根据SSID配置示例的ISE策略

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[配置](#)
[配置](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

本文在思科身份服务引擎(ISE)方面描述如何配置授权策略区分区别服务集标识符(Ssid)之间。它是非常普通为了组织能有在他们的无线网络的多个SSID多种目的。其中一个最普通的目的是有员工的一公司SSID和访客的一访客SSID对组织。

此指南假设那：

1. 无线局域网控制器(WLC)设置并且为介入的所有Ssid工作。
2. 验证在所有Ssid工作介入ISE。

其他文档此系列

- 与交换机和身份服务引擎配置示例的中央Web验证
- 在WLC和ISE配置示例的中央Web验证
- ISE RADIUS/802.1x身份验证配置示例的访客帐户
- 线型VPN摆姿势使用iPEP ISE和ASA

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 无线局域网控制器版本7.3.101.0

- 身份服务引擎版本1.1.2.145

更早版本也有这两个功能。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

配置

本文档使用以下配置：

- 方法 1：Airespace WLAN Id
- 方法 2：被呼叫状态ID

仅应该每次使用一个配置方法。如果两配置同时实现， ISE处理的数量增加，并且影响规定可读性。此本文探讨了每个配置方法优点和缺点。

方法 1：Airespace WLAN Id

在WLC (WLAN)创建的每个无线局域网有WLAN ID。WLAN ID在WLAN汇总页显示。

当客户端连接对SSID时，对ISE的RADIUS请求包含Airespace-WLAN-Id属性。此简单属性用于做出在ISE的政策决策。如果WLAN ID在多个控制器间，被传播的SSID不配比对此属性的一个缺点是。如果这描述您的部署，请继续对方法2。

在这种情况下， Airespace WLAN Id使用作为情况。它可以用于作为一个单纯条件(单独)或在一个复合条件(与另一个属性一道)取得预期结果。本文包括两个使用案件。使用以上两的Ssid，这两个规则可以创建。

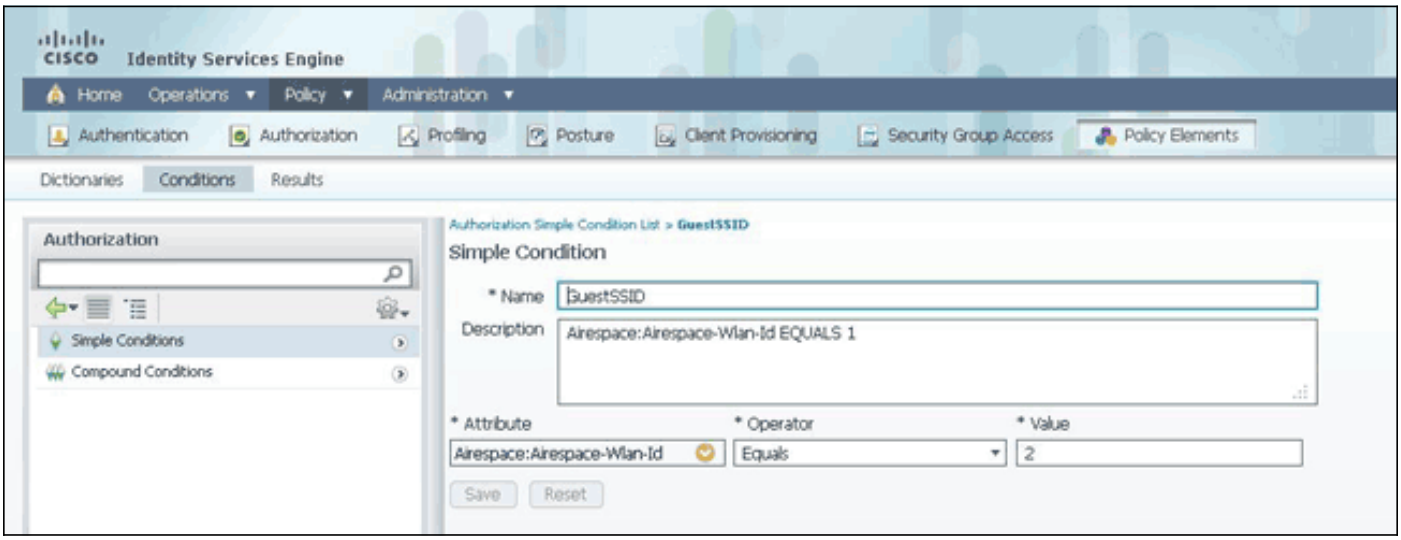
A) 来宾用户必须登录到访客SSID。

B) 集群用户必须是在激活目录(AD)组“域用户”中并且必须登录到公司SSID。

规定A

规定A有一个需求，因此您能建立一个单纯条件(根据以上的值) ：

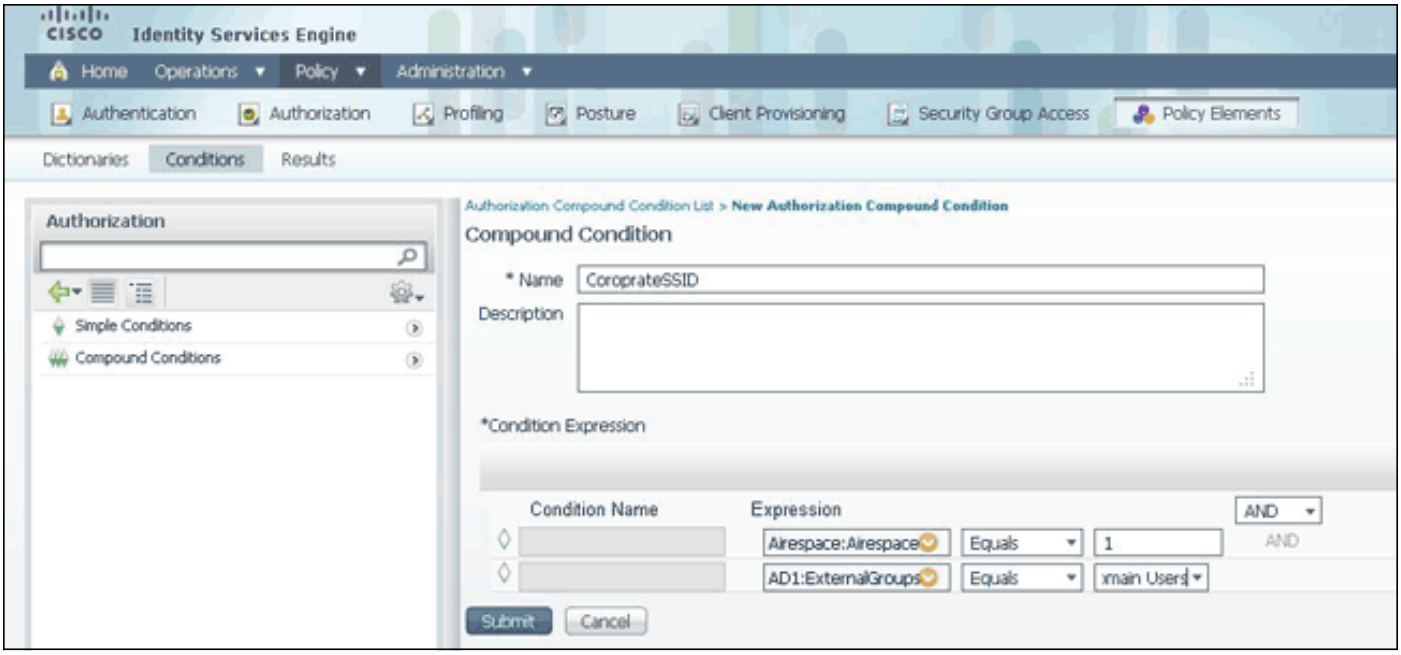
1. 在ISE，去**策略>Policy元素>情况>授权>单纯条件**并且创造新的条件。
2. 在Name字段，请输入条件名
3. 在说明字段，请输入说明(可选)。
4. 从属性下拉列表，请选择**Airespace > Airespace WLAN Id[1]**。
5. 从操作员下拉列表，请选择**等于。**
6. 从值下拉式列表，请选择**2。**
7. Click **Save**.



规定B

规则B有两个需求，因此您能建立一个复合条件(根据以上的值) ：

1. 在ISE，去**策略>Policy元素>情况>授权>复合条件**并且创造新的条件。
2. 在Name字段，请输入条件名。
3. 在说明字段，请输入说明(可选)。
4. 选择**创造新的条件(预先的选项)**。
5. 从属性下拉列表，请选择**Airespace > Airespace WLAN Id[1]**。
6. 从操作员下拉列表，请选择**等于。**
7. 从值下拉式列表，请选择**1。**
8. 单击齿轮在右边并且选择**添加属性/值**。
9. 从属性下拉列表，请选择**AD1 >外部组**。
10. 从操作员下拉列表，请选择**等于。**
11. 从值下拉式列表，请选择需要的组。在本例中，它设置为域用户。
12. Click **Save**.



注意： 在本文中我们使用简单授权配置文件配置在策略>Policy元素>结果>授权>授权配置文件下。他们设置允许访问，但是可以适应适合您的部署的需要。

即然我们有条件，我们能应用他们到授权策略。去**策略>授权**。在哪里确定插入在列表的规则或编辑您的现有规则。

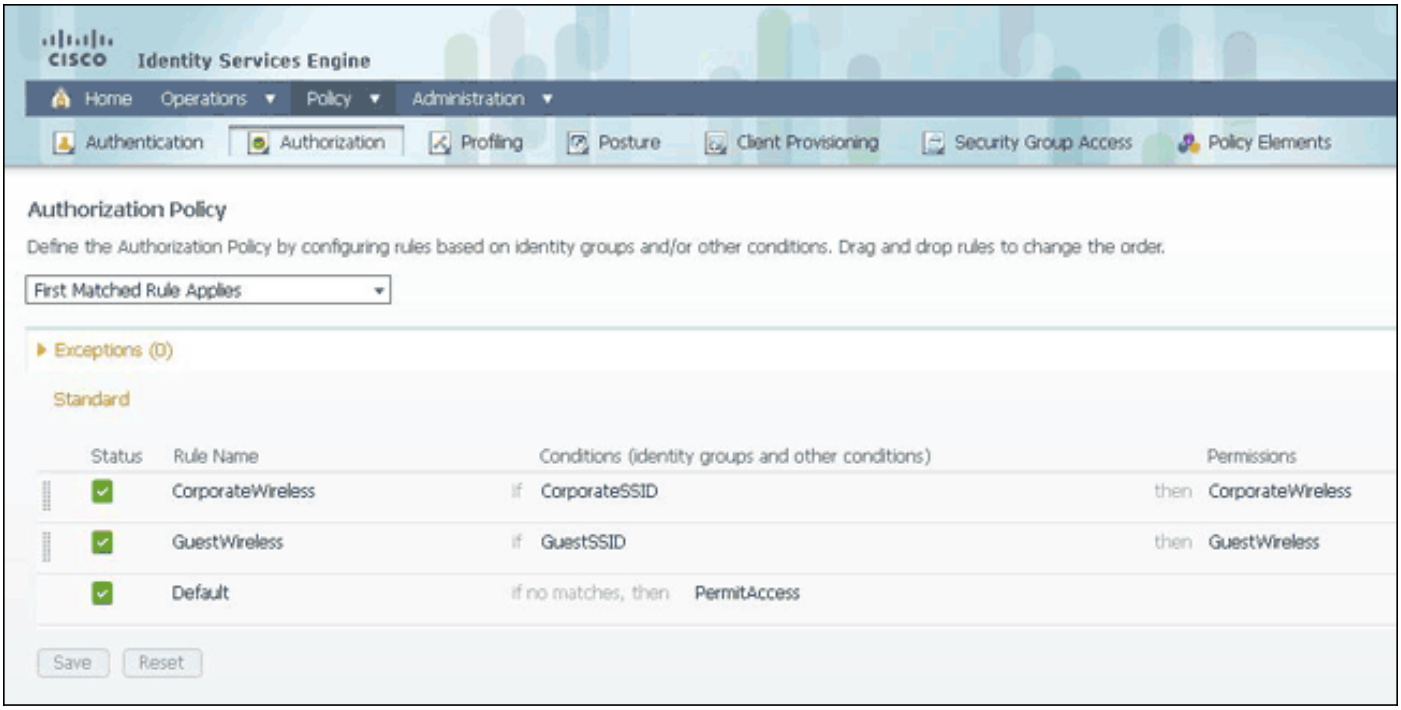
访客规则

1. 在一个现有规则右边单击下箭头并且选择**插入新规则**。
2. 输入一名称对于您的访客规则并且留下标识组字段设置对其中任一。
3. 在情况下，请点击加号并且单击**选择从库的现有情况**。
4. 在条件名下，请选择**单纯条件> GuestSSID**。
5. 在权限下，请选择您的来宾用户的适当的授权配置文件。
6. 点击**完成**。

公司规则

1. 在一个现有规则右边单击下箭头并且选择**插入新规则**。
2. 输入一名称对于您的公司规则并且留下标识组字段设置对其中任一。
3. 在情况下，请点击加号并且单击**选择从库的现有情况**。
4. 在条件名下，请选择**复合条件> CorporateSSID**。
5. 在权限下，请选择您的集群用户的适当的授权配置文件。
6. 点击**完成**。

注意： 直到您在策略列表的底部单击“Save”，在此屏幕做的变动不会应用对您的部署。



方法 2：被呼叫状态ID

WLC可以配置发送在RADIUS被呼叫状态ID属性的SSID名称，可以反过来使用作为在ISE的一个条件。此属性优点是可以使用不管什么WLAN ID被设置至开WLC。默认情况下， WLC不发送在被呼叫状态ID属性的SSID。启用在WLC的此功能，去**安全>AAA > RADIUS>验证**和设置呼叫站ID类型为AP MAC地址：SSID。这设置被呼叫状态ID的格式为*用户连接to> AP的<MAC ：<SSID Name>*。

您能看到什么SSID名称从WLAN汇总页发送。

因为呼叫站点Id属性也包含AP的MAC地址，常规表示(REGEX)用于匹配在ISE策略的SSID名称。操作员'匹配的在情况配置里能读从Value字段的一REGEX。

REGEX示例

'开始时' —例如，请使用REGEX值**^ (Acme)。*** —此情况配置作为证书：组织匹配的Acme' (任何匹配以从"Acme"开始)的情况。

'结束与' —例如，请使用REGEX值。*** (mktg) $** —此情况配置作为证书：组织匹配的mktg' (任何匹配以该的情况与"mktg的"末端)。

'包含' —例如，请使用REGEX值.*(1234).* —此情况配置作为证书：组织匹配'1234' (任何匹配以包含"1234"，例如Eng1234， 1234Dev的情况和Corp1234Mktg)。

'不开始时' —例如，请使用REGEX值**^ (？！LDAP)。*** —此情况配置作为证书：组织匹配的LDAP' (任何匹配以不从"LDAP"开始的一个条件，例如usLDAP或CorpLDAPmktg)。

被呼叫状态ID以SSID名称结束，因此使用的REGEX在本例中是**。* (：<SSID NAME>) $**。记住此，您通过配置。

使用以上两的Ssid，您能创建与这些需求的两个规则：

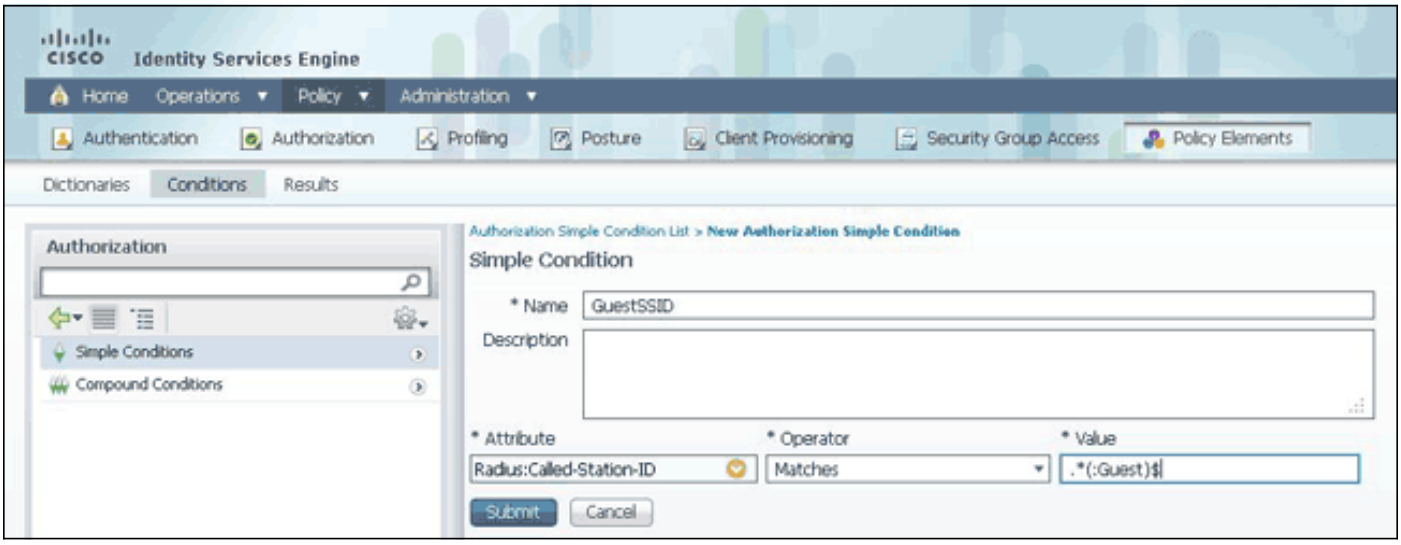
A) 来宾用户必须登录到访客SSID。

B) 集群用户必须是在AD组"域用户"中并且必须登录到公司SSID。

规定A

规定A有一个需求，因此您能建立一个单纯条件(根据以上的值) ：

1. 在ISE，去**策略>Policy元素>情况>授权>单纯条件**并且创造新的条件。
2. 在Name字段，请输入条件名。
3. 在说明字段，请输入说明(可选)。
4. 从属性下拉列表，请选择**Radius - >呼叫站点ID[30]**。
5. 从操作员下拉列表，请选择**匹配。**
6. 从值下拉式列表，请选择。*** (：访客) $**。这区分大小写。
7. Click **Save**.

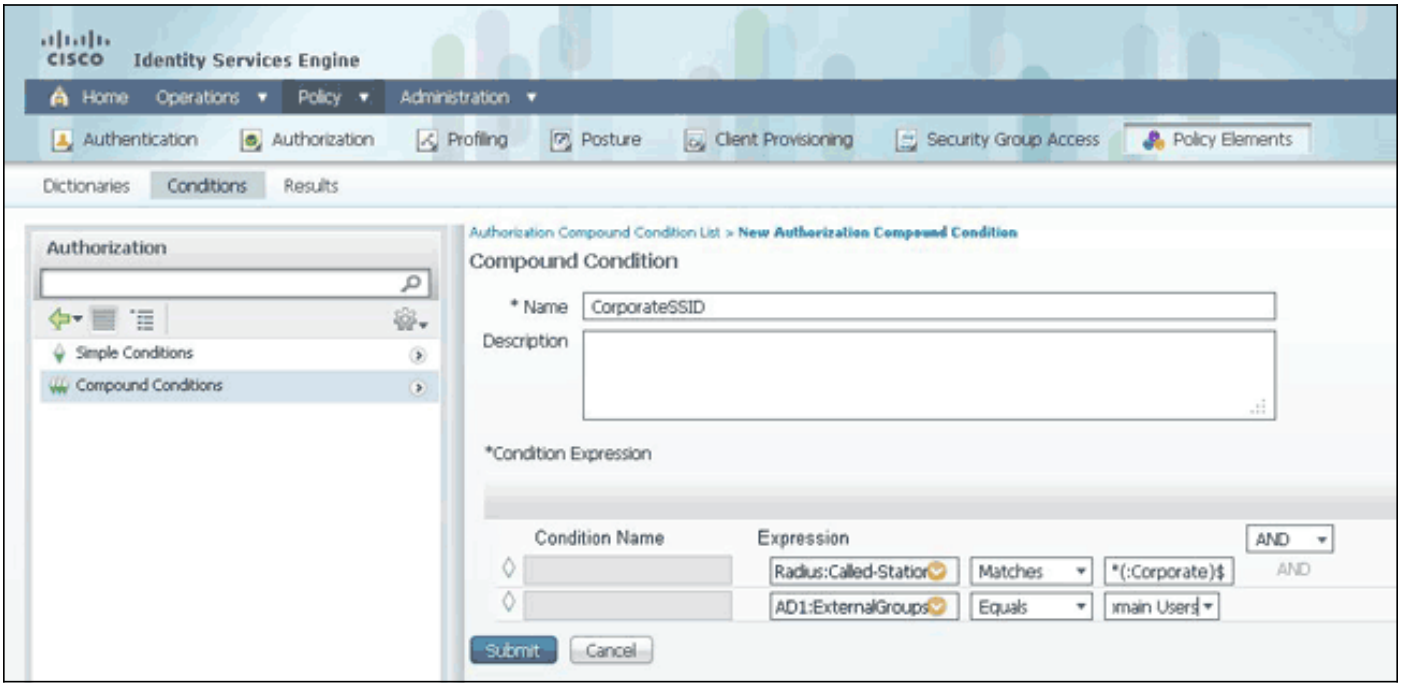


规定B

规则B有两个需求，因此您能建立一个复合条件(根据以上的值) ：

1. 在ISE，去**策略>Policy元素>情况>授权>复合条件**并且创造新的条件。

2. 在Name字段，请输入条件名。
3. 在说明字段，请输入说明(可选)。
4. 选择**创造新的条件(预先的选项)**。
5. 从属性下拉列表，请选择**Radius - >呼叫站点Id[30]**。
6. 从操作员下拉列表，请选择**匹配。**
7. 从值下拉式列表，请选择**。* (：公司) $**。这区分大小写。
8. 单击齿轮在右边并且选择**添加属性/值**。
9. 从属性下拉列表，请选择**AD1 >外部组**。
10. 从操作员下拉列表，请选择**等于。**
11. 从值下拉式列表，请选择需要的组。在本例中，它设置为域用户。
12. Click **Save**.



注意： 在本文中，我们使用简单授权配置文件配置在策略>Policy元素>结果>授权>授权配置文件下。他们设置允许访问，但是可以适应适合您的部署的需要。

即然条件配置，请应用他们对授权策略。去**策略>授权**。在适当的位置插入在列表的规则或编辑一个现有规则。

访客规则

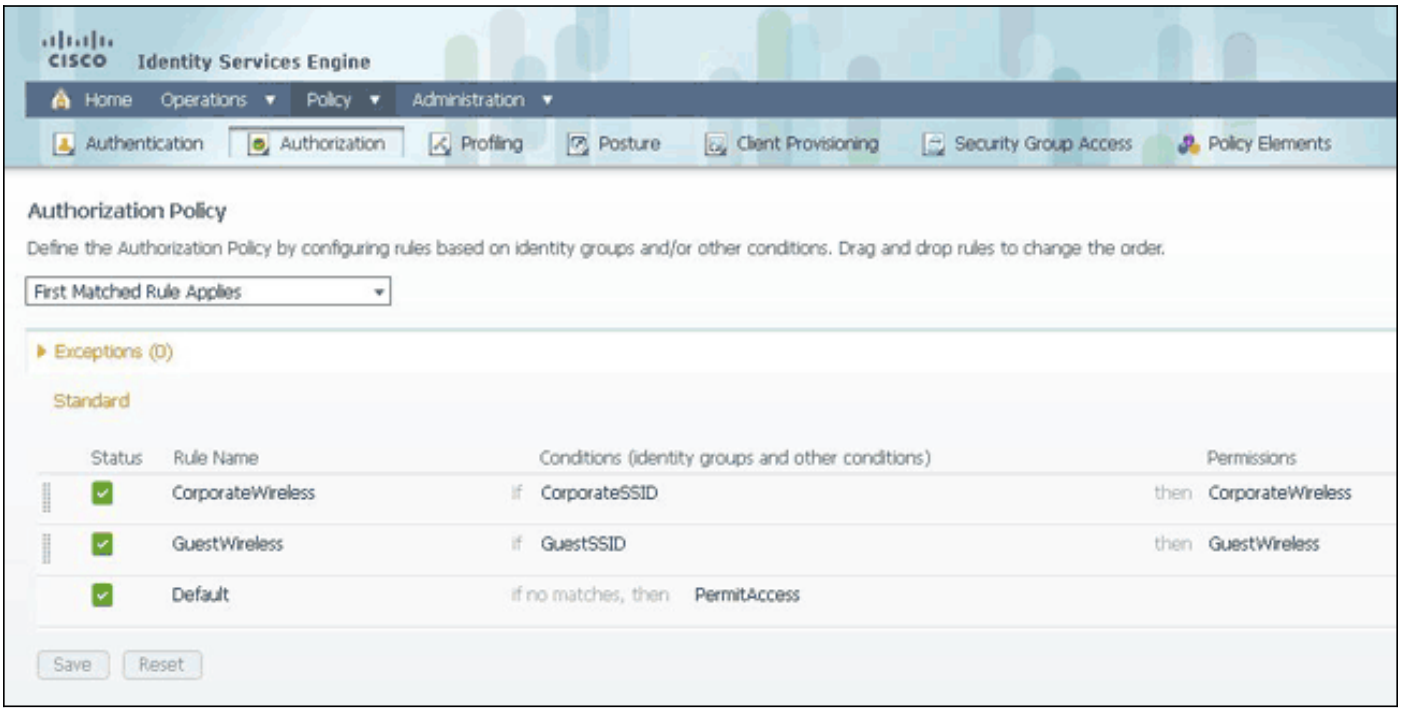
1. 在一个现有规则右边单击下箭头并且选择**插入新规则**。
2. 输入一名称对于您的访客规则并且留下标识组字段设置对其中任一。
3. 在情况下，请点击加号并且单击**选择从库的现有情况**。
4. 在条件名下，请选择**单纯条件> GuestSSID**
5. 在权限下，请选择您的来宾用户的适当的授权配置文件。
6. 点击**完成**。

公司规则

1. 在一个现有规则右边单击下箭头并且选择**插入新规则**。
2. 输入一名称对于您的公司规则并且留下标识组字段设置对其中任一。
3. 在情况下，请点击加号并且单击**选择从库的现有情况**。
4. 在条件名下，请选择**复合条件> CorporateSSID**。
5. 在权限下，请选择您的集群用户的适当的授权配置文件。

6. 点击**完成**。
7. 在策略列表的底部单击**"Save"**。

注意： 直到您在策略列表的底部单击"Save"，在此屏幕做的变动不会应用对您的部署。



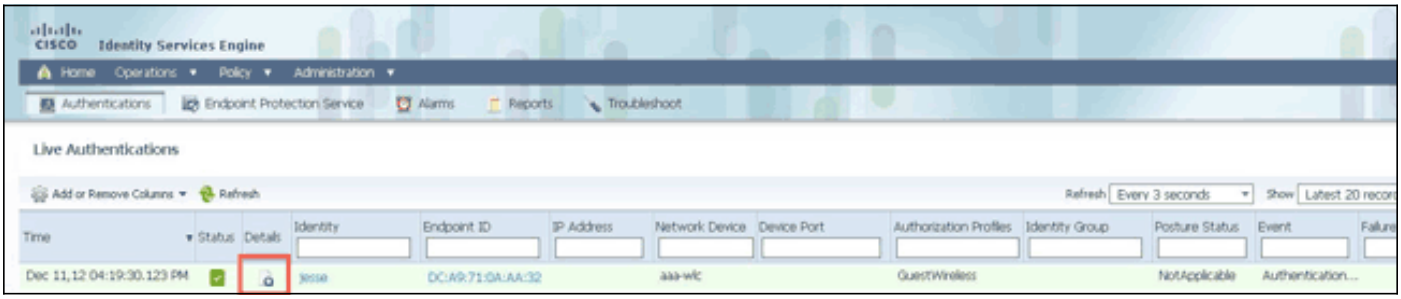
验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

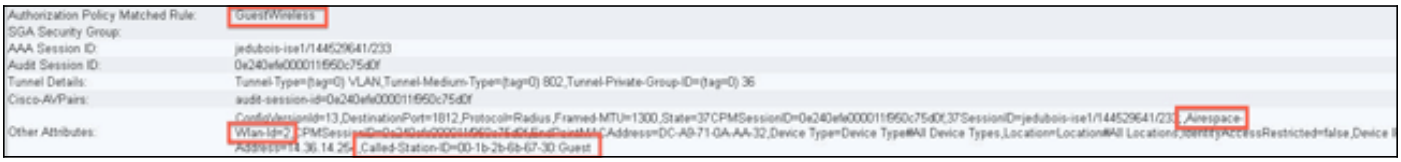
要欲知，如果策略适当地创建，并且确保ISE接收适当的属性，请查看一合格或失败的认证的详细的验证报告用户的。选择**操作>认证**然后单击**Details图标**验证的。



首先，请检查验证摘要。这显示验证的基础哪些包括什么授权配置文件提供了给用户。

Authentication Summary	
Logged At:	December 11,2012 4:19:30.123 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	jesse
MAC/IP Address:	DC:A9:71:0A:AA:32
Network Device:	aaa-wlc : 14.36.14.254 :
Allowed Protocol:	Default Network Access
Identity Store:	AD1
Authorization Profiles:	GuestWireless
SGA Security Group:	
Authentication Protocol :	PEAP(EAP-MSCHAPv2)

如果策略不正确，验证详细信息将显示什么Airespace WLAN Id，并且什么呼叫站点Id从WLC发送。相应地调节您的规则。授权策略匹配的规则确认验证是否匹配您的打算的规则。



这些规则通常是不正确的配置的。要显示配置问题，规则与什么相符在验证详细信息被看到。如果在另一个属性字段看不到属性，请确保WLC适当地配置。

相关信息

- 技术支持和文档 - Cisco Systems