



集成

以下各节介绍思科ISE上的无线设置配置以及交换机和无线控制器上支持思科ISE功能所需的配置。

- [使交换机能够支持标准 Web 身份验证，第 1 页](#)
- [为综合 RADIUS 事务定义本地用户名和密码，第 2 页](#)
- [配置 NTP 服务器以获得准确的日志和记账时间戳，第 2 页](#)
- [启用 AAA 功能的命令，第 2 页](#)
- [交换机上的 RADIUS 服务器配置，第 3 页](#)
- [将交换机配置为向 Inline Posture 节点发送 RADIUS 记帐开始/停止消息，第 3 页](#)
- [启用交换机处理 RADIUS 更改授权 \(CoA\)，第 4 页](#)
- [在交换机端口上启用设备跟踪和 DHCP 监听，第 4 页](#)
- [为交换机端口启用 802.1X 基于端口的身份验证，第 4 页](#)
- [为关键身份验证启用 EAP，第 5 页](#)
- [使用恢复延迟来限制 AAA 请求，第 5 页](#)
- [根据实施状态定义 VLAN，第 5 页](#)
- [交换机上的本地（默认）访问列表 \(ACL\) 定义，第 6 页](#)
- [对 802.1X 和 MAB 启用交换机端口，第 7 页](#)
- [启用 EPM 日志记录，第 9 页](#)
- [启用交换机以接收 SNMP 陷阱，第 9 页](#)
- [在交换机上启用 SNMP v3 查询以进行分析，第 9 页](#)
- [启用 MAC 通知陷阱以使分析器进行收集，第 9 页](#)
- [在交换机上配置 RADIUS 空闲超时，第 10 页](#)
- [用于 iOS 请求方调配的无线控制器配置，第 10 页](#)
- [Apple 设备的无线 LAN 控制器支持，第 10 页](#)
- [在无线控制器上配置 ACL 以实现 MDM 互操作性，第 11 页](#)

使交换机能够支持标准 Web 身份验证

请确保在交换机配置中包含以下命令，以为思科ISE启用标准 Web 身份验证功能，包括身份验证后的 URL 重定向调配：

```
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.2.3

ip http server
! Must enable HTTP/HTTPS for URL-redirectation on port 80/443

ip http secure-server
```

为综合 RADIUS 事务定义本地用户名和密码

输入以下命令以使交换机像该网络的 RADIUS 一样与思科 ISE 节点通信：

```
username test-radius password 0 abcde123
```

配置 NTP 服务器以获得准确的日志和记账时间戳

输入以下命令，确保在交换机上指定的 NTP 服务器与思科 ISE 中的设置相同：

```
ntp server <IP_address>|<domain_name>
```

启用 AAA 功能的命令

在交换机上输入以下命令可启用交换机与思科 ISE 之间的各种 AAA 功能，包括 802.1X 和 MAB 身份验证功能：

```
aaa new-model
! Creates an 802.1X port-based authentication method list

aaa authentication dot1x default group radius
! Required for VLAN/ACL assignment

aaa authorization network default group radius
! Authentication & authorization for webauth transactions

aaa authorization auth-proxy default group radius
! Enables accounting for 802.1X and MAB authentications

aaa accounting dot1x default start-stop group radius
!

aaa session-id common
```

```
!  
aaa accounting update periodic 1440  
  
! Update AAA accounting information periodically every 1440 minutes  
  
aaa accounting system default start-stop group radius  
  
!
```

交换机上的 RADIUS 服务器配置

输入以下命令，将交换机配置为与用作 RADIUS 源服务器的思科 ISE 进行互操作：

```
!  
radius-server <ISE Name>  
  
! ISE Name is the name of the ISE PSN  
  
address ipv4 <ip address> auth-port 1812 acct-port 1813  
  
! IP address is the address of the PSN. This example uses the standard RADIUS ports.  
  
key <passwd>  
  
! passwd is the secret password configured in Cisco ISE  
  
exit
```



注释 我们建议将死亡标准时间配置为 30 秒，期间允许 3 次重试，为使用 Active Directory 进行身份验证的 RADIUS 请求提供更长的响应时间。

将交换机配置为向 Inline Posture 节点发送 RADIUS 记帐开始/停止消息

将网络接入设备配置为在会话开始和结束时发送 RADIUS 记账“开始”和“停止”消息。发送到内联安全评估节点的消息包含远程设备的 IP 地址。内联安全评估节点将设备 IP 地址与在会话持续期间下载的任何相关授权配置文件关联。例如，某个远程设备在初始登录时可能会有一个“合规性状态未知”授权配置文件，然后在 CoA 之后（假设设备安全评估成功）会改为“合规”授权配置文件。

启用交换机处理 RADIUS 更改授权 (CoA)

请通过输入以下命令，指定设置以确保交换机能够相应地处理 RADIUS CoA 和相关的思科 ISE 的安全状态功能：

```
aaa server radius dynamic-author client <ISE-IP> server-key 0 abcde123
```



注释

- 思科 ISE 将端口 1700（思科 IOS 软件默认端口）与 RFC 默认端口 3799 用于 CoA。现有 Cisco Secure ACS 5.x 客户如果将 CoA 作为现有 ACS 实施的环节，则可能已将此端口设置为端口 3799。
- 密钥应与添加网络设备时在思科 ISE 上配置的密钥相同，并且 IP 地址应为 PSN IP 地址。

在交换机端口上启用设备跟踪和 DHCP 监听

要帮助提供思科 ISE 面向安全的可选功能，请在交换机端口动态 ACL 中针对 IP 替代启用设备跟踪和 DHCP 监听，您可输入以下命令：

```
! Optional
ip dhcp snooping

! Required!

! Configure Device Tracking Policy!device-tracking policy <DT_POLICY_NAME>no protocol
ndp tracking enable

! Bind it to interface!interface <interface_id>device-tracking
attach-policy<DT_POLICY_NAME>
```

在 RADIUS 记帐中，即便已启用 DHCP 监听，DHCP 属性也不会通过 IOS 传感器发送到思科 ISE。在这种情况下，则应启用 VLAN 的 DHCP 监听使 DHCP 成为活动状态。

使用以下命令启用 VLAN 的 DHCP 监听：

```
ip dhcp snooping
ip dhcp snooping vlan 1-100
```

为交换机端口启用 802.1X 基于端口的身份验证

输入以下命令在全局范围内开启交换机端口的 802.1X 身份验证：

```
dot1x system-auth-control
```

为关键身份验证启用 EAP

要支持局域网上的请求方身份验证请求，请输入以下命令，为临界身份验证（不可访问的身份验证绕行）启用 EAP：

```
dot1x critical eapol
```

使用恢复延迟来限制 AAA 请求

在关键身份验证恢复的情况下，配置交换机以自动引入身份验证延迟（以毫秒为单位），确保思科 ISE 可以在恢复后再次启动服务。使用以下命令：

```
authentication critical recovery delay 1000
```

根据实施状态定义 VLAN

输入以下命令，根据网络中已知的实施状态，定义 VLAN 名称、编号和虚拟交换机接口 (SVI)。创建单独的 VLAN 接口，实现网络间路由。对于处理来自终端（如 PC、笔记本电脑）和终端通过其连接到网络的 IP 电话等在同一网段上传递的多个流量源，这特别有帮助。



注释 第一个 IP 助手进入 DHCP 服务器，第二个 IP 助手将 DHCP 请求副本发送至 Inline Posture 节点进行分析。

```
vlan <VLAN_number>
name ACCESS!
vlan <VLAN_number>
name VOICE

!
interface <VLAN_number>
description ACCESS
ip address 10.1.2.3 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
ip helper-address <Cisco_ISE_IP_address>

!
interface <VLAN_number>
description VOICE
ip address 10.2.3.4 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
```

交换机上的本地（默认）访问列表 (ACL) 定义

通过输入以下命令，在较低版本的交换机（使用低于 12.2(55)SE 版本的思科 IOS 软件的交换机）上启用这些功能，确保思科 ISE 能够执行进行身份验证和授权所需的动态 ACL 更新。

```
ip access-list extended ACL-ALLOW

  permit ip any any

!

ip access-list extended ACL-DEFAULT

  remark DHCP

  permit udp any eq bootpc any eq bootps

  remark DNS

  permit udp any any eq domain

  remark Ping

  permit icmp any any

  remark Ping

  permit icmp any any

  remark PXE / TFTP

  permit udp any any eq tftp

  remark Allow HTTP/S to ISE and WebAuth portal
  permit tcp any host <Cisco_ISE_IP_address> eq www

  permit tcp any host <Cisco_ISE_IP_address> eq 443

  permit tcp any host <Cisco_ISE_IP_address> eq 8443

  permit tcp any host <Cisco_ISE_IP_address> eq 8905

  permit udp any host <Cisco_ISE_IP_address> eq 8905

  permit udp any host <Cisco_ISE_IP_address> eq 8906

  permit tcp any host <Cisco_ISE_IP_address> eq 8080

  permit udp any host <Cisco_ISE_IP_address> eq 9996
```

```
remark Drop all the rest

deny ip any any log

!

! The ACL to allow URL-redirectation for WebAuth
ip access-list extended ACL-WEBAUTH-REDIRECT

permit tcp any any eq www

permit tcp any any eq 443
```



注释 无线控制器上的这种配置可以提高 CPU 使用率，但是也会提高系统不稳定的风险。这是 IOS 问题，不会对思科 ISE 产生不利影响。

对 802.1X 和 MAB 启用交换机端口

要为 802.1X 和 MAB 启用交换机端口，请执行以下操作：

步骤 1 使所有接入交换机端口进入接口配置模式：

```
interface range FastEthernet0/1-8
```

步骤 2 启用交换机端口的接入模式（而不是中继模式）：

```
switchport mode access
```

步骤 3 静态配置接入 VLAN。这样，即可在本地调配接入 VLAN，这也是开放模式身份验证所要求的：

```
switchport access vlan <VLAN_number>
```

步骤 4 静态配置语音 VLAN：

```
switchport voice vlan <VLAN_number>
```

步骤 5 启用开放模式身份验证。身份验证完成之前，开放模式允许将流量桥接至数据和语音 VLAN。我们强烈建议您在生产环境中使用基于端口的 ACL，以防止进行未经授权的访问。

启用开放模式身份验证还会在 AAA 服务器响应之前允许预身份验证访问，具体取决于端口 ACL。

```
authentication open
```

步骤 6 应用基于端口的 ACL，确定默认情况下应将哪些流量从未经授权的终端桥接至接入 VLAN。由于您应首先允许所有访问，然后再实施策略，因此您应当应用 ACL-ALLOW，以允许所有流量都流经交换机端口。您已创建默认的思科 ISE 授权，允许到目前为止的所有流量，这是因为我们希望实现完全可见性，并且不希望影响到现有最终用户的体验。

必须配置 ACL 才能从 AAA 服务器预设定动态 ACL。

```
ip access-group ACL-ALLOW in
```

注释 在 DSBU 交换机上使用思科 IOS 软件版本 12.2(55)SE 之前，需提供端口 ACL 才能从要应用的 RADIUS AAA 服务器获取动态 ACL。如果未能设置默认 ACL，交换机将忽略分配的动态 ACL。使用思科 IOS 软件版本 12.2(55)SE 时，系统会自动生成并应用默认 ACL。

注释 我们之所以在实验室中使用 ACL-ALLOW，是因为我们希望启用基于 802.1X 端口的身份验证，但不希望对现有网络造成任何影响。在稍后的练习中，我们将应用不同的 ACL-DEFAULT，以阻止生产环境中产生不需要的流量。

步骤 7 启用多身份验证主机模式。多身份验证可以说是多域身份验证 (MDA) 的超集。MDA 只允许数据域中有一个终端。当配置多身份验证时，语音域中只允许有一个身份验证电话（和 MDA 一样），但在数据域中却可以对不限数量的数据设备进行身份验证。

允许在同一个物理接入端口上使用语音和多个终端

authentication host-mode multi-auth

注释 IP 电话背后的多台数据设备（无论是虚拟设备还是连接到集线器的物理设备）都可以增强接入端口的物理链路状态感知能力。

步骤 8 通过以下命令启用各种身份验证方式的选项：

启用重新进行身份验证：

authentication periodic

通过 RADIUS 会话超时启用重新进行身份验证：

authentication timer reauthenticate server

authentication event fail action next-method

配置服务器故障情况下的关键身份验证 VLAN 方法：

authentication event server dead action reinitialize vlan <VLAN_number>

authentication event server alive action reinitialize

配置 802.1X 和 MAB 的 IOS Flex-Auth 身份验证：

authentication order dot1x mab

authentication priority dot1x mab

步骤 9 在交换机端口上启用 802.1X 端口控制：

authentication port-control auto

authentication violation restrict

步骤 10 启用 MAC 身份验证绕行 (MAB)：

mab

步骤 11 在交换机端口上启用 802.1X：

dot1x pae authenticator

步骤 12 将重传时间设置为 10 秒：

dot1x timeout tx-period 10

注释 应将 802.1X 传输超时时间设置为 10 秒。除非您了解影响，否则请勿更改此值。

步骤 13 启用 portfast 功能：

spanning-tree portfast

启用 EPM 日志记录

在交换机上设置标准日志记录功能，以支持对思科 ISE 功能进行可能的故障排除和记录：

```
epm logging
```

启用交换机以接收 SNMP 陷阱

确保交换机能够通过网段中的适当 VLAN，从思科 ISE 接收 SNMP 陷阱传输：

```
snmp-server community public RO
snmp-server trap-source <VLAN_number>
```

在交换机上启用 SNMP v3 查询以进行分析

使用以下命令来配置交换机，确保按预期执行 SNMP v3 轮询以支持思科 ISE 分析服务。在此之前，请在 **SNMP 设置 (SNMP Settings)** 窗口的思科 ISE GUI 中配置 SNMP 设置。此窗口的导航路径为：**管理 (Administration)** **网络资源 (Network Resources)** **网络设备 (Network Devices)** **添加 (Add)** | **编辑 (Edit)** **SNMP 设置 (SNMP Settings)**。

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>
snmp-server group <group> v3 priv
snmp-server group <group> v3 priv contextvlan-1
```



注释 必须为每个情景配置 `snmp-server group <group> v3 priv context vlan-1` 命令。`snmp show context` 命令会列出所有上下文信息。

如果 SNMP 请求超时并且不存在连接问题，则可以提高超时值。

启用 MAC 通知陷阱以使分析器进行收集

配置您的交换机以传送适当的 MAC 通知陷阱，这样思科 ISE 分析器功能就可以收集网络终端上的信息：

```
mac address-table notification change
mac address-table notification mac-move
snmp trap mac-notification change added
snmp trap mac-notification change removed
```

在交换机上配置 RADIUS 空闲超时

要在交换机上配置 RADIUS 空闲超时，请使用以下命令：

```
Switch(config-if)# authentication timer inactivity
```

其中 *inactivity* 是以秒为单位的非活动时间间隔，这个时间之后，客户端活动将被视为未授权。

在思科 ISE 中，可以为这类会话非活动计时器应用到的任何授权策略启用此选项。依次选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权 (Authorization) > 授权配置文件 (Authorization Profiles)。

用于 iOS 请求方调配的无线控制器配置

对于单 SSID

要支持基于 Apple iOS 的设备 (iPhone 或 iPad) 从一个 SSID 切换至同一无线接入点的另一个 SSID，请将无线控制器配置为启用 **FAST SSID change** 功能。此功能有助于确保基于 IOS 的设备能够在 SSID 之间快速切换。

对于双 SSID BYOD

必须启用快速 SSID 以支持双 SSID BYOD。启用快速 SSID 更改后，无线控制器允许客户端在 SSID 间更快速移动。启用快速 SSID 时，不会清除客户端条目，也不会强制执行延迟。有关在思科无线控制器上配置快速 SSID 的详细信息，请参阅《[Cisco Wireless Controller 配置指南](#)》。

无线控制器配置示例

```
WLC (config)# FAST SSID change
```

当您尝试在某些基于 Apple iOS 的设备中连接无线网络时，您可以会看到以下错误信息：

```
Could not scan for Wireless Networks.
```

您可以忽略该错误消息，因为这不会影响设备的身份验证。

Apple 设备的无线 LAN 控制器支持

Apple 设备包括 Apple Captive Network Assistant (CNA) 功能，此功能可检查强制网络（例如思科 ISE WebAuth 页面），但是会干扰支持访客和个人设备所需的门户重定向。

您可以通过在无线 LAN 控制器 (WLC) 上启用 **web-auth captive-bypass enable** 命令绕过此功能：

```
WLC > config network web-auth captive-bypass enable
```

```
Web-auth support for Captive-Bypass will be enabled.
```

```
You must reset system for this setting to take effect.
```

```
WLC > save config
Are you sure you want to save? (y/n) y
Configuration Saved!
WLC >
```

在无线控制器上配置 ACL 以实现 MDM 互操作性

在无线控制器上配置 ACL 以用于授权策略，从而重定向未注册的设备证书调配。ACL 必须采用以下顺序。

- 步骤 1 允许所有从服务器到客户端的出站流量。
- 步骤 2 （可选）允许从客户端到服务器的 ICMP 进站流量以进行故障排除。
- 步骤 3 允许未注册和不合规设备访问 MDM 服务器，以下载 MDM 代理和执行合规检查。
- 步骤 4 允许从客户端到服务器再到 ISE 的所有进站流量以执行 Web 门户和请求方以及证书调配流程。
- 步骤 5 允许从客户端到服务器的进站域名系统 (DNS) 流量以进行名称解析。
- 步骤 6 允许从客户端到服务器的进站 DHCP 流量以获取 IP 地址。
- 步骤 7 拒绝所有从客户端到服务器再到企业资源的进站流量，以重定向至思科 ISE（根据公司策略）。
- 步骤 8 （可选）允许其余流量。

示例

以下示例显示的 ACL 用于将未注册的设备重定向至 BYOD 流程。在本例中，思科 ISE IP 地址为 10.35.50.165，内部企业网络 IP 地址为 192.168.0.0 和 172.16.0.0（重定向），MDM 服务器子网为 204.8.168.0。

图 1: 用于重定向未注册设备的 ACL

General									
Access List Name		NSP-ACL							
Deny Counters		0							
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。