Aruba Clearpass 与 Meraki AP 结合

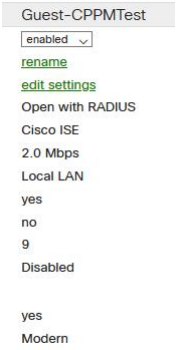
实现 Web 认证

目录

目录

第一章 Meraki 设置（摘取自网络）

(1) 创建 SSID，选择启用，然后单击编辑设置



(2) 后续部分配置

a. Association requirements: *MAC-based access control (no encryption)
b. Splash page: *Cisco Identity Services Engine (ISE) Authentication
c. RADIUS servers: *<IP of the ClearPass Server(s)> port: 1812 and the secret you put in for your Meraki APs in the Network Devices of the ClearPass server
d. RADIUS testing: *RADIUS testing enabled
e. RADIUS CoA support: *RADIUS CoA enabled
f. RADIUS attribute specifying group policy name: *Aruba-User-Role
g. RADIUS accounting: *RADIUS accounting is enabled
h. RADIUS accounting servers: *<IP of the ClearPass Servers> port 1813 and the secret you put in for your Meraki APs in the Network Devices of the ClearPass server
i. RADIUS proxy: *Do not use Meraki proxy
j. Assign group policies by device type: (Whatever your network requires here) I chose: Disabled: do not assign group policies automatically
k. Walled garden: *Walled garden is enabled: Put your IPs of the ClearPass servers/floating IPs.
l. Client IP assignment: Bridge mode: Make clients part of the LAN
m. VLAN tagging: *(If your guest/employee/etc network requires VLANS put your VLAN in here)
n. RADIUS override: Ignore VLAN attribute in RADIUS responses (This is what I’m using, for more advanced setups you can choose to enable this)
o. Content filtering: Whatever your network requires
p. Bonjour forwarding: Disable Bonjour Forwarding (Whatever your network requires)
q. Mandatory DHCP: (Whatever your network requires)
r. Band selection: (Whatever your network requires)
s. Minimum bitrate (Mbps): (Whatever your network requires)

Access control

SSID: Guest-CPPMTest

Network access

Association requirements

- ○ Open (no encryption)
  Any user can associate
- ○ Pre-shared key (PSK)
  Users must enter a passphrase to associate
- ◉ MAC-based access control (no encryption)
  RADIUS server is queried at association time
- ○ Enterprise with Meraki Cloud Authentication
  User credentials are validated with 802.1X at association time
- ○ Identity PSK with RADIUS
  RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address

Splash page

- ○ None (direct access)
  Users can access the network as soon as they associate
- ○ Click-through
  Users must view and acknowledge your splash page before being allowed on the network
- ○ Sponsored guest login
  Guests must enter a valid sponsor email and own email address before being allowed on the network
- ○ Sign-on with Meraki Cloud Authentication
  Users must enter a username and password before being allowed on the network
- ○ Sign-on with SMS Authentication
  Users enter a mobile phone number and receive an authorization code via SMS.
  After a trial period of 25 texts, you will need to connect with your Twilio account on the Network-wide settings page.
- ◉ Cisco Identity Services Engine (ISE) Authentication
  Users are redirected to the Cisco ISE web portal for device posturing and guest access
- ○ Systems Manager Sentry enrollment
  Only devices with Systems Manager can access this network

RADIUS servers

#	Host	Port	Secret	Actions	
1	[redacted]	1812	••••••••••••••		Test
2	[redacted]	1812	••••••••••••••		Test

Add a server

RADIUS testing RADIUS testing enabled

RADIUS CoA support RADIUS CoA enabled

RADIUS attribute specifying group policy name Aruba-User-Role

RADIUS accounting RADIUS accounting is enabled

RADIUS accounting servers

#	Host	Port	Secret	Actions
1	[redacted]	1813	••••••••••••••	
2	[redacted]	1813	••••••••••••••	

Add a server

RADIUS proxy Do not use Meraki proxy

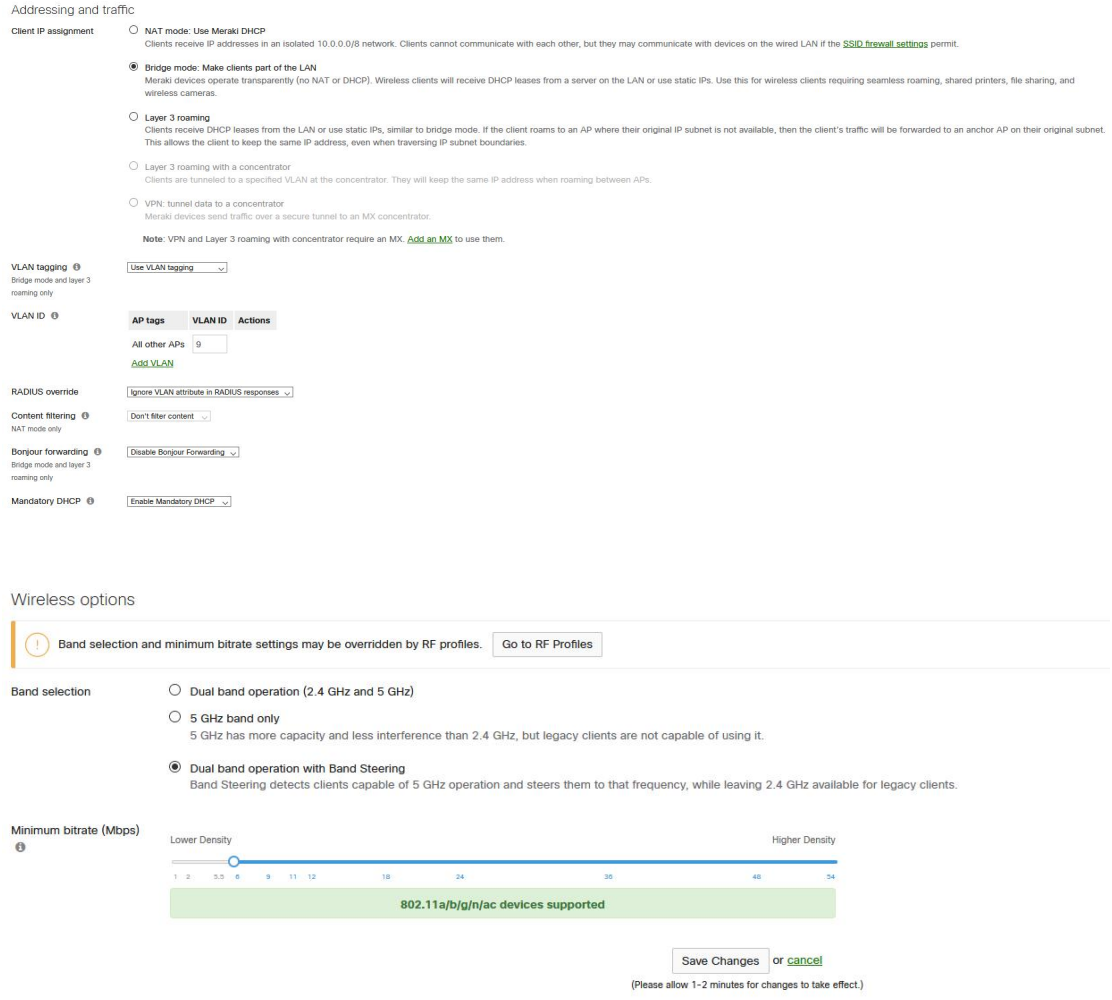
Assign group policies by device type Disabled: do not assign group policies automatically

Walled garden Walled garden is enabled

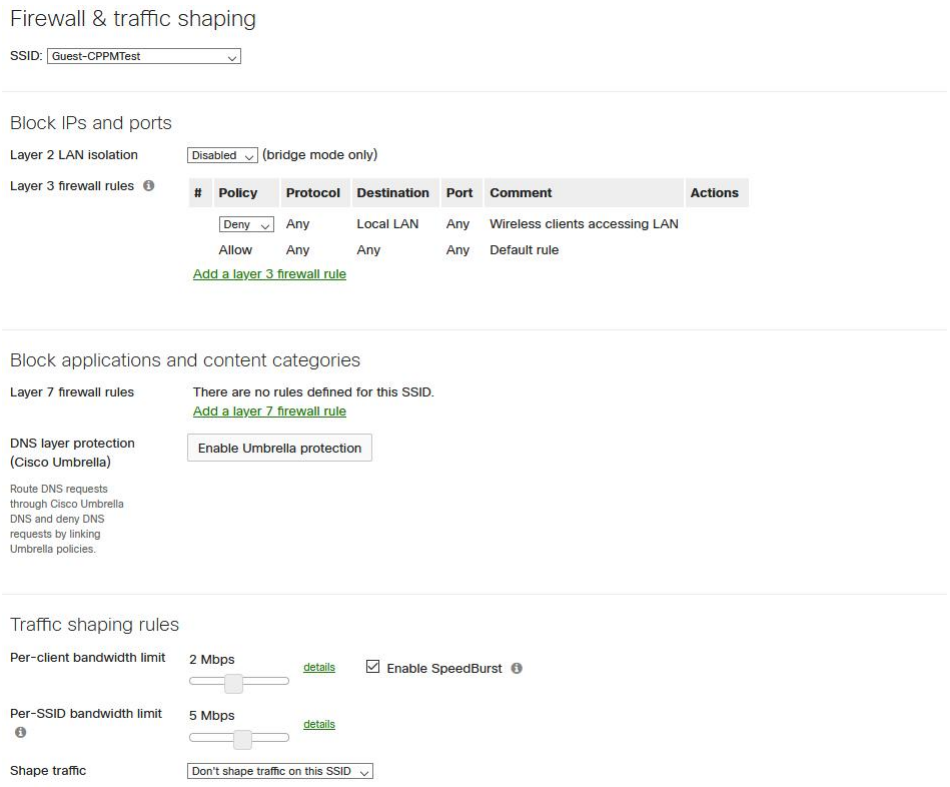
Walled garden ranges

[redacted]/32
[redacted]/32
[redacted]/32
[redacted]2/32

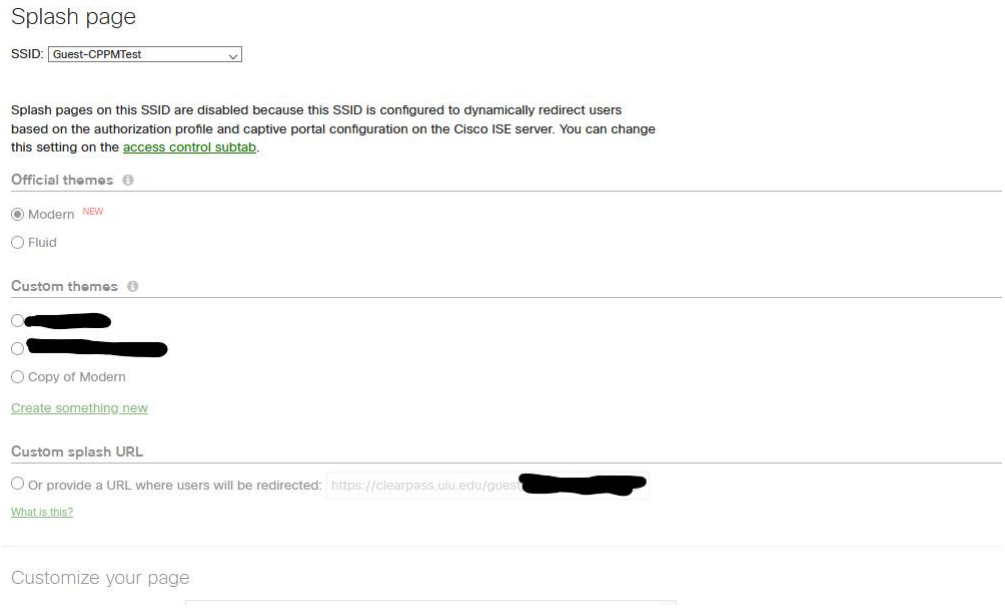
What do I enter here?



(3) 在防火墙和流量整形中，选择您的环境所需的内容。这不会影响 **ClearPass** 服务器（除非您出于某种原因阻止对服务器的访问）



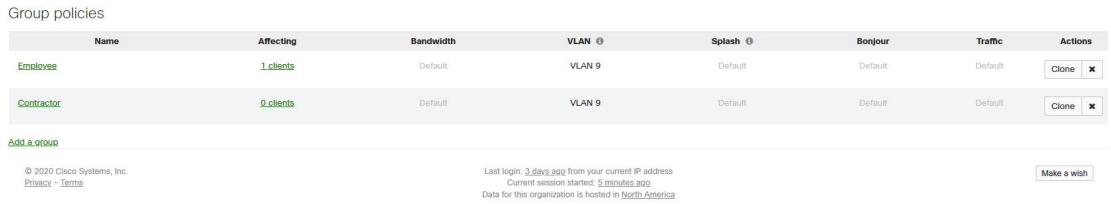
(4) 对于 **Splash** 页面，这将显示为灰色。你将无法改变任何事情



(5) 根据您的环境要求设置其余的无线部分。本节中没有 **ClearPass** 设置。

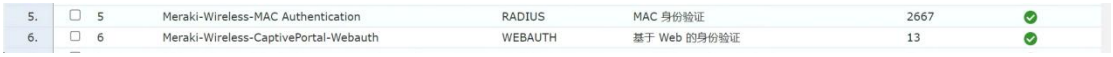
(6) 转到 Network-wide -> Group policies

a.您需要设置与您在 ClearPass 中为设备配置文件设置的 Role 相对应的 Group policies Name。
b.可以设置 Employee 和 Contractor 角色。与 ClearPass 上 Role 配合，本功能未测试。



第二章 ClearPass Policy Manager 设置

1) 确保您的 Meraki 接入点与 ClearPass 能互相通信，并带有两边设置的相应的 RADIUS 密钥。
2) 本次测试涉及到两个服务。为了方便识别，我们在服务前面添加了对应的标识字段，比如 Meraki-Wireless，就像下面的例子一样。



a) 您需要创建一个强制配置文件，可以配置对应的 Role 相关的强制策略，与 Merike Group policies 配置 Name 保持一致，本次全访客网络不涉及此配置

b) 您需要创建一个强制配置文件，将认证用户做一个 1 周的 MAC Caching（缓存时间自定义）

配置


配置 » 强制 » 配置文件 » Edit Enforcement Profile - YST-Guest Guest MAC Caching

强制配置文件 - YST-Guest Guest MAC Caching

注意: 此强制配置文件由服务模板创建

摘要 | 配置文件 | 属性

配置文件:

名称:	YST-Guest Guest MAC Caching
描述:	来宾的端点属性更新
类型:	Post-Authentication
操作:	
设备组列表:	-

属性:

	类型	名称		值
1.	Endpoint	Username	=	%{Authentication:Username}
2.	Endpoint	Guest Role ID	=	%{GuestUser:Role ID}
3.	Endpoint	MAC-Auth Expiry	=	%{Authorization:[Time Source]:One Week DT}

c) 您需要创建一个强制配置文件，将用户重定向到您创建的访客门户。


配置 » 强制 » 配置文件 » Edit Enforcement Profile - Meraki-Wireless-Redirect

强制配置文件 - Meraki-Wireless-Redirect

摘要 | 配置文件 | 属性

配置文件:

名称:	Meraki-Wireless-Redirect
描述:	
类型:	RADIUS
操作:	Accept
设备组列表:	-

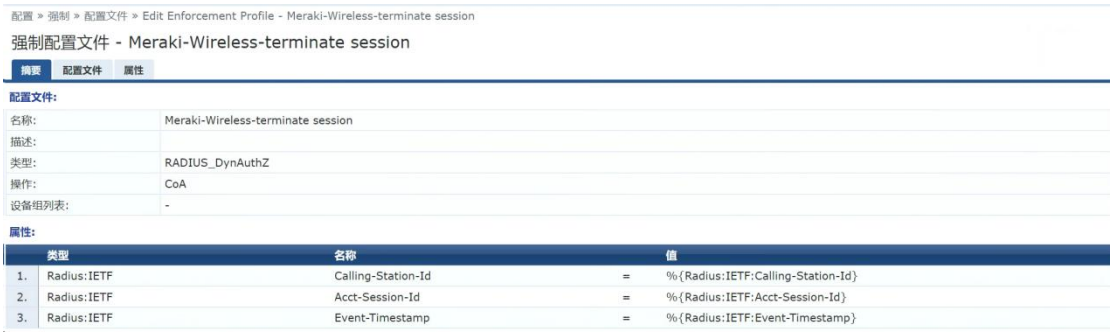
属性:

	类型	名称		值
1.	Radius:Cisco	Cisco-AVPair	=	url-redirect=https://[redacted]al_meraki.php?switchip=%{Connection:NAD-IP-Address}&mac=%{Connection:Client-Mac-Address-NoDelim}

Meraki AP 不支持在 AP 上定义 URL，需要通过 Radius 属性内带 URL 给 Meraki AP 弹 Portal。格式如下：

(url-redirect=https://<ClearPassURL or IP>/guest/<Guest-Page>.php?switchip=%{Connection:NAD-IPAddress}&mac=%{Connection:Client-Mac-Address-NoDelim})

d) 您需要创建一个强制配置文件来终止会话，此配置用于改变用户状态，让客户端重新发起认证请求。


配置 » 强制 » 配置文件 » Edit Enforcement Profile - Meraki-Wireless-terminate session

强制配置文件 - Meraki-Wireless-terminate session

摘要 | 配置文件 | 属性

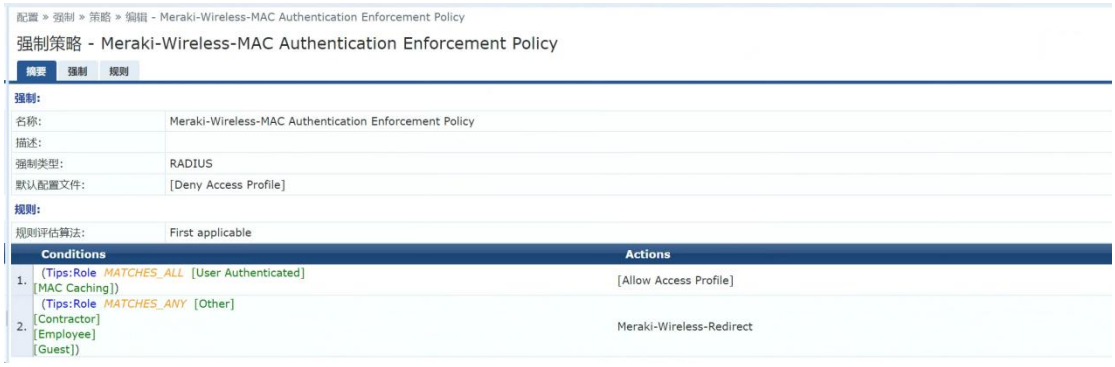
配置文件:

名称:	Meraki-Wireless-terminate session
描述:	
类型:	RADIUS_DynAuthZ
操作:	CoA
设备组列表:	-

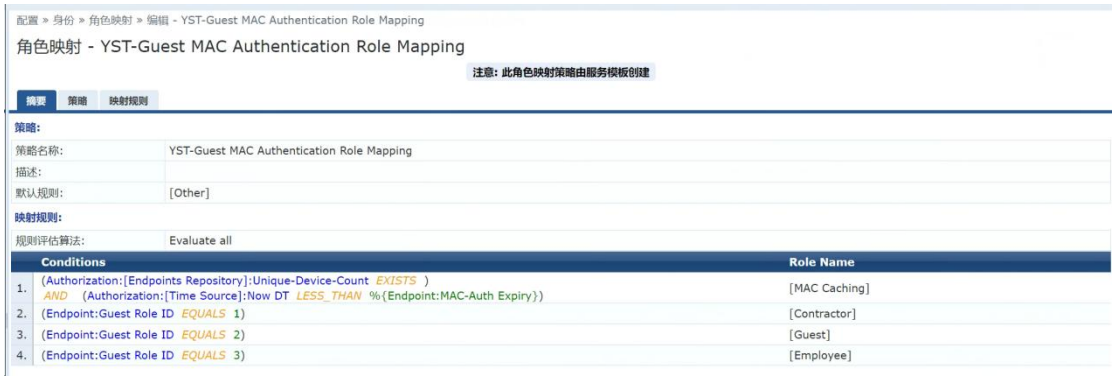
属性:

	类型	名称		值
1.	Radius:IETF	Calling-Station-Id	=	%{Radius:IETF:Calling-Station-Id}
2.	Radius:IETF	Acct-Session-Id	=	%{Radius:IETF:Acct-Session-Id}
3.	Radius:IETF	Event-Timestamp	=	%{Radius:IETF:Event-Timestamp}

3) 您还需要创建两个执行策略。

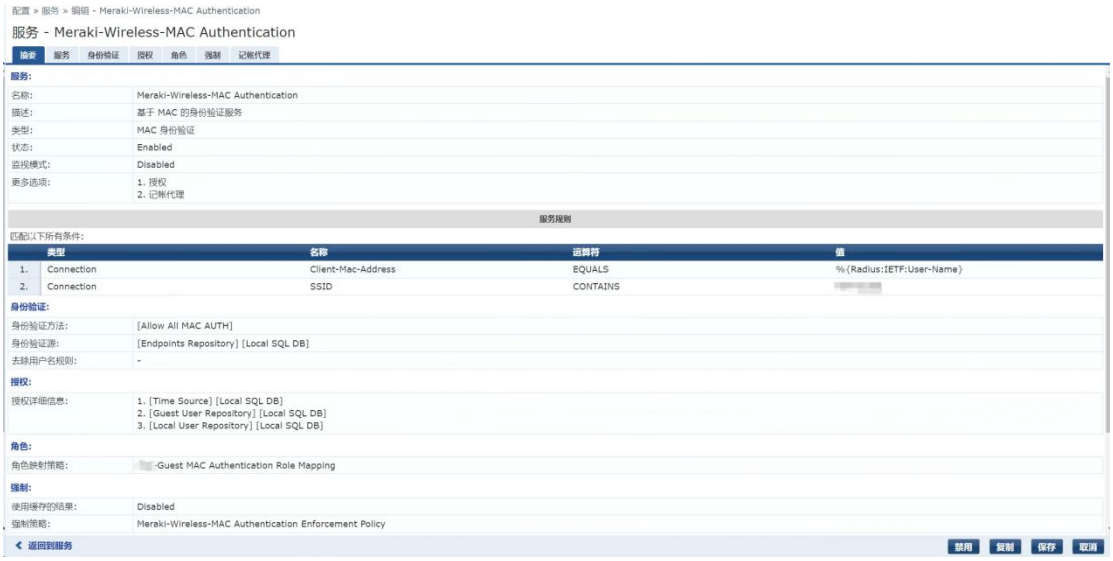


4) 您需要创建一个角色映射

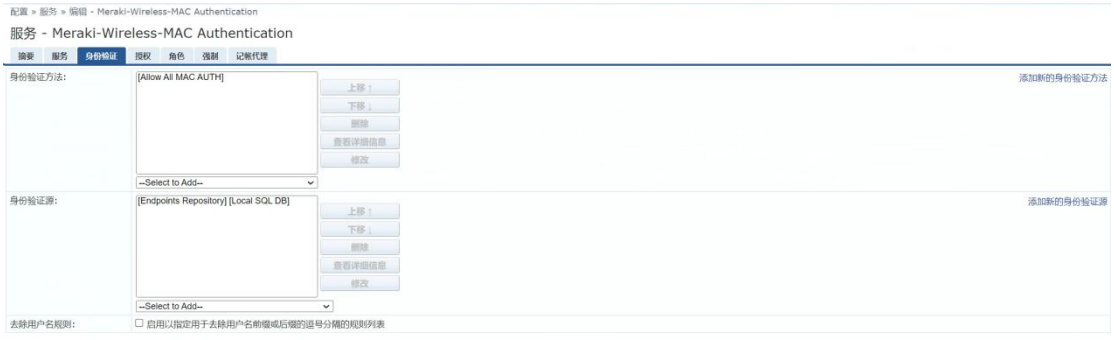


5) 您需要创建两个服务

a. Meraki-Wireless-MAC Authentication


配置 » 服务 » 编辑 - Meraki-Wireless-MAC Authentication
服务 - Meraki-Wireless-MAC Authentication
摘要 服务 身份验证 授权 角色 强制 记帐代理
服务:
名称: Meraki-Wireless-MAC Authentication
描述: 基于 MAC 的身份验证服务
类型: MAC 身份验证
状态: Enabled
监视模式: Disabled
更多选项: 1. 授权
2. 记帐代理
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. Connection SSID CONTAINS
身份验证:
身份验证方法: [Allow All MAC AUTH]
身份验证源: [Endpoints Repository] [Local SQL DB]
去除用户名规则: -
授权:
授权详细信息: 1. [Time Source] [Local SQL DB]
2. [Guest User Repository] [Local SQL DB]
3. [Local User Repository] [Local SQL DB]
角色:
角色映射策略: -Guest MAC Authentication Role Mapping
强制:
使用缓存的结果: Disabled
强制策略: Meraki-Wireless-MAC Authentication Enforcement Policy
返回到服务
禁用 复制 保存 取消


配置 » 服务 » 编辑 - Meraki-Wireless-MAC Authentication
服务 - Meraki-Wireless-MAC Authentication
摘要 服务 身份验证 授权 角色 强制 记帐代理
名称: Meraki-Wireless-MAC Authentication
描述: 基于 MAC 的身份验证服务
类型: MAC 身份验证
状态: Enabled
监视模式: 启用以监视无强制的网络访问
更多选项: 授权 审核终端主机 分析端点 记帐代理
服务规则
匹配 任何或 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. Connection SSID CONTAINS
3. Click to add...


配置 » 服务 » 编辑 - Meraki-Wireless-MAC Authentication
服务 - Meraki-Wireless-MAC Authentication
摘要 服务 身份验证 授权 角色 强制 记帐代理
身份验证方法: [Allow All MAC AUTH]
上移 下移 删除 查看详细信息 修改
--Select to Add--
添加新的身份验证方法
身份验证源: [Endpoints Repository] [Local SQL DB]
上移 下移 删除 查看详细信息 修改
--Select to Add--
添加新的身份验证源
去除用户名规则: 启用以指定用于去除用户名前缀或后缀的逗号分隔的规则列表


配置 » 服务 » 编辑 - Meraki-Wireless-MAC Authentication
服务 - Meraki-Wireless-MAC Authentication
摘要 服务 身份验证 授权 角色 强制 记帐代理
授权详细信息:
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 SQL DB] [Endpoints Repository] [Local SQL DB]
用于获取角色映射属性的其他授权源 -
[Time Source] [Local SQL DB]
[Guest User Repository] [Local SQL DB]
[Local User Repository] [Local SQL DB]
删除 查看详细信息 修改
--Select to Add--
添加新的身份验证源


配置 » 服务 » 编辑 - Meraki-Wireless-MAC Authentication

服务 - Meraki-Wireless-MAC Authentication

摘要 | 服务 | 身份验证 | 授权 | 角色 | 强制 | 记帐代理

角色映射策略: YST-Guest MAC Authentication Role Mapping 修改 添加新的角色映射策略

角色映射策略详细信息

描述:

默认规则: [Other]

规则评估算法: evaluate-all

	条件	角色
1.	(Authorization:[Endpoints Repository]:Unique-Device-Count EXISTS) AND (Authorization:[Time Source]:Now DT LESS_THAN %{Endpoint:MAC-Auth Expiry})	[MAC Caching]
2.	(Endpoint:Guest Role ID EQUALS 1)	[Contractor]
3.	(Endpoint:Guest Role ID EQUALS 2)	[Guest]
4.	(Endpoint:Guest Role ID EQUALS 3)	[Employee]


配置 » 服务 » 编辑 - Meraki-Wireless-MAC Authentication

服务 - Meraki-Wireless-MAC Authentication

摘要 | 服务 | 身份验证 | 授权 | 角色 | 强制 | 记帐代理

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: Meraki-Wireless-MAC Authentication Enforcement Policy 修改 添加新的强制策略

强制策略详细信息

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 MATCHES_ALL [User Authenticated] [MAC Caching])	[Allow Access Profile]
2.	(Tips:Role MATCHES_ANY [Other] [Contractor] [Employee] [Guest])	Meraki-Wireless-Redirect

b. Meraki-Wireless-CaptivePortal-Webauth


配置 » 服务 » 编辑 - Meraki-Wireless-CaptivePortal-Webauth

服务 - Meraki-Wireless-CaptivePortal-Webauth

摘要 | 服务 | 身份验证 | 授权 | 角色 | 强制

服务:

名称: Meraki-Wireless-CaptivePortal-Webauth

描述:

类型: 基于 Web 的身份验证

状态: Enabled

监视模式: Disabled

更多选项: 授权

服务规则

匹配以下任何条件:

	类型	名称	运算符	值
1.	Host	CheckType	MATCHES_ANY	Authentication

身份验证:

身份验证源: [Guest User Repository] [Local SQL DB]

去除用户名规则: -

授权:

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

角色:

角色映射策略: YST-Guest User Authentication with MAC Caching Role Mapping

强制:

使用缓存的结果: Disabled

强制策略: Meraki-Wireless-Webauth


配置 » 服务 » 编辑 - Meraki-Wireless-CaptivePortal-Webauth

服务 - Meraki-Wireless-CaptivePortal-Webauth

摘要 | 服务 | 身份验证 | 授权 | 角色 | 强制

名称: Meraki-Wireless-CaptivePortal-Webauth

描述:

类型: 基于 Web 的身份验证

状态: Enabled

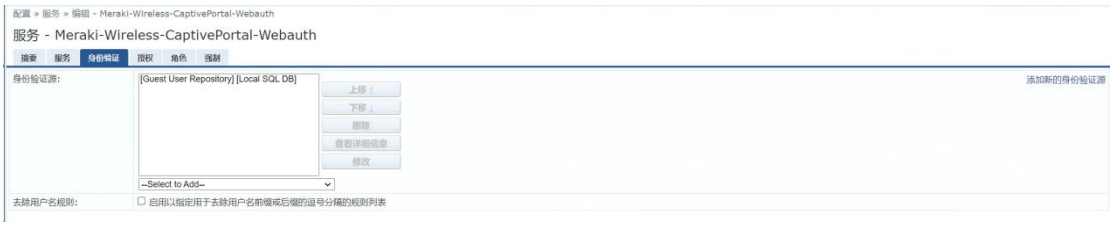
监视模式: 启用以监视无强制的网络访问

更多选项: 授权 状况合规性

服务规则

匹配 任何或 以下所有条件:

	类型	名称	运算符	值
1.	Host	CheckType	MATCHES_ANY	Authentication
2.	Click to add...			


配置 » 服务 » 编辑 - Meraki-Wireless-CaptivePortal-Webauth

服务 - Meraki-Wireless-CaptivePortal-Webauth

摘要 | 服务 | 身份验证 | 授权 | 角色 | 强制

身份验证源: [Guest User Repository] [Local SQL DB]

上移 | 下移 | 删除 | 查看详细信息 | 修改

--Select to Add--

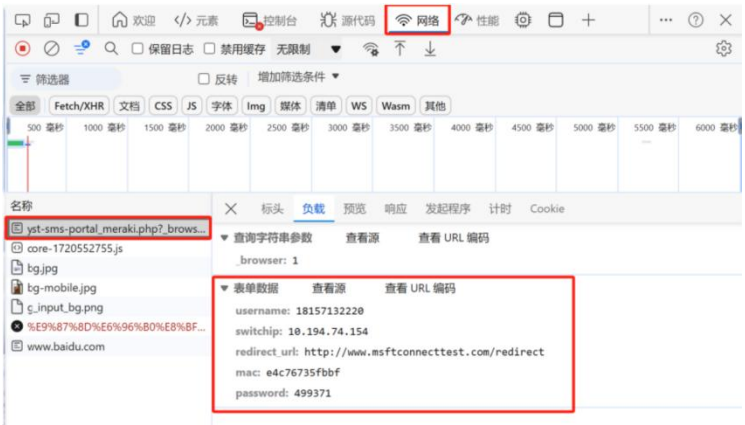
添加新的身份验证源

去除用户名规则: 启用以指定用于去除用户名前缀或后缀的逗号分隔的规则列表

第三章 ClearPass Guest 设置

由于 Meraki 不支持 Post 的方式提交表单，来做 Portal 认证。目前测试下来 Meraki 支持 MAC+WEBAuth 的方式认证。
WEBAuth 表单提交的是给 Clearpass 的，Clearpass 内置 Portal Html 字段都已经配置在内，因此无需定制开发，但是，如果客户想自定义 Portal 需要我们自己写 Html 脚本。

如何找到需要的字段呢？
ClearPass Guest 内置 Portal 是已经可以认证的界面，因此我们只需要抓取内置 Portal 的交互就可以。

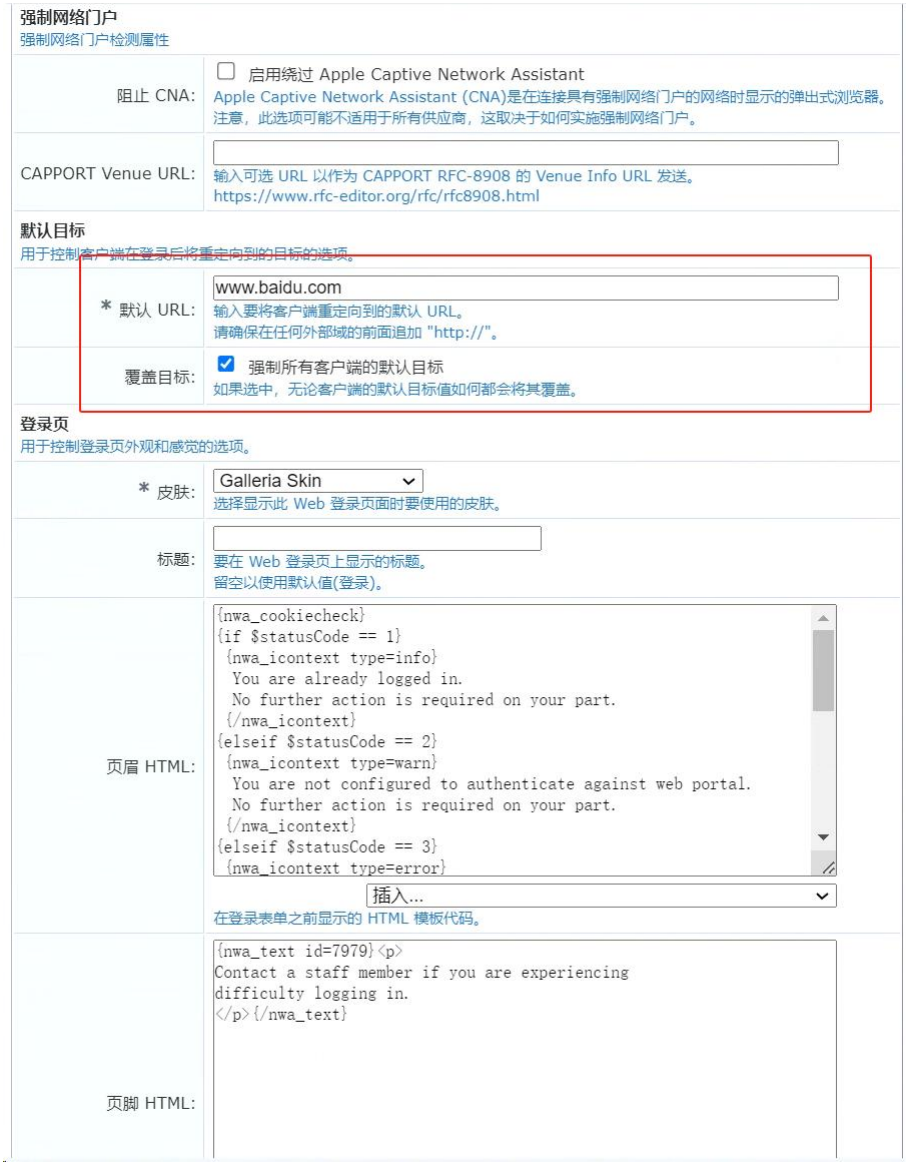


打开浏览器开发者模式，打开 Portal 页面提交一次正常的认证，就可以看到内置 Portal 提交了哪些数据上去。后续提交给开发就可以把这个界面做出来。

1) ClearPass Guest 内置 Portal

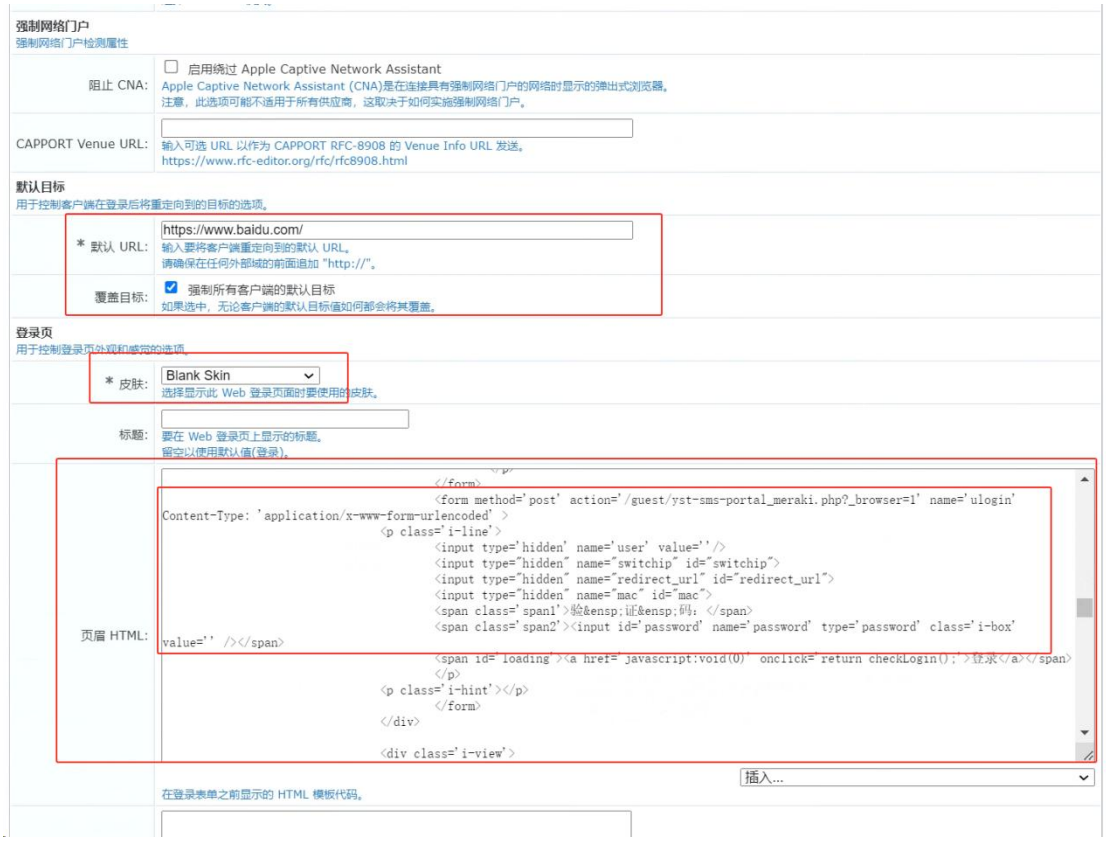
创建一个新的“WEB 登入”页面，随意命名。红色框部分需要注意，按照 Meraki 无线要求调整。

重定向必须配置，但是 URL 可以随意填写



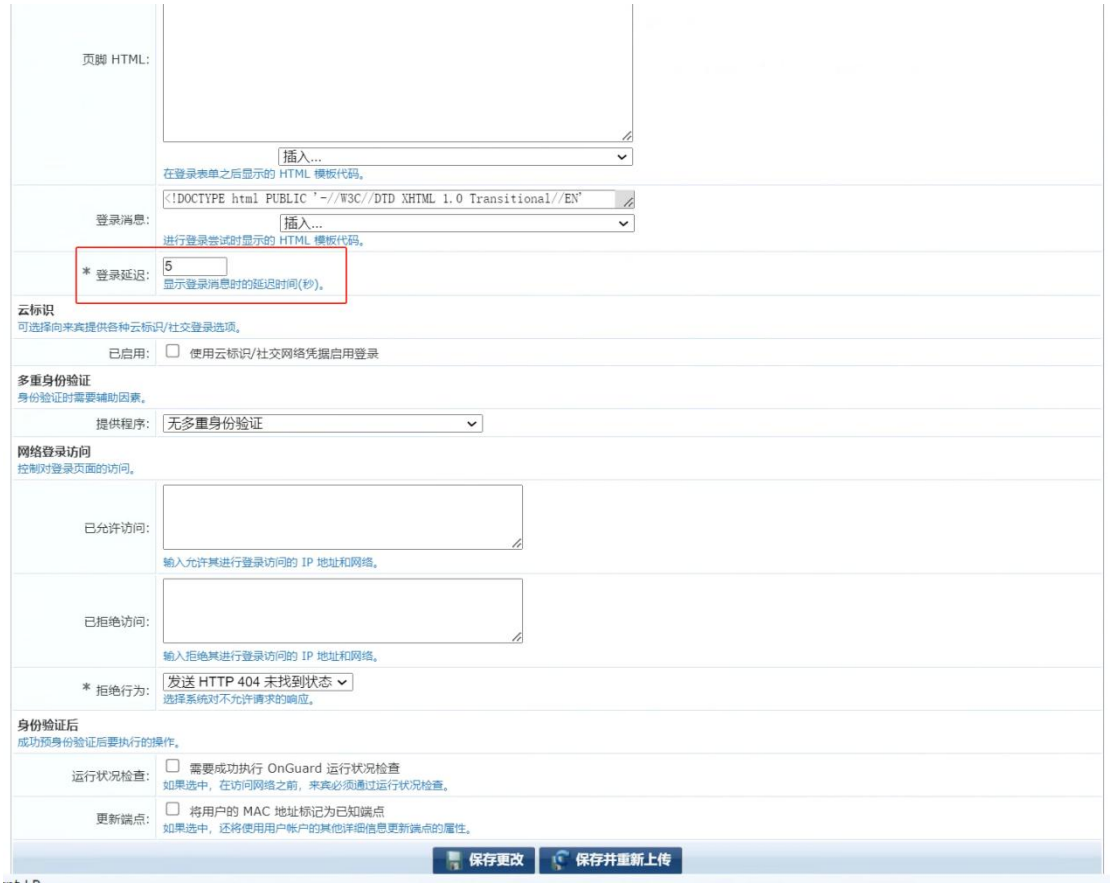
这个登入延迟必须写，建议 5 秒以上。

2) ClearPass Guest 自定义 Portal



Post　动作指回到自己登入页面即可。

Input 字符还需要通过 html 函数把实际客户端提交的参数填写进去，因此，最好需要网页开发的人员配合实施。



第四章 Mac+WebAuth 流程

初次连接：

新客户端接入时，首先进行 MAC 认证。

获取 Portal 指令：

完成 MAC 认证后，客户端会接收到弹出 Portal 的指令，提示用户填写账号密码。

提交数据到 ClearPass：

用户在 Portal 中填写账号密码后，数据会提交至 ClearPass 进行身份验证。

验证成功：

ClearPass 会将客户端的认证信息缓存，同时踢下线客户端（COA），使其重新进行认证。

重新认证：

客户端可能不会自动关联到原有的 SSID。此时，用户需要手动选择 SSID 重新连接。客户端此时会再次进行 MAC 认证，但由于已有 MAC 地址缓存，认证会直接通过。

缓存失效：

如果 MAC 地址缓存过期，客户端将重新获取到弹出 Portal 的策略，再次进行 Portal 认证。