



# ISE 的通用 WLC FlexConnect 配置

安全访问操作指南系列

作者: Hosuk Won

日期: 2012 年 12 月



## 目录

ISE 与 WLC FlexConnect 的集成	3
交换机配置	4
WLC 配置步骤	5
将 ISE 配置为 RADIUS 服务器	6
配置 RADIUS 回退选项	8
将 AP 更改为 FlexConnect AP	9
创建安全 WLAN	10
创建开放式 WLAN	10
创建 FlexConnect ACL	11
创建 FlexConnect 组	13
配置其他 WLC 功能	15
ISE 配置	16
配置授权配置文件	

# ISE 与 WLC FlexConnect 的集成

本文档针对如何将 ISE 与包含以 FlexConnect 模式部署的接入点 (AP) 的 CUWN 环境相集成提供分步指南。 FlexConnect 模式(以前称为 H-REAP 模式)允许 AP 通过本地方式交换通常部署在分支机构中的某些 WLAN 的用户流量,从而使无线流量能够保留在分支机构内。

### 整体设计



图 1. ISE 与 WLC FlexConnect 的集成

上图显示组件的整体布局。在中心站点将有两个按如下方式定义的 VLAN:

#### 表 1.

VLAN ID	名称	用途
201	服务器	ISE、AD、DNS、DHCP
202	WLC	WLC 管理

在远程办公室将有三个按如下方式定义的 VLAN:

#### 表 2.

VLAN ID	名称	用途
80	AP 管理	FlexConnect AP 本机 VLAN
30	员工	映射的安全 WLAN
40	访客	映射的开放式 WLAN

在本设计中,当终端与已启用 FlexConnect 的 WLAN 相关联时,该终端将通过从 LAP 到控制器的 CAPWAP 隧 道进行身份验证,但是,在完成身份验证后,流量交换将从 LAP 到本地 LAN 以本地方式实现,而不是通过中 央无线控制器进行。本设计配置有两个 WLAN:一个是带有 MAC 过滤功能的开放式 SSID WLAN,另一个是 已启用 WPA2/802.1X 的 WLAN。与 example\_open SSID 关联的终端将切换到在 FlexConnect AP 上本地定义的 VLAN 40,而与 example\_secure SSID 关联的终端则将切换到 VLAN 30。与 example\_open SSID 关联的终端将依 据 WLC 上定义的 FlexConnect ACL (发布在 FlexConnect AP 上)限制为只能访问互联网。此 ACL 在授权期间 将使用 Airespace RADIUS 属性从 ISE 应用于会话。

虽然 FlexConnect 模式支持诸如本地身份验证等其他配置,但在 ISE 集成过程中不会讨论这些选项。此外,尽管本文档涉及 ISE 与 FlexConnect 模式进行集成的必要配置,但有一些其他配置(包括分析和详细的访客访问)未涵盖在本文档中。有关这些配置的详细信息,请参阅相应的操作指南。

### 使用的组件

- Cisco ISE 1.2.0.899
- Cisco 2504 CUWN AireOS 7.5.102.0
- (以下传统和网状 AP 型号不支持使用 RADIUS 的 FlexConnect ACL: 1130、1240、1520 和 1550。
   有关 FlexConnect 模式和 AAA 覆盖功能的详细信息,请参阅 WLC 指南: http://www.cisco.com/en/US/docs/wireless/controller/7.5/config guide/b cg75 chapter 010001010.html)
- 作为 AD/DNS/DHCP 服务器的 MS Windows 2008 Server

注: 仅支持将此处描述的通过 ACL 进行授权的 FlexConnect 与运行 AireOS 7.5.102.0 和更高版本的 WLC 配合用 于受支持的 AP 型号。对于其他版本的 WLC 和 AP,可以在 FlexConnect 组级别上改用静态 VLAN 分配来控制 流量。有关使用 FlexConnect VLAN 分配的说明,请参阅以下 URL 中提供的 BYOD 2.5 CVD: http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless\_Networks/Unified\_Access/BYOD\_Wireless.html

### 交换机配置

由于此设计要求为不同的 WLAN 映射本地 VLAN,因此需要将连接到 LAP 的接口配置为中继端口。

```
Remote-Switch(config)#interface GigabitEthernet x/y/z
Remote-Switch(config-if)#description AP
Remote-Switch(config-if)#switchport mode trunk
Remote-Switch(config-if)#switchport trunk native vlan 80
Remote-Switch(config-if)#no shut
```

连接到 WLC 的接口可以是中继接口,也可以是接入接口。如果要将 WLC 用于像本地模式下部署的 AP 那样集中交换用户流量,则需要中继。由于本文档重点针对 flex-connect 模式 AP,因此接口将配置为接入端口。

DC-Switch(config)#interface GigabitEthernet x/y/z DC-Switch(config-if)#description WLC DC-Switch(config-if)#switchport mode access DC-Switch(config-if)#switchport access vlan 202 DC-Switch(config-if)#no shut



### WLC 配置步骤

#### 初始 WLC 配置

以下步骤将引导您完成思科无线局域网控制器的初始配置。

步骤 1. 连接至 WLC 的控制台端口。请参阅以下设置来引导 WLC。

#### 示例输出

(Cisco Controller) Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup Would you like to terminate autoinstall? [yes]:yes AUTO-INSTALL: process terminated -- no configuration loaded System Name [Cisco 91:e2:64] (31 characters max): 2500wlc-1 Enter Administrative User Name (24 characters max): admin Enter Administrative Password (3 to 24 characters): \*\*\*\*\*\*\*\* : \*\*\*\*\*\*\* Re-enter Administrative Password Service Interface IP Address Configuration [static][DHCP]:dhcp Enable Link Aggregation (LAG) [yes][NO]: no Management Interface IP Address: 192.168.202.61 Management Interface Netmask: 255.255.255.0 Management Interface Default Router: 192.168.202.1 Management Interface VLAN Identifier (0 = untagged): 0 Management Interface Port Num [1 to 8]: 1 Management Interface DHCP Server IP Address: 192.168.201.72 Virtual Gateway IP Address: 1.1.1.1 Mobility/RF Group Name: example Configure DHCP Bridging Mode [yes] [NO]: no Allow Static IP Addresses [YES][no]: no Configure a RADIUS Server now? [YES][no]: no Warning! The default WLAN security policy requires a RADIUS server. Please see documentation for more details. Enter Country Code list (enter 'help' for a list of countries) [US]:us Enable 802.11b Network [YES][no]: yes Enable 802.11a Network [YES][no]: yes Enable 802.11g Network [YES][no]: yes Enable Auto-RF [YES][no]: yes Configure a NTP server now? [YES][no]: yes Enter the NTP server's IP address: 192.168.201.72 Enter a polling interval between 3600 and 604800 secs: 3600 Configuration correct? If yes, system will save it and reset. [yes][NO]: yes

### 将 ISE 配置为 RADIUS 服务器

Cisco WLC 使用 Cisco ISE 作为 RADIUS 服务器。以下步骤将引导您完成配置 Cisco WLC 以使用 Cisco ISE 作为其 RADIUS 服务器的过程。

- **步骤 1.** 访问 WLC GUI 并导航至 Security → RADIUS → Authentication。
- 步骤 2. 点击右上角的 New... 以添加新的 RADIUS 身份验证服务器。

系统将在下表列出 RADIUS 身份验证服务器设置(如果未指定,则使用默认值)。

表 3.

属性	值
服务器索引(优先级)	1
服务器 IP 地址	192.168.201.88
共享密钥格式	ASCII
共享密钥	cisco123
端口号	1812
服务器状态	启用(选中)
支持 RFC 3576	启用(选中)
服务器超时	10 秒
网络用户	启用(选中)



Firefox 🔨 门 2500wlc-1		+							- 7 🛛
https://192.168.202.61/s	screens/frameset.html			か r	7 C 8 - Google		<i>P</i> +		• 🦗 🖣 🖸
ululu cisco	<u>M</u> ONITOR <u>W</u> LANS	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	onfiguratio HE <u>L</u> P	on   <u>P</u> ing   <u>F</u> EEDBACk	Lo <u>q</u> out   <u>R</u> efresh
Security	RADIUS Authentie	cation Servers	s > Edit					< Back	Apply
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication Accounting Fallback</li> <li>TACACS+ LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Password Policies</li> </ul>	Server Index Server Address Shared Secret Form Shared Secret Confirm Shared Sec Key Wrap Port Number Server Status	at ret	1 192.168.201.1 ASCII 💌 •••• (Designed for 1812 Enabled 💙	7 FIPS custome	ers and requires a	key wrap compl	iant RADI	(US server)	
Local EAP	Support for RFC 357	6	Enabled 💌						
Priority Order	Server Timeout		10 seconds						
Certificate     Access Control Lists     Wireless Protection     Policies	Network User Management IPSec		⊻ Enable ✓ Enable						

图 2.

- **步骤 3.** 点击 Apply 并保存配置。
- **步骤 4.** 点击 Accounting 和 New... 以添加 RADIUS 记帐服务器。

系统将在下表中列出 RADIUS 记帐服务器设置(如果未指定,则使用默认值)。

属性	值
服务器索引(优先级)	1
服务器 IP 地址	192.168.201.88
共享密钥格式	ASCII
共享密钥	cisco123
端口号	1813
服务器状态	启用(选中)
服务器超时	10 秒
网络用户	启用(选中)

#### 表 4.

Firefox T 2500wlc-1			+							- 7 🛛
← ▲ https://192.168.202.61/	A https://192.168.202.61/screens/frameset.html				☆ -	🛡 🤁 🔻 Google	•	<i>P</i> +		- 🖗 - 🖸
սիսիս							Sa <u>v</u> e Co	onfigurati	on   <u>P</u> ing	Logout <u>R</u> efresh
CISCO	<u>M</u> ONITOR <u>V</u>	<u>V</u> LANS <u>(</u>	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBAC	K
Security	RADIUS Ac	counting	g Servers >	Edit					< Back	Apply
<ul> <li>AAA         General         General         Authentication         Accounting         Fallback         TACACS+         LoAP         Local Net Users         MAC Filtering         Disabled Clients         User Login Policies         AP Policies         Password Policies         Local EAP         Priority Order</li> </ul>	Server Inde Server Addr Shared Secr Confirm Sha Port Number Server Statu Server Time Network Use IPSec	x ess et Format et red Secret	1 192.1 ••• 1813 Enabl 10 ¥ En	68.201.88 I v ed v seconds able Enable				]		

图 3.

步骤 5. 点击 Apply 并保存配置。

### 配置 RADIUS 回退选项

假设主 RADIUS 服务器(具有最低服务器索引的服务器)是最适合 Cisco WLC 的服务器。如果主服务器无响应,则控制器会切换到下一个活动备份服务器(具有次低服务器索引的服务器)。除非将控制器配置为从可用 备份服务器回退到主 RADIUS 服务器(当其恢复并可响应时)或回退到更合适的服务器,否则控制器会继续使 用此备份服务器。

步骤 1. 导航至 Security → AAA → RADIUS → Fallback。

**步骤 2.** 将 Fallback Mode 设置为 Active。

注:选择 Active 会导致 Cisco WLC 通过使用 RADIUS 探测消息主动确定已标记为处于不活动状态的服务器是 否恢复联机来从可用备份服务器恢复到优先级较低的服务器。控制器会忽略所有活动 RADIUS 请求的所有非活 动服务器。选择 Passive 会导致 Cisco WLC 从可用备份服务器恢复到优先级较低的服务器,而不使用无关的探 测消息。控制器会在某个时间段忽略所有非活动服务器,并在后来需要发送 RADIUS 消息时重试。

步骤 3. 对于 Username,请输入要在非活动服务器探测中发送的名称"radius-test"。

**步骤 4.** 为 Interval in Sec. 字段输入值。

时间间隔在被动模式下是指非活动时间,在活动模式下是指探测时间间隔。有效范围是 180 至 3600 秒,默认 值为 300 秒。

### 将 AP 更改为 FlexConnect AP

通过 CUWN,可在不同模式下部署 LAP。在典型的集中无线部署中,LAP 在本地模式下进行部署,其中所有 流量都通过 CAPWAP 隧道以隧道方式从 LAP 传输到 WLC,并由 WLC 交换到各个 VLAN 以匹配 WLAN。为 在 LAP 上以本地方式交换流量,需要将 AP 模式更改为 FlexConnect 模式。

- 步骤 1. 导航至 Wireless 并点击要转换为 FlexConnect 模式 AP 的 AP。
- **步骤 2.** 为 AP Mode 下拉菜单选择 **FlexConnect**,然后点击"Apply"按钮。点击后,AP 将会重新加载,并 作为 FlexConnect 模式 AP 重新加入控制器。



- 步骤 3. AP 重新加入 WLC 后,请点击 AP,然后点击 FlexConnect 选项卡以配置中继。
- **步骤 4.** 选中 VLAN Support 并输入在 LAP 所连接的交换机上配置的本机 VLAN。受生成树影响, AP 重新连接到 WLC 可能需要几秒钟时间。

Firefox T 2500wlc-1		+					
← ▲ https://192.168.202.61/	screens/frameset.html			☆ ▼	C 8 - Google		<i>P</i> -
	<u>M</u> ONITOR <u>W</u> LANs		WIRELESS	<u>s</u> ecurity	MANAGEMENT	Sa⊻e Co C <u>O</u> MMANDS	onfigura <sup>.</sup> HE <u>L</u> P
Wireless  Access Points All APs Radios 802.11a/n/ac	All APs > Details fo	or AP4c4e.350	)d.35f8 faces Hig	yh Availability	Inventory	FlexConne	ect 📔
8U2.11D/g/n Dual-Band Radios Global Configuration Advanced	VLAN Support I	80 VLAN	N Mappings				



# 注: 虽然 VLAN 映射可以配置为在 AP 级别将 VLAN 映射到 WLAN,但是我们将配置 FlexConnect 组来简化多 个 AP 上的常规设置

**步骤 5.** 点击 Apply。

### 创建安全 WLAN

此 WLAN 将配置有采用 802.1X 的 WPA2/AES,并将用于允许员工访问内部资源。在 BYOD 的情况下,如果 要使用单 SSID 配置,则这是需要创建的唯一 SSID。

- **步骤 1.** 导航至 WLAN。
- 步骤 2. 点击 Add New 并创建具有以下参数的 WLAN。
- 表 5.

属性	值
WLAN ID	1
配置文件名称/SSID	Example_secure
2 层安全	WPA+WPA2、AES、802.1X
AAA 服务器	启用身份验证和记帐
RADIUS 服务器记帐	启用,900
允许 AAA 优先	启用
启用会话超时	启用,7200
客户端用户空闲超时	启用,7200
FlexConnect 本地交换	启用
NAC 状态	RADIUS NAC

注:如果有全局定义的多个 RADIUS 服务器,请从用于此 WLAN 的 RADIUS 服务器列表中选择 ISE 节点。

### 创建开放式 WLAN

此 WLAN 将配置有带有 MAC 过滤功能的开放式 SSID,以允许访客访问并可能用于具有双 SSID 部署的 BYOD。

- **步骤 1.** 导航至 WLAN。
- 步骤 2. 点击 Add New 并创建具有以下参数的 WLAN。

表 6.

属性	值
WLAN ID	2
配置文件名称/SSID	Example_open
2 层安全	无,MAC 过滤
AAA 服务器	启用身份验证和记帐
RADIUS 服务器记帐	启用,900
允许 AAA 优先	启用
覆盖盲区检测	禁用
启用会话超时	启用,7200
客户端用户空闲超时	启用,7200
FlexConnect 本地交换	启用
DHCP 地址 分配	必要
NAC 状态	RADIUS NAC

注:如果有全局定义的多个 RADIUS 服务器,请从用于此 WLAN 的 RADIUS 服务器列表中选择 ISE 节点。

### 创建 FlexConnect ACL

系统将创建两个 FlexConnect ACL,一个用于重定向访客 CWA 和 BYOD 进程的流量,另一个用于将访客用于限制为仅互联网访问。首先我们将开始创建仅互联网 ACL。

- 步骤 1. 导航至 Security → Access Control Lists → FlexConnect ACLs。
- 步骤 2. 点击 New 并创建具有以下参数的"INTERNET-ONLY" ACL。

表 7.

操作	来源 IP/掩码	目标 IP/掩码	协议	源端口	目标端口
允许	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	任何环境	DNS
拒绝	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	任何环境	任何环境	任何环境
拒绝	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	任何环境	任何环境	任何环境
拒绝	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	任何环境	任何环境	任何环境
允许	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	任何环境	任何环境	任何环境

步骤 3. 点击"Back"并创建具有以下参数的"REDIRECT-ACL" ACL。

表 8.

操作	来源 IP/掩码	目标 IP/掩码	协议	源端口	目标端口
允许	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	任何环境	DNS
允许	192.168.201.88 / 255.255.255.255	0.0.0.0 / 0.0.0.0	任何环境	任何环境	任何环境
允许	0.0.0.0 / 0.0.0.0	192.168.201.88 / 255.255.255.255	任何环境	任何环境	任何环境

步骤 4. 导航至 Security → Access Control Lists → Access Control Lists。

步骤 5. 点击"New"并创建"REDIRECT-ACL"(除 ACL 名称以外无需任何其他条目)。

注: 虽然 FlexConnect ACL 用于重定向,但如果在控制器上没有匹配的 ACL 作为常规 ACL,则控制器无法将 重定向 ACL 应用于会话。为解决此问题,我们将在控制器上创建与 FlexConnect ACL 具有相同名称的虚拟 ACL。(如果控制器同时用于本地模式和 FlexConnect LAP,则表明可能已存在控制器重定向 ACL,在此情况 下,我们只需确保 FlexConnect ACL 名称与现有控制器重定向 ACL 相匹配)

### 创建 FlexConnect 组

FlexConnect 组可以配置为高效管理具有相似设置(例如 ACL 和 VLAN 映射等)的多个 FlexConnect LAP。可 以根据 AP 配置这些设置,但是使用 FlexConnect 组将更易于管理包含多个 AP 的部署。此处我们将创建适用于 远程办公室中的所有 FlexConnect AP 的组。

- **步骤 1.** 导航至 Wireless → FlexConnect Groups。
- **步骤 2.** 点击 New 并创建名称为"flex1"的组。
- 步骤 3. 点击组名。
- 步骤 4. 点击 "Add AP" 按钮将以前恢复的 AP 添加到此 FlexConnect 组。
- **步骤 5.** 选中"Select APs from current controller", 然后从下拉菜单中选择 AP。



图 6. FlexConnect 组

- **步骤 6.** 点击 ACL Mapping 选项卡。
- **步骤 7.** 点击 Policies 子选项卡。
- 步骤 8. 添加先前步骤中创建的两个 FlexConnect ACL。



8 7. FlexConnect ACL

- **步骤 9.** 点击 WLAN VLAN Mapping 选项卡。
- 步骤 10. 添加具有以下参数的 WLAN VLAN 映射。
- 表 9.

WLAN ID	VLAN ID
1	30
2	40



图 8.

**步骤 11.** 点击 Apply。

### 配置其他 WLC 功能

- **步骤 1.** 通过导航至 Controller → General 启用 fast-ssid-change 功能。
- 步骤 2. 启用 Fast SSID Change。



图 9.

注:通过 Fast-SSID-Change 功能,客户端可从一个 SSID 移至另一个 SSID 而没有延迟。此功能允许客户端在 BYOD 的双 SSID 场景中从开放式 SSID 移至安全 SSID 而没有延迟,这主要是为处理短期时间内从一个 SSID 转至另一个 SSID 的 Apple iOS 设备。

- 步骤 3. 通过进入 WLC CLI 启用强制门户绕行功能。
- 步骤4. 启用强制门户绕行命令。

> config network web-auth captive-bypass enable

#### 步骤 5. 保存控制器上的配置。

> save config

步骤 6. 您必须重新启动控制器以应用此更改。

> reset system

注: 当存在强制门户时, Apple 引入了 iOS 功能以促进网络访问。此功能尝试通过在连接到无线网络时发送 Web 请求来检测是否存在强制门户,并将请求重定向到 <u>http://www.apple.com/library/test/success.html</u>。如果收到 回应,则假设进行互联网访问,并且无需进一步交互。如果未收到回应,则假设互联网访问被强制门户阻止, 并且 CNA 会自动启动虚拟服务器以在受控窗口中请求进行门户登录。当重定向到 ISE 强制门户时, CNA 可能 会中断。

## ISE 配置

ISE 没有专门的配置来与 3850 交换机集成以进行无线接入。3850 可以通过与 Catalyst 交换机相同的方式进行集成,以支持诸如 CWA、BYOD 和状态评估等高级 ISE 功能。由于本文档涵盖与 BYOD 相关的策略,请参阅 BYOD 操作指南以了解如何配置基础服务来启用 BYOD。这包括 CA 服务器、外部身份源和请求方调配策略的 配置。

### 创建身份序列

我们将创建一个身份序列处理来自交换机的身份验证请求。此序列将通过证书、AD 或内部用户数据库对终端 进行身份验证。

- 步骤 1. 登录到 ISE 主管理员节点。
- 步骤 1. 导航至 Administration → Identity Management → Identity Source Sequences。
- **步骤 2.** 点击 Add。
- **步骤 3.** 创建名称为 CAP\_AD\_Internal 的序列。

Firefox 🔹 🔞 ISE	- RADIUS Servers - 192.168.201.88	+			
https://192.168	3.201.88/admin/#pageId=com_cisco	_xmp_web_page_identity_	_source_seq	∰ ⊽ <b>C</b>	8 - G
cisco Identity	/ Services Engine	🏠 Home	Operations   🔻	Policy   🔻 🕠	<sub>ise12</sub> Administra
🐝 System 🛛	🧏 Identity Management 🛛 📱	Network Resources	🛃 Web Por	tal Management	<b>D</b> F
Identities Grou	ups External Identity Sources	Identity Source Se	equences Set	ttings	
Identity Source Sequence	es List > CAP_AD_Internal Sequence				
<ul> <li>Identity Source</li> </ul>	Sequence				
* Name CA	P_AD_Internal				
Description					
<ul> <li>Certificate Bas</li> <li>Select C</li> </ul>	ed Authentication Certificate Authentication Profile	CAP	*		
<ul> <li>Authentication</li> </ul>	Search List				
Aseto	of identity sources that will be acc	essed in sequence unt	til first authenticat	ion succeeds	
Available Internal Endpu Guest Users LDAP	oints	Selected AD1 Internal Users	s	X	× ×

图 10. 创建身份序列

**步骤 4.** 点击 Save。

### 创建用户组并分配用户

在此示例中,合同用户将通过 ISE 内部数据库进行身份验证,而员工用户将通过证书或 AD 用户帐户进行身份 验证。将为合同用户创建 ISE 用户组。

- 步骤 1. 导航至 Administration → Identity Management → Groups → User Identity Groups。
- **步骤 2.** 点击 Add。
- 步骤 3. 输入 Contractor 作为组名并点击 Submit。
- 步骤 4. 导航至 Administration → Identity Management → Identities → Users。
- **步骤 5.** 点击 Add。
- 步骤 6. 输入 "contractor1" 作为用户名并输入密码。
- 步骤 7. 选择"Contractor"作为 User Groups, 然后点击"Submit"。

#### 启用策略集

通过 ISE 1.2 中的策略集功能,管理员可以创建复杂身份策略。在本文档中,我们将创建两个映射到各 WLAN 的策略集,并在每个策略集内创建基础策略。借此可明确了解策略如何应用于具有 ISE 策略结构的每个使用 案例。

**步骤 1.** 要启用策略集功能,请导航至 Administration → System → Settings → Policy Sets。 **步骤 2.** 选择"Enabled",然后点击"Save"。

**注**: 启用策略集功能后,如果要返回到经典模式,则需要重新创建策略。但是,启用该功能后,初始策略将复制到默认策略集。

#### 创建可下载 ACL

此处我们将创建要在授权期间应用的 DACL(可下载 ACL)。

- **步骤 1.** 导航至 Policy → Policy Elements → Results → Authorization → Downloadable ACLs。
- 步骤 2. 点击 Add 以创建具有以下参数的 NSP 授权配置文件。

表 10. NSP 授权配置文件

名称	仅限互联网
DACL 内容	permit udp any host 192.168.201.72 eq domain
	permit udp any any eq bootpc
	deny ip any any

**步骤 3.** 点击 Save。

### 配置授权配置文件

创建三个授权配置文件。

- **步骤 1.** 导航至 Policy → Policy Elements → Results → Authorization → Authorization Profiles。
- **步骤 2.** 点击 Add 以创建具有以下参数的 NSP 授权配置文件。

名称	NSP
常见任务	Web 重定向
Web 重定向类型	本机请求方调配
ACL	REDIRECT-ACL

#### **步骤 3.** 点击 Save。

步骤 4. 点击 Add 以创建具有以下参数的 WebAuth 授权配置文件。

名称	WebAuth
常见任务	Web 重定向
Web 重定向类型	集中 Web 身份验证
ACL	REDIRECT-ACL

- **步骤 5.** 点击 Save。
- 步骤 6. 点击 Add 以创建具有以下参数的互联网授权配置文件。

名称	互联网
常见任务	DACL 名称
ACL	仅限互联网

### 配置策略

- **步骤 1.** 导航至 Policy → Policy Set。
- 步骤 2. 点击左窗格上的+符号,然后点击 Create Above。



**图 11.** 配置策略

**步骤 3.** 定义名称为 example\_secure 的策略集和以下参数。

Define the Polic	y Sets by configuring rules	s based on conditions. Drag and drop sets on the left	t hand side to change the order.
Status	Name example_secure	Description	Conditions Airespace:Airespace-Wlan-Id EQUALS 1
<ul> <li>Authentica</li> </ul>	tion Policy		
	Default Rule (If no match)	: Allow Protocols : Default Network Access	and use : CAP_AD_Internal
<ul> <li>Authorizati</li> </ul>	ion Policy		
Status	EAP-TLS	Conditions (identity groups and other cond if Network Access:EapAuthentication EQUAL EAP-TLS	ditions) Permissions LS then PermitAccess
<b>~</b>	Default	if no matches, then NSP	

**图 12.** 定义策略

**步骤 4.** 点击 Submit。

步骤 5. 定义名称为 "example\_open" 的策略集和以下参数。

_		<b>~</b>	example_open	Airespace:Aire	espace-Wlan-Id EQUALS 2	
•	Auth	nenticatio	n Policy			
			Default Rule (If no match)	: Allow Protocols : Default Network Access and use :	Internal Endpoints	
•	<ul> <li>Authorization Policy</li> </ul>					
		Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
		<b>~</b>	NSP	if (Network Access:UseCase EQUALS Guest Flow then AND AD1:ExternalGroups EQUALS example.com/Users/Domain Users )	NSP	
		2	Internet	if Guest AND Network Access:UseCase EQUALS then Guest Flow	Internet	
		<b>~</b>	Default	if no matches, then WebAuth		

#### **图 13.** 定义策略

#### **步骤 6.** 点击 Submit。

### 配置 ISE 以抑制 RADIUS 测试消息

您可以配置集合过滤器禁止发送到监控和外部服务器的日志消息。抑制可以根据不同的属性类型的策略服务节点级别执行,您也可以禁用抑制。您可以定义特定属性类型和相应的值的多个过滤器。

注: 建议将集合过滤器的数量限制为 20。

- 步骤1. 登录到 ISE 主管理员节点。
- **步骤 2.** 导航至 Administration > System > Logging。
- **步骤 3.** 点击左窗格上的 Collection Filters。
- 步骤 4. 点击右窗格顶部的 Add。

🔆 🔆 System 🦉 Identity Management	Network Resources	🛃 Web Portal Mar	nagement 🛛 🗔 F	Feed Service
Deployment Licensing Certificates	Logging Maintenance	Backup & Restore	Admin Access	Settings
LoggingI Local Log SettingsRemote Logging TargetsI Logging CategoriesI Message CatalogDebug Log ConfigurationI Collection Filters	Collection Filter List Collection Filter List * Attribute Us * Value ra * Filter Type Fil Save Res	t > User Name ilters ser Name adius-test Iter Failed set	▼ ▼	

图 14. 添加集合过滤器

- 步骤 5. 从 Attribute 下拉菜单中选择"User Name"。
- 步骤 6. 为 Value 输入"radius-test"。
- **步骤 7.** 从 Filter Type 下拉菜单中选择"Filter All"。
- 步骤 8. 点击 Save。