

# ClearPass 通过 AD userDN 属性实现 802.1x 认证准入

## 需求：

- 需通过 WLAN 对接 AD 实现 802.1X PEAP 认证，同时要限制 AD 中不同部门的准入，以及每个账号登陆设备的数量。

## 实现思路：

- ClearPass 的 Policy 可以通过 Authorization : AD userDN “xxx” 并返回给无线控制器准入信息。
- 通过 Profile 中 Post\_Authentication 返回无线控制器 Active-Session-Count=2
- 不使用 clearpass role-mapping 功能，某些客户对于 role-mapping 的配置逻辑理解不够深入

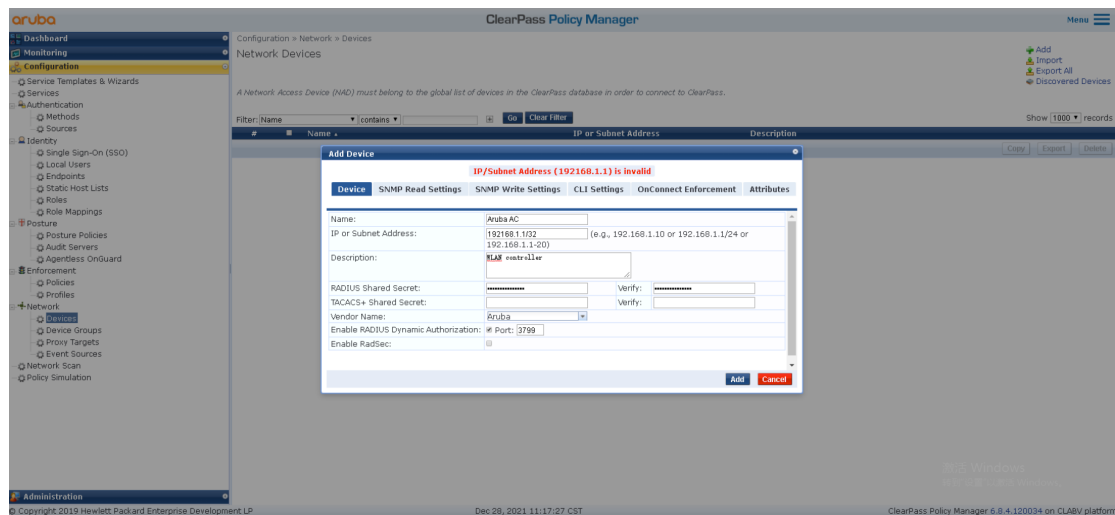
## 1. ClearPass 中添加 Devices

配置路径：

configuration - Network - Devices - Add

说明：

- **Name**：ARUBA AC
- **IP or Subnet Address**:填写无线控制器的 IP，如有多台可多次添加或添加一个网段
- **RADIUS Shared Secret**：需要在 Aruba 无线控制器和 ClearPass 保持一致的密钥
- **Vendor Name**：选择 Aruba
- **Enable RADIUS Dynamic Authorization**：开启
- **SAVE**



添加完成如下：



## 2. 创建 Authentication Sources

配置路径：

Configuration - Authentication - Sources - Add

说明：

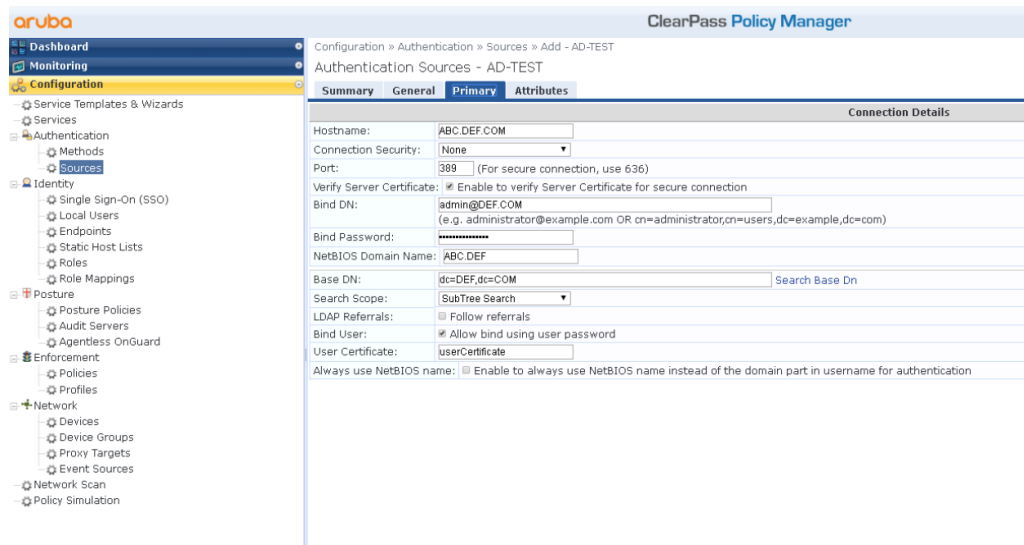
- **Name**：填写设备名称或自己方便记忆的标识
- **Description**：填写描述/备注信息
- **Type**：选择 Active Directory
- **Use for Authorization**:勾选 (Enable to use this Authentication Source to also fetch role mapping attributes)
- **Authorization Sources**:如果有除了当前 AD 以外的其他 Authorization Sources, 可以填写, 反之则无
- **Server Timeout**：10s
- **Cache timeout**：36000s, 建议修改为 180s

The screenshot shows the Aruba ClearPass Policy Manager web interface. The left sidebar contains a navigation menu with categories like Dashboard, Monitoring, Configuration, Services, Authentication, Identity, Posture, Enforcement, and Network. The main content area is titled 'ClearPass Policy Manager' and shows the configuration for 'Authentication Sources - AD-TEST'. The configuration is divided into tabs: Summary, General, Primary, and Attributes. The 'General' tab is active, showing fields for Name (AD-TEST), Description, Type (Active Directory), Use for Authorization (checked), Authorization Sources (a dropdown menu), Server Timeout (10 seconds), Cache Timeout (180 seconds), and Backup Servers Priority (a list with Move Up and Move Down buttons). There are also buttons for Add Backup and Remove.

## 2.1. AD 域控服务器信息

说明：

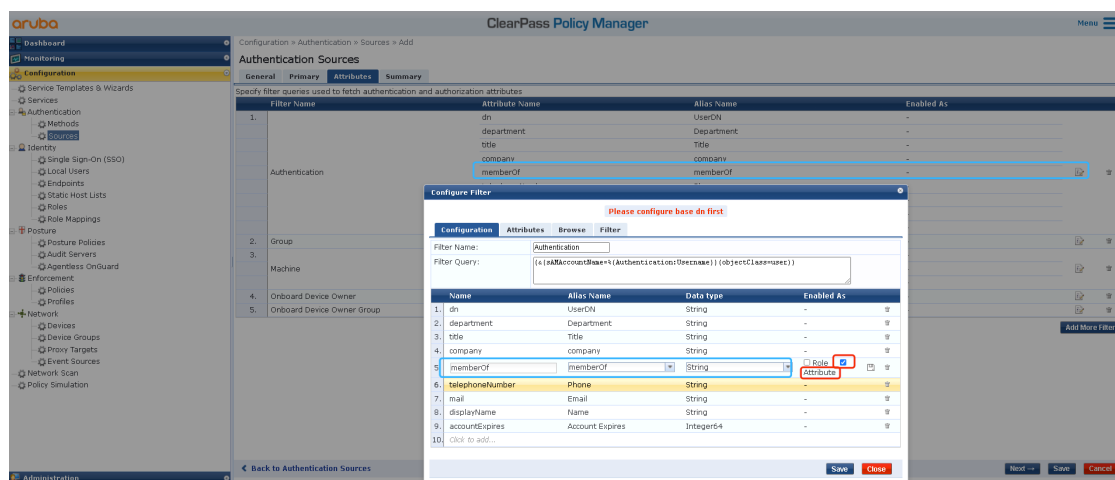
- 在填写完 Bind DN 与 Bind Password 后，可以点击右侧 Search Base Dn，如果可以检索出 OU，则填写的信息可以使用。
- 其他参数保持默认即可
- SAVE



## 2.2. Authentication Sources -AD Attributes

说明：此处勾选 memberOf，用于后续通过 AD 中这个属性作为授权使用

SAVE



## 3. Profile 配置

### 3.1. Return Aruba-User-Role Profile 配置

配置路径：

Configuration - Enforcement - Profiles - Add

参数配置：

- **Template:** Aruba RADIUS Enforcement
- **Name:** Return Aruba User Role
- **Description:** 描述/备注
- **Action :** Accept
- **Service Attributes:** (此条 rule 用于返回给 Aruba 无线控制器，因此 **EMPLOYEE** 仅被 Aruba 无线控制器识别)
  - Type : RADIUS : Aruba、Name : Aruba-User-Role、Value : **EMPLOYEE** (大小写需要与 Aruba Controller 一致)

SAVE

The screenshot shows the 'ClearPass Policy Manager' interface. The breadcrumb navigation is 'Configuration > Enforcement > Profiles > Edit Enforcement Profile - Return Aruba User Role'. The page title is 'Enforcement Profiles - Return Aruba User Role'. The 'Attributes' tab is active, displaying a table with one attribute:

Type	Name	Value
1. RADIUS:Aruba	Aruba-User-Role	EMPLOYEE

The 'Value' field for the attribute is highlighted with a blue box. At the bottom right, there are 'Copy', 'Save', and 'Cancel' buttons. The footer shows '© Copyright 2019 Hewlett-Packard Enterprise Development LP', 'Dec 28, 2021 12:28:53 CST', and 'ClearPass Policy Manager 6.8.4.120034 on CLABV platform'.

## 3.2. Enforcement Profiles – Device Count Profile 配置

配置路径：

Configuration -Enforcement -Profiles -Add

参数配置：

- **Template:** Session Restrictions Enforcement
- **Name:** Device Count Profile
- **Description:** 描述/备注
- **Type :** Post\_Authentication (无法变更)
- **Action :** accept (无法变更)
- **Service Attributes:**
  - **Type :** Session-Check、**Name :** Active-Session-Count、**Value :** 2

SAVE

The screenshot shows the 'ClearPass Policy Manager' interface. The left sidebar contains a navigation tree with categories like Dashboard, Monitoring, Configuration, Services, Authentication, Identity, Posture, Enforcement, and Network. The 'Enforcement' section is expanded to show 'Profiles'. The main content area displays the configuration for an 'Enforcement Profile - Device Count Profile'. It includes fields for Name, Description, Type, and Action. Below these fields is a table for 'Attributes' with the following data:

Type	Name	Value
1.	Session-Check	Active-Session-Count
		2

At the bottom of the interface, there are buttons for 'Back to Enforcement Profiles', 'Copy', 'Save', and 'Cancel'. A Windows activation watermark is visible in the bottom right corner.

TIPS:

以上创建的 2 条 Profile，需要同时调用在 Policies 一个 rule 中使用；  
针对不同的 Role (Aruba Controller Role) 需要写多条 Profile rule.

## 4. Policies 配置

配置路径：

Configuration - Enforcement - Policies - Add

参数配置：

- **Enforcement:**
  - **Name:** ARUBA-WLAN-802.1X
  - **Description:**
  - **Enforcement Type:** 勾选 RADIUS
  - **Default Profile:** OTHER DENY
- **Rules:** (同理写 rule 1-3)
  - **Rules Evaluation Algorithm:** Select first match
  - **Enforcement Policy Rules:**
    - 1、 Type : Authorization:GM-AD、 Name : UserDN、 Operator : CONTAINS、  
VALUE: OU=MOS,DC=MOS,DC=COM
    - 2、 Type : Tips、 Name : Role、 Operator : EXISTS
    - 3、 **Enforcement Profiles (调用 3.1、 3.2) :**
      - 3.1. Return Aruba User Role
      - 3.2. Device Count Profile
    - 4、 SAVE

The screenshot shows the 'ClearPass Policy Manager' interface. The main content area is titled '服务 - GoerMicro\_Service'. It displays configuration details for an enforcement policy named 'GM-EMPLOYEE-Enforcement-Policy'. The policy is described as 'Goermicro 最新策略' and has a default profile of 'OTHER DENY'. The policy rules are defined as follows:

条件	强制配置文件
1. (Authorization:GM-AD:UserDN CONTAINS OU=RE.A,OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS)	OTHER DENY
2. (Authorization:GM-AD:UserDN CONTAINS OU=Computers,OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS)	OTHER DENY
3. (Authorization:GM-AD:UserDN CONTAINS OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS)	GM-Employee-Profile; Device Count Profile

The interface also shows a left-hand navigation menu with options like '仪表盘', '配置', '身份验证', '策略', etc. At the bottom, there are buttons for '禁用', '复制', and '保存'.



## 5. Services 配置

配置路径：

Configuration -Services -Add

参数模板关联配置：

- **Service :**

**Type:** Aruba 802.1X Wireless

**Name:** ----Aruba WLAN 802.1X----

**Description:** Aruba 802.1X Wireless Access Service

**Service Rule:**

Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:			
Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Radius:Aruba	Aruba-Essid-Name	EQUALS ABC
4.	Click to add...		

- **Authentication:**

**Authentication Sources:**选择以添加的认证源 AD “GM-AD”

- **Authorization:**

Additional authorization sources from which to fetch role-mapping attributes –

[GM-AD \[Active Dictory\]](#)

- **Roles :** 空

- **Enforcement:**

**Enforcement Policy:** “ARUBA-WLAN-802.1X”

- **SAVE**

下图为实验环境模拟，请忽略 AD-TEST (同 GM-AD)

The screenshot shows the 'ClearPass Policy Manager' configuration interface. The left sidebar contains a navigation tree with categories like Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'ClearPass Policy Manager' and shows the configuration for a service named 'Aruba WLAN 802.1X'. The configuration is divided into several tabs: Summary, Service, Authentication, Authorization, Roles, and Enforcement. The 'Service' tab is active, showing details such as Name, Description, Type, Status, Monitor Mode, and More Options. Below this, there is a 'Service Rule' section with a table of conditions. The 'Authentication' section lists authentication methods and sources. The 'Authorization' section shows authorization details and roles. The 'Enforcement' section indicates that 'Use Cached Results' is disabled and the 'Enforcement Policy' is 'ARUBA-WLAN-802.1X'. At the bottom, there are buttons for 'Disable', 'Copy', 'Save', and 'Cancel', and a 'Windows' activation watermark.

## 6. ClearPass 开启 RADIUS ACCOUNTING

配置路径：

Administration – Server Manager – 选择配置的这台 CPPM – Service Parameters –

Select Service : RADIUS SERVER

Accounting Log Accounting Interim-Update Packets : **TRUE**

The screenshot shows the 'ClearPass Policy Manager' 'Service Parameters' configuration page for a 'Radius server'. The left sidebar shows the navigation tree, and the main content area is titled 'Service Configuration - Lab1-CPPM-1'. The 'Service Parameters' tab is active, showing a table of parameters for the selected service. The 'Accounting' section is highlighted, and the 'Log Accounting Interim-Update Packets' parameter is set to 'TRUE'. Other parameters include EAP-FAST, Proxy, Thread-Pool, AD Errors, Security, and Main. At the bottom, there are buttons for 'Save' and 'Cancel', and a 'Windows' activation watermark.

Parameter Name	Parameter Value	Default Value	Allowed Values
<b>EAP-FAST</b>			
Master Key Expire Time	1 weeks	1 weeks	
Master Key Grace Time	3 weeks	3 weeks	
PA-Cs are valid across cluster	TRUE	TRUE	
<b>Proxy</b>			
Maximum Response Delay	5 seconds	5	1-5
Maximum Reconnection Time	120 seconds	120	60-3600
Maximum Retry Counts	5 retries	5	2-10
<b>Accounting</b>			
Log Accounting Interim-Update Packets	TRUE	FALSE	
<b>Thread-Pool</b>			
Maximum Number of Threads	20 threads	20	10-300
Number of Initial Threads	10 threads	10	5-300
<b>AD Errors</b>			
Window Size	5 minutes	5	1-60
Number of Errors	150	150	10-1000
Recovery Action	None	None	
<b>Security</b>			
Reject Packet Delay	1 seconds	1	0-5
Maximum Attributes	200 attributes	200	0-512
Process Server-Status Request	FALSE	FALSE	
<b>Main</b>			
Authentication Port	1812, 1645	1812, 1645	
Accounting Port	1813, 1646	1813, 1646	
Maximum Request Time	30 seconds	30	5-120
Cleanup Time	5 seconds	5	2-10
Local DB Authentication Source Connection Count	32	32	5-150
AD/LDAP Authentication Source Connection Count	64	64	5-300
SQL DB Authentication Source Connection Count	32	32	
	0*	0*	

## 7. 无线控制器开启 ACCOUNTING

### 7.1. 修改 802.1x authentication default role & 开启 Accounting

说明：

在 ClearPass 通过 VSA (Return User Role 的方式) 返回给 Aruba 无线控制器 user-role 时，此处 AAA Profile 写的 802.1X Authentication Default Role 为 authenticated 会被 ClearPass 返回的 **EMPLOYEE** 覆盖

Role Derivation Sequence :

*VSA > SDR > UDR > Default Role.*

The screenshot shows the Aruba configuration interface for AAA Profiles. The 'AAA Profiles' tab is selected, and the profile '802.1X-AAA-PRO' is highlighted. The configuration details for this profile are shown on the right:

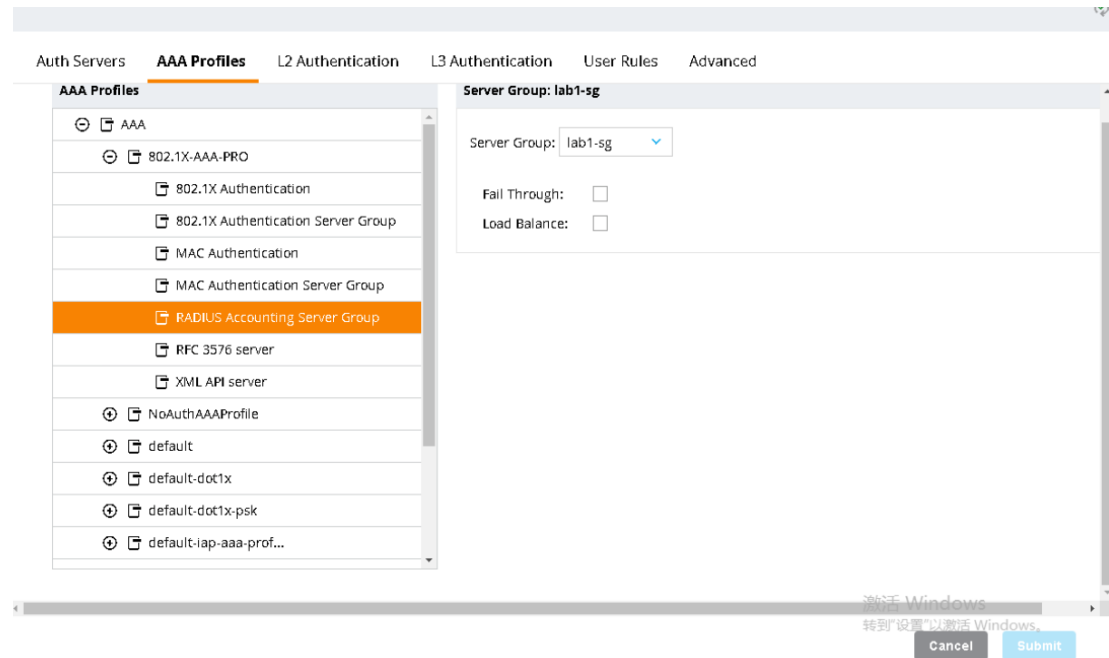
- Initial role: logon
- MAC Authentication Default Role: guest
- 802.1X Authentication Default Role: authenticated** (highlighted with a blue box)
- Download Role from CPPM:
- Set username from dhcp option 12:
- L2 Authentication Fail Through:
- Multiple Server Accounting:
- User idle timeout: [ ] seconds
- Max IPv4 for wireless user: 2
- RADIUS Roaming Accounting:
- RADIUS Interim Accounting:**  (highlighted with a blue box)
- RADIUS Acct-Session-Id In Access-Request:
- User derivation rules: -None-
- Wired to Wireless Roaming:
- Reauthenticate wired user on VLAN change:
- Device Type Classification: [ ]

At the bottom of the interface, there are buttons for 'Cancel', 'Submit', and 'Submit As'.

## 7.2. AAA Profile 调用 RADIUS ACCOUNTING SERVER-GROUP

说明：

如不调用 RADIUS ACCOUNTING SERVER-GROUP，则 ClearPass 无法收到 Accounting 报文



## 8. 测试验证-1

**测试方法：**使用在对应 UserDN 属性值的组成员账号连接 ARUBA WLAN

**测试结果：**在 ClearPass Tracker 中查看日志信息

**测试结果说明：**

Summary -Status : AUTHEN\_STATUS\_PASS 成功通过认证 (ACCEPT)

The screenshot displays the ClearPass Policy Manager interface. A modal window titled '访问跟踪器' (Access Tracker) is open, showing details for a specific log entry. The main interface shows a list of log entries with columns for ID, IP, Service, and Status.

ID	IP	Service	Status	Request Timestamp
14	10.80.18.6	RADIUS	REJECT	2022/01/05 17:23:55
15	10.80.18.6	RADIUS	ACCEPT	2022/01/05 17:23:53
16	10.80.18.6	RADIUS	REJECT	2022/01/05 17:23:53
17	10.80.18.6	RADIUS	REJECT	2022/01/05 17:23:53

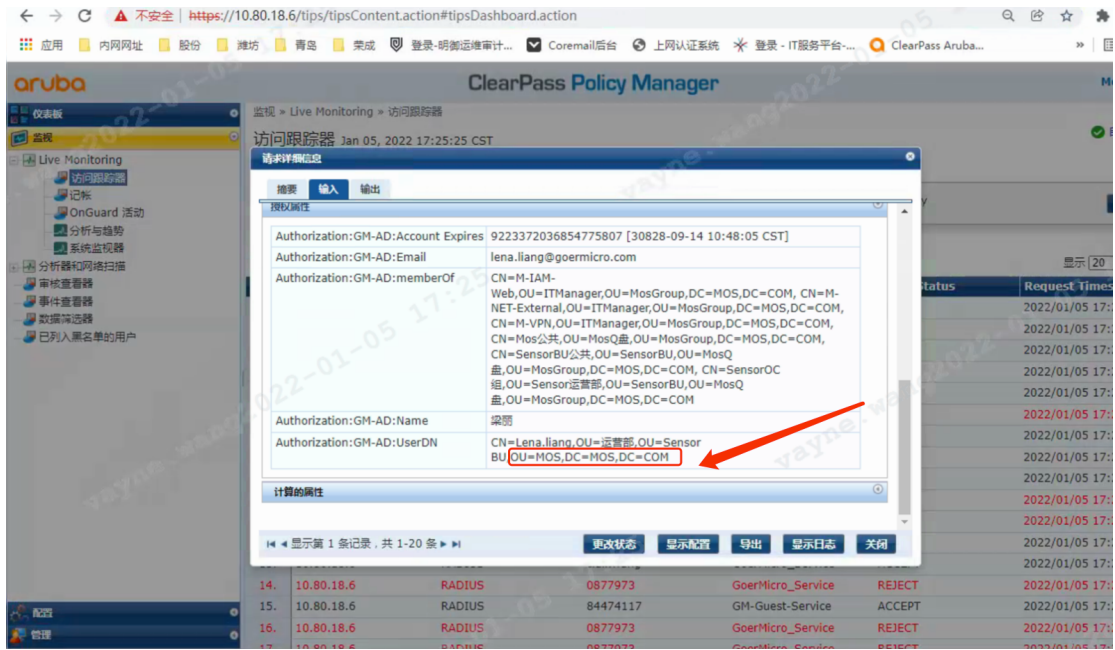
**访问跟踪器 详细详细信息**

登录状态:	ACCEPT
会话标识符:	R000c49d1-01-61d563f9
日期和时间:	Jan 05, 2022 17:25:13 CST
终端主机标识符:	38-BA-F8-10-F4-23
用户名:	lena.liang
访问设备 IP/端口:	10.80.66.19
访问设备名称:	10.80.66.17
系统状况状态:	UNKNOWN (100)

使用的策略 -

服务:	GoerMicro_Service
身份验证方法:	EAP-PEAP,EAP-MSCHAPV2
身份验证源:	AD:DC01-WF.mos.com
授权源:	GM-AD
角色:	[User Authenticated]
强制配置文件:	GM-Employee-Profile

8.1. Authorizations -Status : Pass ////获得相关权限授权



1.	(Authorization:GM-AD:UserDN CONTAINS OU=P.E.A,OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS )	OTHER DENY
2.	OU=Computers,OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS )	OTHER DENY
3.	(Authorization:GM-AD:UserDN CONTAINS OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS )	GM-Employee-Profile

## 9. 测试验证-2

**测试方法：** 使用在非对应 UserDN 属性值的组成员账号连接 ARUBA WLAN

**测试结果：** 在 ClearPass Tracker 中查看日志信息

**测试结果说明：**

**CN=it,OU=P.E.A,OU=MOS,DC=MOS,DC=COM** 匹配情况如下图所示

Rules:	
Rules Evaluation Algorithm: First applicable	
Conditions	Actions
1. (Authorization:AD-TEST-UserDN CONTAINS OU=P.E.A,OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS )	[Deny Access Profile]
2. (Authorization:AD-TEST-UserDN CONTAINS OU=Computers,OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS )	[Deny Access Profile]
3. (Authorization:AD-TEST-UserDN CONTAINS OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS )	Device Count Profile, Return Aruba User Role

### 9.1. 使用 Rule 1 对应的 OU，获取 Deny Access Profile 的权限

- 登陆状态：**REJECT**  
强制配置文件：“**OTHER DENY**”

请求详细信息

摘要 输入 输出 警报

登录状态:	REJECT
会话标识符:	R000b7e65-01-61c80a6e
日期和时间:	Dec 26, 2021 14:23:43 CST
终端主机标识符:	E4- (Computer / Windows / Windows)
用户名:	it
访问设备 IP/端口:	10. ( )
访问设备名称:	10. ( )
系统状况状态:	UNKNOWN (100)
使用的策略 -	
服务:	GoerMicro_Service
身份验证方法:	EAP-PEAP,EAP-MSCHAPv2
身份验证源:	AD:D com
授权源:	GM-AD
角色:	[User Authenticated]
强制配置文件:	OTHER DENY

显示第 54 条记录, 共 41-60 条

显示配置 导出 显示日志 关闭

RADIUS 请求	
授权属性	
Authorization:GM-AD:Account Expires	9223372036854775807 [30828-09-14 10:48:05 CST]
Authorization:GM-AD:Email	it@goermicro.com
Authorization:GM-AD:memberOf	CN=M-IAM-MGMT,OU=ITManager,OU=MosGroup,DC=MOS,DC=COM
Authorization:GM-AD:Name	it
Authorization:GM-AD:UserDN	CN=it,OU=P.E.A,OU=MOS,DC=MOS,DC=COM

## 9.2. 使用非 AD 内的设备登陆

配置文件为 **OTHER DENY**

请求详细信息

摘要 输入 输出 警报

日期和时间:	Jan 05, 2022 17:30:44 CST
终端主机标识符:	B2-2-..._2
用户名:	@goermicro.com
访问设备 IP/端口:	10. ...
访问设备名称:	10. ... .7
系统状况状态:	UNKNOWN (100)

使用的策略 -

服务:	GoerMicro_Service
身份验证方法:	EAP
身份验证源:	None
授权源:	GM-AD
角色:	-
强制配置文件:	OTHER DENY
服务监视器模式:	Disabled
在线状态:	不可用

显示第 2 条记录, 共 1-20 条

显示配置 导出 显示日志 关闭



Authorization : GM-AD : UserDN 为 **空**

请求详细信息

摘要 输入 输出 警报

用户名:	ang@goermicro.com
终端主机标识符:	B2-26
访问设备 IP/端口:	10.8

**RADIUS 请求**

授权属性

Authorization:GM-AD:UserDN **空**

计算的属性

请求详细信息

摘要 输入 输出 警报

强制配置文件:	OTHER DENY
系统状况状态:	UNKNOWN (100)
审核状况状态:	UNKNOWN (100)

**RADIUS 响应**

Radius:Aruba:Aruba-User-Role DENYALL