配置与ISE 2.0和阿鲁巴WLC的访客流

目录

简介

本文配置访客门户的descrbies步骤用阿鲁巴无线局域网控制器(WLC)。从身份服务引擎(ISE)第三方网络访问的版本2.0支持设备(NAD)介绍。ISE当前支持集成用访客的阿鲁巴无线，状态并且带来您自己的设备(BYOD)流。

> **Note**:思科对配置或支持不负责设备的从其他供应商。

先决条件

要求

Cisco 建议您了解以下主题：

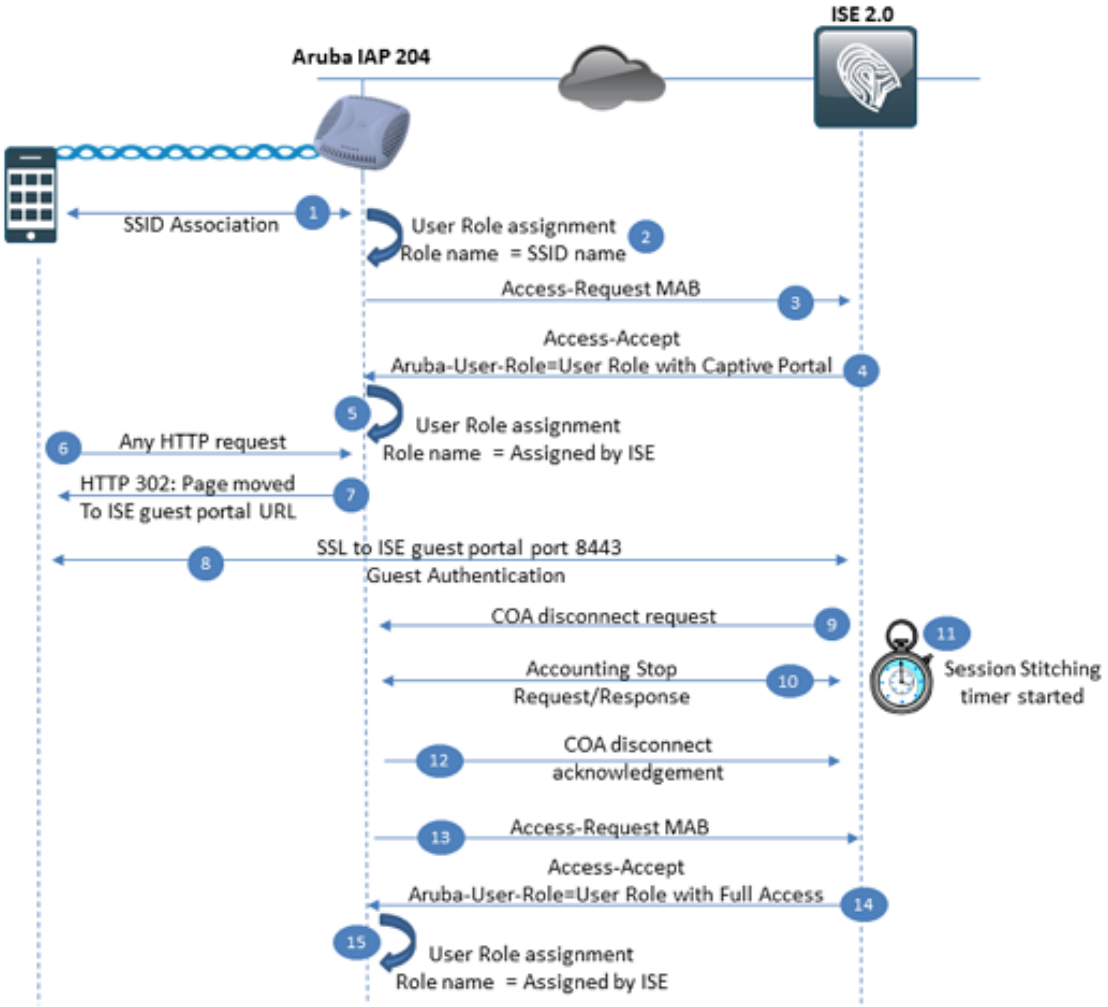
- 阿鲁巴IAP配置
- 在ISE的访客流

使用的组件

- 阿鲁巴IAP 204软件6.4.2.3
- 思科身份服务引擎2.0

背景信息

访客流



步骤1.用户关联对服务集Identifer (SSID)。SSID可以配置如开放或与预先共享密钥验证。

步骤2.阿鲁巴应用用户角色对此连接。第一个用户角色总是SSID。用户角色包含不同的设置类似VLAN，访问控制限制，俘虏PORTAL设置等等。在当前示例默认用户角色分配到SSID有Permit仅所有语句。

步骤3. SSID配置提供过滤在外部RADIUS服务器的MAC。Radius MAB (MAC验证旁路)访问请求发送对ISE。

第四步：在策略评估时间ISE选择访客的授权配置文件。此授权配置文件包含访问类型相等与ACCESS_ACCEPT和阿鲁巴用户角色相等与用户角色在阿鲁巴WLC配置的本地名称(无线局域网控制器)。此用户角色为俘虏PORTAL配置，并且流量重定向往ISE。

阿鲁巴用户角色

由阿鲁巴WLC使用的主要组件是用户角色。用户角色定义了访问限制可适用对用户在连接时。访问

限制能包括：俘虏门户重定向，访问控制表， VLAN (虚拟局域网)，带宽限制和其他。在阿鲁巴WLC存在的每SSID有用户角色与SSID名称是相等的默认用户角色，所有用户连接对特定SSID从默认角色最初获得限制。用户角色可以由RADIUS服务器覆盖， Access-Accept应该在这种情况下包含阿鲁巴卖方细节属性阿鲁巴用户角色。WLC用于从此属性的值查找本地用户角色。

第五步：使用属性阿鲁巴用户角色本地WLC检查对于已配置的用户角色和应用需要的一个。

步骤6.用户启动在浏览器的HTTP请求。

步骤7.阿鲁巴WLC截住请求由于为俘虏门户配置的用户角色。对此请求WLC的一答复返回HTTP代码302页移动与ISE访客门户作为一个新的位置。

步骤8.用户在访客门户建立对ISE的SSL连接在端口8443，并且提供用户名/密码。

步骤9. ISE传送COA Disconnect请求信息对阿鲁巴WLC。

步骤 10在COA断开消息WLC切与用户的连接并且通知ISE后使用Radius记帐请求(终止)消息，应该终止连接。ISE必须确认此消息接收与核算。

步骤11. ISE启动会话缝的计时器。此计时器用于在一起地粘合会话在COA前后。在此时间ISE记住所有会话参数类似用户名等等。在此计时器超时选择客户端的前，正确授权策略第二个认证尝试必须完成。万一，如果计时器超时，新建的Access-Request将解释作为一全新的会话，并且与访客重定向的授权策略再将应用。

步骤 12阿鲁巴WLC确认以前与COA断开确认的已接收COA断开请求。

步骤 13阿鲁巴WLC发送新建的MAB Radius Access-Request。

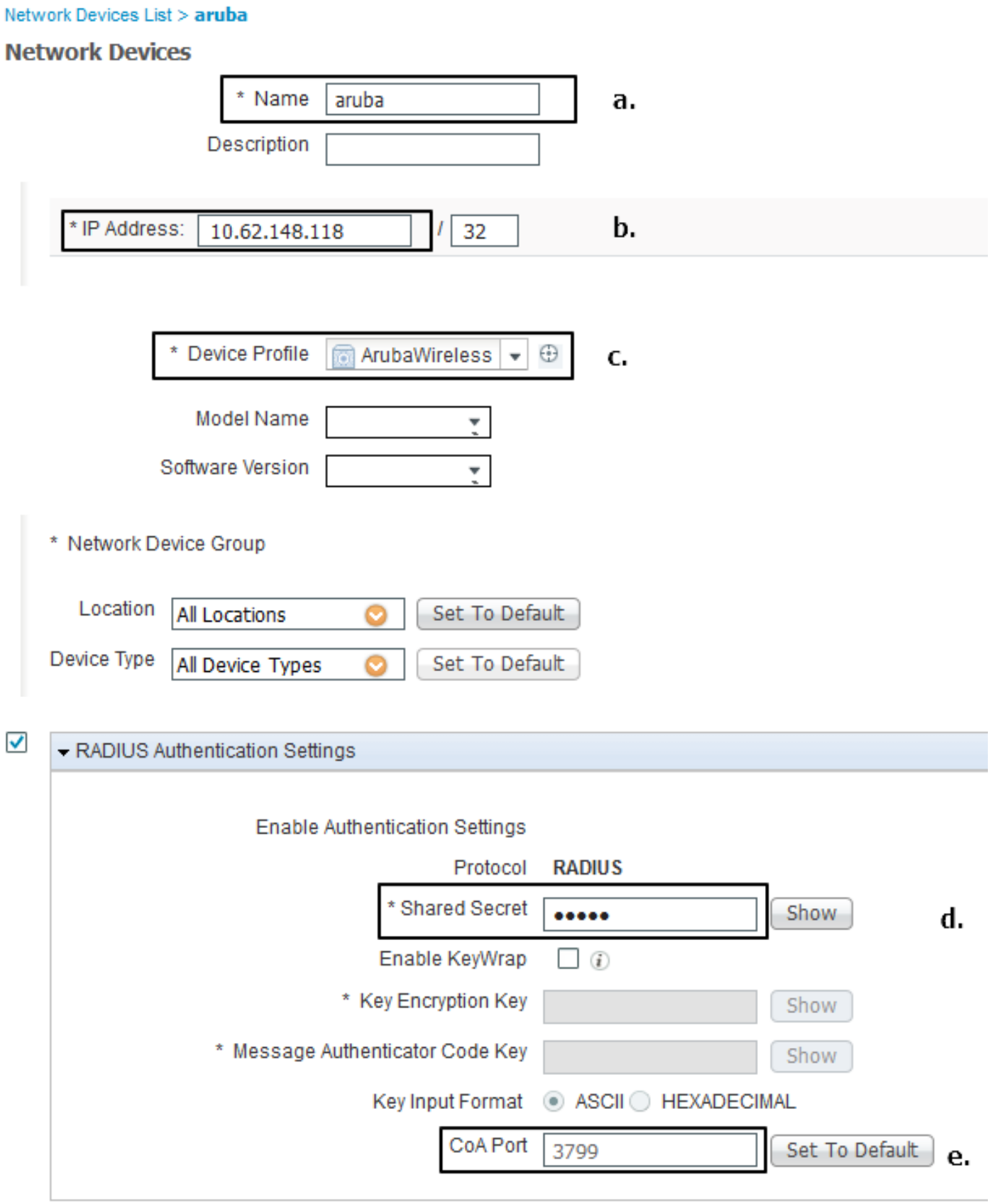
步骤 14在策略评估时间ISE在验证以后选择访客的授权配置文件。此授权配置文件包含访问类型相等与ACCESS_ACCEPT和阿鲁巴用户角色相等与用户角色在阿鲁巴WLC配置的本地名称。配置的此用户角色允许所有流量。

步骤 15使用属性阿鲁巴用户角色WLC检查本地配置的用户角色并且应用需要的一个。

配置

步骤1.添加阿鲁巴WLC作为ISE的纳季。

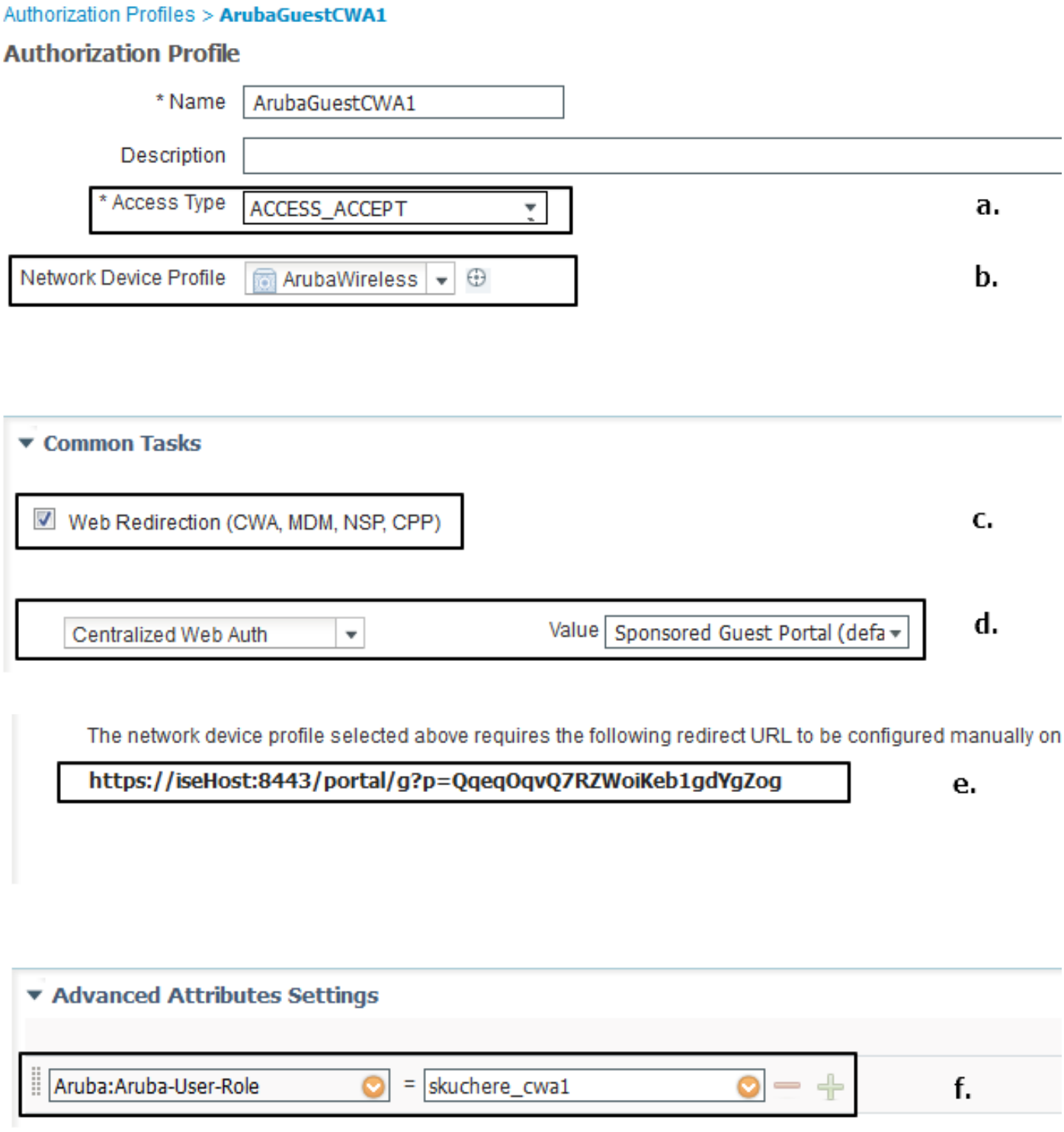
导航到**Administration >网络资源>网络设备**并且单击**添加**



1. 提供网络接入设备(纳季)名称。
2. 指定纳季IP地址。
3. 选择网络设备配置文件。对于阿鲁巴WLC您可以使用内置的配置文件ArubaWireless。
4. 提供预先共享密钥。
5. 定义COA端口 ， COA的设备表当前示例使用UDP端口3799。

步骤2.配置授权配置文件。

导航对**策略>Policy元素>结果>授权>授权配置文件**并且单击**添加。**首先您必须创建中央Web验证(CWA)如镜像所显示，重定向的授权配置文件。

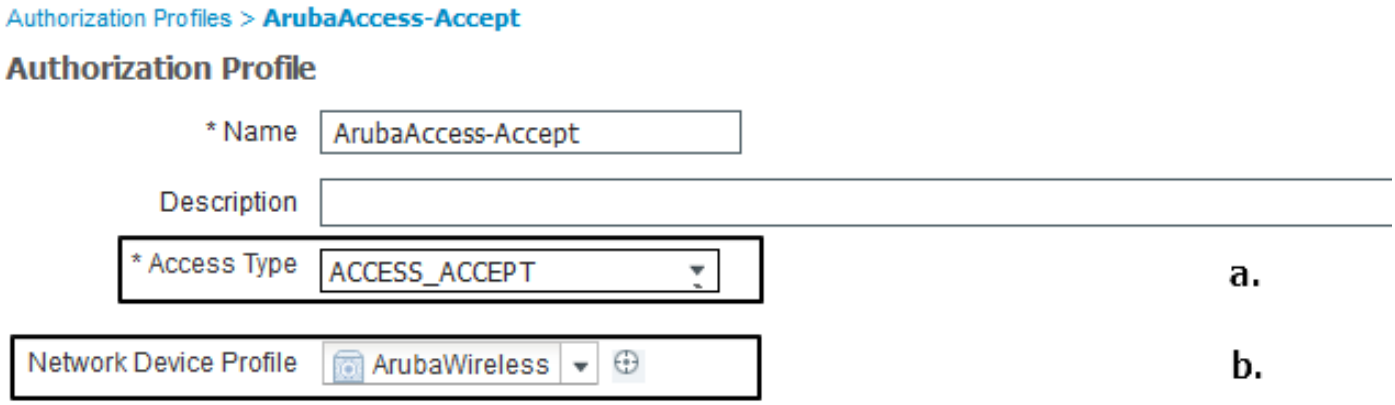


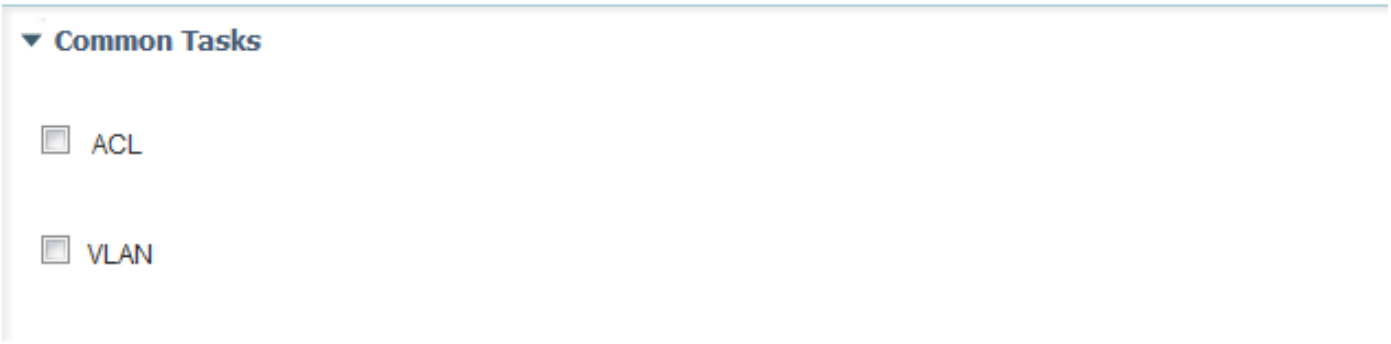
Note:默认情况下所有授权配置文件有网络设备设备类型相等与思科。如果纳季配置作为ArubaWireless，并且授权配置文件为其它设备设备类型创建，此配置文件为此设备从未匹配。

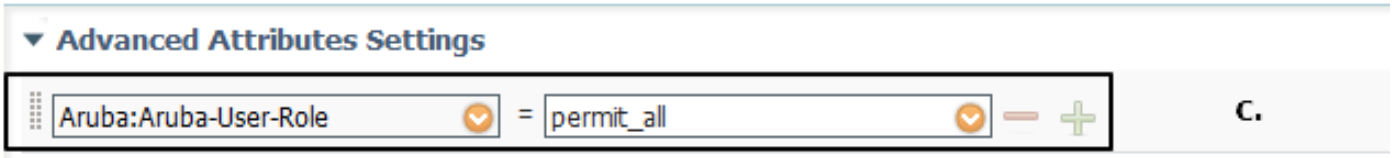
1. 定义**访问类型**作为Access-Accept。
2. 在网络设备**配置文件请**选择ArubaWireless。
3. 在普通的Task部分，请启用**Web重定向**选项。
4. 因为重定向类型选择**集中化Web验证**并且选择您希望使用重定向的访客门户。
5. ISE提交的URL在阿鲁巴WLC应该定义作为外部俘虏门户URL。

6. 在**先进的属性**设置部分，请定义阿鲁巴用户角色属性值。

应该创建第二授权配置文件为来宾用户提供访问在门户验证以后：







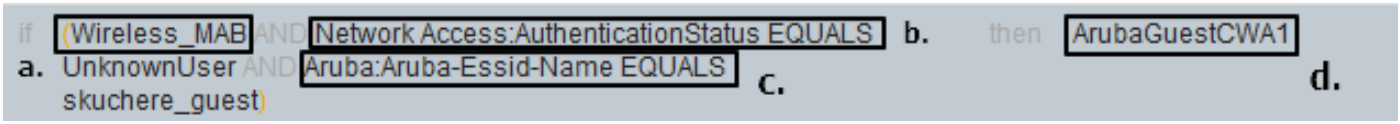
1. 定义**访问类型**作为Access-Accept。
2. 在**网络设备配置文件请**选择ArubaWireless。
3. 在**先进的属性**设置部分请定义阿鲁巴用户角色属性值。稍后您将配置在阿鲁巴WLC的本地用户角色与同一名称。

步骤3.配置授权策略。

第一项授权策略对用户重定向负责对访客门户。在最简单的案件中，您在复合条件能使用构件

- Wireless_MAB (a.)和
- 网络访问对未知用户(b.)的AuthenticationStatus等于和
- 阿鲁巴阿鲁巴Essid NAME相等与您的访客SSID名称(c.)。

对于此策略，请配置与重定向的授权配置文件到访客门户结果(D.)



第二项授权策略应该为来宾用户提供访问在验证以后通过门户。此策略能依靠会话数据(用户标识组/用例访客流等等)。在此方案中，在会话缝的计时器超时前，用户应该重新连接：

if	GuestType_Contractor (default) AND (Wireless_MAB AND Aruba:Aruba-Essid-Name EQUALS skuchere_guest)	then	ArubaAccess-Accept

从您在终端数据能取决于而不是会话数据的会话缝的计时器失效保护。默认情况下， ISE的2.0被赞助的访客门户为自动访客设备已注册配置(访客设备在Guest_Endpoints终端标识组中自动地安置)。此组可以使用作为情况：

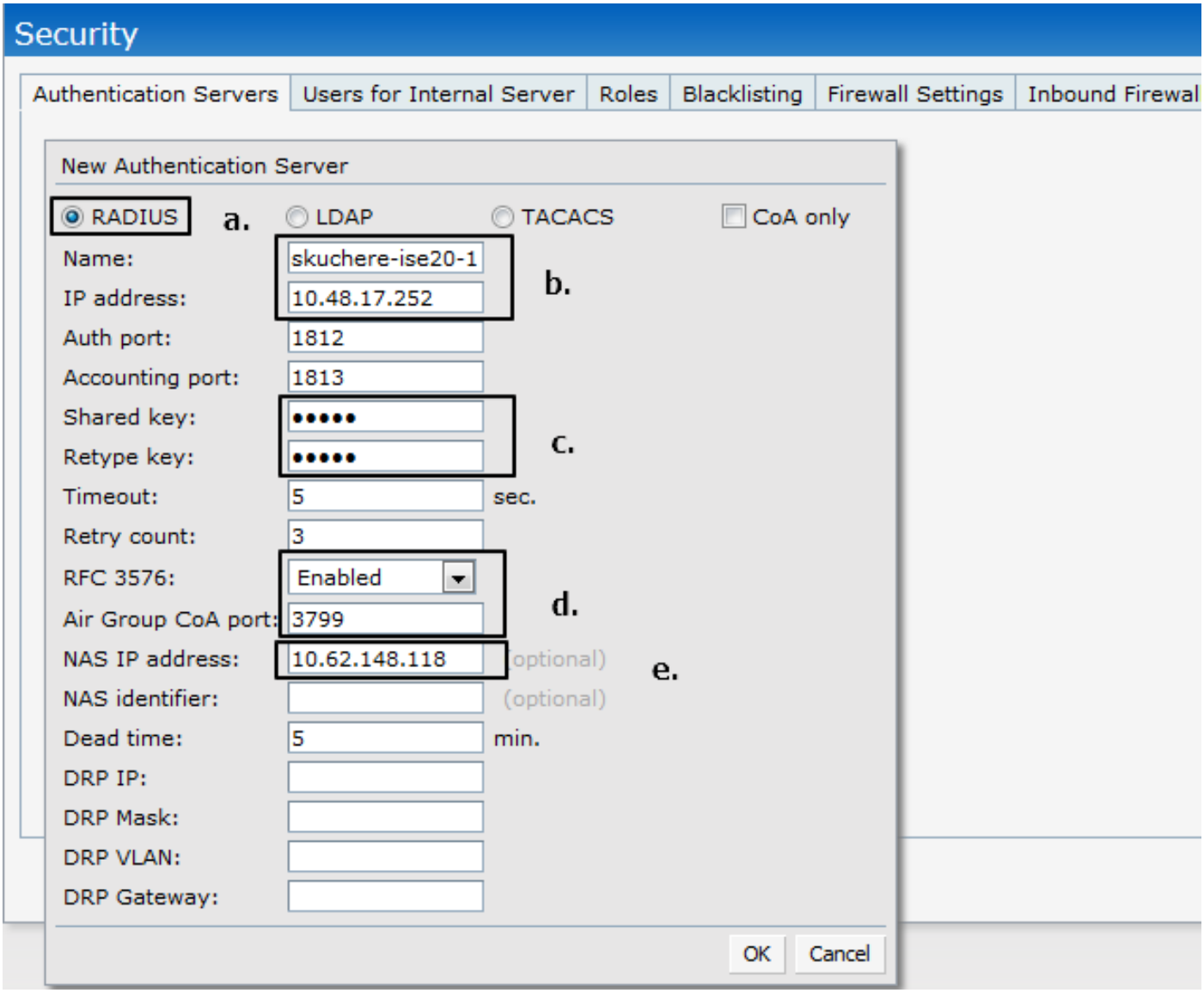
if	GuestEndpoints AND (Wireless_MAB AND Aruba:Aruba-Essid-Name EQUALS skuchere_guest)	then	ArubaAccess-Accept

授权策略按正确顺序：

if	**GuestEndpoints** AND (Wireless_MAB AND Aruba:Aruba-Essid-Name EQUALS skuchere_guest)	then	ArubaAccess-Accept
if	(Wireless_MAB AND Network Access:AuthenticationStatus EQUALS UnknownUser AND Aruba:Aruba-Essid-Name EQUALS skuchere_guest)	then	ArubaGuestCWA1

步骤4.配置在阿鲁巴的RADIUS服务器。

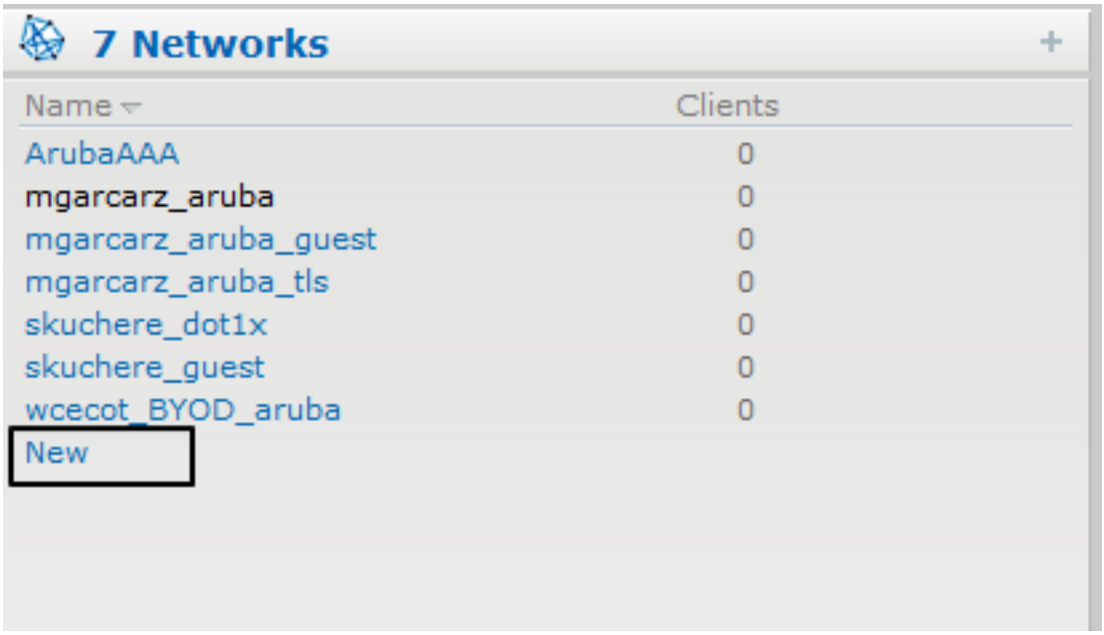
导航到**Security > Authentication服务器**并且点击**新**：



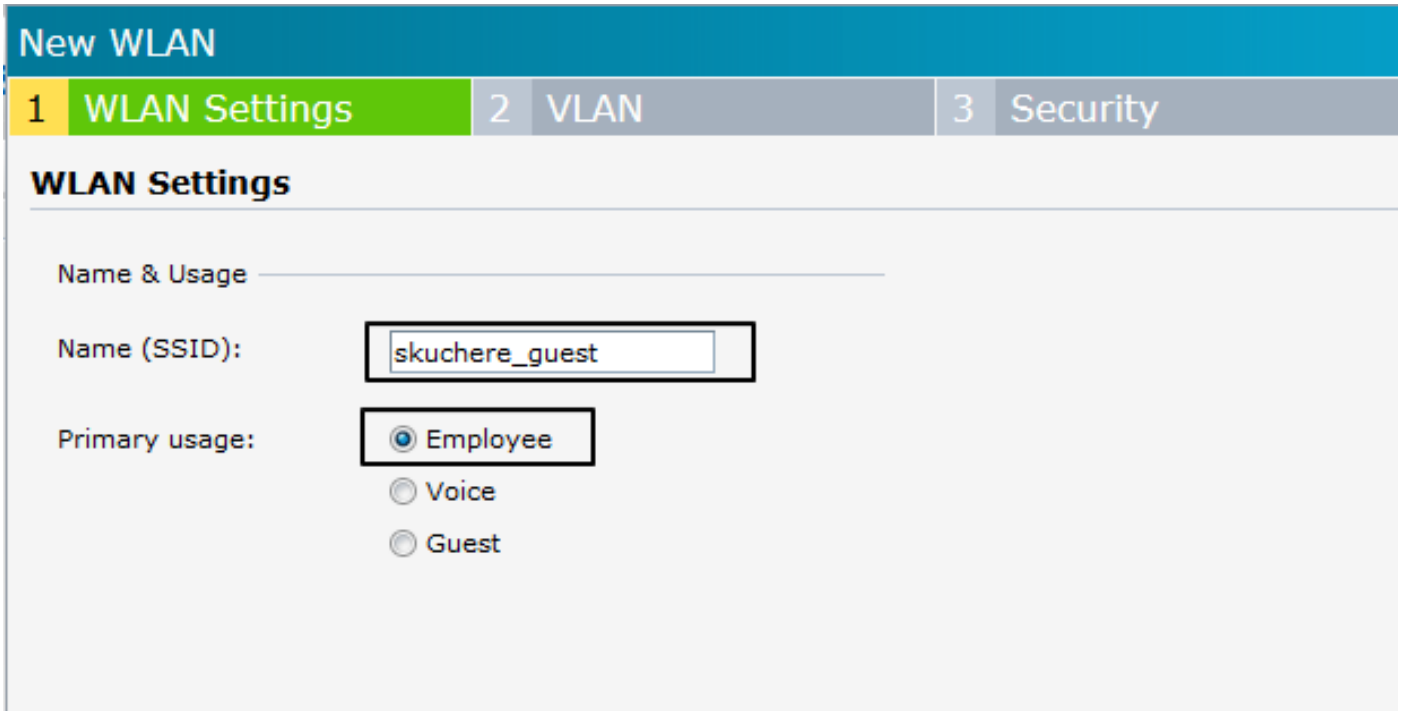
1. 选择RADIUS作为AAA协议。
2. 定义AAA服务器名称和IP地址。
3. 指定预先共享密钥。
4. 启用RFC 3576支持并且定义COA端口。
5. 指定阿鲁巴WLC管理接口IP作为NAS IP地址。

步骤5.创建在阿鲁巴的访客SSID。

在控制板页请选择**新**在网络列表结束时。SSID创建向导应该启动。遵从向导步骤。

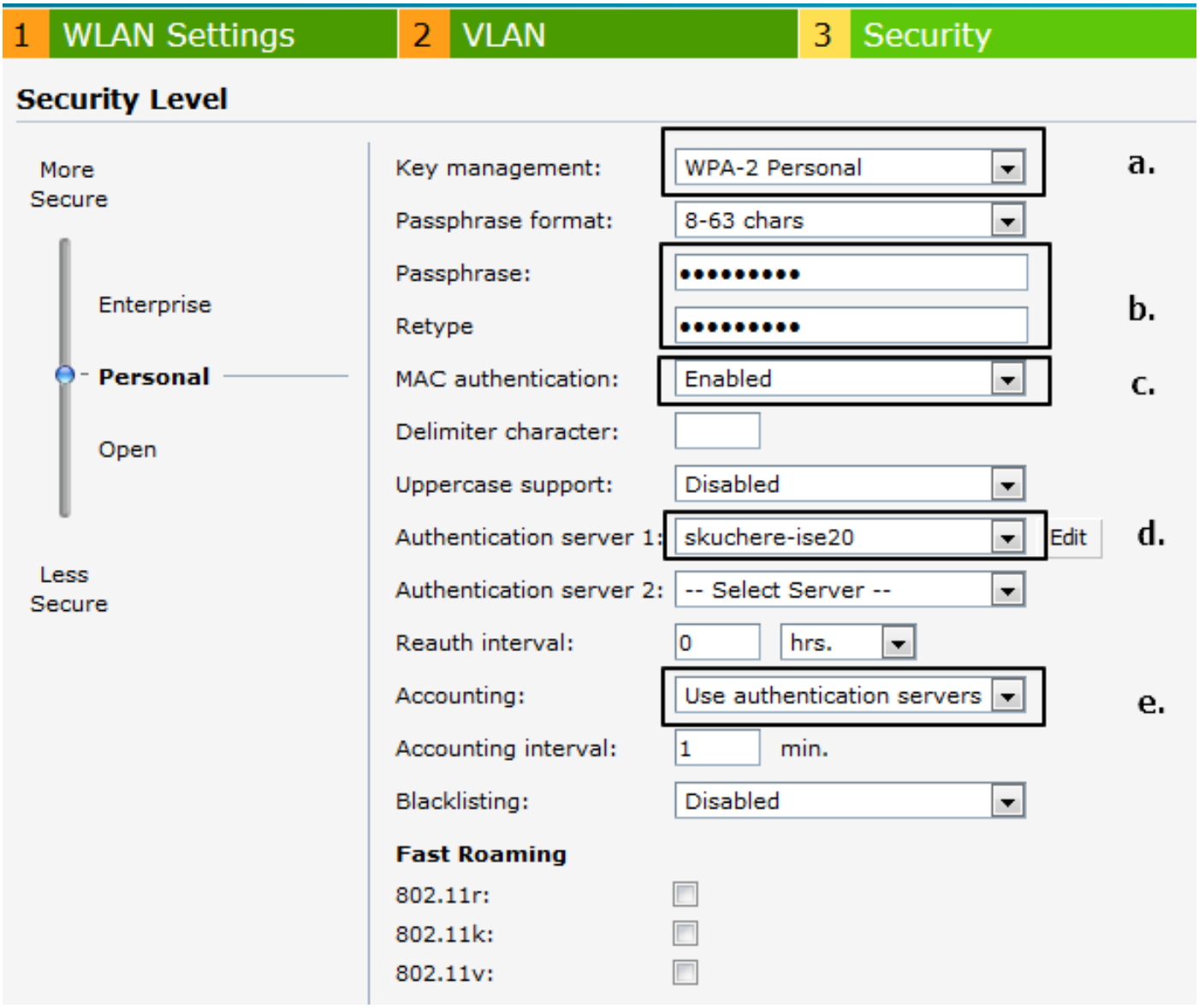


步骤1.定义SSID名称和挑选SSID类型。这里， SSID使用类型员工。此SSID类型没有与permit的默认角色全部和俘虏门户执行。并且，您能选择类型访客。在这样方案中您应该在SSID配置时定义俘虏门户设置。



步骤2. VLAN和IP地址分配。这里，如镜像所显示，设置被留下作为默认。

步骤3.安全设置。对于访客SSID您能选择打开或个人。个人要求PRE细片密钥。

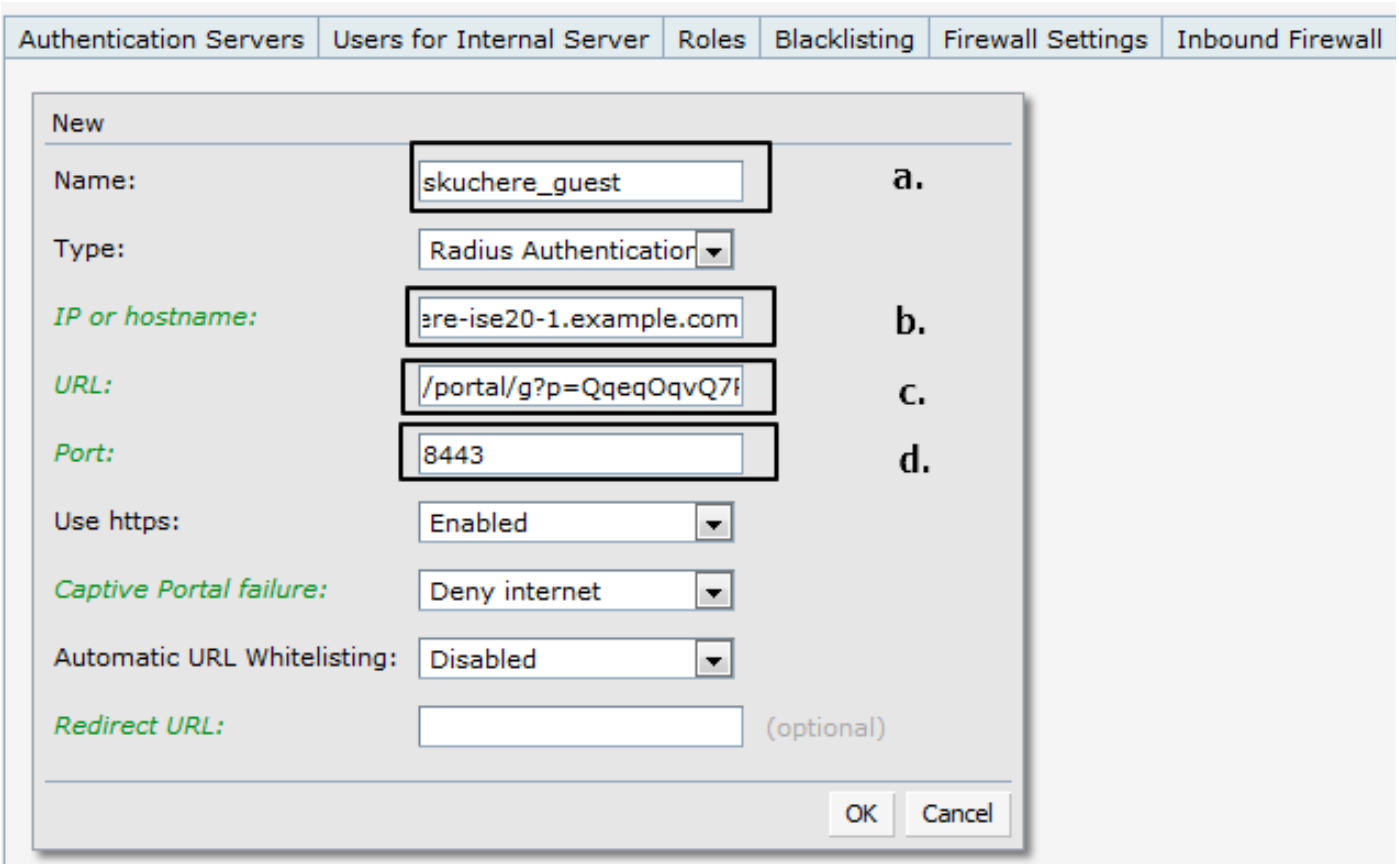


1. 选择密钥管理机制。
2. 定义预先共享密钥。
3. 利用ISE验证用户使用过滤需要的MAB MAC启用。
4. 在认证服务器列表中请选择您的AAA服务器。
5. 对往以前定义AAA服务器的启用帐户请选择在下拉列表的使用认证服务器。

Note:核算是关键的与第三部分NAD。如果策略服务节点(PSN)不接收用户的核算终止从纳季，会话可能陷在开始的状态。

步骤6.配置俘虏门户。

如镜像所显示，导航对**安全>外部俘虏门户**并且创建新的门户， ：



步骤1.指定俘虏门户名称。

Steo 2.定义了您的ISE FQDN或IP地址。如果使用IP地址，请保证在访客门户证书附属的代替Name(SAN)字段定义的此IP。

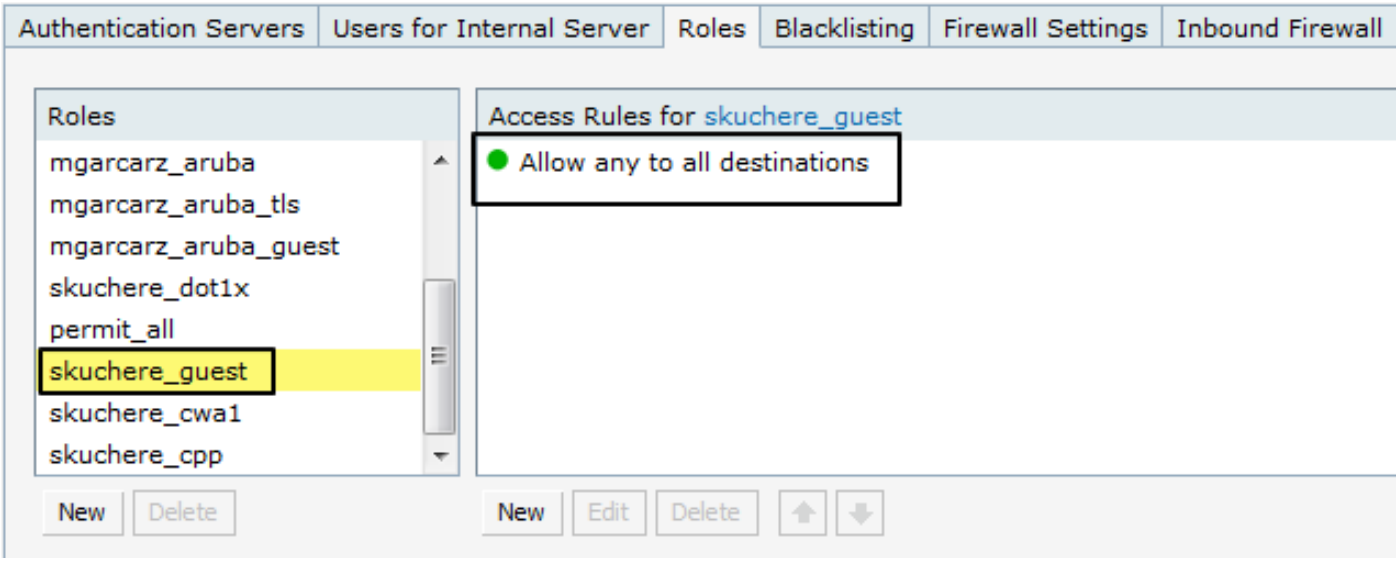
Note:您也许使用所有PSN服务器，但是用户应该总是重定向到MAB发生的服务器。通常您必须定义在SSID配置RADIUS服务器的FQDN。

步骤3.提供从ISE授权配置文件的重定向。您应该在端口号以后放置此处零件，

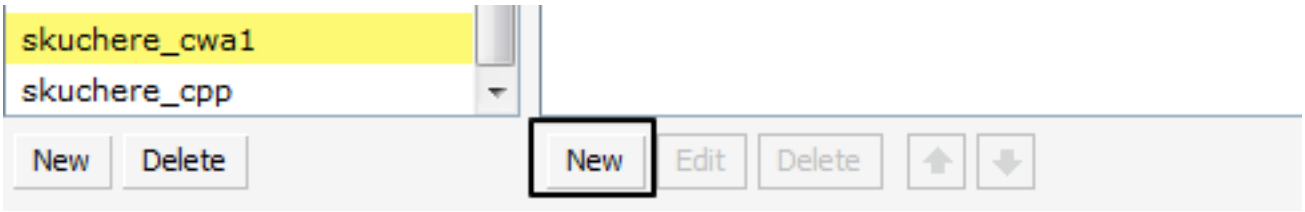
步骤4.定义ISE访客门户端口。

步骤7.配置用户角色。

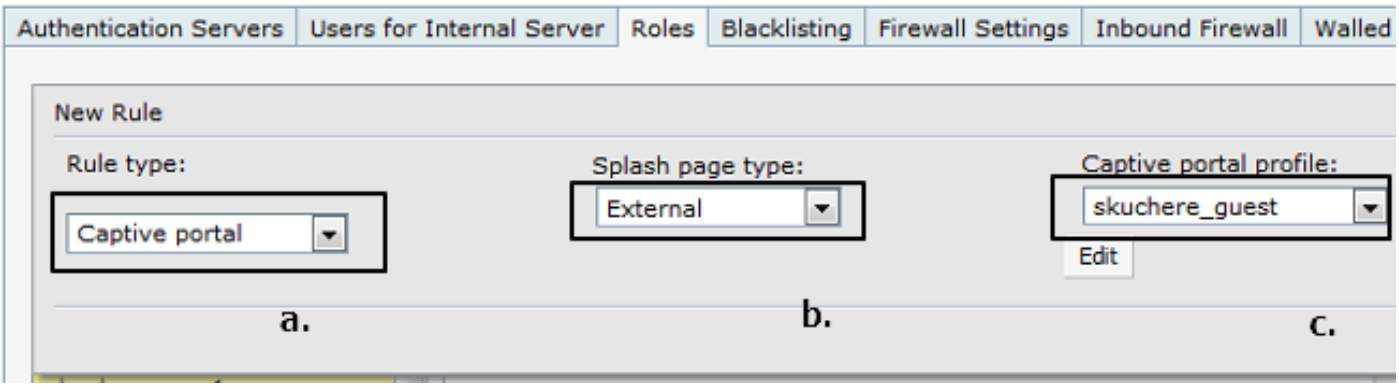
导航对**安全>角色。**保证，在SSID创建后，与同一名称的新角色是存在与访问规则permit的列表其中任一对所有目的地。另外，请创建两个角色：一CWA重定向的和其次在验证以后的permit访问的在访客门户。这些角色名称应该是相同的与定义的阿鲁巴作用在ISE授权配置文件。



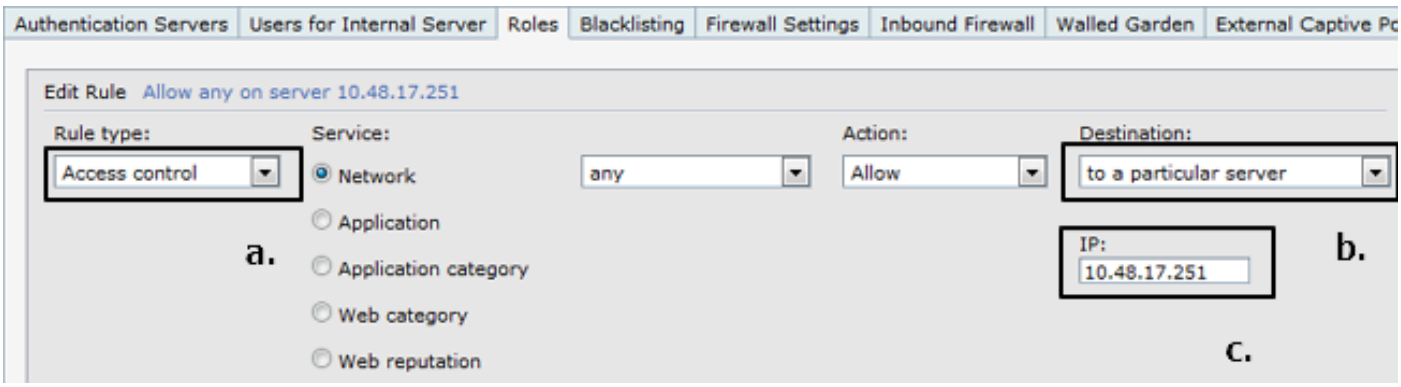
如镜像所显示，请创建重定向的新用户角色并且添加安全限制。



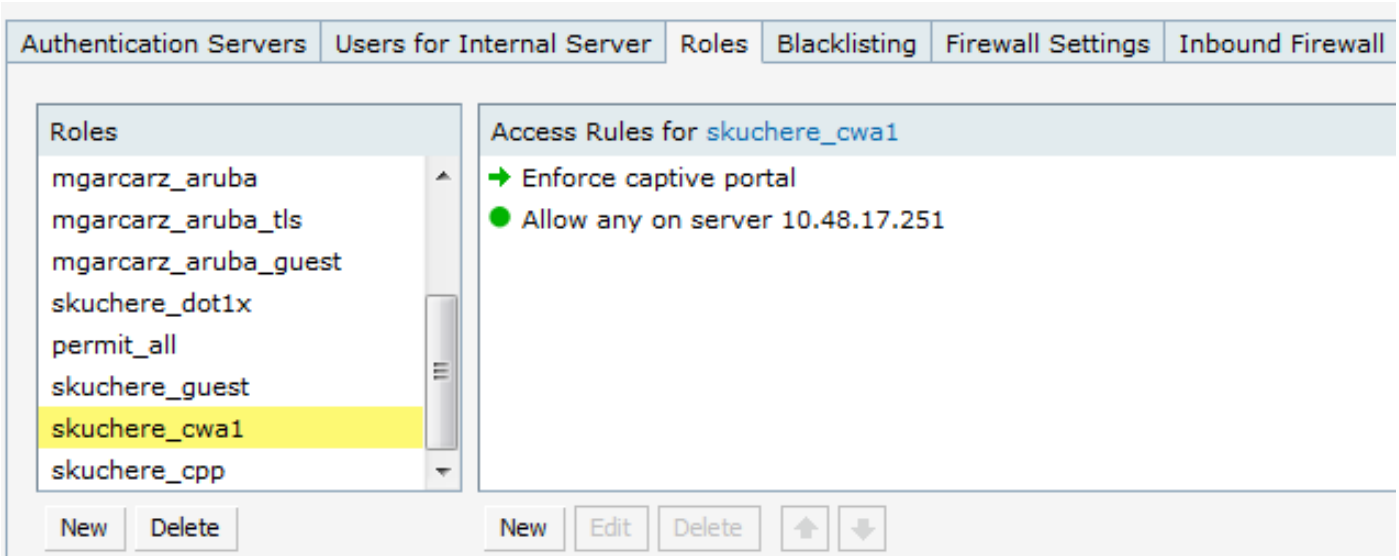
对于第一限制您需要定义：



对于第二限制您需要定义：

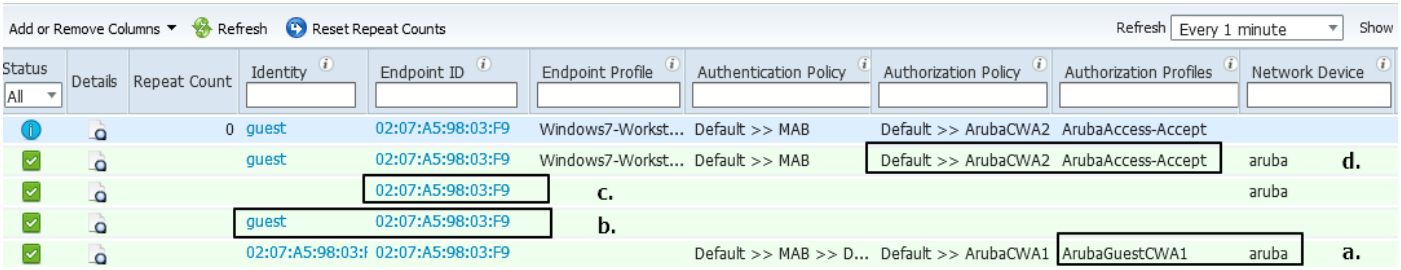


如镜像所显示，默认规则允许其中任一对所有目的地可以删除。这是角色一种概略的结果配置。



验证

访客流示例在ISE**操作> Radius Livelog的**。



1. 有在阿鲁巴侧配置的俘虏门户结果的第一个MAB和，一授权配置文件与CWA重定向和用户角色。
2. 访客验证。
3. 授权(CoA)的成功的崔凡吉莱。
4. 结果第二个MAB和一授权配置文件与有permit所有规则在阿鲁巴侧的permit访问和用户角色。

在阿鲁巴侧您能使用**显示客户端**命令保证用户连接由于验证， IP地址分配并且更正用户角色分配：

```
04:bd:88:c3:88:14# show clients

Client List
-----------
Name              IP Address    MAC Address        OS     Network        Access Point       Channel  Type  Role
----              ----------    -----------        --     -------        ------------       -------  ----  ----
02-07-A5-98-03-F9  10.62.148.77  02:07:a5:98:03:f9  Win 7  skuchere_guest  04:bd:88:c3:88:14  11       GN    skuchere_cwa1
Number of Clients   :1
Info timestamp      :92552
```

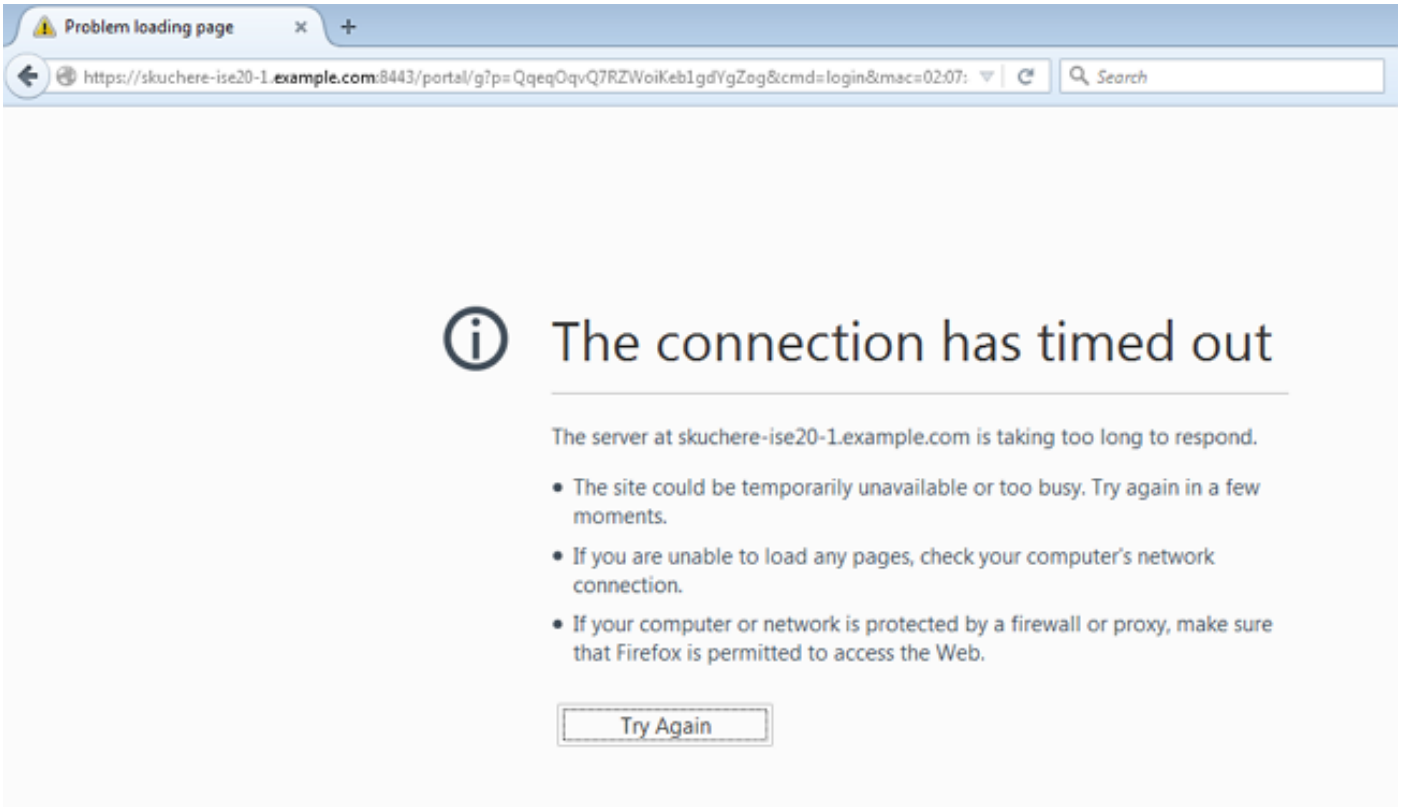
故障排除

失败的COA

在ISE设置，请保证阿鲁巴纳季配置与在ISE侧的正确网络设备设备类型，并且COA端口在纳季设置正确地定义。在阿鲁巴侧请保证RFC 3576在认证服务器设置启用，并且COA端口正确地定义。从网络的角度请检查UDP端口3799允许在ISE和阿鲁巴WLC之间。

重定向问题

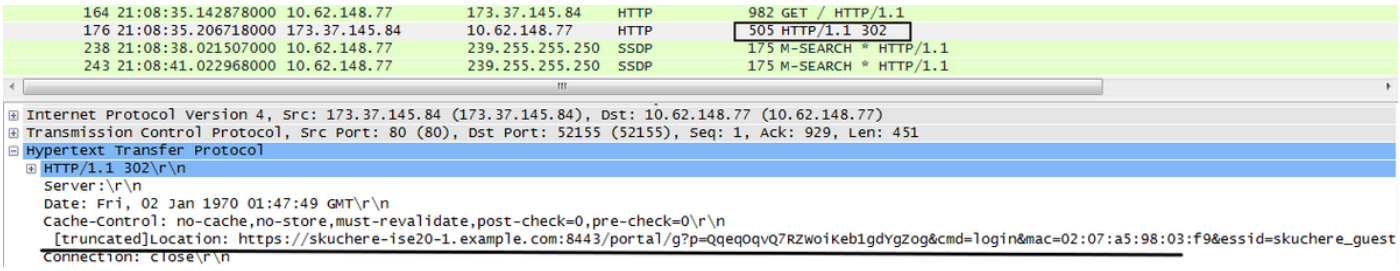
用户看到在浏览器的ISE URL如镜像所显示，但是ISE页没有显示， ：



在用户端请保证可以成功地解决ISE FQDN更正IP。在阿鲁巴旁边检查ISE URL在俘虏门户设置和流量正确地定义往在用户角色允许的ISE访问限制。并且请检查在SSID和ISE PSN的RADIUS服务器在俘虏门户设置是同一个设备。从网络的角度请检查TCP端口8443从用户分段允许到ISE。

在用户浏览器的没有重定向URL存在

在用户端，结果每个HTTP请求阿鲁巴WLC回归HTTP代码302页移动与ISE URL，请保证。



超时的会话缝的计时器

此问题典型症状是用户重定向在对访客门户的第二次。在这种情况下，在第二证书机构配置文件的COA与CWA再后，选择在ISE Radius Livelog您应该看到。在阿鲁巴侧，请检查实际用户角色在帮助下**显示客户端**命令。

此问题的一应急方案您可能使用终端在ISE的基于授权策略连接在成功的访客验证以后。