配置ISE访客临时和永久性访问

目录

简介

本文描述身份服务引擎(ISE)访客访问配置的不同的说法。基于在授权规则的不同的条件：

- 可以提供对网络的永久性访问(随后的认证的没有需求)
- 可以提供临时访问对于网络(要求访客验证，在会话超时)后

并且会话删除的特定无线局域网控制器(WLC)行为沿在临时访问方案的影响被提交。

先决条件

要求

Cisco 建议您了解以下主题：

- ISE部署和访客流
- 无线局域网控制器(WLCs)的配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

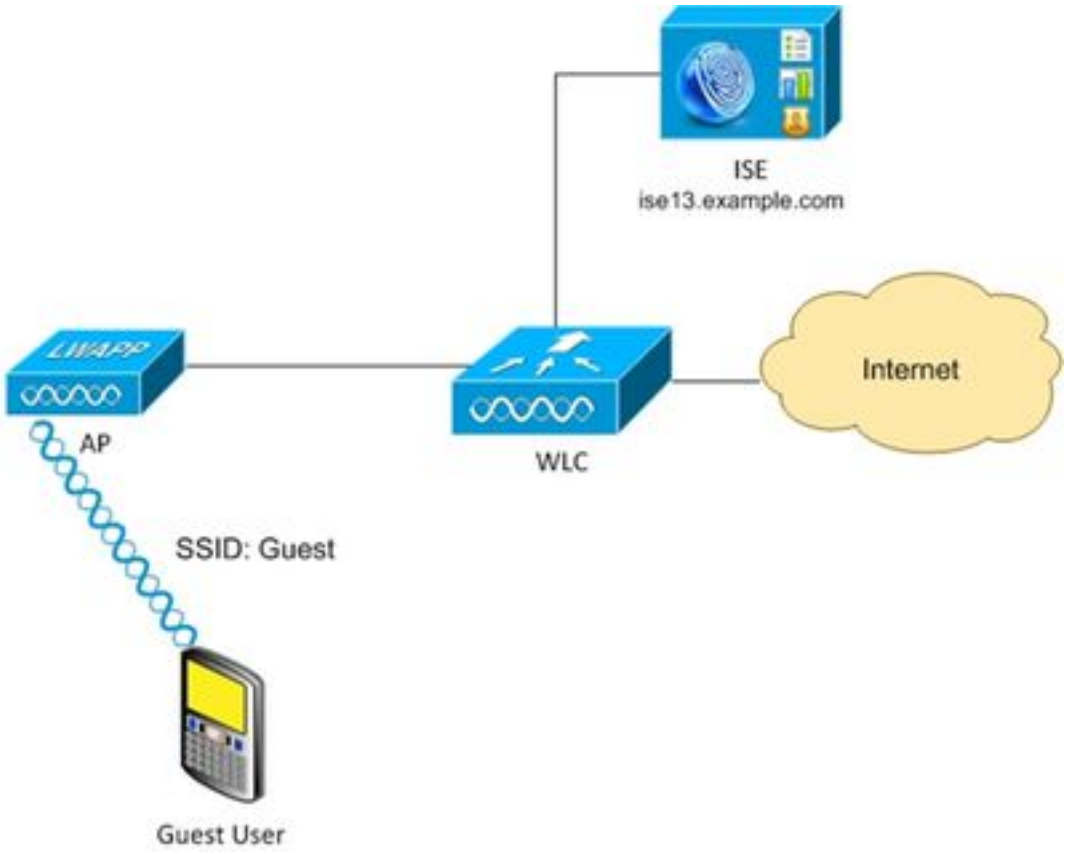
- Microsoft Windows 7
- Cisco WLC版本7.6和以上

- ISE软件，版本1.3和以上

配置

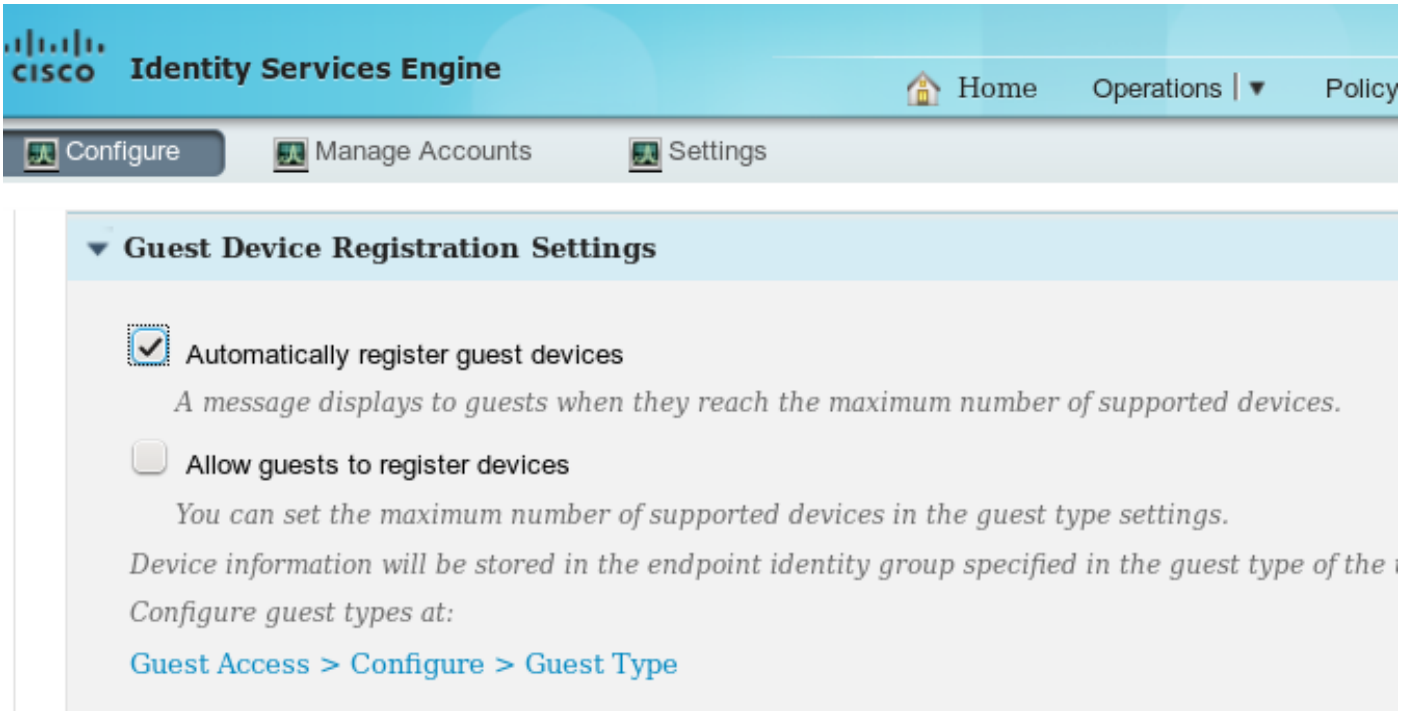
对于基本访客访问配置请用配置示例请检查参考。此条款着重在授权条件的授权规则配置和差异。

网络图

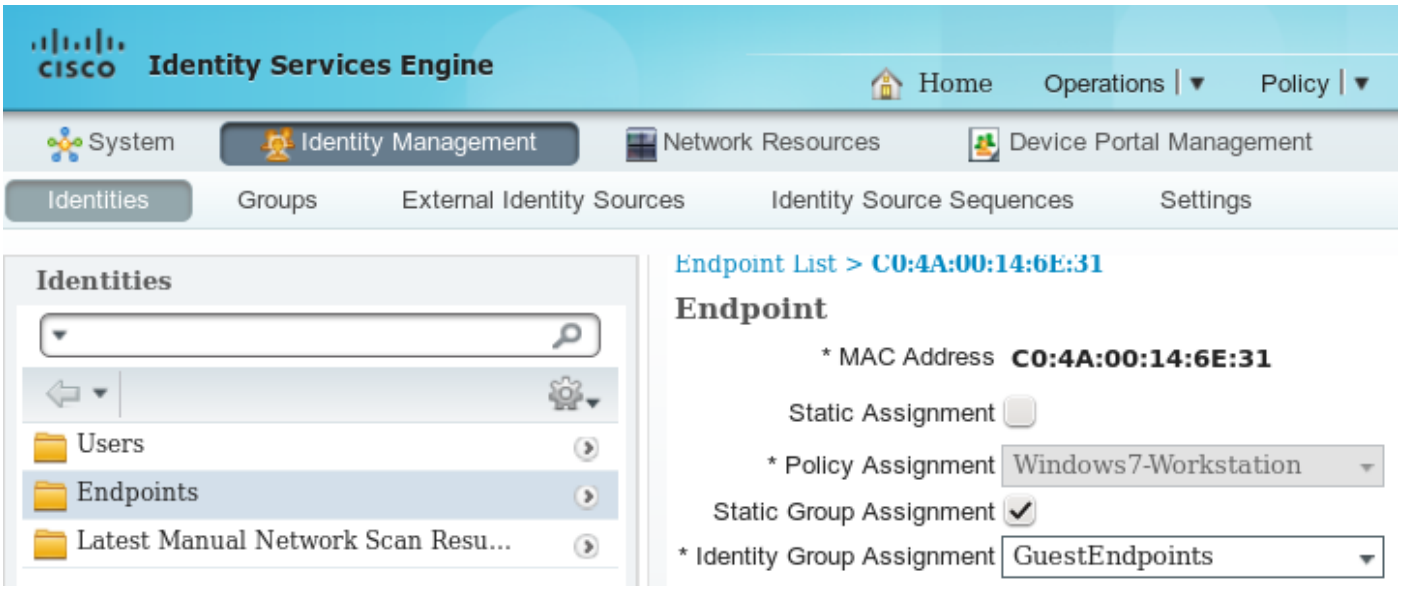


永久性访问

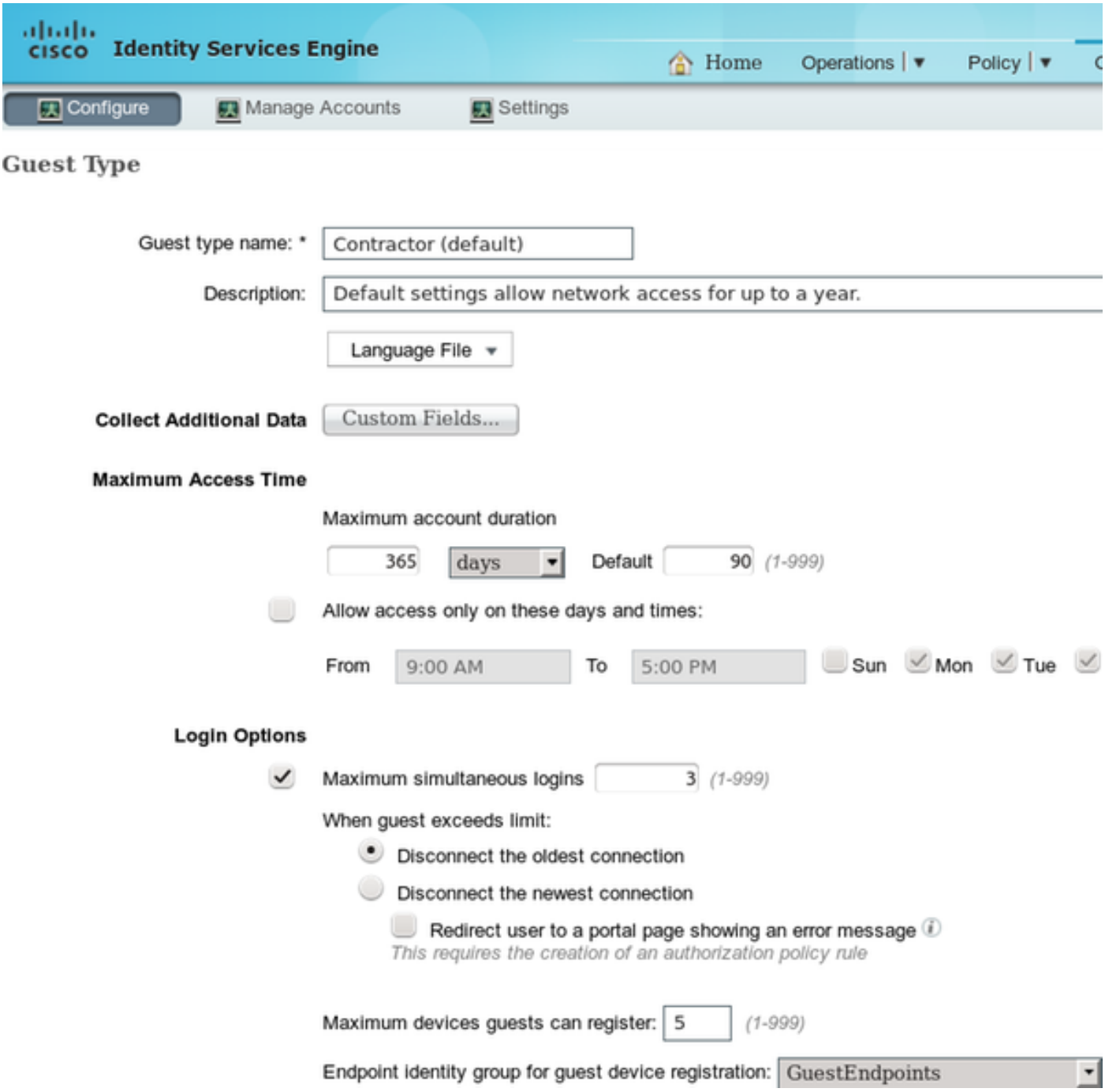
ISE版本1.3和以上在访客门户的成功认证以后有启用的设备已注册的。



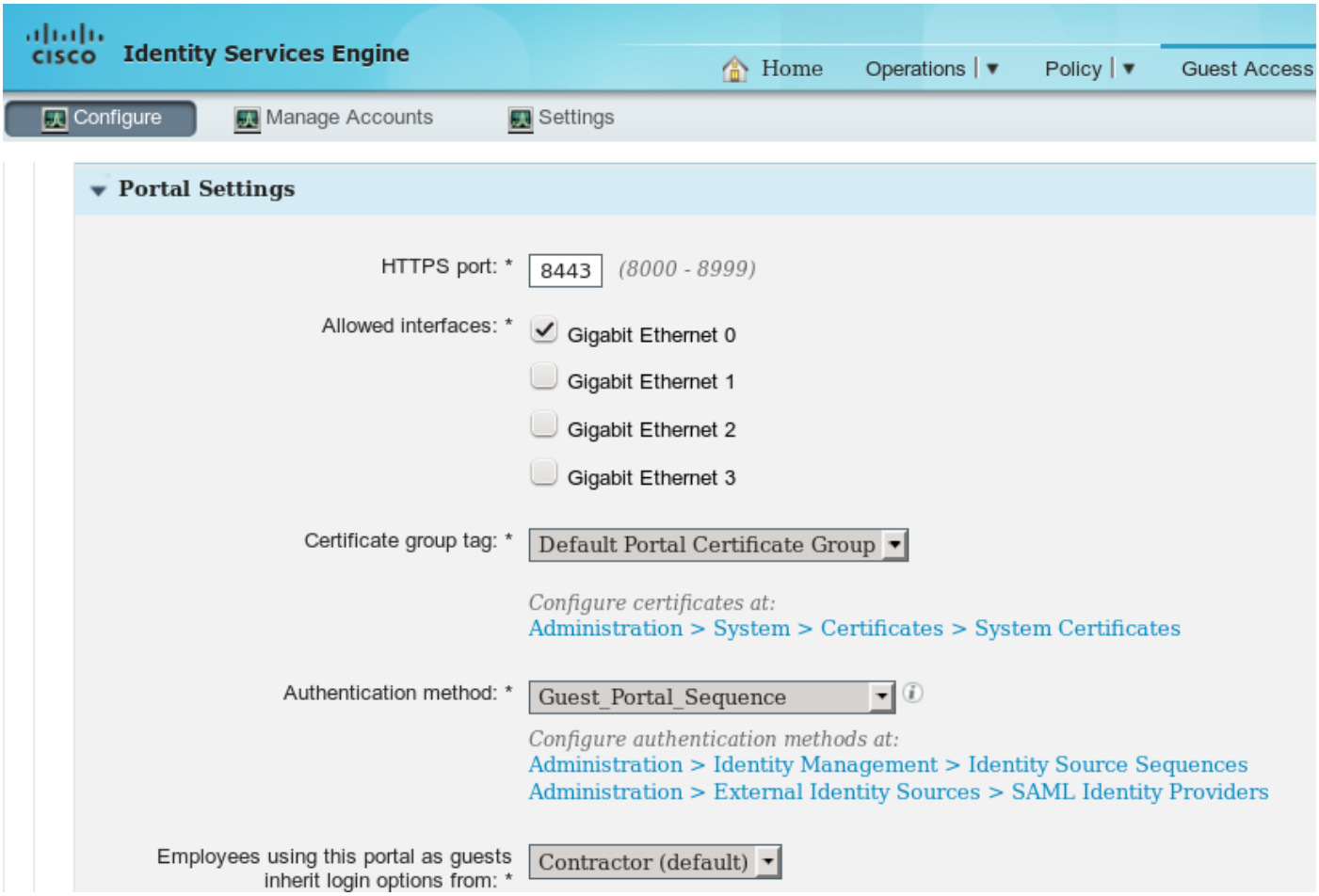
端点设备(MAC地址)在特定终端组(在本例中的GuestEndpoints中静态注册)。



如此镜像所显示，该组从用户的访客类型派生。



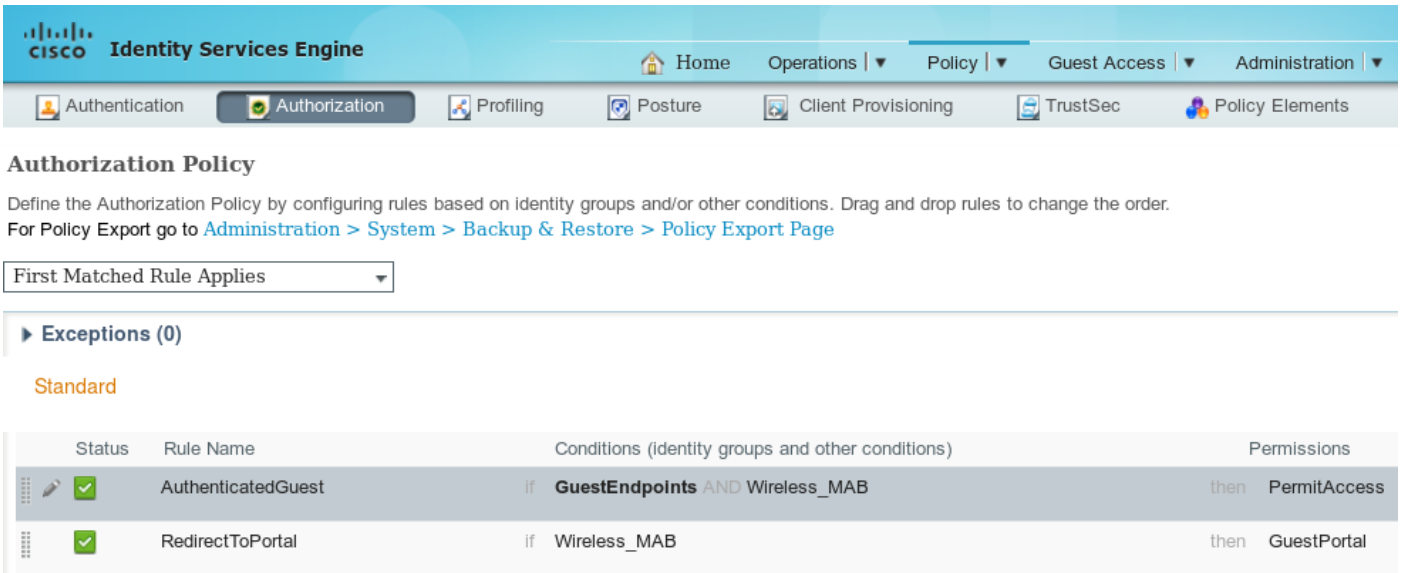
如果它是集群用户(标识存储其他然后访客)该设置从门户设置派生。



结果MAC地址关联与访客总是属于该特定标识组。那不可能自动地更改(例如由仿形铣床服务)。

Note:可以使用要运用仿形铣床结果EndPointPolicy授权情况。

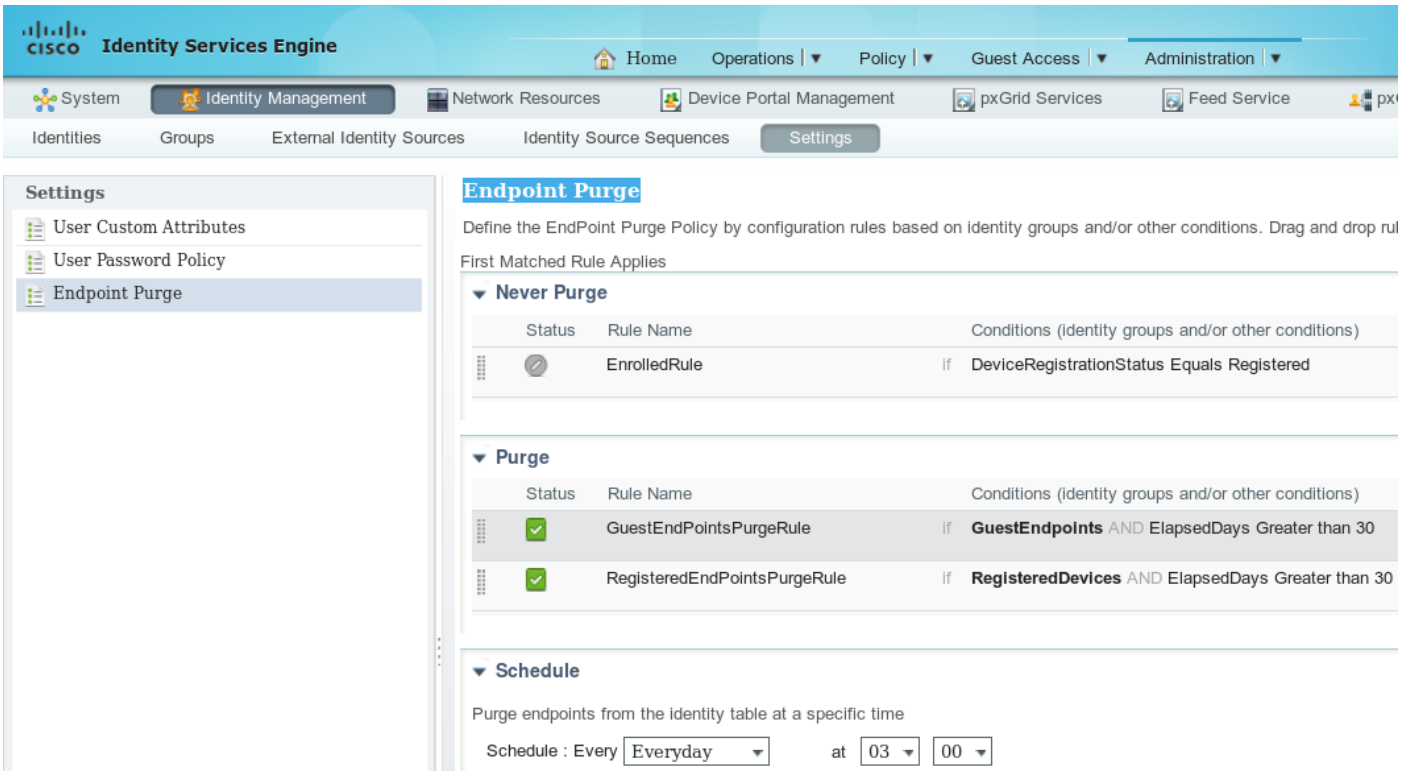
知道设备总是属于的特定终端标识组建立根据那的授权规则是可能的，如此镜像所显示。



一旦用户没有验证，授权匹配通用的规则RedirectToPortal。在对访客门户和验证的重定向以后，终端在特定终端标识组中安置。第一使用那，更多特殊的例子。该终端的所有随后的认证点击第一个授权规则没有需要重新鉴别在访客门户，并且用户是提供的全双工网络访问。

访客帐户的终端清除

此情况能持续永久。但是在ISE 1.3清除终端功能介绍。使用默认配置。



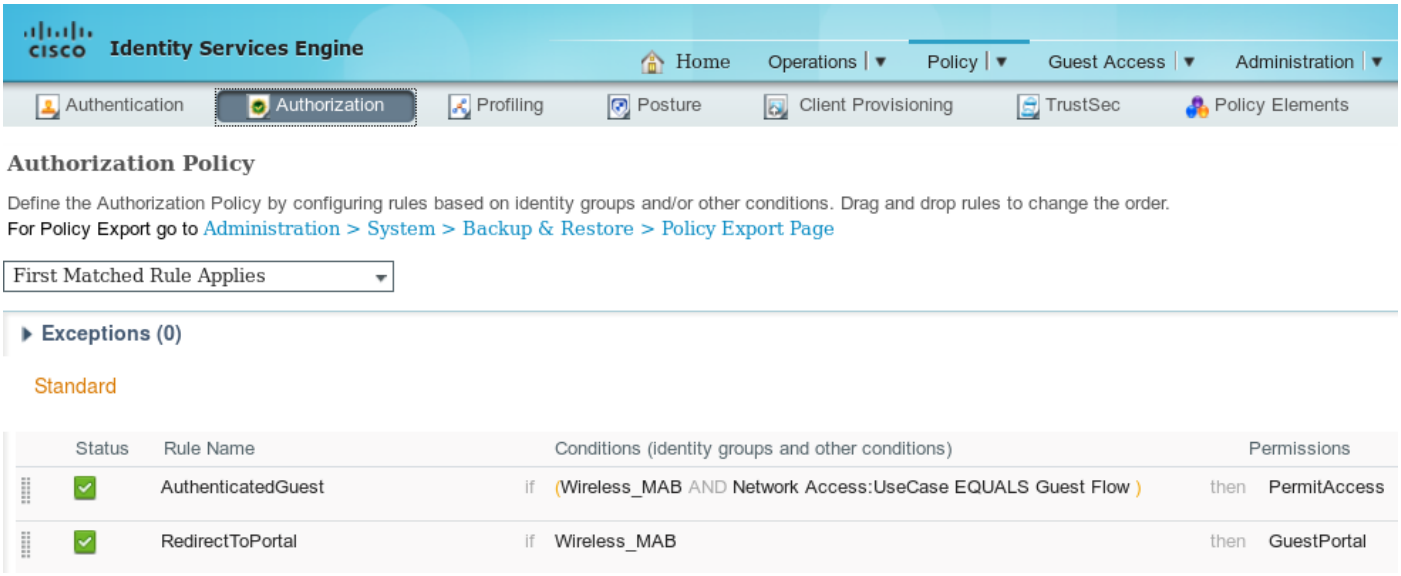
用于访客验证的所有终端在30天之后删除(从终端创建)。结果通常在尝试30天的来宾用户以后访问网络命中数RedirectToPortal授权规则和为验证重定向。

> **Note**:终端清除功能对立于访客帐户清除策略和访客帐户有效期。

> **Note**:在ISE 1.2终端能自动地删除，只有当点击内部仿形铣床队列限制时。然后最少最近使用终端删除。

临时访问权限

访客访问的另一个方法将使用访客流动条件。



情况检查对ISE和此的激活的会话是属性。如果该会话有表明的属性来宾用户顺利地以前验证请调节匹配。在ISE收到从网络接入设备(纳季)后的Radius认为的终止消息，会话终止及以后已经删除。在那阶段情况网络访问：UseCase =访客流不再满足。结果该终端的所有随后的认证点击重定向为访客验证的通用的规则。

> **Note**:不支持的访客流，当用户通过热点门户验证。对于那些方案UseCase属性设置为主机查找而不是访客流。

WLC断开行为

在客户端从无线网络后断开(例如使用在Windows的断开按钮)发送解除验证帧。但是那由WLC省略，并且可以被确认使用“调试客户端xxxx” - WLC不提交调试，当客户端从WLAN时断开。结果在Windows客户端：

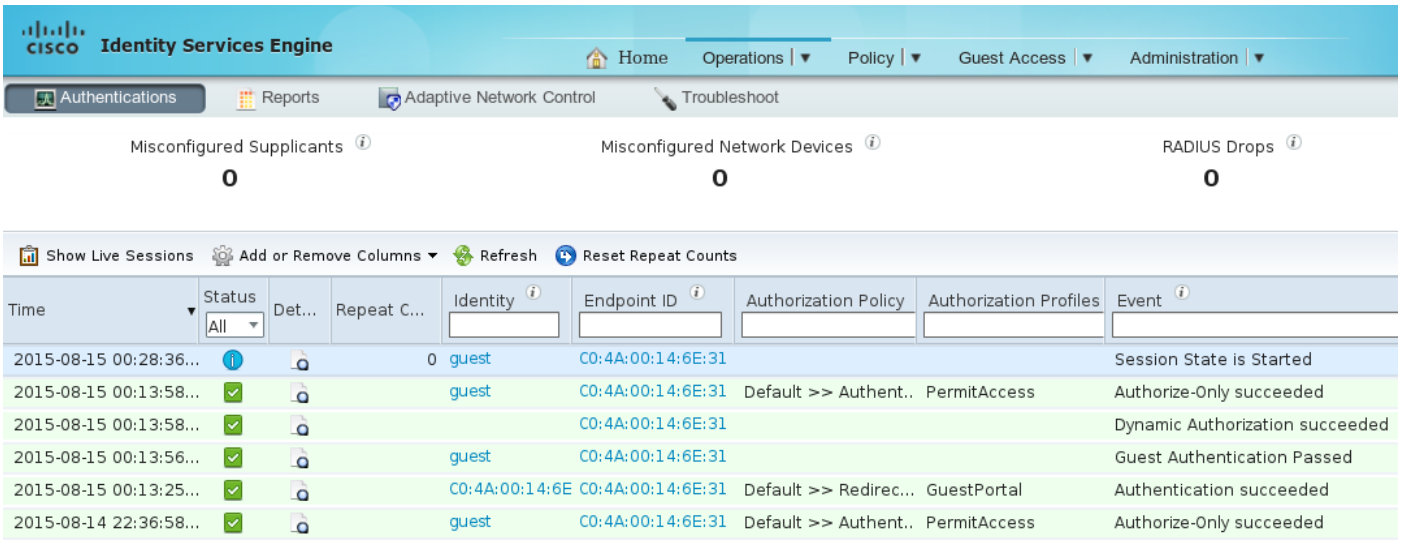
- IP地址从接口删除
- 接口在状态：被断开的媒体

但是在WLC状态不可更改(仍然客户端运转状态的)。

那是WLC的方案设计，会话删除，当

- 用户空闲超时命中数
- session-timeout命中数
- 如果曾经L2加密，那么，当组密钥循环间隔点击
- 其他造成AP/WLC插入客户端(即AP无线电重置，某人关闭WLAN等等)

使用该行为和临时访问配置，在用户从WLAN会话后断开没有从ISE删除，因为WLC从未清除它(和从未发送的Radius认为的终止)。如果会话没有删除， ISE仍然记住旧有会话，并且访客流动条件是满足的。在断开和重新连接用户以后请得以进入全双工网络访问，不用需求重新鉴别。



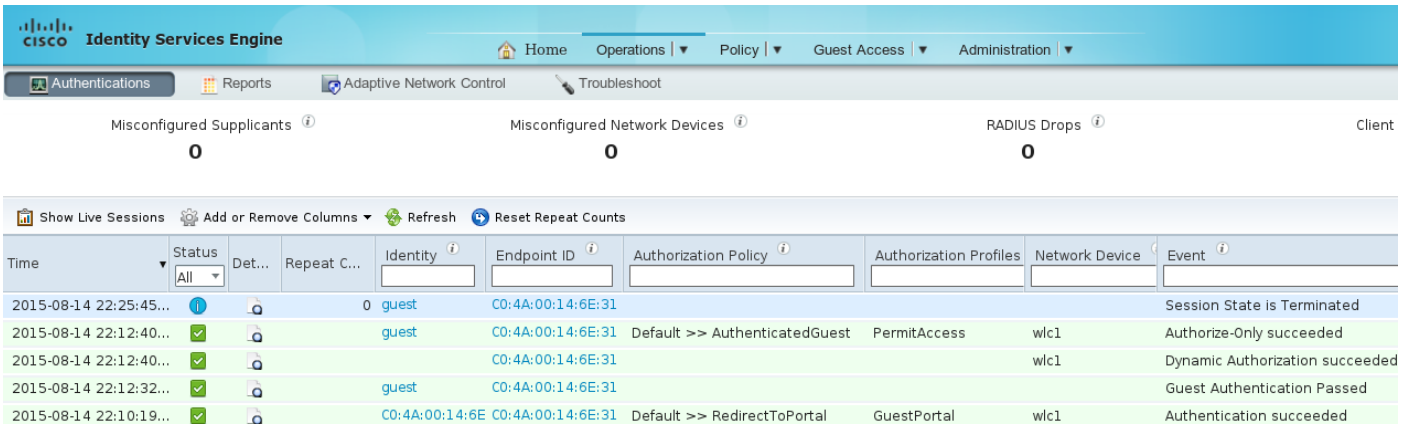
但是，如果，在断开用户连接对不同的WLAN后，然后WLC决定清除旧有会话。Radius认为的终止发送，并且ISE删除会话。如果客户端设法联络到原始WLAN访客流动条件不是满足的，并且的用户为验证重定向。

> **Note**:WLC配置与管理帧保护(MFP)接受从CCXv5 MFP客户端的已加密解除验证帧。

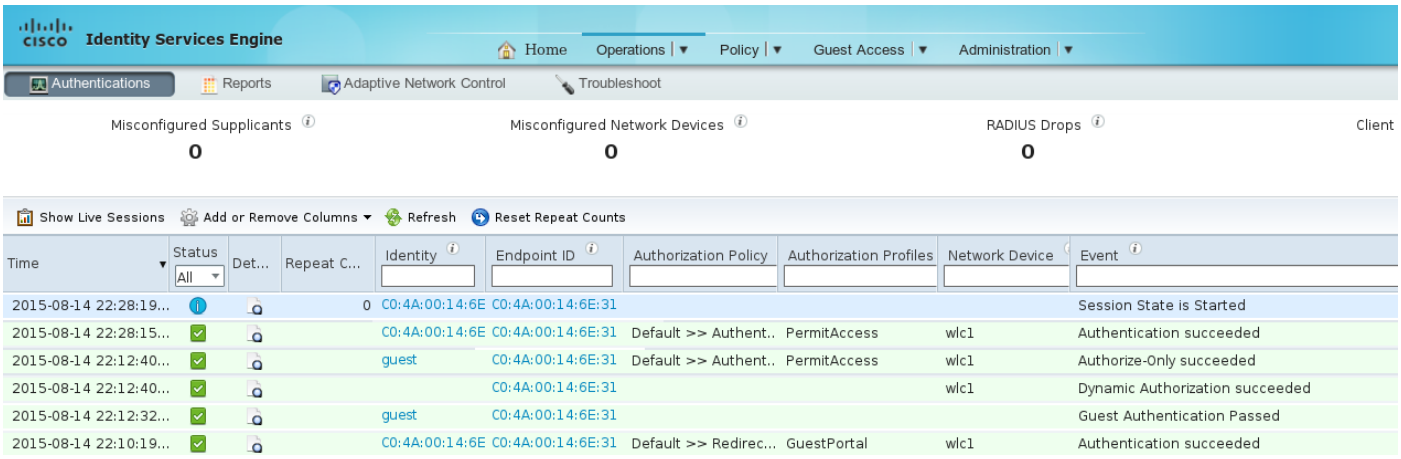
验证

永久性访问

在对访客门户和成功认证ISE发送崔凡吉莱的重定向以后授权(CoA)触发重新验证。结果新建的MAC验证旁路(MAB)会话被建立。这次终端属于GuestEndpoints标识组，并且匹配规定提供完全权限。

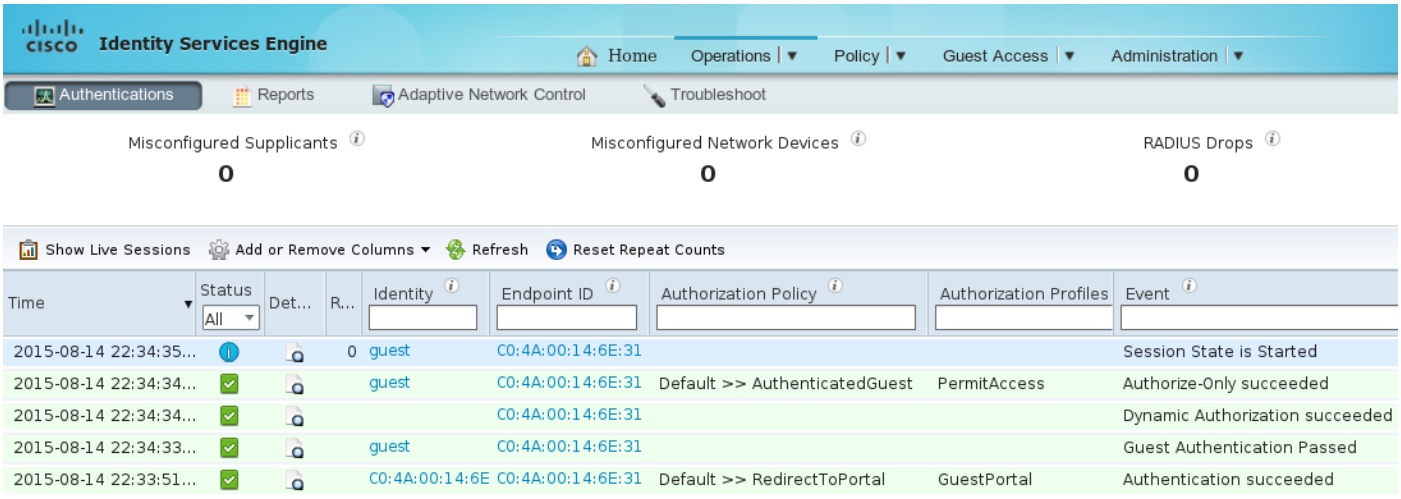


在该阶段无线用户能断开，连接到不同的WLAN，然后重新连接。所有那些随后的认证使用根据MAC地址的标识，但是点击第一个规则由于属于特定标识组的终端。全双工网络访问提供，不用访客验证。

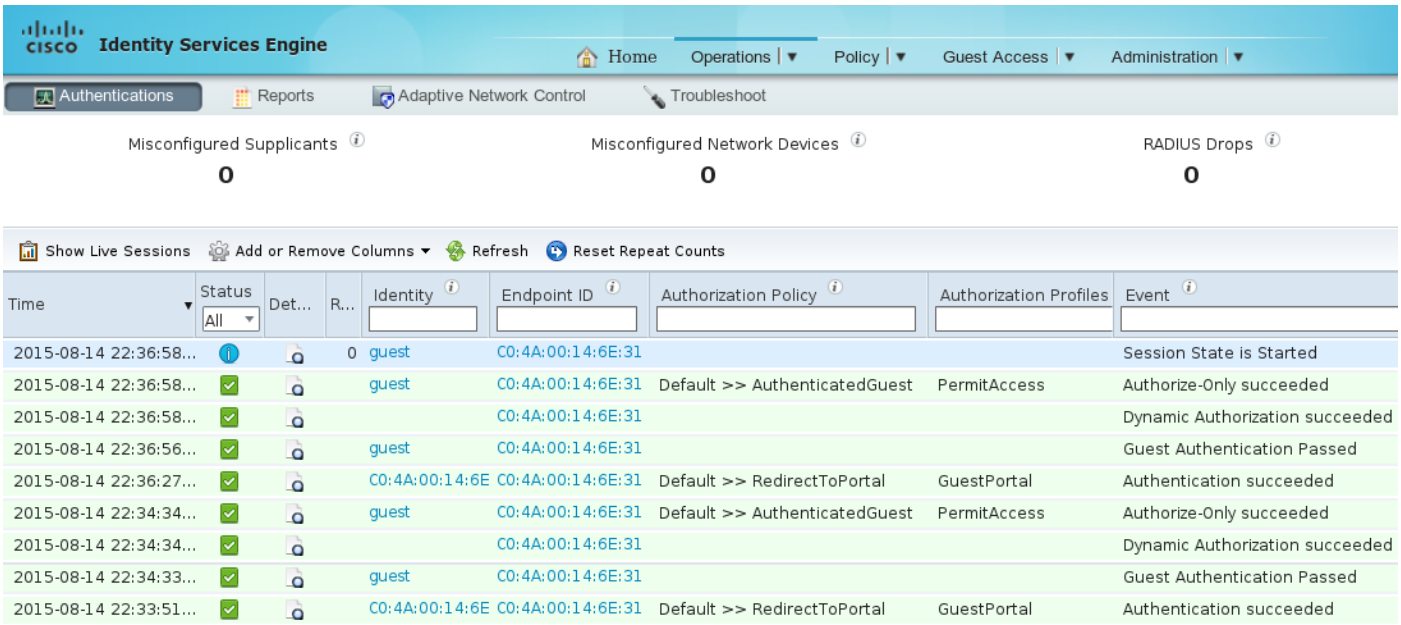


临时访问权限

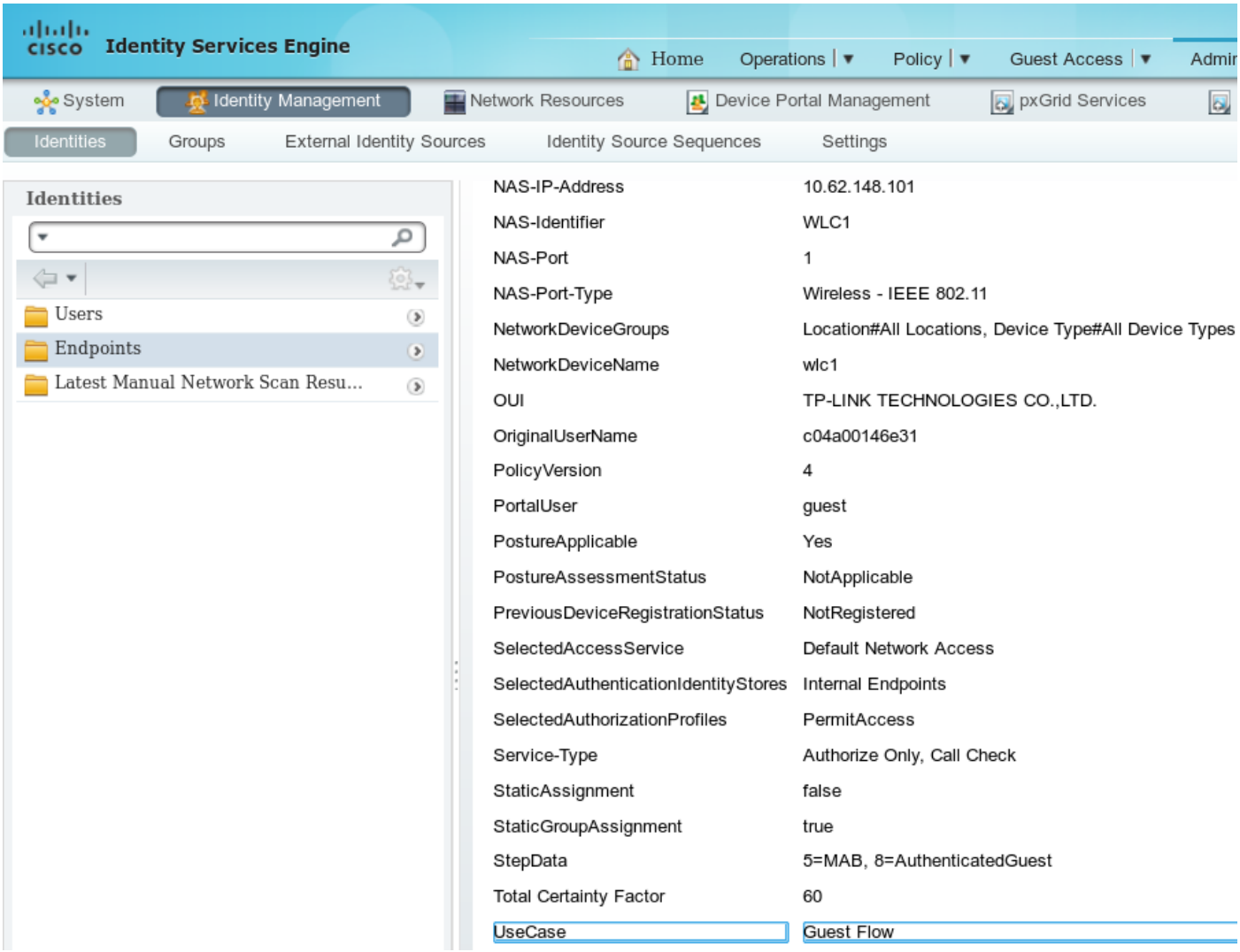
对于第二个场景(当情况根据访客流)开始是相同的。



但是，在会话为所有随后的认证后删除，访客点击通用的规则和为访客验证再重定向。



访客流动条件是的是满足的，当正确属性为会话时是现有。那可以通过查看终端属性验证。成功的访客验证结果指示。




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

Bug

CSCuu41157 ISE ENH CoA终止在访客帐户删除或终止的发送。

(增强请求在访客帐户删除或终止以后终止访客会话)

参考

- 思科ISE 1.3管理员指南
- 思科ISE 1.4管理员指南
- ISE版本1.3热点配置示例
- ISE版本1.3 Self已注册访客门户配置示例
- 在WLC和ISE配置示例的中央Web验证
- 与FlexConnect AP的中央Web验证在与ISE配置示例的一WLC
- 技术支持和文档 - Cisco Systems