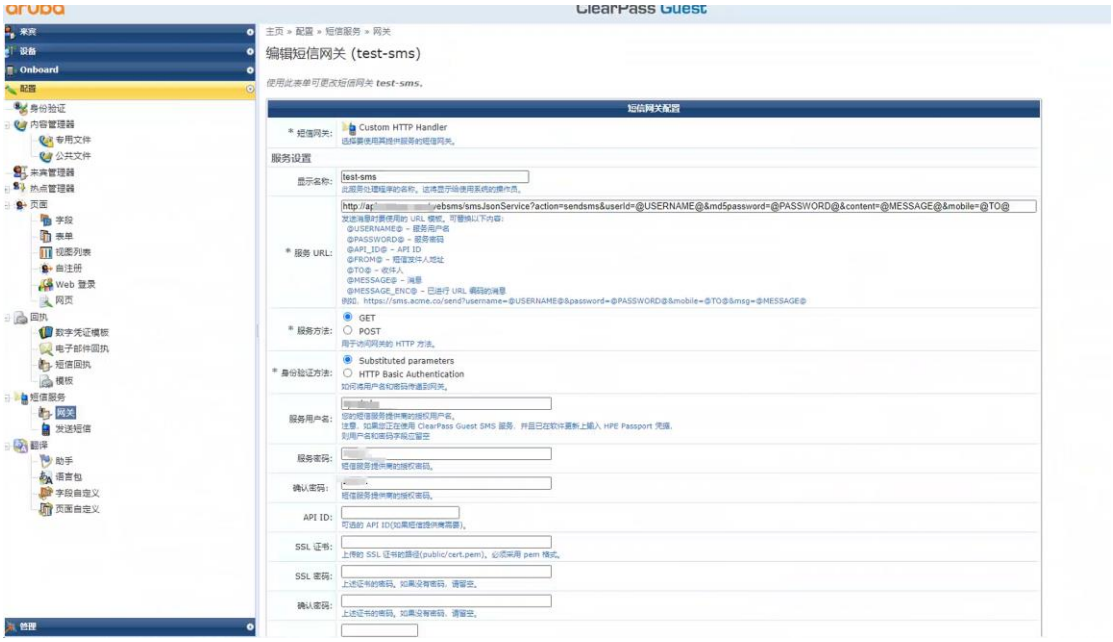
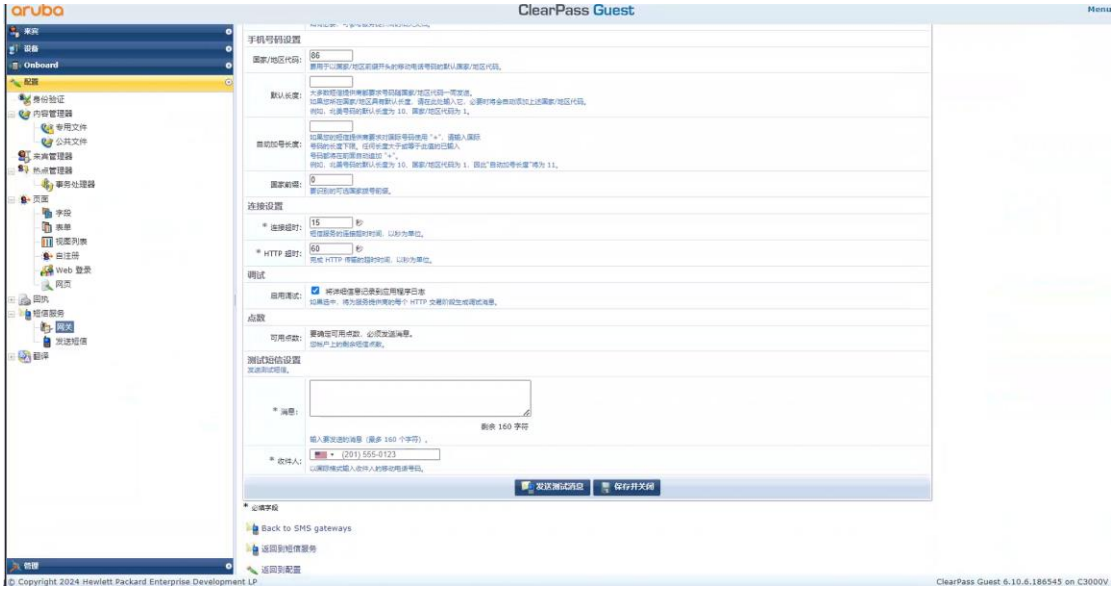
ClearPass MAC+Portal（短信）无感知认证新建流程

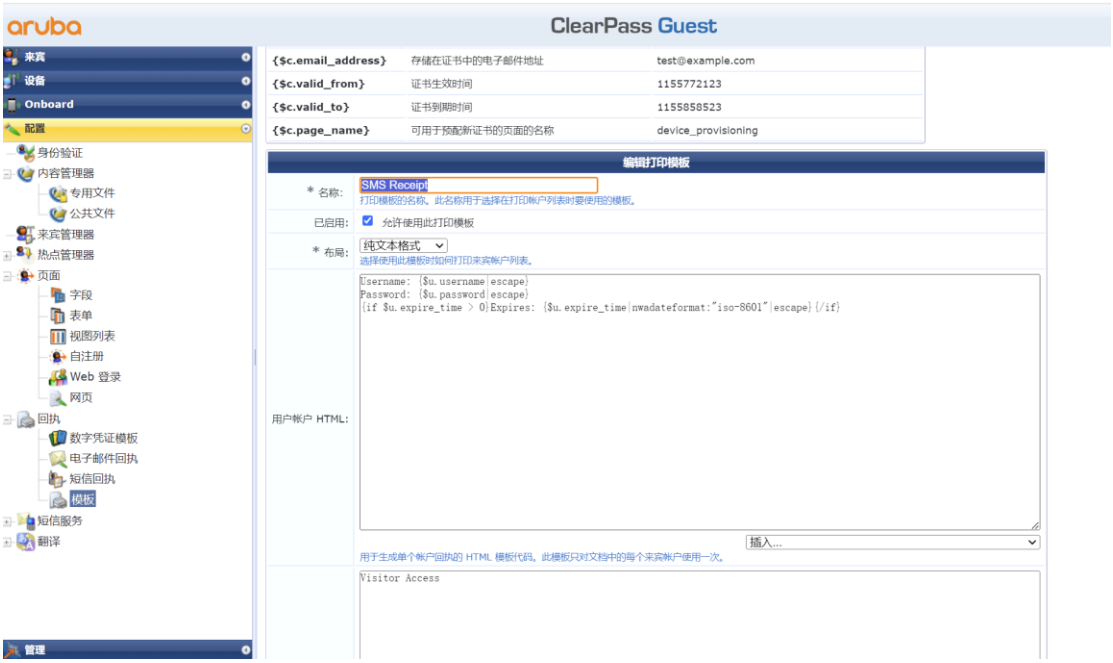
目录

1.配置短信网关

按照对应属性写入相关的 url 字段，使用 get 方式，填入可以正常对接网关的用户名和密码具体的短信格式可以在短信模板那边进行自定义。
也有可能因为短信的格式问题导致无法接收到短信，具体还请于短信网关的方的 SE 进行沟通。





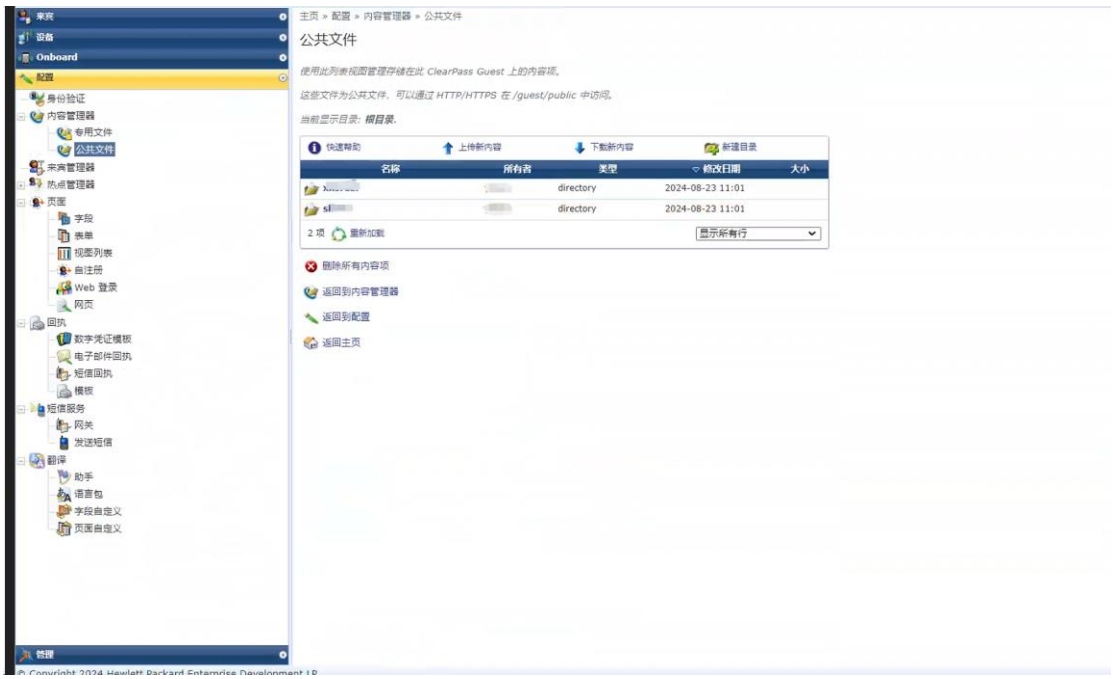


验证短信网关是否可以正常发送，点击发送短信，可以填写自己的手机号进行测试

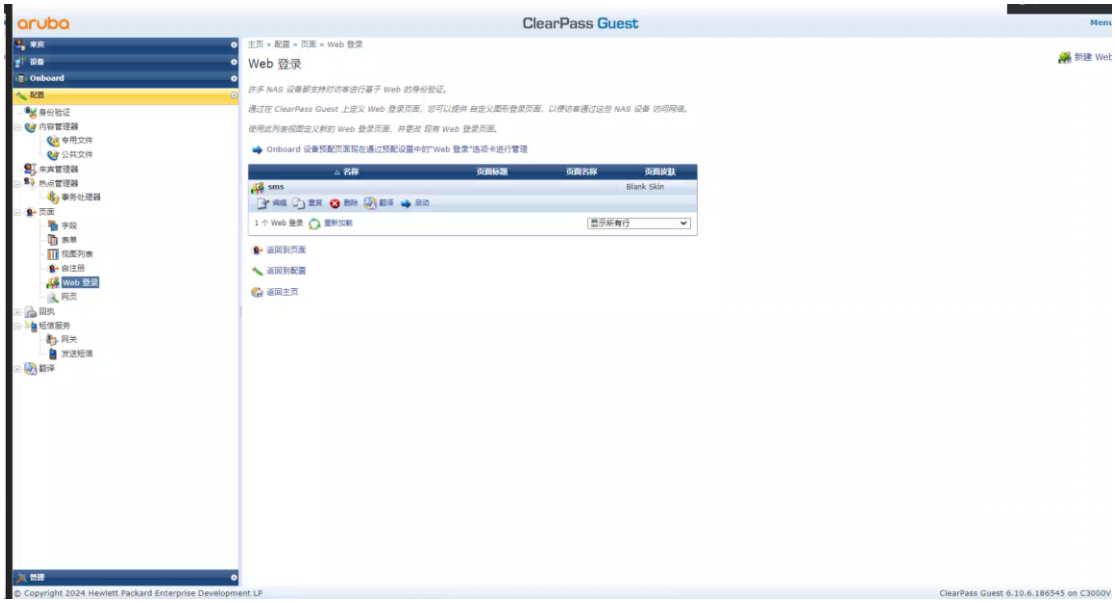
也可以使用 post 的方式，具体要看客户提供的短信网关对接方式

2.新建自注册

1. 上传公共文件，将页面需要的样式和图片上传（注意 6.11 版本的 ClearPass 无法建立文件夹，需要联系 tac 进入底层修复，此 bug 在 6.11.9 的版本中修复，若客户可以进行升级，还请升级到 6.11.9）



2.点击页面，选择 web 登录，选择右上角的新建 web 登录页



进入后，填写对应的页面名称，并将提供自定义表单勾选上

在“Web 登录”的页面编辑窗口，设置下面的参数：

✓ 名字 : self-registration-weblogin（自定义名称）

✓ 页面名称 :self-registration-weblogin（自定义名称，也就是页面 URL 的后缀）

✓ 自定义表单 :提供自定义登录表单 （勾选）

✓ 皮肤:Blank Skin

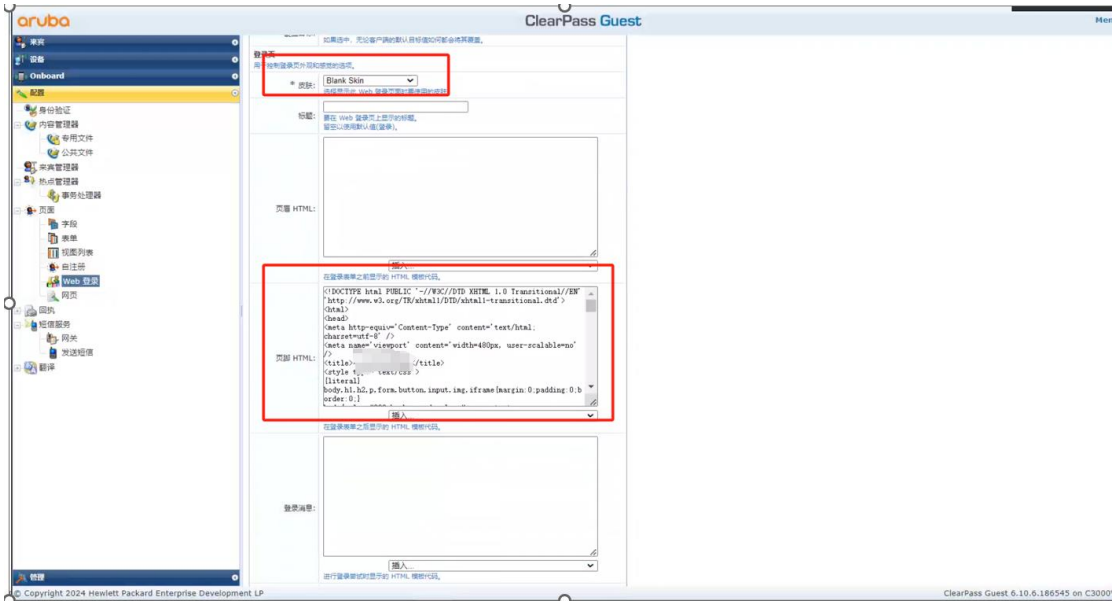
✓ 标题 :self-registration-weblogin

✓ HTML 页脚（实际是 Header HTML，翻译错误） ：将当前文本框中的内容删除掉，将准备好 html 页面贴入（可能由于书写格式的问题，会导致报错，若提示报错，可根据报错原因修改。）

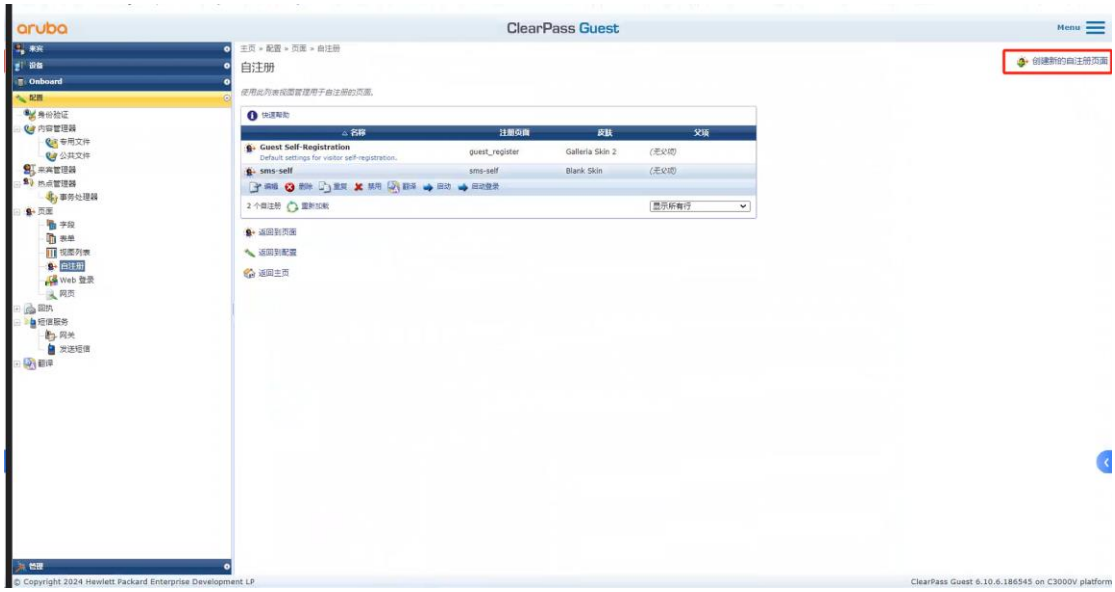
✓ HTML 页脚（实际是 Footer HTML） ：将当前文本框中的内容删除掉。

✓ 登陆消息：将当前文本框中的内容删除掉。

最后点击 保存更改 按钮



3.找到 配置 -> 页面-> 自助注册 ，点击右上角的“创建新的自助登记页面”。



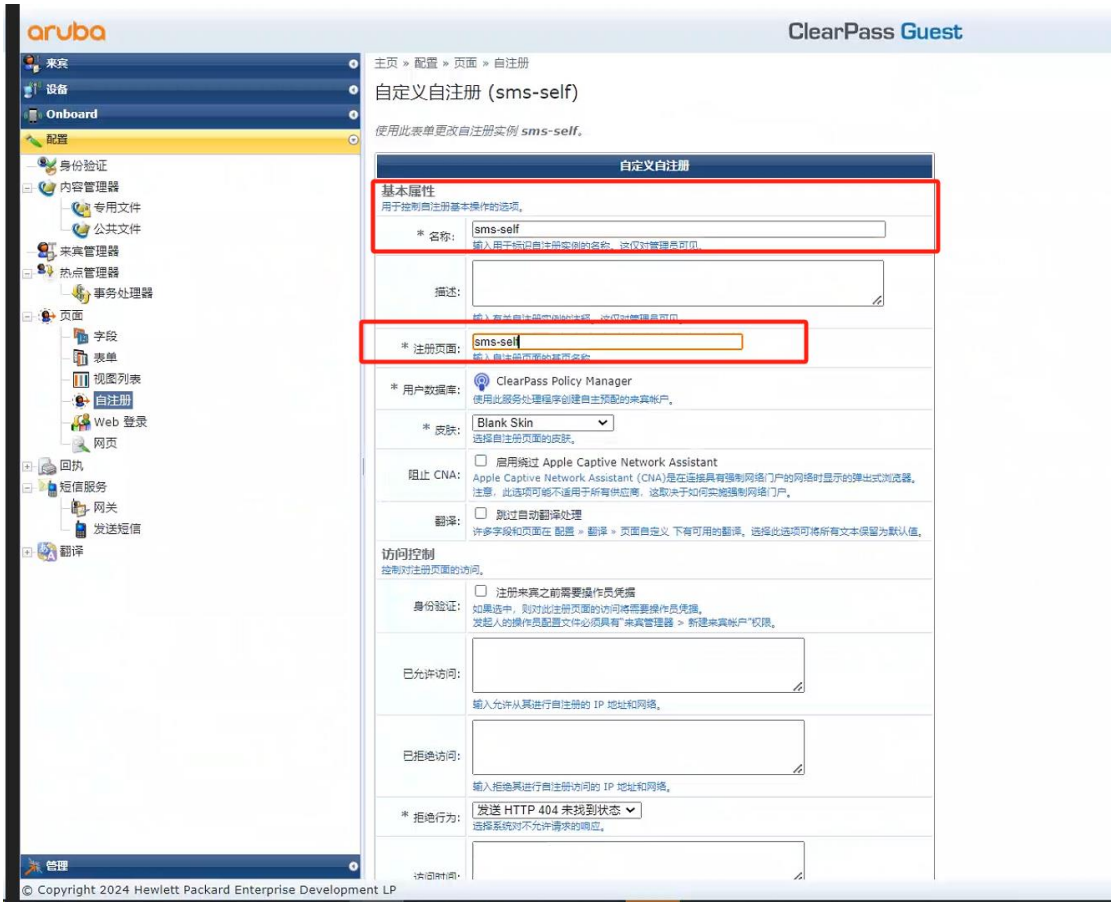
在“自助登记”的页面编辑窗口，设置下面的参数：

名字 :sms-self（自定义名称）

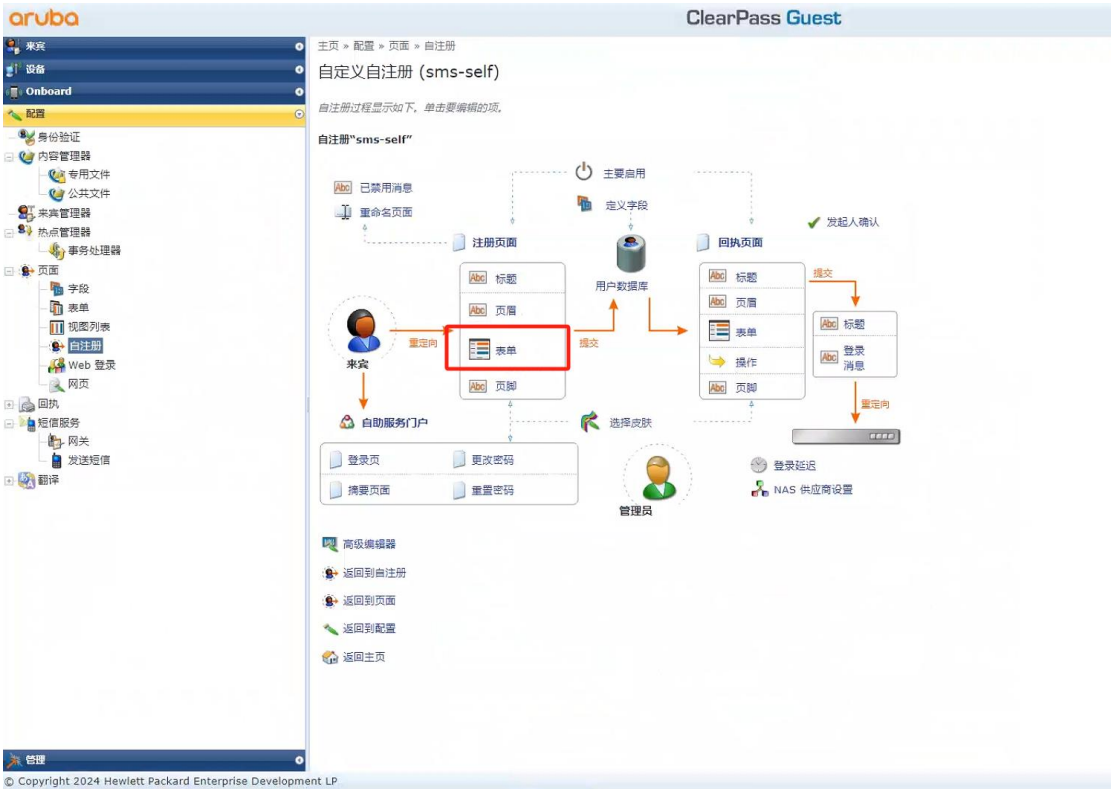
✓注册页面 ： sms-self（必须和 self_register.html 文件中的自助注册页面名称一致）

最后点击 保存更改 按钮

自定义注册的界面填写的的注册页面会去调用我们之前创建的 web login 的页面。

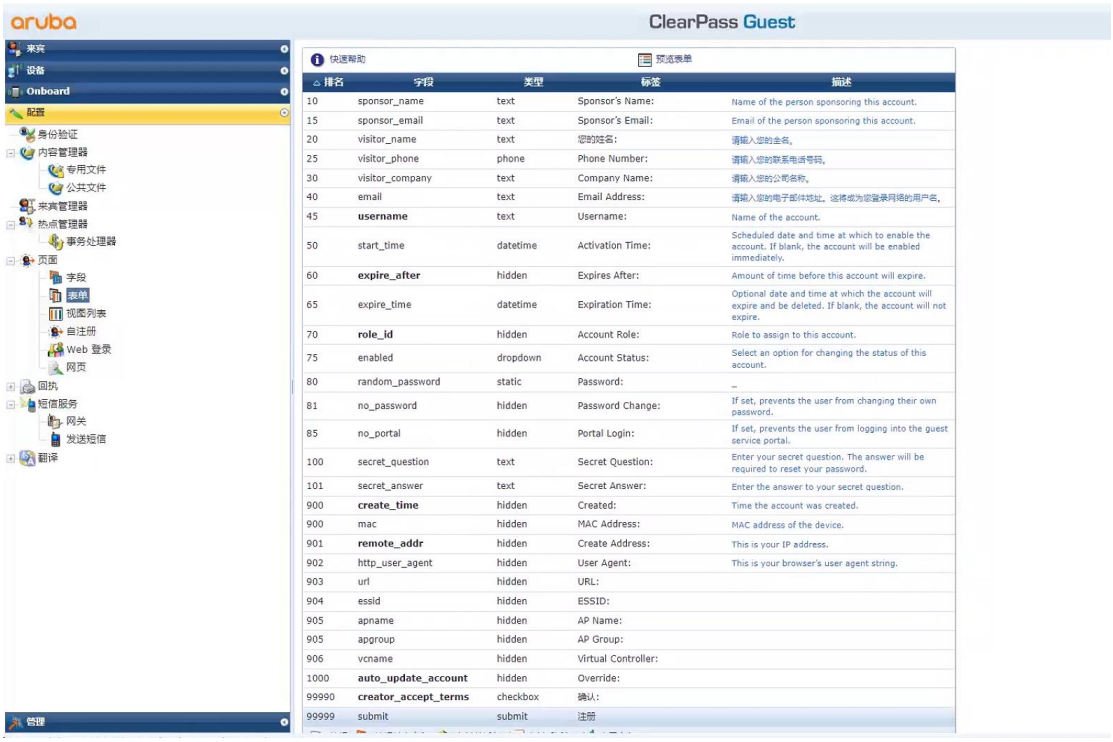


保存后，系统自定进入到该自助注册页面的编辑窗口，然后点击注册页面的 表单 按钮，进入到表单编辑界面。



在自助注册页面的"表单"编辑窗口，设置下面的参数:

✓ visitor_name：禁用该默认字段
✓ email ： 禁用该默认字段
✓ username：在 sponsor_name 后 插入 username 字段



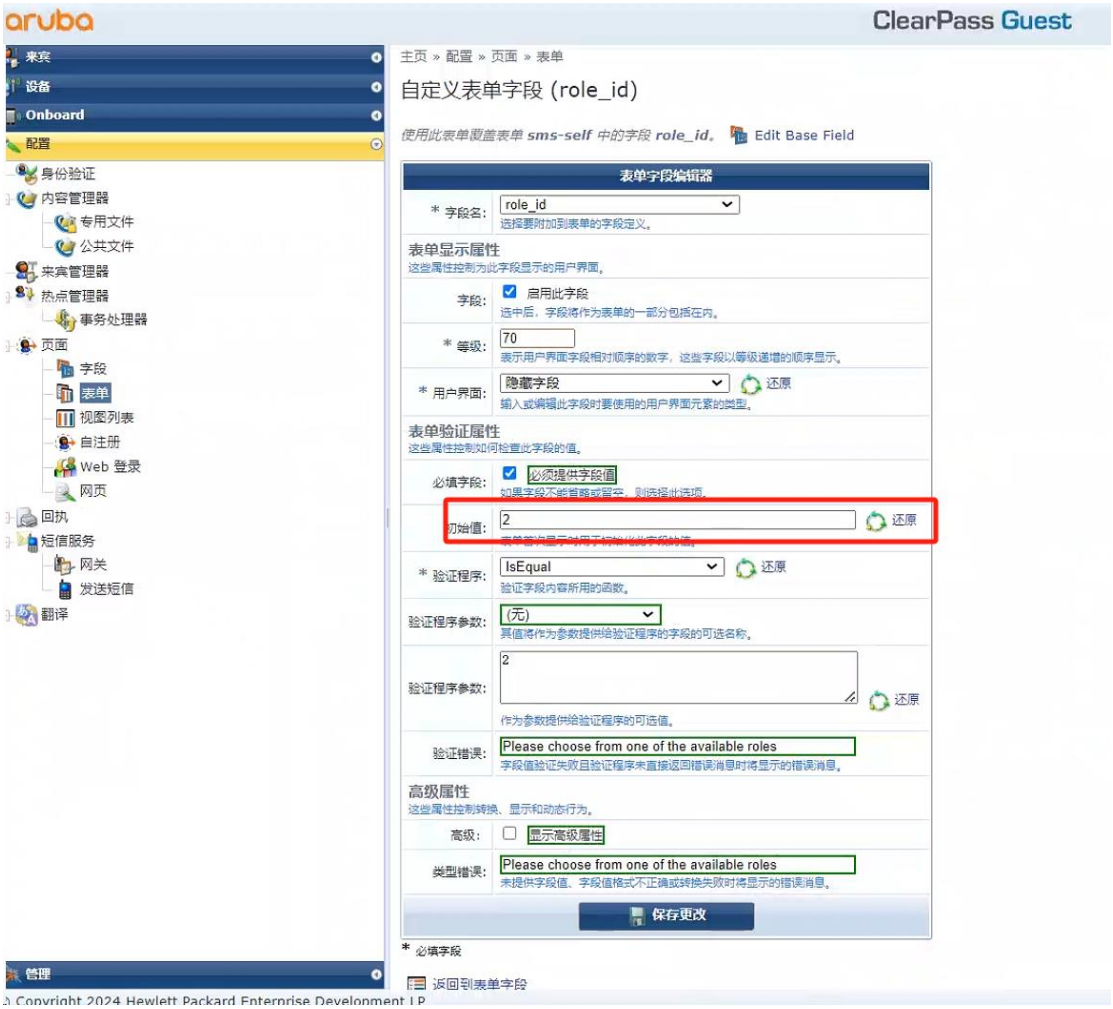
排名	字段	类型	标签	描述
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.
20	visitor_name	text	您的姓名:	请输入您的全名。
25	visitor_phone	phone	Phone Number:	请输入您的联系电话号码。
30	visitor_company	text	Company Name:	请输入您的公司名称。
40	email	text	Email Address:	请输入您的电子邮件地址。这将成为您登录网络的用户名。
45	**username**	text	Username:	Name of the account.
50	start_time	datetime	Activation Time:	Scheduled date and time at which to enable the account. If blank, the account will be enabled immediately.
60	**expire_after**	hidden	Expires After:	Amount of time before this account will expire.
65	expire_time	datetime	Expiration Time:	Optional date and time at which the account will expire and be deleted. If blank, the account will not expire.
70	**role_id**	hidden	Account Role:	Role to assign to this account.
75	enabled	dropdown	Account Status:	Select an option for changing the status of this account.
80	random_password	static	Password:	–
81	no_password	hidden	Password Change:	If set, prevents the user from changing their own password.
85	no_portal	hidden	Portal Login:	If set, prevents the user from logging into the guest service portal.
100	secret_question	text	Secret Question:	Enter your secret question. The answer will be required to reset your password.
101	secret_answer	text	Secret Answer:	Enter the answer to your secret question.
900	**create_time**	hidden	Created:	Time the account was created.
900	mac	hidden	MAC Address:	MAC address of the device.
901	**remote_addr**	hidden	Create Address:	This is your IP address.
902	http_user_agent	hidden	User Agent:	This is your browser's user agent string.
903	url	hidden	URL:	
904	essid	hidden	ESSID:	
905	apname	hidden	AP Name:	
905	apgroup	hidden	AP Group:	
906	vcname	hidden	Virtual Controller:	
1000	**auto_update_account**	hidden	Override:	
99990	**creator_accept_terms**	checkbox	确认:	
99999	submit	submit	注册	

我们此时回到 配置 -> 页面->Web 登录 ,鼠标点击下“self-registration-weblogin”页面名称， 下方会出现隐藏菜单，接着点击下 启动按钮，在新的页面会打开您创建好的自定义页面（具体出现的页面因人而异）

可以看到页面代码中字段的默认值，需要和 CPPM 中的字段值保持一致。

```
<body>
<div class='i-main'>
    <div class='i-fill'></div>
    <div class='i-wrap'>
        <div class='i-login'>
            <form method='post' action='http://10.23.188.51/guest/sms-self.php? browser=1' name='getPass' target='j'>
                <input type='hidden' name='expire_after' value='2' />
                <input type='hidden' name='role_id' value='2' />
                <input type='hidden' name='auto_update_account' value='1' />
                <input type='hidden' name='country' value='1' />
                <input type='hidden' name='create_time' value='' />
                <input type='hidden' name='remote_addr' value='' />
                <input type='hidden' name='creator_accept_terms' value='1' />
                <div class='i-hided'><input type='checkbox' id='declaration' onclick='return agree();'/></div>
                <p class='i-agree'><img id='checkPic' src='public/general/blank.gif' class='i-ck0' onclick='return agree();' /><label for='declaration'> 我已阅读并同意免责声明</label>
</p>
                <select>
                    <option value="CN"> 86</option>
                    <option value="US">1</option>
                    <option value="UK">2</option>
                </select>
                <p class='i-line'>
```

Tips：在测试中，我发现表单这边如果使用 https 就没办法传参，后续我改成 http 才正常。



将代码中表单字段的属性的 value 值设定为和 CPPM 上初始值一致。来实现代码和表单的对应关系，保证在页面输入手机号码之后，CPPM 来宾页面能够看到此手机号的记录，以完成正常的接入流程。

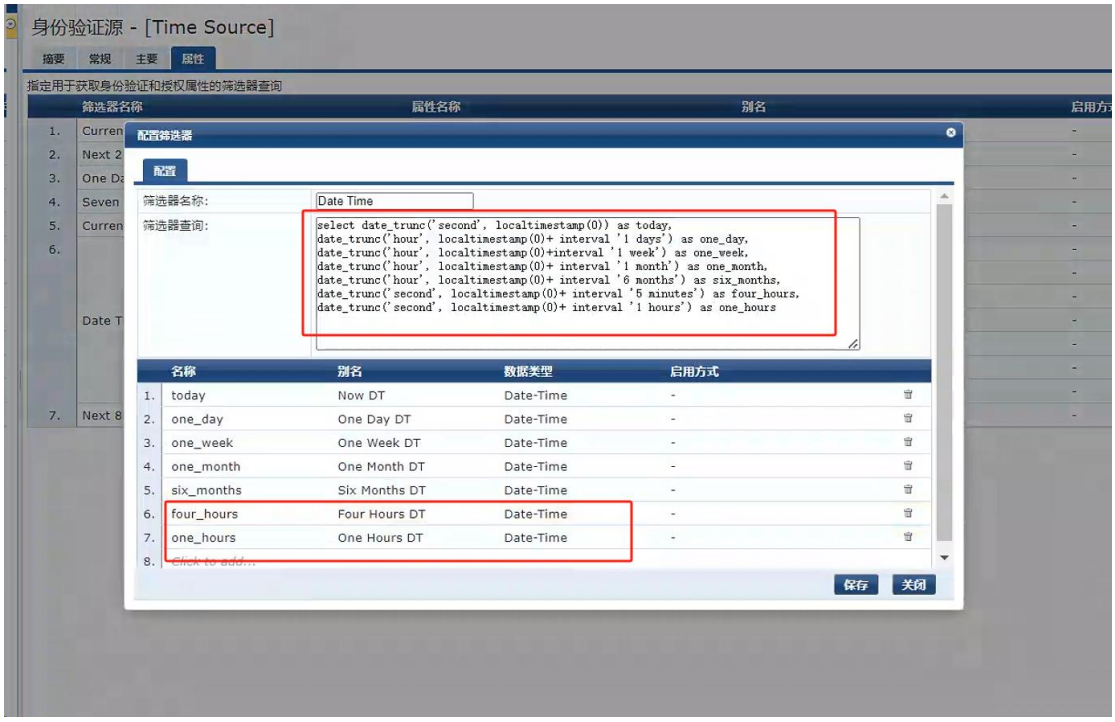
完成上述创建之后，点击页面选择自注册，选择之前创建的服务，点击启动登录，完成流程后，可以在来宾选择中的管理账户看见我们刚才创建的账户，若能看见代表传参成功。

在控制器上完成 portal 认证的 SSID 的创建，并将之前我们页面中的 url 贴到 MD L3 配置中

的 login page 中
Tips：若客户需要支持切换区号，可以给国外的手机号发送短信
1. 需要支持国外手机号的短信网关
2. 在传参时，需要将区号一起传给 clearpass 由 clearpass 发给短信网关
可以在代码表单中新建一个字段，这个字段会把手机号和区号合并之后一起传给 clearpass。之后在短信回执的界面将字段选择为之前新建的字段，由这个字段去发送短信！这个就可以实现区号的选择了

3.ClearPass 服务配置

本次认证服务配置会使用到 ClearPass 本地的 time source 认证源
可以根据需求去修改 MAC 认证的时效性
Tips:需要注意的是查询语句中默认的取值是 hour 是取整的，若需要精确到分钟和秒需要将单位修改
注意：在 clearpass6.11.1 和 6.11.3 的版本中修改语句会导致 time source 的数据库名称和端口号改变，在 6.10 版本中 time source 的数据库名称和端口号为 insightDB 和 5432，在 6.11 版本中改为 insightDB 和 5433。6.11 版本对外开放的数据库没有 tipsDB 了。



◆ ClearPass 配置一个 MAC Caching 认证服务，用来匹配 portal 认证请求，并更新 Endpoint 数据库

新增一个强制配置文件，将认证后的用户信息更新到 Endpoint 数据库中

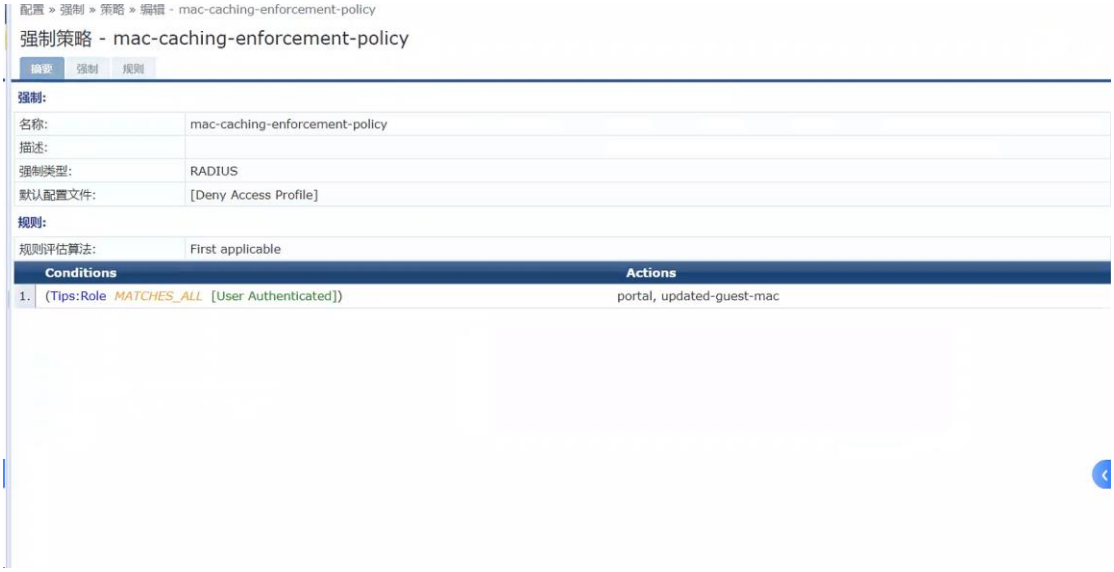
取名：updated-guest-mac

新增一个强制配置文件

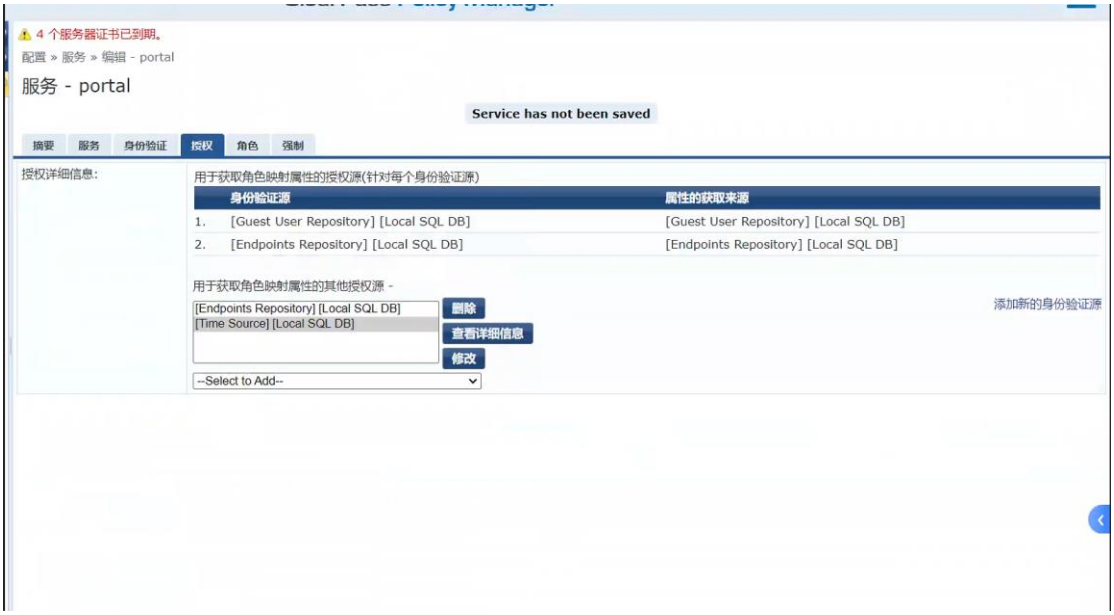
取名：portal

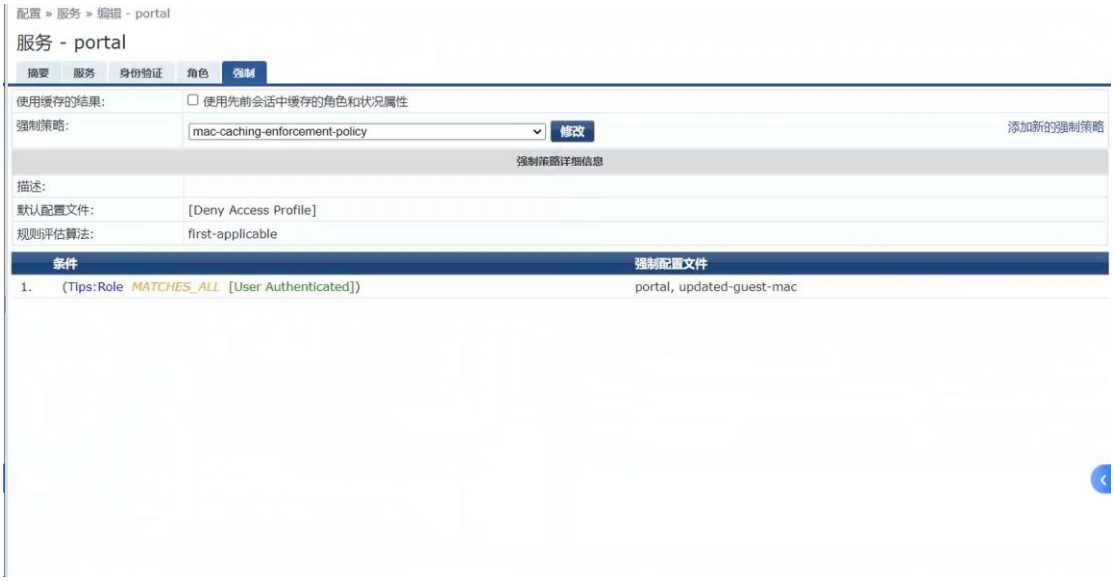
新增一个策略文件

将上诉新建的两个强制文件调用到这个策略文件中



新建服务





◆ ClearPass 配置一个 MAC 认证服务，用来匹配 mac 认证请求，利用 MAC caching 认证阶段更新的
Endpoint 数据库进行无感知认证，并返回缓存的用户名
新增一个配置文件
Mac 认证阶段给控制器返回 portal 认证阶段的用户名


强制配置文件 - return-username

摘要 配置文件 属性

配置文件:

名称:	return-username
描述:	
类型:	RADIUS
操作:	Accept
设备组列表:	-

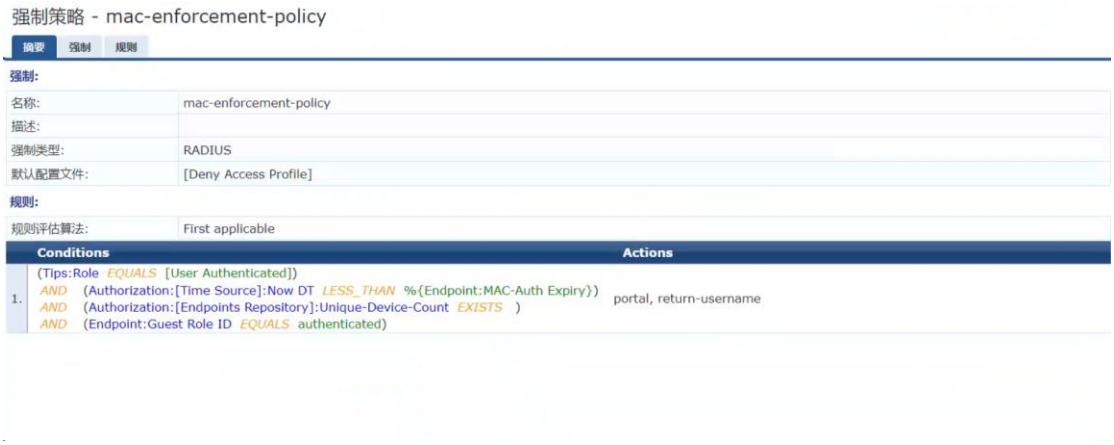
属性:

	类型	名称		值
1.	Radius:IETF	User-Name	=	%{Endpoint:Username}

新增一个强制策略

将之前新增的配置文件添加到这个强制策略中

注意: 这个地方的 portal 的配置文件中的 user-role 可以与 portal 的不一致, 但是需要和 mm 上的 mac 认证的 role 保持一致，由于我现在是两边保持一致，所有可以调用同一个配置文件


强制策略 - mac-enforcement-policy

摘要 强制 规则

强制:

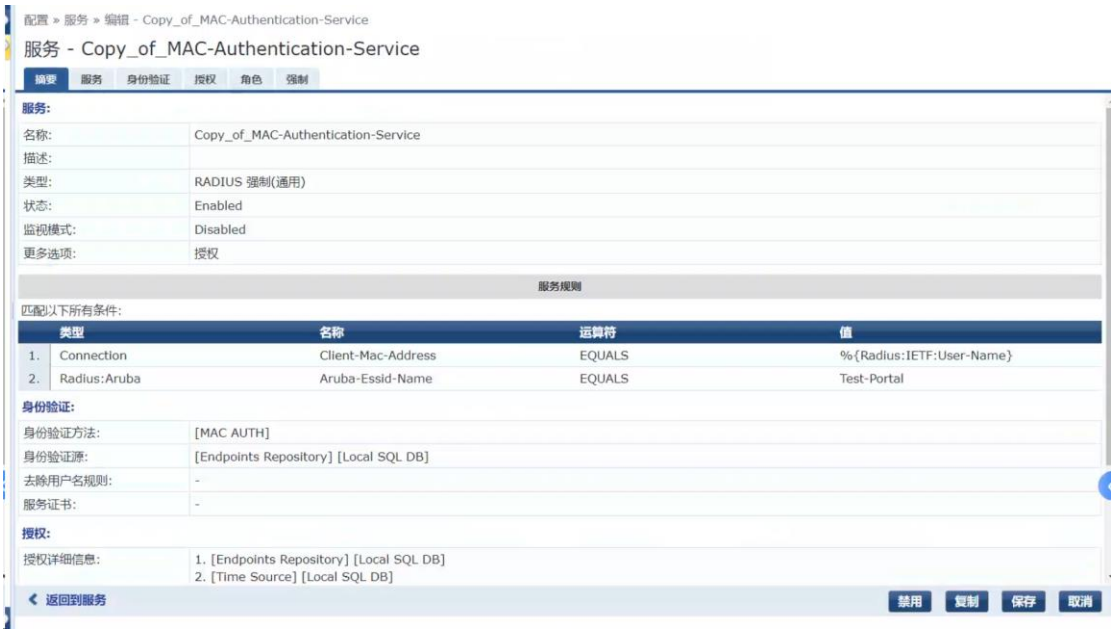
名称:	mac-enforcement-policy
描述:	
强制类型:	RADIUS
默认配置文件:	[Deny Access Profile]

规则:

规则评估算法:	First applicable

	Conditions	Actions
1.	(Tips:Role *EQUALS* [User Authenticated]) *AND* (Authorization:[Time Source]:Now DT *LESS_THAN* %{Endpoint:MAC-Auth Expiry}) *AND* (Authorization:[Endpoints Repository]:Unique-Device-Count *EXISTS*) *AND* (Endpoint:Guest Role ID *EQUALS* authenticated)	portal, return-username

新增一个服务


配置 » 服务 » 编辑 - Copy_of_MAC-Authentication-Service

服务 - Copy_of_MAC-Authentication-Service

摘要 服务 身份验证 授权 角色 强制

服务:

名称:	Copy_of_MAC-Authentication-Service
描述:	
类型:	RADIUS 强制(通用)
状态:	Enabled
监视模式:	Disabled
更多选项:	授权

服务规则

匹配以下所有条件:

	类型	名称	运算符	值
1.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
2.	Radius:Aruba	Aruba-Essid-Name	EQUALS	Test-Portal

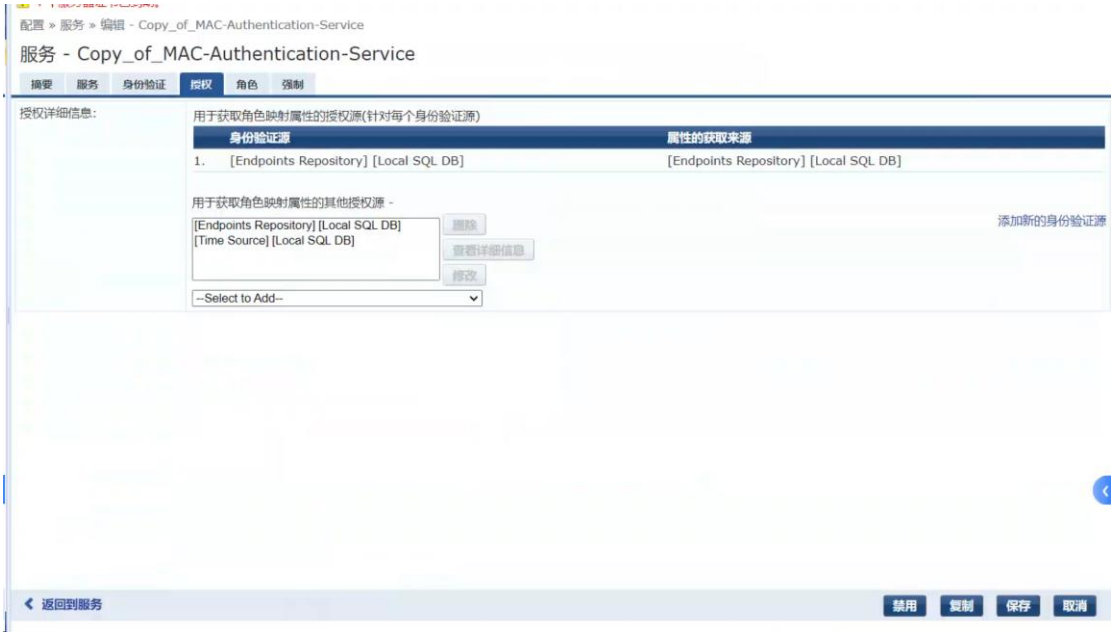
身份验证:

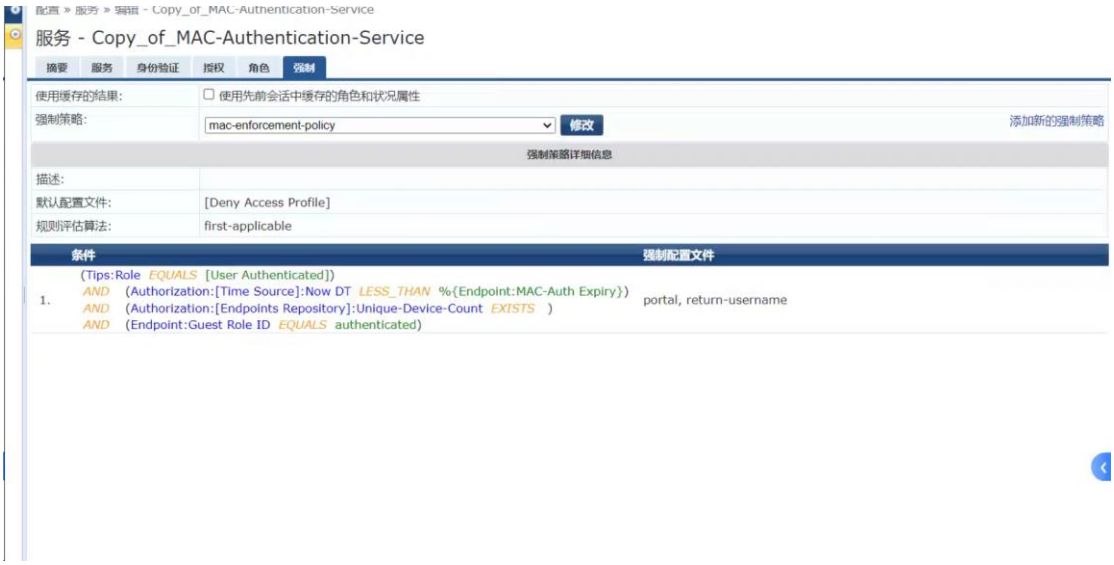
身份验证方法:	[MAC AUTH]
身份验证源:	[Endpoints Repository] [Local SQL DB]
去除用户名规则:	-
服务证书:	-

授权:

授权详细信息:	1. [Endpoints Repository] [Local SQL DB] 2. [Time Source] [Local SQL DB]

返回到服务 禁用 复制 保存 取消





正常完成流程

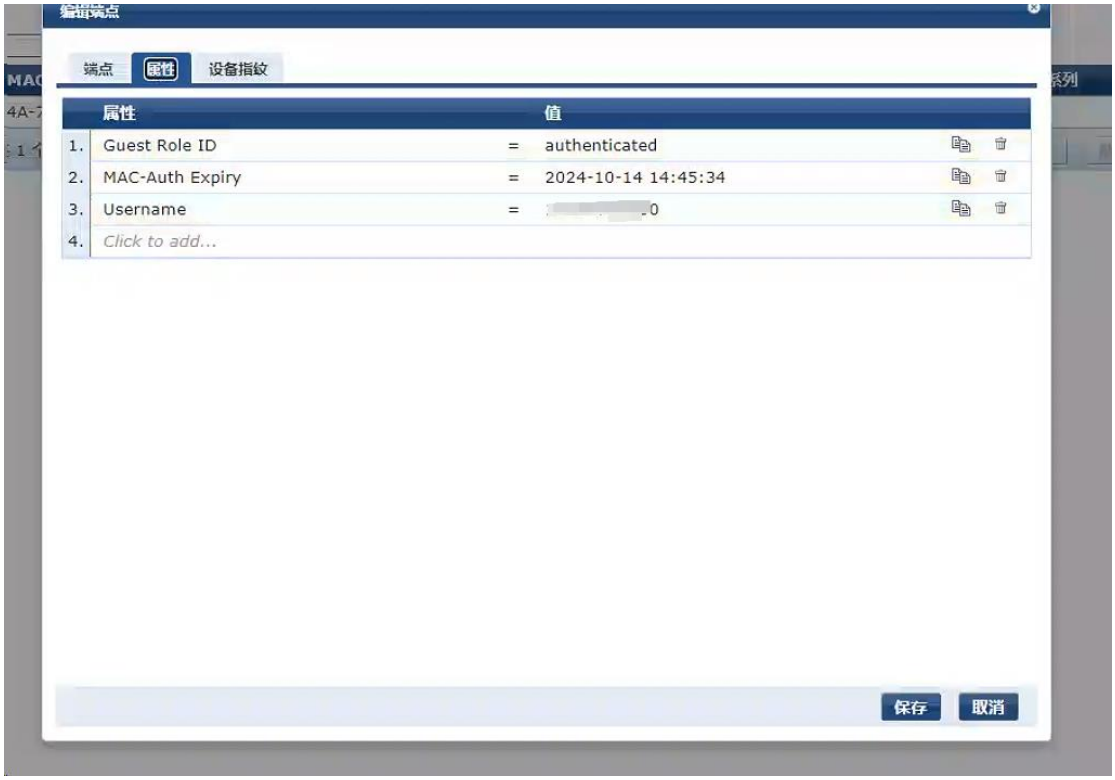
可以看到 ClearPass 上呈现这三次认证的记录

第一次为 mac 认证，由于此时用户终端的 mac 并未进入到 endpoint 数据库中，所以认证失败

第二次则是 portal 认证，正常完成流程后，会将用户终端的 mac 地址更新到数据库中，并且携带我们上诉服务所设置的到期时间和创建时间。

第三次还是 mac 认证，我们将用户踢下线或者用户断开重新连接，不会触发 portal 认证，直接走 mac 完成认证。

Tips:完成 portal 认证后，可以查看终端的端点属性，正常是会携带下面三种属性的。



Tips:

若 CPPM 较多，建议使用域名的方式进行认证，需要去申请公签证书，分别在 CPPM 和控制器上进行导入。

若重定向的 url 包含域名，需要 MD 上配置 DNS 可以去解析这个域名，且 url 需要使用 https。