bem sucedida do convidado é indicado.




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

Erros

O CoA CSCuu41157 ISE ENH termina envia sobre a remoção ou a expiração da conta do convidado.

(requisição de aprimoramento terminar sessões do convidado após a remoção ou a expiração da conta do convidado)

Referências

- Guia de administradores de Cisco ISE 1.3
- Guia de administradores de Cisco ISE 1.4
- Exemplo de configuração do ponto quente da versão 1.3 ISE
- Exemplo de configuração registrado auto do portal do convidado da versão 1.3 ISE
- Autenticação da Web central no exemplo de configuração WLC e ISE

- Autenticação da Web central com FlexConnect AP em um WLC com exemplo de configuração ISE
- Suporte Técnico e Documentação - Cisco Systems