ClearPass MAC+Portal (短信) 无 感知认证新建流程

目录

1.配置短信网关	3
2.新建自注册	4
3.ClearPass 服务配置	10

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。

aruba	LiearPass Guest							
• 来宾	 主页 > 配圖 > 短信服务 > 网关 							
1 26	编辑符(G网关 (test-sms)							
Onboard								
- 配置	● 使用就表单可更充短信码关 test-sms,							
● 身份验证	海南國大都國							
🗉 🥶 内容管理器	* Alexandre backston HTTP Handler							
100 专用文件	「知識内不」。这樣要使用其透射最多的地域同共。							
	服务设置							
	显示名称: 但est-sms 是影响我的问题。这些思示这种自己的问题。							
- 9- 页面	http://ar' /ebsms/sms.JsonService?action=sendsms&userid=@USERNAME@&md5password=@PASSWORD@&content=@MESS.	AGE@&mobile=@TO@						
· · · · · · · · · · · · · · · · · · ·	対地議員が費用用のしたに構成、可能強い下方容: のUSERNAMEの一般を発売中名							
一 前 表単	epessworeDa - 服务条码 使用 Data - 如务条例							
	一般時以には、金融の時に、一般的な年代の時代							
K Web 登录	enessadee - we							
网页	WHICSSHUE_LINU字 - CUETY ONE WERE/NWF UNDERNAME@&password=@PASSWORD@&mobile=@TO@&msg=@MESSAGE@ 男怒記、HUBs://wmi.acme.co/senfluyemame=@USERNAME@&password=@PASSWORD@&mobile=@TO@&msg=@MESSAGE@							
	e GET							
 ・ ・ ・	■ 2005万元: ○ POST 用于1005月3月20日 月1日7日2月3日 日日1日2日2日 日日1日1日1日1日 日日1日1日1日1日1日1日1日1日							
一般、短信回説	Substituted parameters							
國 模板	* 最份報送汚法: 〇 HTTP Basic Authentication 助何序用户名印密语传递影问先。							
1 通短信服务								
 ·	服務用户者: SDI短信服务提供用的股份用户名。 住意,如果您在使用(DearPass Guest SMS 服务、件目已在的注意新上版入 HPE Passoont 等级。							
のため	则用户省和运动字段宣誓至							
一秒助手	服务者得: 据在思想供一篇phill的方案码							
ある語言包								
· 李段自定义	·····································							
- (1) 负重目定义	API ID: TTORe API ID(STERIOR ID)							
	Product of a second sec							
	aps. 证书: 上傳的 SSL 证书的描述(public/cert.pem), 必须希用 pem 稿式。							
	SSL 應時: 计可示例用语言 如果你想像话,请提本							
	1801 (1977) -							
ALC: NOTE	上述过来的电码、如果没有电码、调量型、							
A DIR								
aruba	ClearPass Guest	Men						
👷 来宾	O ANNELSE - SPECIAL INCLUSE							
el un	→ 非机带钥边置 ● ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■							
(Onboard	■ 國家/地区代码: 圖用于山原的/地区和國外外的市场成等點的對人面影/地区代码。							
▲ 股票								
· · · · · · · · · · · · · · · · · · ·	MAN REAL 这些学校的实现和这些具有的人生活,就在此处地入了。这种时候会由创发过去还要做"地区"代码。 例如,当得可考虑的优化学生为,这是我们还可能开入。							
2010年月文件								
2 公共文件	無助如果決測。 時間的如果決測。 時間的如果比較。 時間的一個計算。 一個一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一							
2013 未再管理器 2013 \$1 秋点世界器	等于部本中本部建造社组织14-1-4-5-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6							
· (4) 事务处理器								
 会 页面 () 一页面 	连接设置							
表单	* 連接通行: 15 助							
- 111 視壓列表	Buryon star. 60 0							
- 19+ 白注映 - 2004 Web 登录	用いた 2023 現在 HTTP 存在的間分気化、以此力単位。							
风风页	4月25 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)							
	展用電気は 均単日本、将力振発性の取り着くHTTP交通的設定或環境改良。							
1 1日 2日 20 日 20 日 20 日 20 日 20 日 20 日 20	点散							
● 波送短信	可用伝数: 長确定可用元数: 公规定通用用。 因为用上的制杂低度考虑。							
	测试运行设置							
-								
	* 洞思:							
	输入要求进的消息(最多 160 个字符)。							
	* 684A: • (201) 555-0123							
	* 20100 2010							
	and a section of gateways							
a este								
Copyright 2024 Hewlett Packard Enterpris	e Development LP	ClearPass Guest 6.10.6.186545 on C3000V						

aruba			Clear	Pass G	uest		
🕴 来宾 🛛 🛛 🛛 🖉	{\$c.email_addr	ess}	存储在证书中的电子邮件地址	tes	t@example.com		
11 设备 🔹 💿	{\$c.valid_from}	}	证书生效时间 1155772123				
Onboard O	{\$c.valid_to}		证书到期时间 1155858523				
🔪 配置 💿	{\$c.page_name	•}	可用于预配新证书的页面的名称	dev	vice_provisioning		
▶ 身份验证				编辑打印机	製板		
🥶 内容管理器		SMS Re	ceipt	4941443 3 - 1 - 1			
- 0 # 充作	* 名称:	打印模板的	名称。此名称用于选择在JT印帐户列表时要使用	的模板。			
	已启用:	允许	使用此打印模板				
■ 未兵官理器 ■ 热点管理器	* 布局:	纯文本格 选择使用此	弐 ~ 横板时如何打印来宾帐户列表。				
 ○ (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	用户帐户 HTML:	Username Password {if \$u.e 用于生成单 Visitor	: (Su username descape) : (Su password escape) xpire_time > 0)Expires: (Su expire /\%7~MENAMO HTML MEETCES, #UMEETCES Access	time nwadate	format:"iso-8601" escape}{//if) F@明一次。		

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)

19. 来安	 主页 » 配置 » 内容管理器 	。公共文件			
1 88	• 公共文件				
Cnboard	0				
▲ 配置	● 使用此列表视問管理存储在	比 ClearPass Guest 上的内	皇项。		
- 😼 身份验证	这些文件为公共文件,可以	通过 HTTP/HTTPS 在 /gues	t/public 中访问。		
 ・ ・	当前显示目录: 枳目录 .				
() 公共文件	① 快速期前	★ 上後新内容	👃 下氢新内容	() 新建目录	
8 未完管理器	名称	所有者	美型	▽ 修改日期	大小
▲ 热点管理器	Same and	5	directory	2024-08-23 11:01	
● 页面	📦 sl	1000	directory	2024-08-23 11:01	
- 10 表单	2 项 💭 重新加载			显示所有行	~
- III 视图列表 	😵 删除所有内容项				
Web 登录	0 运回到内容管理器				
网页					
- 🚵 回执	· 返回到配置				
● 数字先证模板 ● 由子配供同物	🚱 返回主页				
1 短信回执					
() 横板					
1 2 1 短信服务					
四天 四					
● 翻译					
助手					
ある语言包					
学校自定义					
All XHEREY					
No. AND					
A 94					

2.点击页面,选择 web 登录,选择右上角的新建 web 登录页

an the		Clear Daga Crust	
aroba		LiearPass Guest	
-, *A •	主页 > 配置 > 页图 > Web 登录		
	Web 登录		
I Onesare 6	许多 NAS 设备都支持对访客进行基于 Web 的身份验证。		
Colors	通过在 ClearPass Guest 上定义 Web 登录页面,彩可以	《提供 自定义图形登录页面,以便访客通过这些 NAS à	设备 访问网络。
	使用此列麦视图完义新的 Web 登录页面,并更改 现有 W	eb 登录页面.	
全部 专用文件	→ Onboard 设备标题页原理方通过模型设置由的"Web	新帝小王派上出行管理	
○ 公共文件		JALAN ALIYA PALITI BAR	
- 20) 米丹市理由 - ²	△ 名称	页曲标题 页曲名称	负目放扶 nk Skin
(4)事务处理器		Dig	INK SKIN
□-\$-页面		用品红妆店	
· 19 字段 [19 本例	A THE TR	22/2-011013	÷
- 111 視壓列表	● 返回到页面		
- (1) 自注册	🔨 返回到配置		
- Meb 登录	《 通回主页		
□ ■ 短信服务			
- 67- 网关			
■ 发送短信			
3 MB	4		
Copyright 2024 Hewlett Packard Enterprise Developm	nent LP		

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

aruba		ClearPass Gue	st Me
9 RR	•	WWW ADDRESS	
	o * 88:	SIDS	
I Onboard		BALL HED BRAADON,	
▲ 配置	0 原業名称:	カ此 Web 登录第人页面名称。 Web 登录第二/Vue#(foom name sho"声示示意思	
****	i i i i i i i i i i i i i i i i i i i	The second s	
◎ 🤡 內容管理器	继述:		
● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●		#关 Web 登录的注释或描述性文本。	
85 来声管理器	* 供应商设置:	Aruba 👻	
- \$ 热点管理器			
	登录方法:	な新聞式版 - 米井県辺定園547 F11 P 米甲提文 (*) 各部の位地画中が時間登録 総合語文社が留存着すたが用中的 MAC 地址、連邦来自于指制同语「P重定用収穫」	
● 算 字段 ● 】 表单	* HEAL:	securelogin anubanetworks.com 在此比較人物回用戶品的生的名(FQOH)。 出意用 HTTPS 安全量量时,此名和互当均成量上资册的 HTTPS 证书的名称相匹配。	
● 11 税率列表 ● ● ● 車注册	安全登录:	通过 HTTP 发送明文团码 ✔ 394夏纪用于 Web 量争过程的安全活动。	
- ⁴⁴ Web 200	和市地址: 2	一 抽制器等发送 IP 以應免完備 在身站制器部署中, 经常需要消费需求方利均用于原始重压内的不需地址。 当参数不可用或无法需要以下要求时, 将使用上述地址。	
10000000000000000000000000000000000000	西義重定向 用于描述初始重定用中保	送的景教的击 现。	
2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	安全地料:	不检查 - 始終允许整要	
	登录表单 用于描述登录表单的行为	和内容的迅速。	
	最份验证:	2月2日 (東京市今日2日3日) 2月2日 (東京市今日2日3年) 月日の市台に営業人、一学会局市中島) 2月1日 (日本市中島) 2月1日 (日本市中国) 2月11 (日本) 2月11 (日本)	
	間止 CNA: 4	周囲構成 Apple Captive Network Assistant Apple Captive Network Assistant (CNA)並在並展有機能回答[3]中的网络2型分析第45式用范幕。 主意,此恐可能不能用于所有供应用,这就由于如何实践器能回答[7]中。	
	自定义表举:	· 编件目音文量录表单 如果选中、必须在任务或交给 HTHL 医城中提供应告已的 HTML 呈杂表单。	
	自建文标签:	夏無数以所签約確認與意 如果这支, 如何的事業次均能設長素単的存在和確認的意。	
	* 身份验证机检查:	本地 · 匹配本地秩户 💙	
	0	C BRAND READER	

aruba	ClearPass Guest	Mer
S. 来究	0 如果是中、无论客户确的影以目标像的问题会将其要重。	
1 08	0 B ²²	
Onboard	科·拉利國政策分析與和國政的語識。	
1 E E	* 問題: Blank Skin V 网络学生中 Web 经承担管理的资源	
 ※ 身份验证 ○ ※ 内容管理器 ○ ※ 内容管理器 ○ ◎ 本用文件 	19월	
	Die HTHL:	
● 日注符 《● 四注符 《● 四百日 》 月四 ○ ● ● 三注符 ○ ● ● 三注符 ○ ● 日注符 ○ 月四 ● 日注符 ○ ● 日注 ○ ● 日: ○ ● 日 ● 日: ○ ● 日: ○ ● 日: ○ ● 日: ○ ● 日 ● 日 ● ● ● 日: ○ ● 日: ○ ● 日 ● ● ● ● ● □ ● ● ● ● ● ● ● ● ● ● ● ●	Image: A control of the second sec	
A 69	登泉湖谷: (西入	

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"。

aruba		Clear	Pass Guest				Menu 🚍
* #R	 主页 = 配置 = 页度 > 由注册 						
1 08)	 自注册 						创建新的自注册页面
Onboard	0						
12m	● 使用此均表按面管理用于自注册的页面。						
● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	0 (REPR)						
(1) 内容管理器	△ 名将	注意负責	皮肤	父頃			
25 专用文件	g. Guest Self-Registration	guest_register	Galleria Skin 2	(无父吻)			
OT age Hill	Default settings for visitor self-registration.	eme salf	Black Skin	/=018V			
1) 的点管理器			Diality Skill	CALCOL			
(4) 事务处理器		and a mailed					
9 +页面	2个角连般 〇 重数加数			显示所有行	•		
1 字段	8+ 运用到资源						
- 0- FEBRER	38.049.9100.38						
(G Web 登录	超回主页						
國際							
and the second s							
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1							
- D - R关							
2 次送短信							
AN BELT							
and the second							
	0						
Copyright 2024 Hewlett Packard Ente	rprise Development LP					ClearPass Gu	est 6.10.6.186545 on C3000V platform

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

aruba				Clear	Pass Guest
* * <u>*</u>	6 (0)3	変換目力		1	
1 设备 (A 188	余倍	*型	标签	描述
Onboard C	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
◎¥ 身份验证	20	visitor_email	text	Sponsor s cmain.	att) (rable-st
- 🥶 内容管理器	25	visitor_name	phone	Phone Number:	
使 专用文件	30	visitor_priore	text	Company Name:	調査となかの思想です。
- 🧐 公共文件	40	email	text	Email Address:	
- 87. 来宾管理器	45	username	text	Username:	Name of the account
→ ¹⁹ 热点管理器 	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.
- <mark>雨 表単</mark> - III 视题列表	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.
() 自注册	70	role_id	hidden	Account Role:	Role to assign to this account.
👫 Web 登录 💫 网页	75	enabled	dropdown	Account Status:	Select an option for changing the status of this account.
回执	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.
3. 1. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2.	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)

L 我i	己阅读并同意免责声明
手机号	码: china → 获取登录验证码
验 证	码: 🖌 🔍
	大东方百货无线网络免责声明
構築的第二 次122 男式語的 東国新語 「和品」	中,物好。 物理用大玩方首孩无狂网络,我们崩成为应遵供绝。 回联用无纸网络像入环境,并负击你证互联网应用
	大东方百货
	新収所有 Q 大志方百姓

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-ma
<div class=
<div class=</th><th>in"> 'I-fill'></div> 'Fwrao'></body>	
<div.< td=""><td></td></div.<>	
	<pre><form action="http://10.23.188.51/guest/sms-self.php? browser=1" method="post" name="getPass" target="i"></form></pre>
	<input name="expire after" type="hidden" value="2"/>
	<input name="role id" type="hidden" value="2"/>
	<input name="auto update account" type="hidden" value="1"/>
	<input name="country" type="hidden" value="1"/>
	<input 06="" checkpic'="" class="1-ck0'" cloptions<="" cni"s="" name="create time" onclick="return agree();'/><lapel for='declaration'>&ubsp;我已阅读并同意免责声明</label></pre></td></tr><tr><td></td><td>and a state of the state of the</td></tr><tr><td></td><td><pre><select> conting value=" pre="" src="public/general/blank.git" type="hidden" value=" /></td></tr><tr><td></td><td><input type='hidden' name='remote addr' value='' /></td></tr><tr><td></td><td><input type='hidden' name='creator accept terms' value='1' /></td></tr><tr><td></td><td><div class='i-hided'> <input type='checkbox' id='declaration' onclick='return agree();'/> </div></td></tr><tr><td></td><td><pre>
	<pre>copiion value= UN > doc/objion> copiion value="115" + 2 (option> </pre>
	contion value = "IIK" > contions
	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。

aruba		ClearPass	Guest
来宾	• 主页 » 配置 » 页	页面 » 表单	
1°设备	• 自定义表单	字段 (role_id)	
) Onboard	0		
	⊙ 使用此表单覆盖:	表单 sms-self 中的字段 role_id。 🌇 Edit Base Field	
— 😼 身份验证		表单字段编辑器	
 2 (2) 内容管理器 - (2) 专用文件 	* 字段名:	role_id ▼ 远指要附加到表单的字段定义。	
_ 🥶 公共文件	表单显示屋性 这些属性控制为此	字段显示的用户界面。	
● \$ 热点管理器 ● ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	字段:	展用此字段 适中后,字段将作为表单的一部分包括在内。	
	* 等级:	[70] 表示用户界面字段相对顺序的数字,这些字段以等级递增的顺序显示。	
— 113 字段 — 111 麦单	* 用户界面:	- - - - - - - - - - - - -	
	表单验证属性		
— <mark>经希</mark> Web 登录 — 🔍 网页	必填字段:	必须提供字段画 如果字段不能首奏或音字、则选择此选项。	
→ 回执	初始值:		
● ● - ●	* 验证程序:	[sEqual → 〕 🏠 还原 验证字段内容所用的函数。	
3 4 翻译	验证程序参数:	【元) 其值將作为参数提供培验证程序的字段的可选名称。	
	验证程序参数:	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	
	验证错误:	Please choose from one of the available roles 李段值验证失败且验证程序来直接返回错误消息时将显示的错误消息。	
	高级属性 这些属性控制转换	、显示和动态行为。	
	高级:	□ 显示高级属性	
	类型错误:	Please choose from one of the available roles 未提供字段值、字段值格式不正确或转换失败时将显示的错误消息。	
		保存更改	
※ 管理	* 必填字段		
Convrint 2024 Hewlett Packard Enternrise Devel	onment I P	1字段	

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。

	蒲洗器名	称		属性名称	1	别名			Ê
1.	Curren	81.92	拉 坍型				_	0	-
2.	Next 2	ACE	940 <u>755</u> fat						_
з.	One Da	Ĩ	25						-
4.	Seven	筛	选器名称:	Date Time				^	-
5.	Curren Date T	筛ì	先器查询:	<pre>select date_trunc('seco date_trunc('hour', locs date_trunc('hour', locs date_trunc('hour', locs date_trunc('nour', locs date_trunc('second', lc date_trunc('second', lc</pre>	nd', localtimestamp(0)) ltimestamp(0)+interval ltimestamp(0)+interval ltimestamp(0)+ interval ltimestamp(0)+ interval caltimestamp(0)+ interva caltimestamp(0)+ interva	as today, '1 days') as one_day, 1 week') as one_week, '1 month') as one_month, '6 months') as six_months, 1 '5 minutes') as four_houn 1 '1 hours') as one_hours	τε,		-
				·			11		-
			名称	別名	数据类型	启用方式			
-		1.	today	Now DT	Date-Time	-		<u><u></u></u>	-
7.	Next 8	2.	one_day	One Day DT	Date-Time	1-1		8	-
		з.	one_week	One Week DT	Date-Time			8	
		4.	one_month	One Month DT	Date-Time			3	
		5.	six_months	Six Months DT	Date-Time	-		3	
		6.	four_hours	Four Hours DT	Date-Time			9	
		7.	one_hours	One Hours DT	Date-Time	-			
		8.	Chek to add			-	Inter .	-	
							保住	大四	

◆ 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

强制配置文件 - updated-guest-mac

_			-			
摘要	配置文件	屋性				
配置了	(件:					
名称:			updated-guest-mac			
描述:						
类型:			Post_Authentication			
操作:						
设备编	国列表:		-			
属性:						
	类型			名称		值
1.	Endpoint			Username	-	%{Authentication:Username}
2.	Endpoint			MAC-Auth Expiry	=	%{Authorization:[Time Source]:Eight Hours DT}
3.	Status-Upda	te		Endpoint	=	Known
4.	Endpoint			Guest Role ID	=	authenticated

新增一个强制配置文件

取名: portal

强制配置文件 - por	tal	
摘要 配置文件 属性		
配置文件:		
名称:	portal	
描述:		
类型:	RADIUS	
操作:	Accept	
设备组列表:	-	
属性:		
类型	名称	
1. Radius:Aruba	Aruba-User-Role	= authenticated
		此处的role需要和MM上的guest认证role保持 一致

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

配置»强制»策略»编辑	- mac-caching-enforcement-policy	
强制策略 - mac-r	caching-enforcement-policy	
	calling enforcement policy	
福制:		
名称·	mac-caching-enforcement-policy	
	mac-caching-enforcement-policy	
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 MATCHE	ES_ALL [User Authenticated])	portal, updated-guest-mac
		٩
新建服务		
服务 - portal		
		Service has not been saved
摘要服务身份验证	角色 强制	
服务:		
名称:	portal	
描述:		
类型:	RADIUS 强制(通用)	
状态:	Enabled	
监视模式:	Disabled	
更多选项:	-	
		新久 (1990)
匹配以下所有条件:		

匹配	以下所有条件:			
	类型	名称	运算符	<u>(</u>
1.	Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}
2.	Radius:Aruba	Aruba-Essid-Name	EQUALS	Test-Portal
身份	验证:			
身份	计验证方法:	1. [PAP] 2. [CHAP] 3. [MSCHAP]		
身份	}验证源:	 [Guest User Repository] [Local SQL DB] [Endpoints Repository] [Local SQL DB] 		
去附	(用户名规则:	-		
明念	山下山・			
<	返回到服务			禁用 复制 保存 取消

	,,,	-9	
A 个服务器证书已到期。			
配置 » 服务 » 编辑 - porta	al		
服务 - portal			
	Servic	e has not been saved	
	105117 4h.ds. 2014al		
1035C 10035 547033244			
按仪讲细信息:	用于获取角色映射属性的授权源(针对每个身份验证源)	開始 的 盐和 亚语	
	1 [Guest User Repetitory] [Local SOL DB]	Guest Liser Repository] [Local SOL DB]	
	[Guest Oser Repository] [Local SQL DB] [Endpoints Repository] [Local SQL DB]	[Endpoints Repository] [Local SQL DB]	
	El [Endpointo repositor/] [Essar e de po]	[rushaura ushaara)] [rada adr aa]	
	用于获取角色映射属性的其他授权源 -		
	[Endpoints Repository] [Local SQL DB]		添加新的身份验证源
	[Time Source] [Local SQL DB] 查看详细信	ē.	
	修改		
	Select to Add		
			64
			(
配置»服务»编辑-porta	d .		
昭冬 - nortal			
portai			
摘要 服务 身份验证	角色 克爾		
使用缓存的结果:	□ 使用先前会话中缓存的角色和状况属性		
强制策略:	mac-caching-enforcement-policy	▼ 修改	添加新的强制策略
		强制莱鹏详细信息	
描述:			
默认配置文件:	[Deny Access Profile]		
规则评估算法:	first-applicable		
条件		强制配置文件	
1. (Tips:Role MATC	HES ALL [User Authenticated])	portal, updated-guest-mac	

◆ 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

置文件:				
3称:	return-username			
截述:				
經:	RADIUS			
影作:	Accept			
全备组列表:				
性:				
类型		名称		@
1. Radius:IETF	F	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	
治夏 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 EQUAL AND (Authoriza AND (Authoriza AND (Endpoint:	S [User Authenticated]) tion:[Time Source]:Now DT LESS_THAN %{Endpoint:MAC-Auth Expiry}) tion:[Endpoints Repository]:Unique-Device-Count EXISTS) Guest Role ID EQUALS authenticated)	portal, return-username

新增一个服务

摘要服务身份	脸证 授权 角色 强制		
资务:			
3称:	Copy_of_MAC-Authentication-Service		
述:			
型:	RADIUS 强制(通用)		
:态:	Enabled		
钢模式:	Disabled		
多选项:	授权		
		服务规则	
and a second state of the second			
配以下所有条件:			
配以下所有条件: 类型	名称	运算符	ũ.
配以下所有条件: 类型 Connection	名称 Client-Mac-Address	运算符 EQUALS	值 %{Radius:IETF:User-Name}
ll以下所有条件: 类型 Connection 2.Radius:Aruba	名称 Client-Mac-Address Aruba-Essid-Name	运算符 EQUALS EQUALS	值 %{Radius:IETF:User-Name} Test-Portal
配以下所有条件: 类型 Connection 2. Radius:Aruba 份验证:	名称 Client-Mac-Address Aruba-Essid-Name	运算符 EQUALS EQUALS	值 %{Radius:IETF:User-Name} Test-Portal
W以下所有条件: 类型 . Connection . Radius:Aruba 份验证: 份验证方法:	名称 Client-Mac-Address Aruba-Essid-Name [MAC AUTH]	运算符 EQUALS EQUALS	值 %{Radius:IETF:User-Name} Test-Portal
WUX下所有条件: 类型 · Connection Radius:Aruba 份验证方法: 份验证方法:	名称 Client-Mac-Address Aruba-Essid-Name [MAC AUTH] [Endpoints Repository] [Local SQL DB]	运算符 EQUALS EQUALS	值 %{Radius:IETF:User-Name} Test-Portal
 L 下所有条件: 类型 Connection Radius:Aruba 份验证方法: 份验证簿: 除用户名规则: 	名称 Client-Mac-Address Aruba-Essid-Name [MAC AUTH] [Endpoints Repository] [Local SQL DB] -	运算符 EQUALS EQUALS	值 %{Radius:IETF:User-Name} Test-Portal
 L 下所有条件: 类型 Connection Radius:Aruba 份验证方法: 份验证序: 納用户名规则: 务证书: 	名称 Client-Mac-Address Aruba-Essid-Name [MAC AUTH] [Endpoints Repository] [Local SQL DB] - -	运算符 EQUALS EQUALS	值 %{Radius:IETF:User-Name} Test-Portal
與以下所有条件: 英型 Connection Radius:Aruba 份验证方法: 份验证方法: ····································	名称 Client-Mac-Address Aruba-Essid-Name [MAC AUTH] [Endpoints Repository] [Local SQL DB] - -	运算符 EQUALS EQUALS	值 %{Radius:IETF:User-Name} Test-Portal

度 服务 另份短证	長权 角色 强制		
又详细信息:	用于获取角色映射属性的授权源(针对每-	个身份验证源)	
	身份验证源	属性的获取来源	
	1. [Endpoints Repository] [Local	I SQL DB] [Endpoints Repository] [Local S	QL DB]
	用于获取角色映射属性的其他授权源。	1000	法加新的自份险
	[Endpoints Repository] [Local SQL DB] [Time Source] [Local SQL DB]		13-01-01-01-01-01-01-01-01-01-01-01-01-01-
		整合注动信息	
		修改	
	Select to Add	~	
返回到服务	ny of Mat-Authentication-Service		禁用复制保存取消
返回到服务 配回 » 服労 » 期間 - Co 服务 - Copy_of, 調要 服务 身份論 使用版存的結果:	py_or_MAC-Authentication-Service _MAC-Authentication-Service 证 授权 角色 交話 □ 使用先前会话中缓存的角色和状况属	Ce 性	禁用 复制 保存 取消
返回到服务 配回 > 服务 > 瑞雨 - Co 服务 - Copy_of. 調要 服务 身份論 使用暖存的結果: 透刺策略:	py_of_MAC-Authentication-Service _MAC-Authentication-Service 证 提取 角色 空話 	Ce 胜	禁用 复制 保存 取消 添加新的研究制
返回到服务 配回 > 服务 > 瑞田 - Co 服务 - Copy_of. 國務 與份論 使用缓存的结果: 强制策略:	py_of_MAC-Authentication-Service _MAC-Authentication-Service 证 规权 角色 交話 □ 使用先的会话中缓存的角色和状况属 mac-enforcement-policy		禁用 复制 保存 取消 添加新699%制度
返回到服务 配回 » 服务 » 場前 - Co 服务 - Copy_of, 病要 服务 身份論 使用缓存的結果: 潮頻策略: 描述:	py_or_MAC-Authentication-Service _MAC-Authentication-Service 证 班权 和色 2004 □ 使用先的会话中缓存的角色和状况属 mac-enforcement-policy	Ce 述 受破解語時详细信息	禁用 复制 保存 取消 添加新699%。续
返回到服务 配后 > 服务 > 羽田 - Co 服务 - Copy_of, 服务 - Popy_of, 服务 - Popy_and R - Popy_and <pr -="" p="" popy_and<=""> R - Popy_and <pr -="" p="" popy_and<=""> <p< td=""><td>py_or_MAC-Authentication-Service _MAC-Authentication-Service 证 提取 加色 2004 □ 使用先的会话中缓存的角色和状况属 「mac-enforcement-policy [Deny Access Profile]</td><td>CE 受制解語詳細信意</td><td>禁用 复制 保存 取消 添加新台9800余</td></p<></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr></pr>	py_or_MAC-Authentication-Service _MAC-Authentication-Service 证 提取 加色 2004 □ 使用先的会话中缓存的角色和状况属 「mac-enforcement-policy [Deny Access Profile]	CE 受制解語詳細信意	禁用 复制 保存 取消 添加新台9800余
返回到服务 配面 > 服务 > 陽田 - Co 服务 - Copy_of 備要 服务 身份續 使用暖存的結果: 週柳焼略: 描述: 試入配置文件: 规则评估解法:	py_or_MAC-Authentication-Service _MAC-Authentication-Service 证 超权 加色 9866 @ 使用先的会话中缓存的角色和状况属 [mac-enforcement-policy [Deny Access Profile] first-applicable	Ce	禁用 复制 保存 取消 添加新的短期的
遼回到服务 総労 > 陽祖 - Co 服务 - Copy_of 酸麥 身份猶 使用缓存的消鼎: 湖湖清略: 描述: 軟八配寬文件: 現明平估爾法: 文件 (Tips:Role ぞ? へいか (Author)	py_of_MAC-Authentication-Service MAC-Authentication-Service 证 規収 角色 9846 回 使用先前会活中缓存的角色和状況属 [mac-enforcement-policy [Deny Access Profile] first-applicable WALS [User Authenticated])) rization:[Time Source]:Now DT LESS_T/	Ce 性 文 修文 强制策器详细信息 操制配置文件 HAN %{Endpoint:MAC-Auth Expiry}) patal return=usemame	禁用 复制 保存 取 添加新伯子服制

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。

C	RADIUS		Copy_of_MAC-	ACCEPT	2024/10/11 20:57:30	
CONTRACTOR OF TAXABLE	RADIUS	200	portal	ACCEPT	2024/10/11 20:53:49	15 1-99-AF
C	RADIUS	705-120-12020.	Copy_of_MAC-	REJECT	2024/10/11 20:53:13	FE-50 JL 12-99-AF

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。

属性	_	值		
Guest Role ID	=	authenticated	C)	Ť
MAC-Auth Expiry	=	2024-10-14 14:45:34	ED.	Ť
Username	=	_ 0		T
Click to add				

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。