使用IBNS 2.0和接口模板标准化有线802.1X AP身份验证

目录

简介

本文档介绍使用IBNS 2.0接口模板的802.1X配置。

问题陈述

使用IEEE 802.1X实现端口安全是常见的最佳实践。除了提高网络安全性外，它还通过允许在整个网络中实现标准化接入端口配置来简化交换机部署。

本指南介绍如何将单个标准化交换机端口配置同时用于终端设备和思科接入点(AP)。 虽然每个交换机端口最初都作为标准接入端口运行，并执行IEEE 802.1X身份验证，但经过身份验证的AP根据其

部署方案可能需要不同的运行模式。

特别是，在FlexConnect本地交换模式下运行的AP必须在中继端口上运行，因为来自多个SSID的客户端流量在本地进行桥接。因此，在身份验证成功后，交换机接口必须动态地从接入端口转换到中继端口。

连接基础设施设备而不是简单终端设备的接入端口通常需要接口配置，而接口配置与默认接入端口行为不同。

因此，必须在身份验证过程中动态修改交换机接口配置。多年来，人们使用多种方法来实现此行为，包括自动智能端口和嵌入式事件管理器(EEM)小程序。现在，推荐的解决方案是IBNS 2.0 [1]与接口模板相结合，它提供了一种可扩展的一致方法，用于在身份验证成功后动态更改接口配置。

方针

要使设置正常运行，必须正确配置各种组件，即

- Radius服务器（身份服务引擎）
- 交换机
- 接入点/无线LAN控制器

由于存在现有文档（请参见结尾处的参考），我们重点关注本文档中的特定场景，并将现有文档作为支持材料。

要求

Cisco 建议您了解以下主题：

- 无线局域网控制器(WLC)和轻量AP(LAP)
- 思科交换机和ISE上的802.1x
- 可扩展认证协议 (EAP)
- 远程用户拨入认证系统(RADIUS)

使用的组件

本文档中的信息基于以下软件和硬件版本：

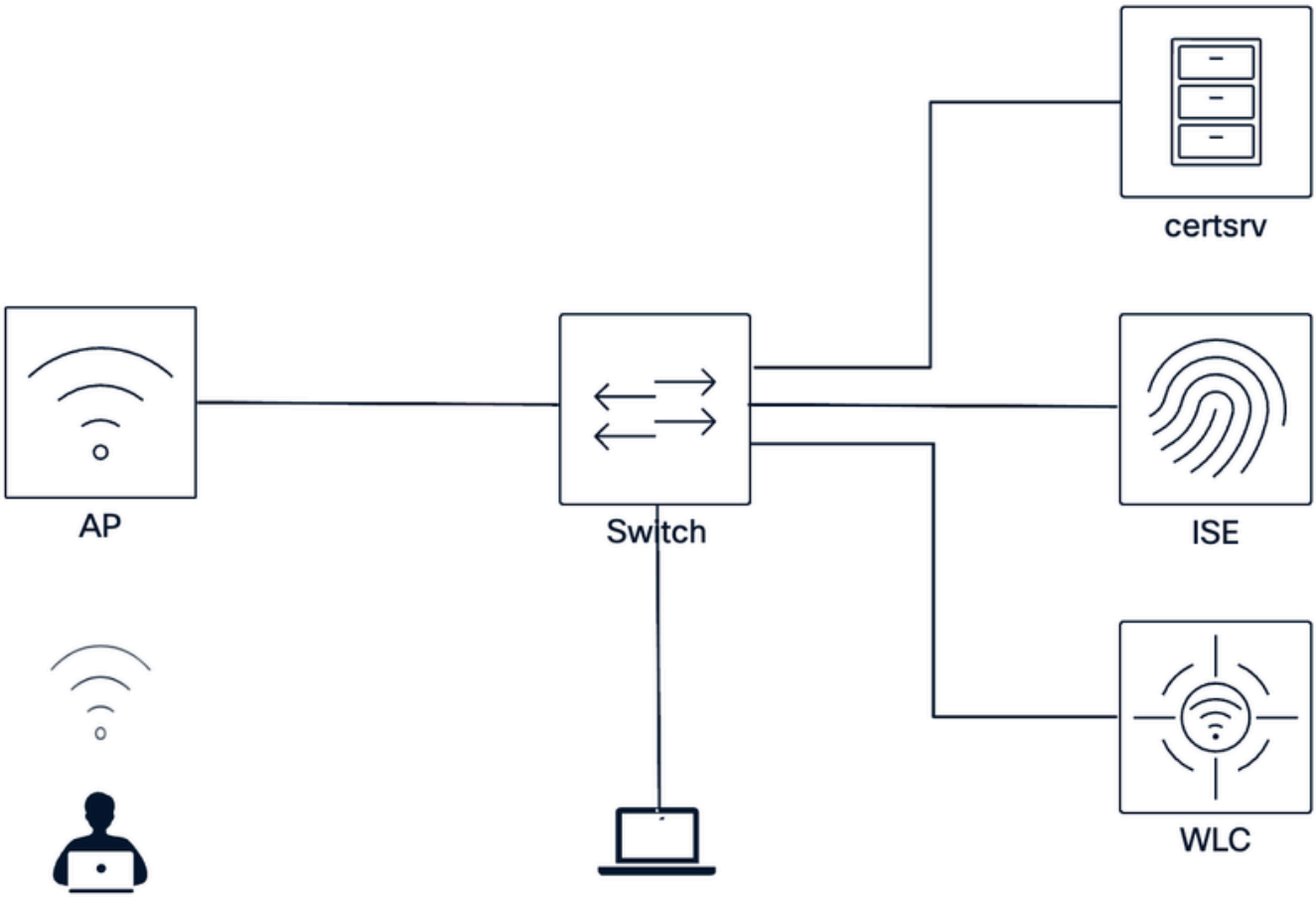
- 思科C9350 - IOS XE 26.1.1a
- 思科C9800-40 WLC - IOS XE 26.1.1
- ISE版本3.5补丁1
- AP CW917x、CW916x

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

netascode.cisco.com中还介绍了用于交换和ISE的数据模型，以便轻松复制设置。

配置

网络图



示例设置

出于我们的目的，我们重点关注单个场景，提供配置片段和分步指导。由于过程中存在各种不同的变体，因此我们会指出这些变体并参考现有文档来实现此目的。

本指南涵盖的场景：

- AP有线Dot1X，采用EAP-FAST身份验证
- 通过C9800 WLC调配的Dot1X凭证
- Flex Connect本地交换模式下的AP

在此设计中，交换机端口最初使用带MAB回退的通用封闭模式802.1X配置。在首次登录期间，AP可能没有802.1X凭证，因此ISE可以通过MAB对AP进行授权，其有限访问权限足以到达WLC或Catalyst Center。调配凭证或证书后，AP会执行有线802.1X身份验证。然后，ISE返回适用于AP_FLEX_TRUNK接口模板的授权结果，将端口转换为所需的FlexConnect中继配置。

Variations				
Auth Types	MAB	EAP-FAST	EAP-PEAP	EAP-TLS
Provisioning of AP Dot1x supplicant	Wireless LAN Controller	Catalyst Center		
Certificate Rollout method	SCEP	EST		

表 1：概述中的其他变体和选项

无线接入点配置

要将有线Dot1x身份验证与您的AP结合使用，您必须首先根据所选身份验证方法向AP推出凭证和/或证书。

Cisco Catalyst AP Dot1x请求方通常支持EAP-FAST、EAP-PEAP或EAP-TLS。此外，MAB也可以作为一个选项，尤其是因为AP需要首先收集凭证或证书才能执行EAP类型身份验证。

- MAB:

    - 无需无线接入点设置
    - 管理硬件MAC地址需要工具
    - 很容易伪装
    - 允许通用端口配置

- EAP-FAST:
    - 基于用户名/密码
    - 易于推广
    - 需要在ISE上启用匿名带内PAC调配

- EAP-PEAP:
    - 基于用户名/密码
    - 服务器验证需要证书
    - 需要相应地规划证书续订

- EAP-TLS:
    - 基于证书
    - 需要相应地规划证书续订

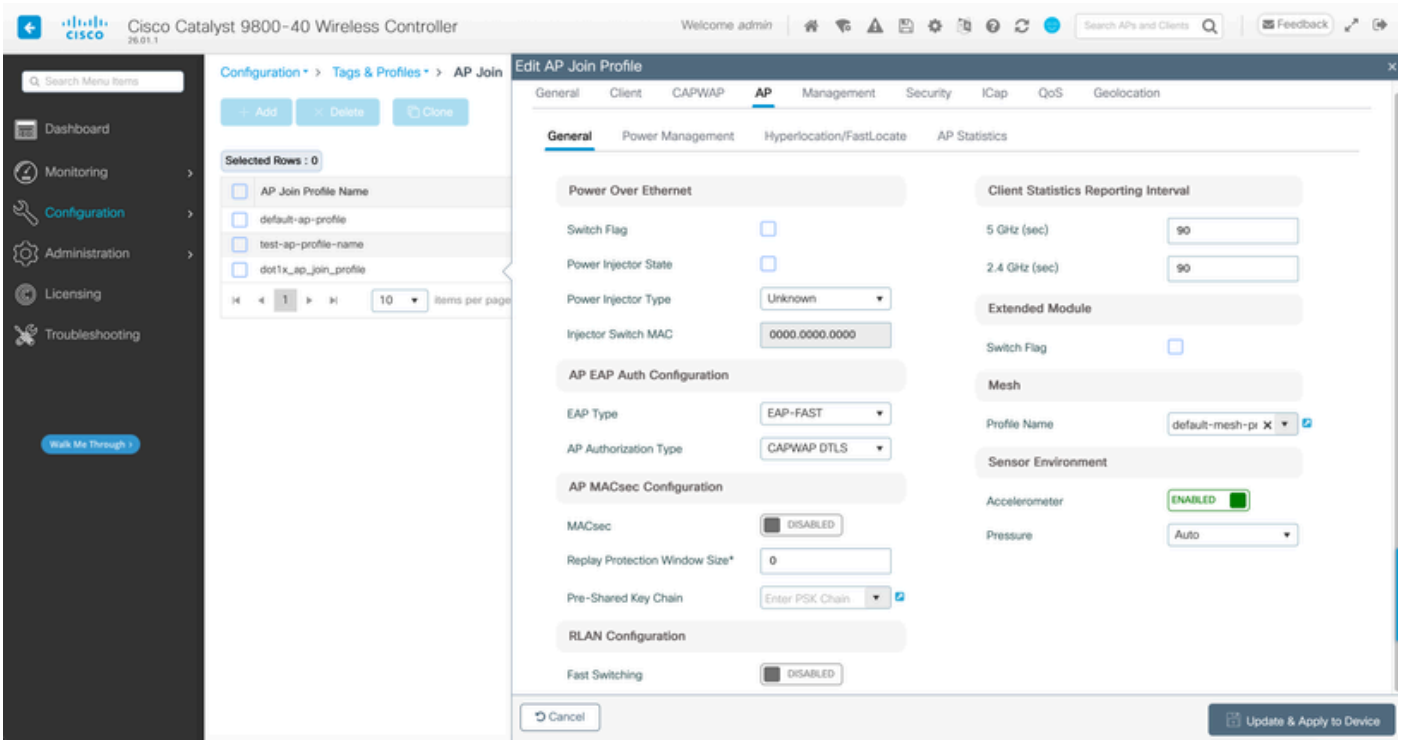
要配置AP有线Dot1X请求方，有两种方法：通过无线LAN控制器或Catalyst Center，如下所述。在详细介绍这些内容之前，必须预先选择您要使用的身份验证类型。

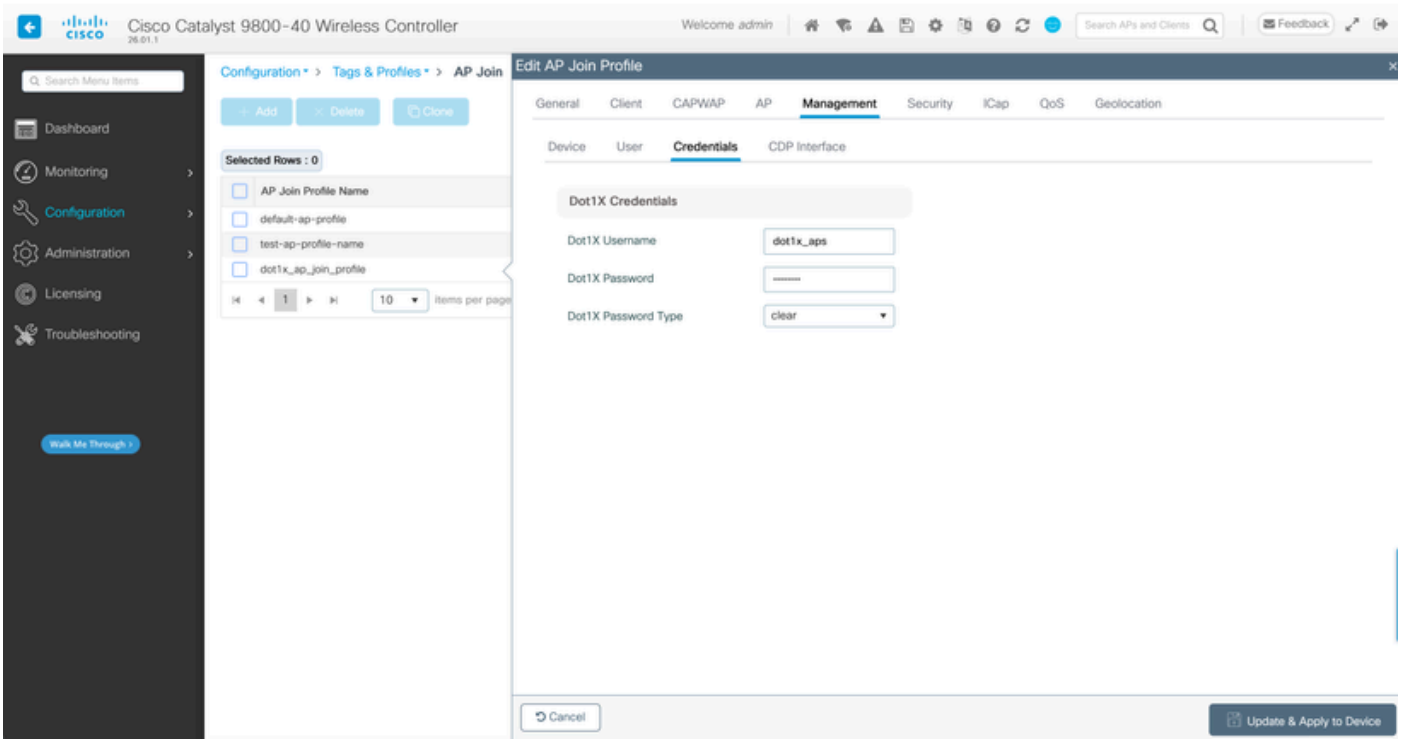
通过Cisco 9800无线LAN控制器设置有线Dot1X

如果您选择了基于证书的身份验证（EAP-PEAP或EAP-TLS[1]），您需要作为下一步决定您计划如何通过SCEP [2]或EST [3]颁发本地有效的AP证书(LSC)的方法。

在我们的场景中使用EAP-FAST时，生成AP加入配置文件就足够了，您可以在其中输入Dot1X用户和密码，将该加入配置文件绑定到Site-Tag并将其分配给AP。

GUI 配置





CLI 配置

```
ap profile dot1x_ap_join_profile
 country DE
description dot1x_ap_join_profile
 dot1x eap-type eap-fast
 dot1x username <DOT1X_USER> password 0 <DOT1X_PASSWORD>
```

通过Catalyst Center即插即用设置有线Dot1X

要使PnP [4]正常工作，需要将Catalyst Center与ISE集成。由于需要证书才能从AP端执行服务器验证以使用ISE进行EAP身份验证，因此部分需要此验证。对于设备端证书，AP将获得由Catalyst Center CA颁发的证书，该证书在默认情况下是自身的内置证书，或者由相应CA的SubCA/SCEP配置。

通过PnP的设置过程允许在设备加入WLC之前调配证书和/或凭证。

交换机配置

除了身份验证是一种安全机制外，它也是一种标准化交换机端口配置的方法。因此，这些部分描述了实现此目标所需的要素。这是一个示例配置，必须对其进行检查并根据您的设置进行调整。通常，此配置允许Dot1x和回退MAB，同时正确处理停用Radius场景、重新身份验证等。

全局Radius属性：

```
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 5 tries 3
radius-server deadtime 3
!
ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

Radius服务器组：

```
!
radius server client-radius-server01
 address ipv4 <ISE01-PSN-IP> auth-port 1812 acct-port 1813
 timeout 10
 retransmit 1
 automate-tester username dummy ignore-acct-port probe-on key 6 <RADIUS-SECRET>
!
!
aaa group server radius client-radius-group
 server name client-radius-server01
 ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

AAA配置：

```
!
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group client-radius-group
aaa authorization network default group client-radius-group
aaa accounting Identity default start-stop group client-radius-group
aaa accounting update newinfo periodic 2880
!
aaa server radius dynamic-author
 client <ISE01-PSN-IP> server-key 6 <RADIUS-SECRET>
!
```

IBNS2.0类映射和服务模板：

```
!
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
service-template CRITICAL_AUTH_VLAN
 vlan <CRITICAL-AUTH-VLAN>
!
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match authorization-status authorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match authorization-status unauthorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
 match authorizing-method-priority gt 20
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
 match result-type method dot1x method-timeout
!
class-map type control subscriber match-any IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
class-map type control subscriber match-all MAB
```

```
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
```

IBNS 2.0服务策略：

```
!
policy-map type control subscriber WiredDot1xClosedAuth_1X_MAB
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 20
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event authentication-failure match-first
  10 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN
   20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   30 authorize
   40 pause reauthentication
  30 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  40 class DOT1X_NO_RESP do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
 50 class MAB_FAILED do-until-failure
  10 terminate mab
  20 authentication-restart 60
 60 class DOT1X_TIMEOUT do-until-failure
  10 authenticate using mab priority 20
 70 class always do-until-failure
  10 terminate dot1x
  20 terminate mab
  30 authentication-restart 60
!
```

接口模板：

```
!
template AP_FLEX_TRUNK
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport trunk native vlan <TRUNK-NATIVE-VLAN>
 switchport trunk allowed vlan <TRUNK-ALLOWED-VLANS>
 switchport mode trunk
 mab
 access-session host-mode multi-host peer
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
template DEFAULT-ACCESS-PORT
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 mab
 access-session host-mode multi-domain
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
```

接口配置:

```
!
interface TenGigabitEthernet1/0/1
 switchport access vlan <DEFAULT-ACCESS-VLAN>
 switchport mode access
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DEFAULT-ACCESS-PORT
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

全局必备：

```
!
dot1x system-auth-control
!
access-session interface-template sticky timer 60
```

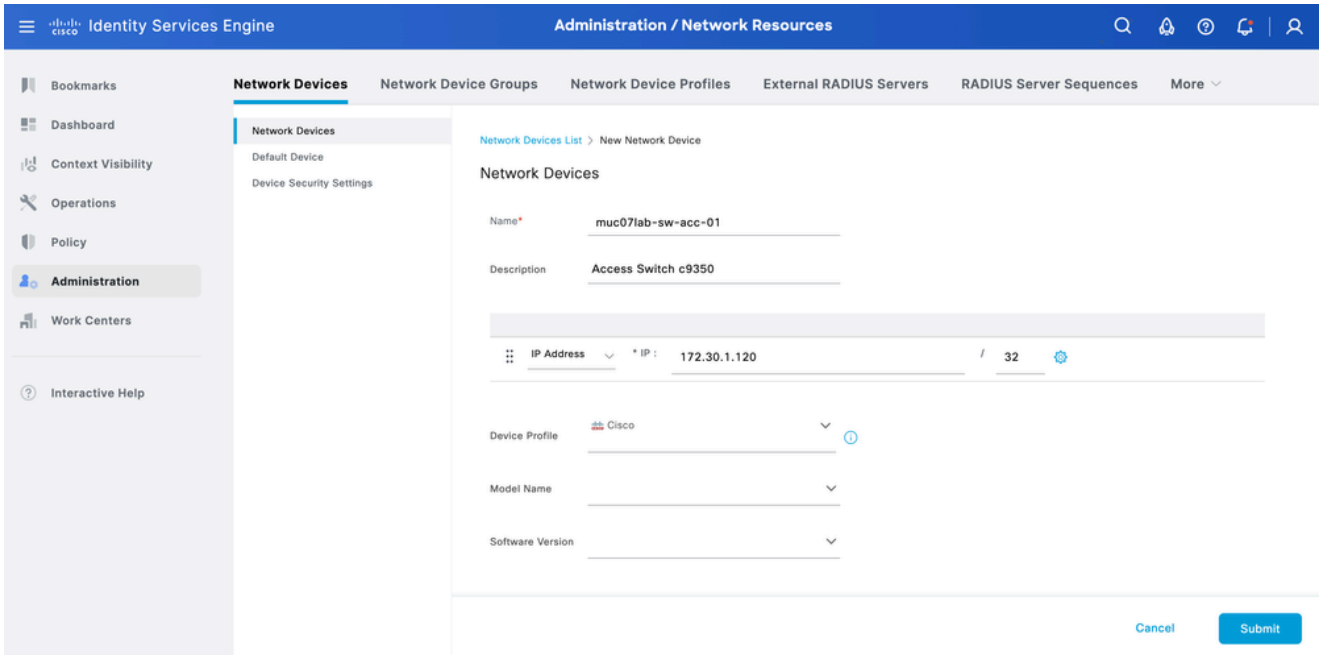
!

注意：使用CW9178时，AP在身份验证期间提供两个MAC地址。要防止交换机端口进入err-disabled状态，必须首先将端口配置为主机模式多重身份验证。在802.1X身份验证成功后，建议将端口配置动态更改为主机模式多主机。

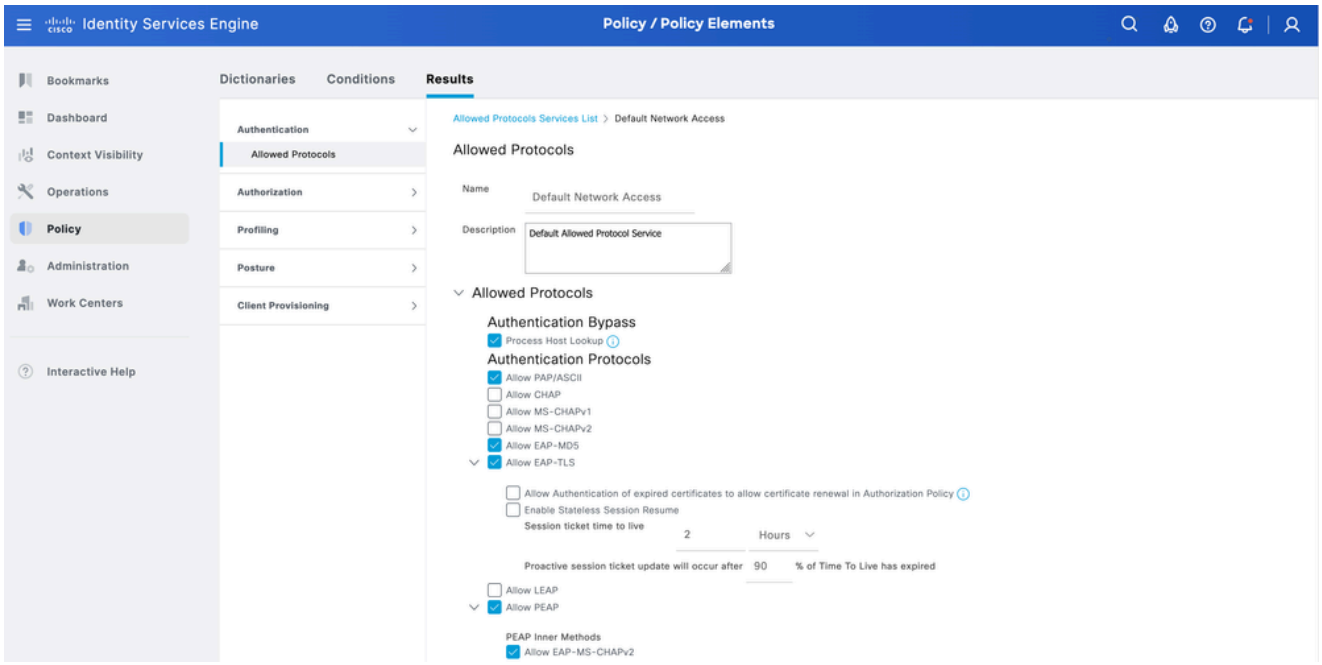
身份服务引擎配置

最后，还需要配置RADIUS服务器以允许身份验证。有线Dot1x有广泛的指南[5],因此我们只关注本案例中的相关部分。

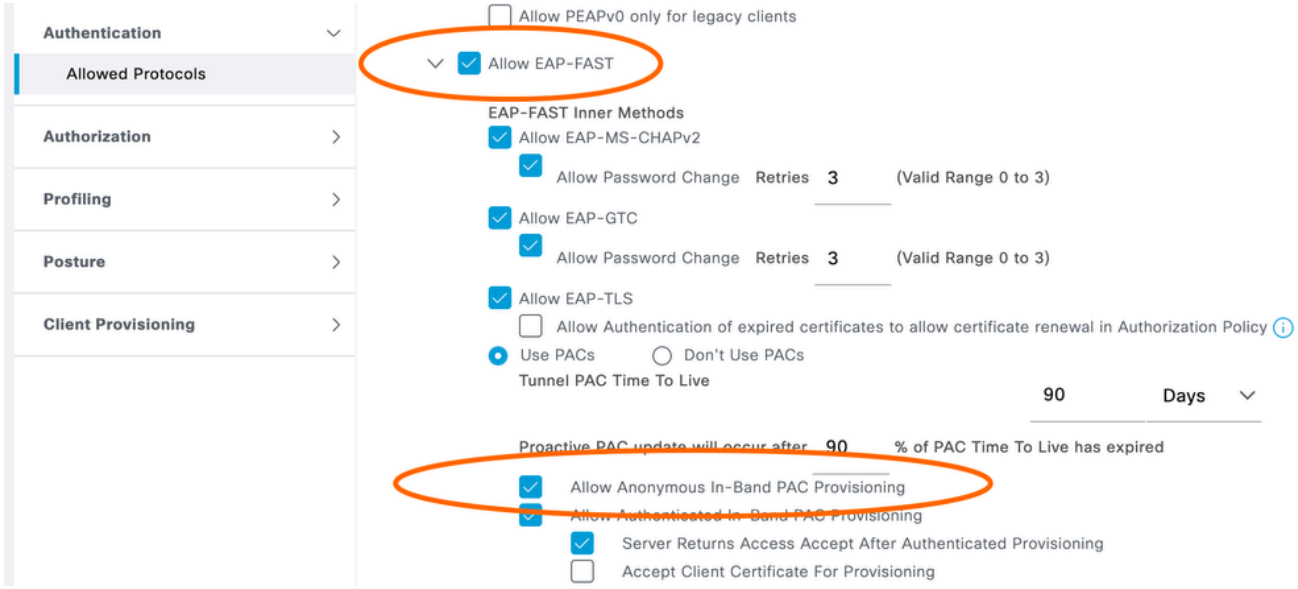
1. 将交换机添加为网络接入设备：
   >管理>网络资源>网络设备>添加



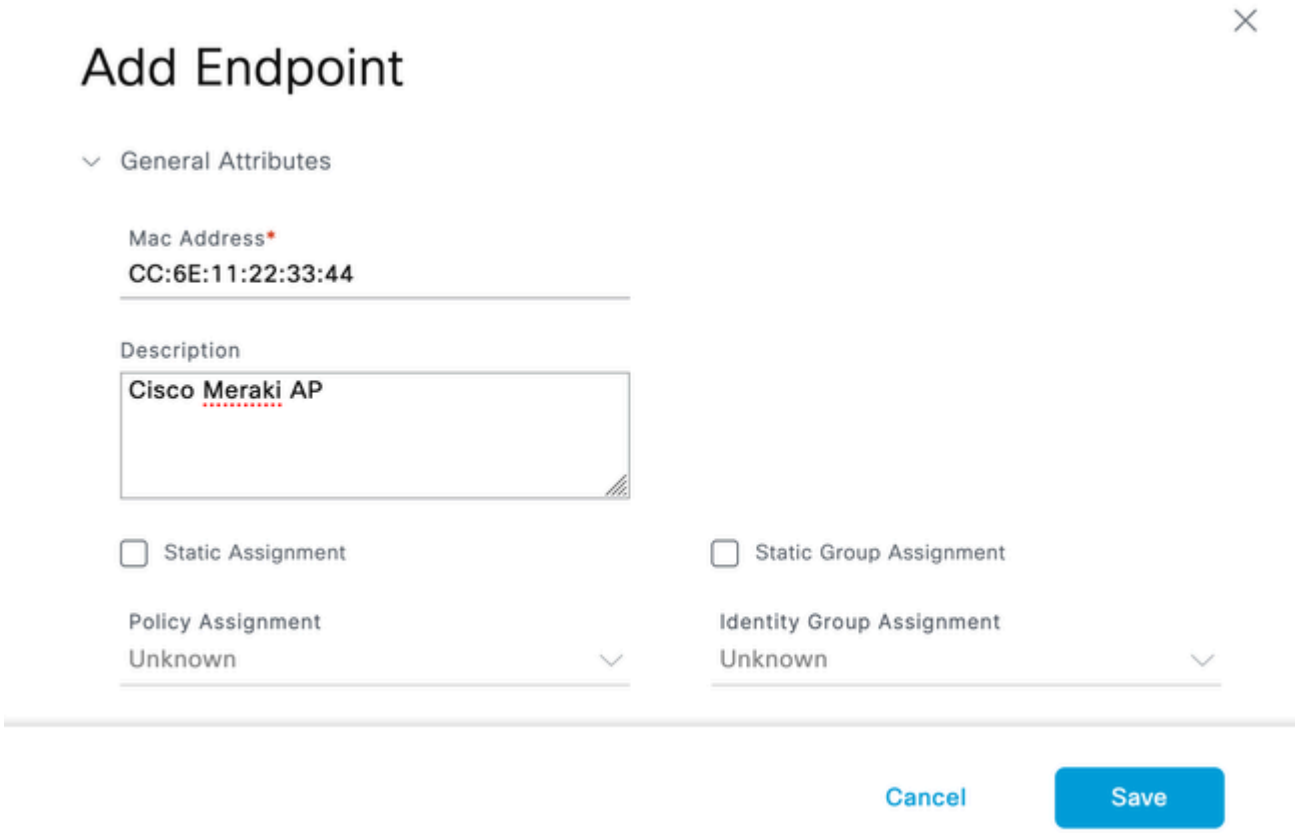
2. 启用您正在使用的EAP协议：
   >策略>Policy元素>结果>身份验证>允许的协议



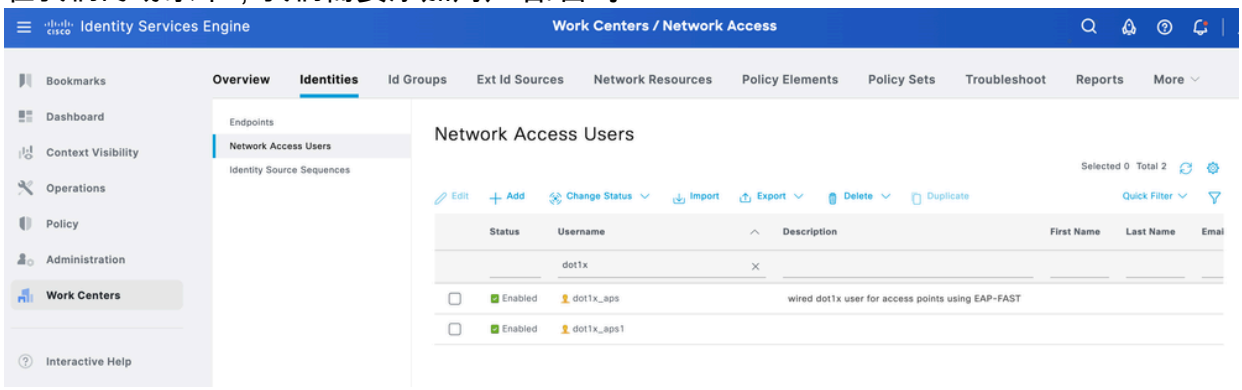
3. 对于我们的场景，由于我们使用EAP-FAST，请记住，必须启用“Anonymous In-band PAC Provisioning”：



4. 添加身份
>工作中心(Work Centers)>网络访问(Network Access)>身份(Identities)
    a. 要成功运行，该过程通常包括两个步骤。最初，AP没有凭证，因此无法响应EAP身份验证。因此，交换机端口必须首先使用MAB对AP进行身份验证。这可以基于通用授权策略、基于位置的策略或设备分析。无论使用何种策略，初始MAB身份验证都必须成功允许AP通过CAPWAP从WLC或通过即插即用(PnP)从Cisco Catalyst Center获取其凭证。

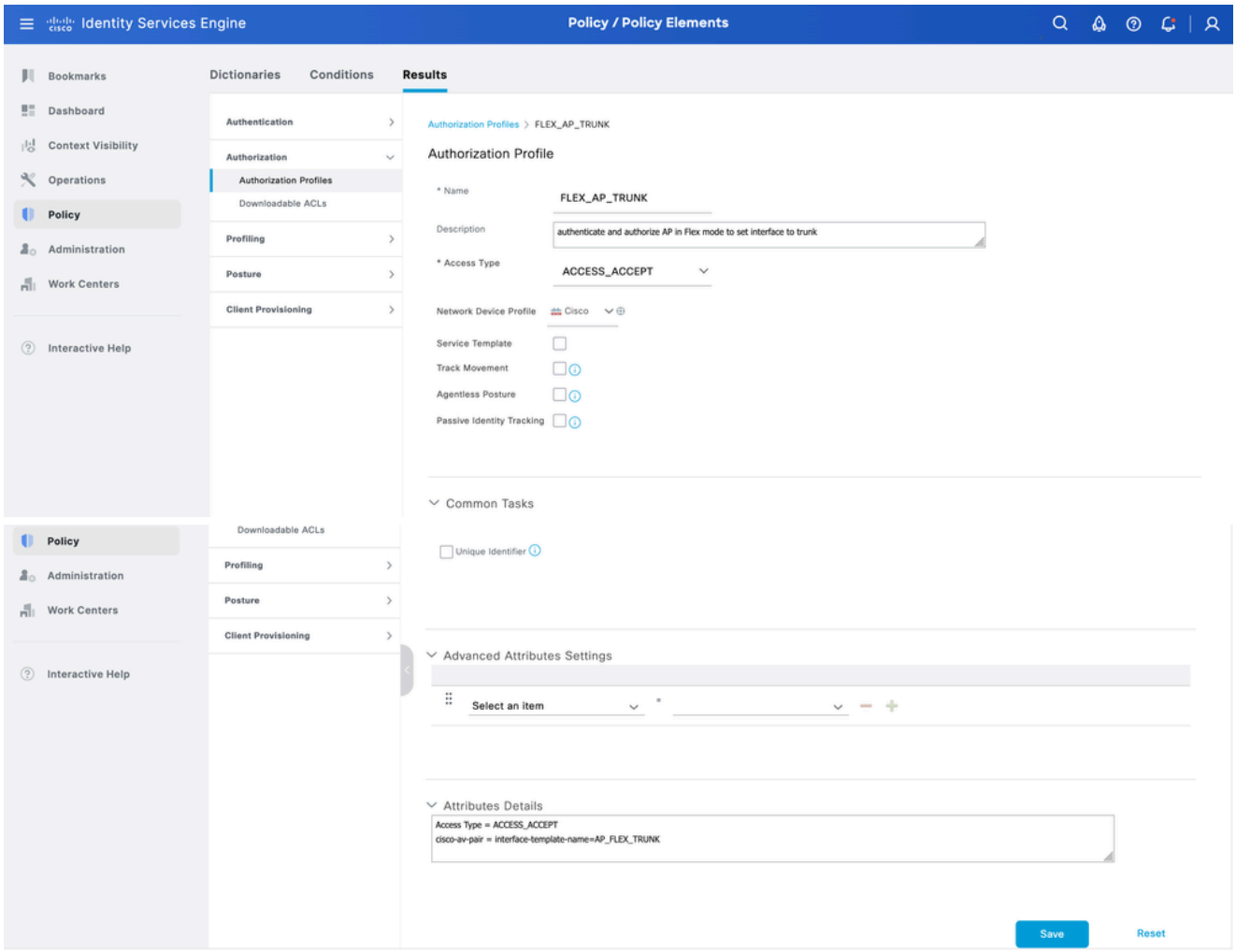


b. AP收集凭证/证书后，AP有线Dot1X请求方响应EAPoL，Dot1X是身份验证的后续方法，用于启用AP以完全访问。
在我们的场景中，我们需要添加用户名/密码：



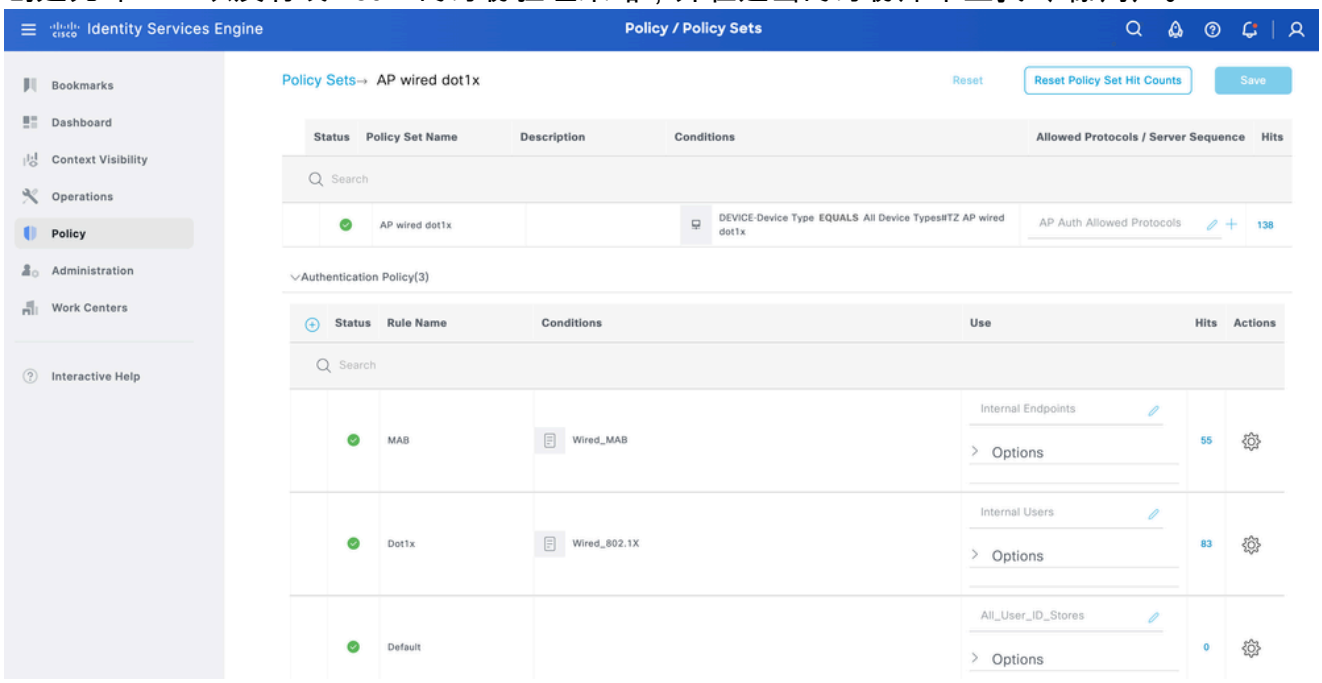
5. 创建授权配置文件
授权配置文件使用所需的av-pair做出响应。在本例中，在动态修改交换机端口时，需要配置接口模板：
> Policy > Policy Elements > Results > Authorization > Authorization Profiles

名称：FLEX_AP_TRUNK
访问类型：ACCESS_ACCEPT
接口模板：AP_FLEX_TRUNK

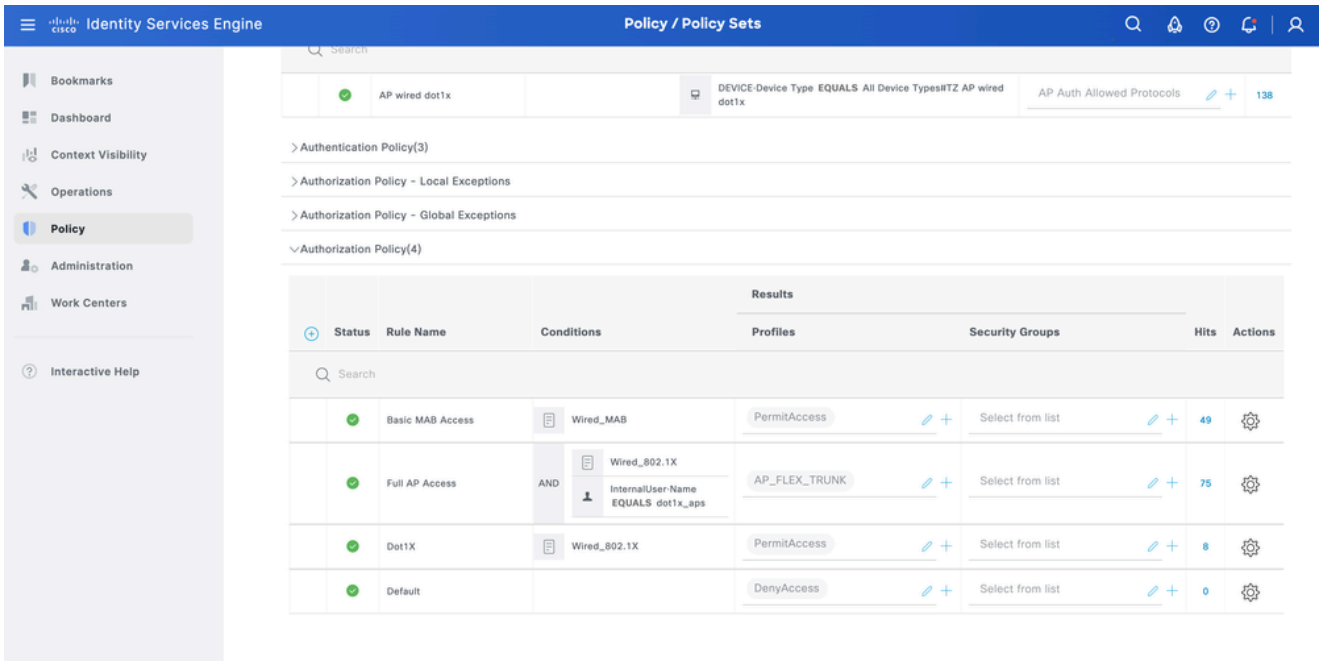


6. 创建授权策略

创建允许MAB以及有线Dot1X的身份验证策略，并在适当的身份库中查找终端/用户。



根据您对MAB的需要，输入有限访问授权结果，并输入完整的AP访问，包括引用的Dot1x接口模板av-pair:



验证

完成此配置后，将AP连接到交换机。作为前提条件，我们预期接入VLAN中的默认网络设置（在本例中带有选项43的DHCP池指向WLC，并且AP可以与WLC进行CAPWAP通信）。

AP命令

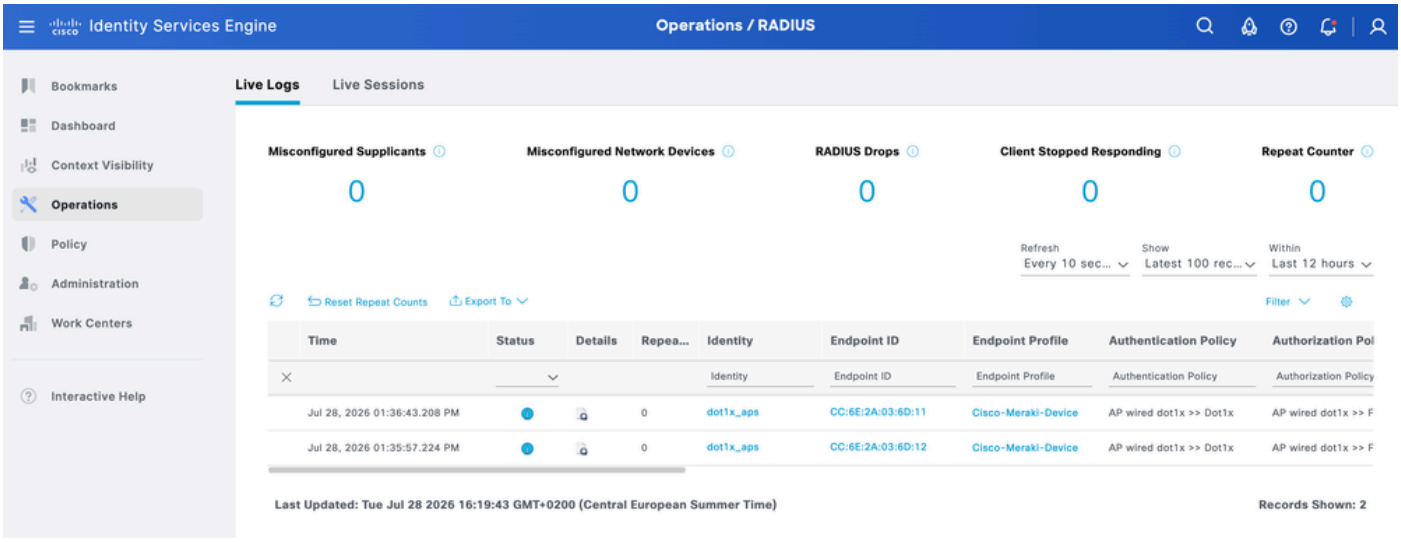
```
show ap authentication status
show crypto
show crypto pki trustpool
```

交换机命令

```
show access-session
show aaa servers
show access-session interface <INTERFACE> details
show template interface binding target <INTERFACE>
show derived-config interface <INTERFACE>

Sample output:
!
C9350-02-R11#show access-session interface te1/0/1
Interface MAC Address Method Domain Status Fg Session ID
-----------------------------------------------------------------------------------------
Te1/0/1 6cef.1122.3344 dot1x DATA Auth 09FE1FAC000000948FF60A2F
```

ISE



缩写词列表

缩写	扩展
AAA	验证、授权和记帐
无线接入点	接入点
身份验证	身份验证
身份验证	授权
CA	证书颁发机构
CISP	客户端信息信令协议
Dot1x	IEEE 802.1X
EAP	可扩展认证协议
EST	通过安全传输进行注册
FAST	通过安全隧道的灵活身份验证
IBNS	基于身份的网络服务
ISE	身份服务引擎
MAB	MAC 身份验证绕行
NAD	网络接入设备
PEAP	受保护的可扩展身份验证协议
SCEP	简单证书注册协议
TLS	传输层安全性

WLC	无线 LAN 控制器

参考资料

[1]在AP上为PEAP或采用LSC的EAP-TLS配置802.1X

[2]在9800 WLC上为本地重要的证书调配配置SCEP

[3]思科无线EST内部部署指南

[4]安全AP自注册 — 增强型网络安全简介

[5] ISE安全有线接入规范部署指南

[6] LSC配置指南部分

[7]配置9800控制器接入点的802.1X请求方

[8]用Dot1x保护Flexconnect AP交换机端口

[9] Cisco Catalyst 9800系列无线控制器软件配置指南，Cisco IOS XE 17.18.x - 802.1x

[11] Cisco Catalyst Center用户指南，版本3.2.x — 为Cisco IOS XE设备的AP配置文件配置管理设置

[12]使用IBNS 2.0和接口模板进行默认交换机端口配置

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。