

Aruba Clearpass 与 Meraki AP 结合 实现 Web 认证

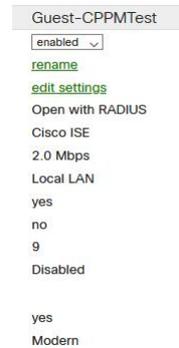
目录

目录

| | |
|---------------------------------------|----|
| 第一章 Meraki 设置（摘取自网络） | 3 |
| 第二章 ClearPass Policy Manager 设置 | 7 |
| 第三章 ClearPass Guest 设置 | 12 |
| 第四章 Mac+WebAuth 流程 | 18 |

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:

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
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
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 | <input type="text" value="REDACTED"/> | 1812 | <input type="text" value="REDACTED"/> | <input type="button" value="🔊"/> <input type="button" value="↕"/> <input type="button" value="✕"/> <input type="button" value="Test"/> |
| 2 | <input type="text" value="REDACTED"/> | 1812 | <input type="text" value="REDACTED"/> | <input type="button" value="🔊"/> <input type="button" value="↕"/> <input type="button" value="✕"/> <input type="button" value="Test"/> |

[Add a server](#)

RADIUS testing ⓘ

RADIUS CoA support ⓘ

RADIUS attribute specifying group policy name ⓘ

RADIUS accounting

RADIUS accounting servers

| # | Host | Port | Secret | Actions |
|---|---------------------------------------|------|---------------------------------------|--|
| 1 | <input type="text" value="REDACTED"/> | 1813 | <input type="text" value="REDACTED"/> | <input type="button" value="🔊"/> <input type="button" value="↕"/> <input type="button" value="✕"/> |
| 2 | <input type="text" value="REDACTED"/> | 1813 | <input type="text" value="REDACTED"/> | <input type="button" value="🔊"/> <input type="button" value="↕"/> <input type="button" value="✕"/> |

[Add a server](#)

RADIUS proxy ⓘ

Assign group policies by device type ⓘ

Walled garden ⓘ

Walled garden ranges

[What do I enter here?](#)

Addressing and traffic

Client IP assignment

NAT mode: Use Meraki DHCP

Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the [SSID firewall settings](#) permit.

Bridge mode: Make clients part of the LAN

Meraki devices operate transparently (no NAT or DHCP). Wireless clients will receive DHCP leases from a server on the LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, file sharing, and wireless cameras.

Layer 3 roaming

Clients receive DHCP leases from the LAN or use static IPs, similar to bridge mode. If the client roams to an AP where their original IP subnet is not available, then the client's traffic will be forwarded to an anchor AP on their original subnet. This allows the client to keep the same IP address, even when traversing IP subnet boundaries.

Layer 3 roaming with a concentrator

Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.

VPN: tunnel data to a concentrator

Meraki devices send traffic over a secure tunnel to an MX concentrator.

Note: VPN and Layer 3 roaming with concentrator require an MX. [Add an MX](#) to use them.

VLAN tagging

Bridge mode and layer 3 roaming only

Use VLAN tagging

VLAN ID

AP tags VLAN ID Actions

All other APs 9

[Add VLAN](#)

RADIUS override

NAT mode only

Ignore VLAN attribute in RADIUS responses

Content filtering

NAT mode only

Don't filter content

Bonjour forwarding

Bridge mode and layer 3 roaming only

Disable Bonjour Forwarding

Mandatory DHCP

Enable Mandatory DHCP

Wireless options



Band selection and minimum bitrate settings may be overridden by RF profiles.

[Go to RF Profiles](#)

Band selection

Dual band operation (2.4 GHz and 5 GHz)

5 GHz band only

5 GHz has more capacity and less interference than 2.4 GHz, but legacy clients are not capable of using it.

Dual band operation with Band Steering

Band Steering detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients.

Minimum bitrate (Mbps)



Lower Density

Higher Density



[Save Changes](#) or [cancel](#)

(Please allow 1-2 minutes for changes to take effect)

(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）

Firewall & traffic shaping

SSID:

Block IPs and ports

Layer 2 LAN isolation (bridge mode only)

Layer 3 firewall rules ⓘ

| # | Policy | Protocol | Destination | Port | Comment | Actions |
|---|-----------------------------------|----------|-------------|------|--------------------------------|---------|
| | <input type="text" value="Deny"/> | Any | Local LAN | Any | Wireless clients accessing LAN | |
| | Allow | Any | Any | Any | Default rule | |

[Add a layer 3 firewall rule](#)

Block applications and content categories

Layer 7 firewall rules
[Add a layer 7 firewall rule](#)

DNS layer protection
(Cisco Umbrella)

Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.

Traffic shaping rules

Per-client bandwidth limit [details](#) Enable SpeedBurst ⓘ

Per-SSID bandwidth limit ⓘ [details](#)

Shape traffic

(4) 对于 Splash 页面，这将显示为灰色。你将无法改变任何事情

Splash page

SSID:

Splash pages on this SSID are disabled because this SSID is configured to dynamically redirect users based on the authorization profile and captive portal configuration on the Cisco ISE server. You can change this setting on the [access control subtab](#).

Official themes ⓘ

- Modern NEW
- Fluid

Custom themes ⓘ

- 
 - 
 - Copy of Modern
- [Create something new](#)

Custom splash URL

Or provide a URL where users will be redirected: 

[What is this?](#)

Customize your page

(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

- 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。
- 可以设置 Employee 和 Contractor 角色。与 ClearPass 上 Role 配合，本功能未测试。

Group policies

| Name | Affecting | Bandwidth | VLAN | Splash | Bonjour | Traffic | Actions |
|------------|-----------|-----------|--------|---------|---------|---------|---------|
| Employee | 1 clients | Default | VLAN 9 | Default | Default | Default | Clone x |
| Contractor | 0 clients | Default | VLAN 9 | Default | Default | Default | Clone x |

[Add a group](#)

© 2020 Cisco Systems, Inc. Last login: 3 days ago from your current IP address
Privacy - Terms Current session started: 5 minutes ago
Data for this organization is hosted in North America

[Make a wish](#)

第二章 ClearPass Policy Manager 设置

- 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。
- 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。

| | | | | | | | |
|----|--------------------------|---|---------------------------------------|---------|--------------|------|---|
| 5. | <input type="checkbox"/> | 5 | Meraki-Wireless-MAC Authentication | RADIUS | MAC 身份验证 | 2667 | ✓ |
| 6. | <input type="checkbox"/> | 6 | Meraki-Wireless-CaptivePortal-Webauth | WEBAUTH | 基于 Web 的身份验证 | 13 | ✓ |

- 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

Enforcement Profiles - TEST-Meraki-Wireless-Employee Device Profile

Note: This Enforcement Profile is created by Service Template

| Summary | | | | |
|--------------------|--|-----------------|-------|----------------------|
| Profile | | | | |
| Attributes | | | | |
| Profile: | | | | |
| Name: | TEST-Meraki-Wireless-Employee Device Profile | | | |
| Description: | Role/VLAN enforcement for Employee | | | |
| Type: | RADIUS | | | |
| Action: | Accept | | | |
| Device Group List: | - | | | |
| Attributes: | | | | |
| Type | Name | | Value | |
| 1. | Radius:Aruba | Aruba-User-Role | = | Employee |
| 2. | Radius:IETF | User-Name | = | %{Endpoint:Username} |

- 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://<ClearPassURL or IP>/guest/<Guest-Page>.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-IP-Address}&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。

配置 > 强制 > 策略

强制策略

ClearPass 通过评估与服务器关联的强制策略来控制网络访问。

添加
导入
全部导出

筛选器: 名称 [包含] mer [执行] [清除筛选器] 显示 20 [记录]

| # | 名称 | 类型 | 描述 |
|----|--|---------|----|
| 1. | <input type="checkbox"/> Meraki-Wireless-MAC Authentication Enforcement Policy | RADIUS | |
| 2. | <input type="checkbox"/> Meraki-Wireless-Webauth | WEBAUTH | |

正在显示 1-2 个, 共 2 个 [复制] [导出] [删除]

配置 > 强制 > 策略 > 编辑 - Meraki-Wireless-MAC Authentication Enforcement Policy

强制策略 - Meraki-Wireless-MAC Authentication Enforcement Policy

摘要 强制 规则

强制:

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

配置 > 强制 > 策略 > 编辑 - Meraki-Wireless-Webauth

强制策略 - Meraki-Wireless-Webauth

摘要 强制 规则

强制:

名称: Meraki-Wireless-Webauth
 描述:
 强制类型: WEBAUTH
 默认配置文件: Meraki-Wireless-terminate session

规则:

规则评估算法: First applicable

| Conditions | Actions |
|---|--|
| 1. (Tips:Role EQUALS [User Authenticated]) | Meraki-Wireless-terminate session, YST-Guest Guest MAC Caching |

4) 您需要创建一个角色映射

配置 > 身份 > 角色映射 > 编辑 - YST-Guest MAC Authentication Role Mapping

角色映射 - YST-Guest MAC Authentication Role Mapping

注意: 此角色映射策略由服务模板创建

摘要 策略 映射规则

策略:

策略名称: YST-Guest MAC Authentication Role Mapping
 描述:
 默认规则: [Other]

映射规则:

规则评估算法: Evaluate all

| Conditions | Role Name |
|--|---------------|
| 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] |

5) 您需要创建两个服务

- a. Meraki-Wireless-MAC Authentication

服务 - Meraki-Wireless-MAC Authentication

摘要 服务 身份验证 授权 角色 强制 记账代理

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. 记账代理

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:ETF: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](#)

服务 - Meraki-Wireless-MAC Authentication

摘要 服务 身份验证 授权 角色 强制 记账代理

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: 启用以监视无限制的网路访问
 更多选项: 授权 审核终端主机 分析锚点 记账代理

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:ETF:User-Name) |
| 2. Connection | SSID | CONTAINS | |
| 3. | Click to add... | | |

服务 - Meraki-Wireless-MAC Authentication

摘要 服务 身份验证 授权 角色 强制 记账代理

身份验证方法: [Allow All MAC AUTH] [添加新的身份验证方法](#)

--Select to Add--

身份验证源: [Endpoints Repository] [Local SQL DB] [添加新的身份验证源](#)

--Select to Add--

去除用户名规则: 启用以指定用于去除用户名或域名后缀的逗号分隔的规则列表

服务 - Meraki-Wireless-MAC Authentication

摘要 服务 身份验证 授权 角色 强制 记账代理

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 - [添加新的身份验证源](#)

[Time Source] [Local SQL DB]

[Guest User Repository] [Local SQL DB]
 [Local User Repository] [Local SQL DB]

--Select to Add--

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

服务 - Meraki-Wireless-MAC Authentication

编辑 服务 身份验证 授权 角色 强制 记账代理

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_THANV %(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

编辑 服务 身份验证 授权 角色 强制 记账代理

使用保存的结果: 使用先前会话中保存的角色和状态属性

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]) [Tips:Role MATCHES_ANY [Other] [Contractor] [Employee] [Guest]]) | [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

编辑 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: 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]

去路用户名规则: -

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:

使用保存的结果: Disabled

强制策略: Meraki-Wireless-Webauth

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

服务 - Meraki-Wireless-CaptivePortal-Webauth

编辑 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: 启用以监视无限制的网页访问

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

编辑 服务 身份验证 授权 角色 强制

身份验证源: [Guest User Repository] [Local SQL DB] 添加新的身份验证源

去路用户名规则: 启用以指定用于去路用户名或后端的逗号分隔的规则列表



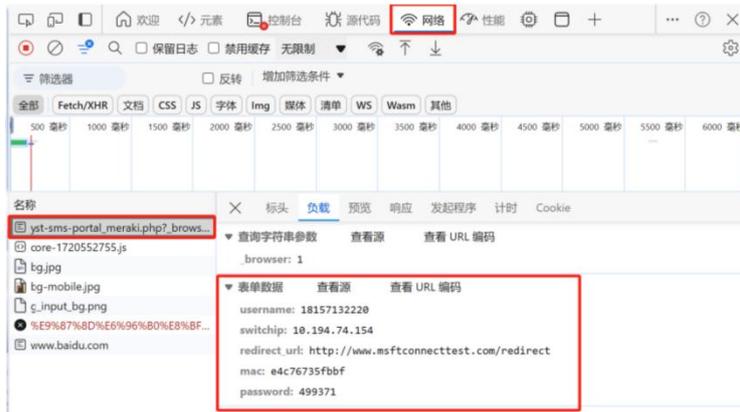
第三章 ClearPass Guest 设置

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。

主页 » 配置 » 页面 » Web 登录

Web 登录 (new)

使用此表单创建新的 Web 登录。

| Web 登录编辑器 | |
|-----------|---|
| * 名称: | Meraki-Local <small>输入此 Web 登录页面的名称。</small> |
| 页面名称: | Meraki-Local2 <small>为此 Web 登录输入页面名称。 Web 登录可从"/guest/page_name.php"进行访问。</small> |
| 描述: | <small>有关 Web 登录的注释或描述性文本。</small> |
| * 供应商设置: | Cisco Systems <small>选择一组适合标准网络配置的预定义设置。</small> |
| 登录方法: | 服务器发起 - 更改发送给控制器的权限(RFC 3576) v <small>选择如何处理用户的网络登录。 服务器发起的登录要求提供用户的 MAC 地址，通常来自于强制网络门户重定向过程。</small> |

登录表单
用于指定登录表单的行为和内容的选项。

| | |
|------------|---|
| 身份验证: | 凭据 - 需要用户名和密码 v <small>选择身份验证要求。 "访问代码"需要输入单个代码(用户名)。 "匿名"允许仅需要条款或"登录"按钮的空白表单。需要预先存在的帐户。 "自动"与"匿名"相似，但页面将自动提交。 "访问代码"和"匿名"要求帐户必须设置"用户名身份验证"字段。</small> |
| 自定义表单: | <input type="checkbox"/> 提供自定义登录表单 <small>如果选中，必须在标题或页脚 HTML 区域中提供您自己的 HTML 登录表单。</small> |
| 自定义标签: | <input type="checkbox"/> 覆盖默认标签和错误消息 <small>如果选定，您将能够更改当前登录表单的标签和错误消息。</small> |
| 用户名后缀: | <small>将登录表单提交到 NAS 之前，后缀将自动附加到用户名。</small> |
| * 身份验证前检查: | 无 - 不进行额外检查 v <small>选择在继续 NAS 身份验证之前应如何检查用户名和密码。</small> |
| 条款: | <input type="checkbox"/> 需要确认条款和条件 <small>如果选中，将会强制用户接受"条款和条件"复选框。</small> |
| CAPTCHA: | 无 v <small>选择 CAPTCHA 模式。</small> |

重定向必须配置，但是 URL 可以随意填写

| | |
|--|---|
| 强制网络门户 强制网络门户检测属性 | |
| 阻止 CNA: | <input type="checkbox"/> 启用绕过 Apple Captive Network Assistant Apple Captive Network Assistant (CNA)是在连接具有强制网络门户的网络时显示的弹出式浏览器。 注意，此选项可能不适用于所有供应商，这取决于如何实施强制网络门户。 |
| CAPPORT Venue URL: | <input type="text"/> 输入可选 URL 以作为 CAPPORT RFC-8908 的 Venue Info URL 发送。 https://www.rfc-editor.org/rfc/rfc8908.html |
| 默认目标 用于控制客户端在登录后将重定向到的目标的选项。 | |
| * 默认 URL: | <input type="text" value="www.baidu.com"/> 输入要将客户端重定向到的默认 URL。 请确保在任何外部域的前面追加 "http://"。 |
| 覆盖目标: | <input checked="" type="checkbox"/> 强制所有客户端的默认目标 如果选中，无论客户端的默认目标值如何都会将其覆盖。 |
| 登录页 用于控制登录页外观和感觉的选项。 | |
| * 皮肤: | <input type="text" value="Galleria Skin"/> 选择显示此 Web 登录页面时要使用的皮肤。 |
| 标题: | <input type="text"/> 要在 Web 登录页上显示的标题。 留空以使用默认值(登录)。 |
| 页眉 HTML: | <pre>{nwa_cookiecheck} {if \$statusCode == 1} {nwa_icontext type=info} You are already logged in. No further action is required on your part. {/nwa_icontext} {elseif \$statusCode == 2} {nwa_icontext type=warn} You are not configured to authenticate against web portal. No further action is required on your part. {/nwa_icontext} {elseif \$statusCode == 3} {nwa_icontext type=error}</pre> <input type="button" value="插入..."/> 在登录表单之前显示的 HTML 模板代码。 |
| 页脚 HTML: | <pre>{nwa_text id=7979}<p> Contact a staff member if you are experiencing difficulty logging in. </p>{/nwa_text}</pre> |

这个登入延迟必须写，建议 5 秒以上。

| | |
|--|--|
| 登录消息: | <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"><p></p> \ nwa_text;</p></div> <div style="text-align: right; margin-top: 5px;"><input type="button" value="插入..."/></div> <p style="font-size: small; color: #0070C0;">进行登录尝试时显示的 HTML 模板代码。</p> |
| * 登录延迟: | <input style="width: 50px;" type="text" value="10"/> <small>显示登录消息时的延迟时间(秒)。</small> |
| 云标识 <small>可选择向来宾提供各种云标识/社交登录选项。</small> | |
| 已启用: | <input type="checkbox"/> 使用云标识/社交网络凭据启用登录 |
| 多重身份验证 <small>身份验证时需要辅助因素。</small> | |
| 提供程序: | <input type="text" value="无多重身份验证"/> |
| 网络登录访问 <small>控制对登录页面的访问。</small> | |
| 已允许访问: | <div style="border: 1px solid #ccc; height: 30px;"></div> <p style="font-size: small; color: #0070C0;">输入允许其进行登录访问的 IP 地址和网络。</p> |
| 已拒绝访问: | <div style="border: 1px solid #ccc; height: 30px;"></div> <p style="font-size: small; color: #0070C0;">输入拒绝其进行登录访问的 IP 地址和网络。</p> |
| * 拒绝行为: | <input type="text" value="发送 HTTP 404 未找到状态"/> <small>选择系统对不允许请求的响应。</small> |
| 身份验证后 <small>成功预身份验证后要执行的操作。</small> | |
| 运行状况检查: | <input type="checkbox"/> 需要成功执行 OnGuard 运行状况检查 <small>如果选中，在访问网络之前，来宾必须通过运行状况检查。</small> |
| 更新端点: | <input type="checkbox"/> 将用户的 MAC 地址标记为已知端点 <small>如果选中，还将使用用户帐户的其他详细信息更新端点的属性。</small> |
| <input type="button" value="保存更改"/> <input type="button" value="保存并重新上传"/> | |

* 必填字段

2) ClearPass Guest 自定义 Portal

主页 » 配置 » 页面 » Web 登录

Web 登录 (yst-sms (meraki))

使用此表单更改 Web 登录 *yst-sms (meraki)*。

| Web 登录编辑器 | |
|-----------------------------------|--|
| * 名称: | <input type="text" value="yst-sms (meraki)"/> 输入此 Web 登录页面的名称。 |
| 页面名称: | <input type="text" value="yst-sms-portal_meraki"/> 为此 Web 登录输入页面名称。 Web 登录可从"/guest/page_name.php"进行访问。 |
| 描述: | <input type="text"/> 有关 Web 登录的注释或描述性文本。 |
| * 供应商设置: | <input type="text" value="Cisco Systems"/> 选择一组适合标准网络配置的预定义设置。 |
| 登录方法: | <input type="text" value="服务器发起 - 更改发送给控制器的权限(RFC 3576)"/> 选择如何处理用户的网络登录。 服务器发起的登录要求提供用户的 MAC 地址, 通常来自强制网络门户重定向过程。 |
| 登录表单 用于指定登录表单的行为和内容的选项。 | |
| 身份验证: | <input type="text" value="凭据 - 需要用户名和密码"/> 选择身份验证要求。 "访问代码"需要输入单个代码(用户名)。 "匿名"允许仅需要条款或"登录"按钮的空白表单。需要预先存在的帐户。 "自动"与"匿名"相似, 但页面将自动提交。 "访问代码"和"匿名"要求帐户必须设置"用户名身份验证"字段。 |
| 自定义表单: | <input checked="" type="checkbox"/> 提供自定义登录表单 如果选中, 必须在标头或页脚 HTML 区域中提供您自己的 HTML 登录表单。 |
| 自定义标签: | <input type="checkbox"/> 覆盖默认标签和错误消息 如果选中, 您将能够更改当前登录表单的标签和错误消息。 |
| 用户名后缀: | <input type="text"/> 将登录表单提交到 NAS 之前, 后缀将自动附加到用户名。 |
| * 身份验证前检查: | <input type="text" value="无 - 不进行额外检查"/> 选择在继续 NAS 身份验证之前应如何检查用户名和密码。 |
| 条款: | <input type="checkbox"/> 需要确认条款和条件 如果选中, 将会强制用户接受"条款和条件"复选框。 |
| CAPTCHA: | <input type="text" value="无"/> 选择 CAPTCHA 模式。 |
| 强制网络门户 强制网络门户检测属性 | |

next ID

| | |
|--|--|
| 强制网络门户 强制网络门户检测属性 | |
| 阻止 CNA: | <input type="checkbox"/> 启用绕过 Apple Captive Network Assistant Apple Captive Network Assistant (CNA)是在连接具有强制网络门户的网络时显示的弹出式浏览器。 注意, 此选项可能不适用于所有供应商, 这取决于如何实施强制网络门户。 |
| CAPPORT Venue URL: | 输入可选 URL 以作为 CAPPORT RFC-8908 的 Venue Info URL 发送。 https://www.rfc-editor.org/rfc/rfc8908.html |
| 默认目标 用于控制客户端在登录后将重定向到的目标选项。 | |
| * 默认 URL: | <input type="text" value="https://www.baidu.com"/> 输入要将客户端重定向到的默认 URL。 请确保在任何外部域的前面添加 "http://", |
| 覆盖目标: | <input checked="" type="checkbox"/> 强制所有客户端的默认目标 如果选中, 无论客户端的默认目标值如何都会将其覆盖。 |
| 登录页 用于控制登录页外观和感知的选项。 | |
| * 皮肤: | <input type="text" value="Blank Skin"/> 选择显示此 Web 登录页面时要使用的皮肤。 |
| 标题: | <input type="text"/> 要在 Web 登录页上显示的标题。 留空以使用默认值(登录)。 |
| 页脚 HTML: | <pre></form> <form method='post' action='/guest/yst-sms-portal_meraki.php?_browser=' name='ulogin' Content-Type: 'application/x-www-form-urlencoded' > <p class='i-line'> <input type='hidden' name='user' value=''/> <input type='hidden' name='switchip' id='switchip'> <input type='hidden' name='redirect_url' id='redirect_url'> <input type='hidden' name='mac' id='mac'> 验证码: <input id='password' name='password' type='password' class='i-box' value=' ' /> 登录 </p> <p class='i-hint'></p> </form> </div> <div class='i-view'></pre> |
| 在登录表单之前显示的 HTML 模板代码。 <input type="button" value="插入..."/> | |

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。

| | |
|--|---|
| 页脚 HTML: | <input type="text"/> <input type="button" value="插入..."/> 在登录表单之后显示的 HTML 模板代码。 |
| 登录消息: | <input type="text" value="<!DOCTYPE html PUBLIC '-//W3C//DTD XHTML 1.0 Transitional//EN'"/> <input type="button" value="插入..."/> 进行登录尝试时显示的 HTML 模板代码。 |
| * 登录延迟: | <input type="text" value="5"/> 显示登录消息时的延迟时间(秒)。 |
| 云标识 可选择向来宾提供各种云标识/社交登录选项。 | |
| 已启用: | <input type="checkbox"/> 使用云标识/社交网络凭据启用登录 |
| 多重身份验证 身份验证时需要辅助因素。 | |
| 提供程序: | <input type="text" value="无多重身份验证"/> |
| 网络登录访问 控制对登录页面的访问。 | |
| 已允许访问: | <input type="text"/> 输入允许其进行登录访问的 IP 地址和网络。 |
| 已拒绝访问: | <input type="text"/> 输入拒绝其进行登录访问的 IP 地址和网络。 |
| * 拒绝行为: | <input type="text" value="发送 HTTP 404 未找到状态"/> 选择系统对不允许请求的响应。 |
| 身份验证后 成功预身份验证后要执行的操作。 | |
| 运行状况检查: | <input type="checkbox"/> 需要成功执行 OnGuard 运行状况检查 如果选中, 在访问网络之前, 来宾必须通过运行状况检查。 |
| 更新端点: | <input type="checkbox"/> 将用户的 MAC 地址标记为已知端点 如果选中, 还将使用用户帐户的其他详细信息更新端点的属性。 |
| <input type="button" value="保存更改"/> <input type="button" value="保存并重新上传"/> | |

第四章 Mac+WebAuth 流程

初次连接:

新客户接入时，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。