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。

• 在无线 LAN 控制器上配置 ACL 以实现移动设备管理互操作 ， 第 21 页

什么是无线设置

无线设置为设置802.1X、访客和BYOD服务无线流提供了一种简单的方法。适当情况下，它还提供工作流程，用于为访客和 BYOD 服务配置和自定义每个门户。这些工作流程提供最常见的建议设置，要比在 Cisco ISE 中配置关联门户流程简单得多。无线设置会代为执行原本您需要在 Cisco ISE 和无线控制器中自己完成的许多步骤，以便您能够快速创建工作环境。

您可以使用无线设置创建的环境来测试和开发自己的流程。无线设置环境正常运行后，您可能希望切换到 Cisco ISE，以便支持高级的配置。有关在 Cisco ISE 中配置访客服务的详细信息，请参阅您的 Cisco ISE 版本对应的 《 ISE 管理员指南》 和 Cisco 社区站点 https://community.cisco.com/t5/security-documents/ise-guest-amp-web-authentication/ta-p/3657224 。有关为 Cisco ISE 配置和使用无线设置的详细信息，请参阅 https://community.cisco.com/t5/security-documents/cisco-ise-secure-access-wizard-saw-guest-byod-and-secure-access/ta-p/3636602。

注释 Cisco ISE 无线设置为测试版软件 - 请勿在生产网络中使用。

- 全新安装思科ISE后，无线设置默认被禁用。您可以在Cisco ISE CLI中使用 **application configure ise** 命令（选择选项 17）或使用 Cisco ISE GUI 主页中的 **无线设置** 选项 ( ) 启用无线设置。
- 如果从以前的版本升级 Cisco ISE，无线设置将不起作用。只有新安装的 Cisco ISE 才支持无线设置。
- 无线设置仅适用于独立节点。
- 一次只能运行一个无线设置的实例。一次只能有一个人运行无线设置。
- 无线设置需要打开端口 9103 和 9104。要关闭这些端口，请使用 CLI 禁用无线设置。
- 如果要在运行某些流程后开始全新安装无线设置，可以使用 CLI 命令 **application reset-config ise**。此命令会重置 Cisco ISE 配置并清除 Cisco ISE 数据库，但保留网络定义。因此，您可以重置 Cisco ISE 和无线设置，而无需重新安装 Cisco ISE 并运行设置。

  如果要从无线设置重新开始，可以通过以下步骤同时重置 Cisco ISE 和无线设置的配置：

  - 在 CLI 中，运行 **application reset-config** 以重置所有 Cisco ISE 配置。如果您在全新安装中测试无线设置，此命令会删除无线设置在 Cisco ISE 中完成的配置。
  - 在 CLI 中，运行 **application configure ise**，然后选择 **[18]重置配置 Wi-Fi 设置**。这将清理无线设置配置数据库。
  - 在无线控制器上，删除无线设置在无线控制器上添加的配置。有关无线设置在无线控制器上的配置的信息，请参阅 通过无线设置流程对 Cisco ISE 和无线控制器进行更改 ， 第 10 页。

  您可以在完成 Cisco ISE 全新安装后为虚拟机创建快照，以便避免这些步骤。

有关 CLI 的详细信息，请参阅 ISE 版本对应的《思科身份服务引擎 CLI 参考指南》。

- 您必须是 Cisco ISE 超级管理员用户才能使用无线设置。
- 无线设置需要至少两个 CPU 核心和 8 GB 内存。
- 仅支持活动目录组和用户。在无线设置中创建一个或多个流后，其他类型的用户、组和授权将可用于无线设置，但必须在 ISE 上进行配置。
- 如果已在 Cisco ISE 中定义 Active Directory，并计划将此 AD 用于无线设置，则：
  - 加入名称和域名必须相同。如果名称不同，请在 Cisco ISE 中使之相同，然后在无线设置中使用该 AD。
  - 如果您的无线控制器已经在 Cisco ISE 上配置好，那么无线控制器必须配置好一个共享密钥。如果无线控制器定义没有共享密钥，请添加共享密钥或从 Cisco ISE 中删除无线控制器，然后在无线设置中配置该无线控制器。
- 无线设置可以配置 Cisco ISE 组件，但在流程启动后无法删除或修改这些组件。有关无线设置在 Cisco ISE 中配置的所有项目的列表，请参阅 ISE 版本对应的 《Cisco 身份服务引擎 CLI 参考指南》 。
- 启动流程时，必须完成该流程。点击流程中的痕迹可停止流程。当您逐步完成流程时，系统会动态更改 Cisco ISE 配置。无线设置会提供配置更改列表，以便您可以手动恢复。您无法在流程中后退以进行额外的更改，只有一个例外。您可以返回以更改访客或 BYOD 门户自定义。
- 支持多个无线控制器和 Active Directory 域，但每个流程只能支持一个无线控制器和一个 Active Directory。
- 无线设置需要思科 ISE Basic 许可证才能运行。BYOD 需要思科 ISE Plus许可证。
- 如果在配置无线设置之前配置了 Cisco ISE 资源，则无线设置可能与现有策略存在冲突。如果发生这种情况，无线设置会建议您在运行该工具后查看授权策略。我们建议在运行无线设置时从干净设置 Ciisco ISE 开始。对无线设置和 Cisco ISE 混合配置的支持有限。
- 无线设置支持英语，但不支持其他语言。如果要在门户中使用其他语言，请在运行无线设置后在 Cisco ISE 中配置。
- BYOD 支持双 SSID。由于冲突，此配置中使用的开放 SSID 不支持访客访问。如果需要同时支持访客和 BYOD 的门户，则无法使用无线设置，并且不在本文档的讨论范围之内。
- **电子邮件和 SMS 通知**
  - 对于自注册访客，支持 SMS 和电子邮件通知。这些通知应在门户自定义通知部分进行配置。您必须将 SMTP 服务器配置为支持 SMS 和电子邮件通知。Cisco ISE 中内置的蜂窝服务提供方（包括 AT&T、T Mobile、Sprint、Orange 和 Verizon）已预先配置，是免费的邮件短信网关。
  - 访客可以在门户中选择其蜂窝网络提供方。如果其提供方不在列表中，则他们无法接收消息。您还可以配置全局提供方，但这不属于本指南的范围。如果访客门户配置了 SMS 和电子邮件通知，则必须为这两项服务输入值。

- 发起的访客流程不会在无线设置中提供 SMS 或电子邮件通知配置。对于该流程，必须在 Cisco ISE 中配置通知服务。
- 为门户配置通知时，请勿选择 SMS 提供方 *Global Default*。未配置此提供方（默认情况下）。

- 无线设置仅支持无 HA 的独立设置。如果决定使用额外的 PSN 进行身份验证，请将这些 PSN 的 Cisco ISE IP 地址添加到w无线控制器的 RADIUS 配置。

无线设置对 Apple 迷你浏览器（强制网络助理）的支持

- **访客流**：Apple伪浏览器的自动弹出功能适用于所有访客流。访客可以使用Apple的强制网络助理浏览器完成整个流程。当 Apple 用户连接到 OPEN 网络时，迷你浏览器会自动弹出，可以让他们接受 AUP（热点），或者完成自我注册或使用其凭证登录。
- **自带设备**
  - **单 SSID**：ISE 2.2 增加了对 Apple 迷你浏览器的支持。但是，为了限制 Apple 设备上潜在的 SSID 流问题，我们向重定向 ACL 中添加了 captive.apple.com，以便抑制迷你浏览器。这会导致 Apple 设备认为它可以访问互联网。用户必须手动启动 Safari 浏览器，才能重定向到门户以进行 Web 身份验证或设备激活。
  - **双 SSID**：对于从初始 OPEN 网络 WLAN 开始，然后启动访客访问，或允许员工经过设备激活 (BYOD) 并重定向到安全 SSID 的双 SSID 流，迷你浏览器也会被抑制。

有关 Apple CAN 迷你浏览器的详细信息，请参阅https://communities.cisco.com/docs/DOC-71122。

在无线网络中配置无线控制器

首次启动无线设置并选择流时，系统会要求您配置无线控制器。无线设置会将必要的设置推送到无线控制器以支持您正在配置的流类型。

- 无线控制器必须是运行 AireOS 8.x 或更高版本 Cisco 无线控制器。
- 虚拟无线控制器不支持基于 DNS 的 ACL。
- 为计划在无线设置部署中使用的接口 VLAN（网络）配置无线控制器。默认情况下，无线控制器具有管理接口，但建议您为访客和安全访问（员工）网络配置其他接口。
- 对于访客流，ACL_WEBAUTH_REDIRECT ACL 用于将访客设备重定向到热点或需要提供凭证的门户，以接受 AUP（热点）、登录或创建凭证。访客获得授权后，系统将允许他们访问 (ACCESS-ACCEPT)。您可以在无线控制器上使用 ACL 来限制客人的权限。要做到这一点，在无线控制器上创建一个 ACL，并在客人权限授权配置文件中使用该 ACL。要允许访问 Cisco ISE 的成功页面，请在无线控制器上添加此 ACL。有关创建限制性 ACL 的详细信息，请参阅 https://communities.cisco.com/docs/DOC-68169。

- 无线设置为每个流配置 WLAN。为流配置 WLAN 后，此 WLAN 便无法用于任何其他流。如果您为自行注册流配置了 WLAN，并且稍后决定将此 WLAN 用于发起的访客流以同时处理访客的自行注册和发起，此情况为唯一例外情况。

  如果在生产环境中运行无线设置，您的配置可能会与某些现有用户断开连接。

- 如果在无线设置中使用无线控制器配置流，请勿在 ISE 中删除此无线控制器。
- 如果已在 Cisco ISE 中配置了无线控制器，但未在 RADIUS 选项中配置共享密钥，则必须先添加共享密钥，然后才能在无线设置中使用此无线控制器。
- 如果已在 ISE 中配置了无线控制器，并且配置了共享密钥，则请勿使用无线设置配置其他共享密钥。无线设置和 Cisco ISE 加密密码必须匹配。您选择的 WLAN 在整个流中处于禁用状态，但可以在流结束时通过点击**上线 (Go Live)** 按钮将其重新启用。
- **远程 LAN**： 如果网络具有远程 LAN，则当无线设置尝试使用已分配给此远程 LAN 的 VLAN ID时将失败。要解决此问题，请在运行无线设置之前删除远程LAN，或者创建您计划在无线控制器上使用的 VLAN。在无线设置中，可以为流启用这些现有 VLAN。
- **FlexConnect**：Flexconnect 本地交换机和 Flexconnect ACL 由无线设置进行配置，但不会使用或支持它们。无线设置仅适用于 Flexconnect 集中式或本地模式无线接入点和 SSID。

无线配置示例

以下无线控制器日志提取内容显示了无线设置在您配置流时执行的配置示例。

```
"config radius auth add 1 192.168.201.228 1812 ascii cisco"
"config radius auth disable 1"
"config radius auth rfc3576 enable 1"
"config radius auth management 1 disable"
"config radius auth enable 1"
"config radius acct add 1 192.168.201.228 1813 ascii cisco"
"config radius acct enable 1"
"config acl create ACL_WEBAUTH_REDIRECT"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule source address ACL_WEBAUTH_REDIRECT 1 192.168.201.228 255.255.255.255"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule destination address ACL_WEBAUTH_REDIRECT 1 192.168.201.228 255.255.255.255"
"config acl apply ACL_WEBAUTH_REDIRECT"
"show flexconnect acl summary"
"config flexconnect acl create ACL_WEBAUTH_REDIRECT"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53"
```

```
"config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule source address ACL_WEBAUTH_REDIRECT 1 192.168.201.228
255.255.255.255"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule destination address ACL_WEBAUTH_REDIRECT 1 192.168.201.228
255.255.255.255"
"config flexconnect acl apply ACL_WEBAUTH_REDIRECT"
```

带无线设置的 Active Directory

需要活动目录域才能创建发起人访客、802.1X 和 BYOD 流。活动目录可以识别发起人组的用户，以访问发起人门户、802.1X 安全访问和关联的 VLAN，以及 BYOD 和设备激活。在无线设置中配置其中任何流之后，可以选择进入 Cisco ISE 身份并添加：

- 映射到发起人组的内部发起人帐户，如 ALL_ACCOUNTS。如果使用的是 Active Directory，则不需要执行此操作。
- 属于 Cisco ISE 内部员工组的员工。确保将内部员工组添加至您的授权策略。

无线设置中的访客门户

当访问公司的人员希望使用公司网络访问互联网或者您的网络上的资源和服务时，您可以通过访客门户为他们提供网络访问权限。在进行配置后，员工可以使用这些访客门户访问您的公司网络。

三种默认访客门户：

- 热点访客门户：授予网络访问权限，而不需要任何凭证。通常，必须在授予网络访问权限之前接受可接受的用户策略 (AUP)。
- 发起人管理的访客门户：网络访问权限由创建访客帐户的发起人授予，并为访客提供登录凭证。
- 自注册访客门户：访客可以创建自己的帐户和凭证，可能需要发起人批准后才能获得网络访问权限。

思科 ISE 可托管多个访客门户，包括一组预定义的默认门户。

默认门户主题有标准思科品牌推广，您可以通过管理员门户进行自定义。

无线设置有自己的默认主题 (CSS)，您可以修改一些基本设置，如徽标、横幅、背景图像、颜色和字体。在思科 ISE 中，还可以选择更改更多设置来进一步自定义门户，并进入高级自定义设置。

访客门户工作流程

1. 选择门户类型后，系统会询问您使用哪个控制器。为每个流配置新的无线网络。您可以选择尚未在无线设置中使用的现有 WLAN，或创建新的 WLAN。

   需要重定向的流可以选择将用户重定向到原始 URL、成功页面或特定 URL（例如，www.cisco.com）。原始 URL 需要无线控制器支持。

注释 直到无线控制器 8.4 版本后才支持原始 URL。

2. 自定义外观并更改门户的基本设置。
3. 完成自定义后，遵循 URL 链接以测试门户。测试门户会向您显示门户测试版本的预览。您可以继续进行此流程，需要时可做出更多更改。请注意，这是唯一能够转到“成功”页面的成功重定向。原始URL 和静态URL 在测试门户不起作用，因为它们需要无线会话来支持重定向。测试门户不支持 RADIUS 会话，因此您将无法看到整个门户流。如果有多个 PSN，思科 ISE 会选择第一个活动 PSN。
4. 配置已完成。您可以下载并查看无线设置在 Cisco ISE 中为您执行的步骤以及工作流程期间的无线控制器。

注释 位置在无线设置中不用于基本访客访问。如果要根据本地时间控制访问，则需要位置。关于在Cisco ISE 中配置时区的信息，请参阅 SMS 运营商和服务。

无线网络自行注册门户

自行注册门户让访客能自行注册并创建自己的帐户，以便访问网络。

我们建议您不要选择登录成功页面，它会在屏幕上向用户显示登录凭证。最佳实践是通过邮件或 SMS 获取邮件凭证，如此可将其与审核用的特定内容相关联。

无线网络发起的访客流

赞助商可以使用赞助商门户为授权的访客创建和管理临时帐户，以安全地访问企业网络或互联网。创建访客帐户后，发起人还可以使用发起人门户以打印文件、邮件或短信的形式向访客提供帐户详细信息。向自助注册的访客提供对公司网络的访问权限之前，系统可能会通过邮件要求赞助商批准其访客帐户。

无线设置在发起流量期间配置赞助门户和赞助访客门户。

无线设置不支持审批流程。

您可以在工作流程中将 Active Directory 组映射到赞助商组。工作流程会将您选择的 AD 组映射到 ALL_ACCOUNTS 赞助商组。它不会配置 GROUP 或 OWN 帐户发起人组。可选，如果要添加其他身份源（如内部或 LDAP 设置）可以在 Cisco ISE 管理员 UI 中执行此操作。有关详细信息，请参阅发起人组。

无线设置 BYOD 流程 - 用于本地请求方和证书调配

自带设备 (BYOD) 门户使员工能够注册其个人设备。可以在允许访问网络之前完成本地请求方和证书调配。员工不直接访问 BYOD 门户，而是在注册个人设备时重定向到此门户。员工首次尝试使用个人设备访问网络时，系统会提示员工手动下载并启动网络设置助理 (NSA) 向导。NSA 会指导他们注册和安装本地请求方。员工注册设备后，就可以使用 My Devices 门户管理设备。

无线设置可以为本地请求方和证书调配配置 Cisco ISE 和控制器。用户与控制器建立 PEAP 连接，提供凭证，然后连接切换到 EAP-TLS（证书）。

无线设置支持以下设备：Apple 设备（Mac 和 iOS）、Windows 桌面操作系统（但不支持移动设备）和 Android。无线设置不支持 Chrome 操作系统激活。

如果是 Android 设备，请确保已启用基本身份验证访问策略，以使单个或两个基于 EAP-TLS 的 BYOD 流成功。转到**策略 (Policy)** > **策略集 (Policy Sets)** > **默认 (Default)** > **授权策略 (Authorization Policy)**，并确保 **Basic_Authenticated_Access** 规则处于活动状态。

注释 双 SSID 流包括用于激活的开放网络和用于身份验证访问的基于 TLS 证书的安全网络。设备可以连接到安全网络，而无需激活。这是因为 **Basic_Authenticated_Access** 默认规则允许任何有效的身份验证通过。当设备连接到安全网络时，它们与 BYOD 受保护的授权规则不匹配，匹配项将落到 **Basic_Authenticated_Access** 规则列表的底部。

解决方法是禁用授权策略下的 **Basic_Authenticated_Access** 规则，或者编辑规则以匹配特定 SSID (WLAN)。两种更改均会阻止 PEAP 连接，阻止不应允许的连接。

注释 无线设置没有授权规则来重定向标记为丢失的设备。此操作通过阻止设备完成，该列表由黑名单门户管理。有关管理丢失和被盗设备的信息，请参阅 http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/Managing_Lost_or_Stolen_Device.pdf。

无线设置中的 BYOD 流程

无线设置中的 BYOD 配置包括以下步骤：

1. 选择或注册无线局域网控制器。
2. 添加无线网络。

注释 新的 Cisco ISE 安装包括默认无线网络。如果是双 SSID BYOD，当用户重定向到第二个 SSID 时，还将在其网络配置文件中看到默认网络 SSID。您可以删除默认 SSID，或告诉用户忽略它。

3. 选择或加入 Cisco ISE 至 Active Directory (AD)：您可以覆盖激活 VLAN 和最终访问 VLAN 二者的默认 VLAN 设置。最终访问 VLAN 会映射到 Active Directory 组。
4. 自定义 BYOD 门户：您可以在此处自定义 BYOD 和“我的设备门户”。您可以在此步骤中自定义 Cisco ISE 支持的所有页面。在此步骤中，提交所有门户自定义，创建策略，并将配置文件链接到相应的策略。

注释 “我的设备门户”使用来自 BYOD 门户定制的基本定制。您不能在无线设置中定制“我的设备门户”。

5. 预览所做的配置更改，然后选择 **完成**。

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》。

建议的 WLC 计时器设置

我们建议在计划用于无线设置的无线控制器上设置以下命令。

```
config radius auth retransmit-timeout {SERVER_INDEX} 5
config radius aggressive-failover disable
config radius fallback-test mode passive
config wlan exclusionlist {WLAN ID} 180
config wlan exclusionlist {WLAN ID} enabled
```

802.1X 无线流

无线设置流使用 PEAP（用户名和密码凭证）配置 802.1X 无线控制器。

部分流会要求您指定 Active Directory (AD)。您可以将员工 AD 组映射到 VLAN。如果要按 VLAN 划分组，可以将不同的员工组配置到不同的 VLAN。点击**访问 (Access)** 旁的下拉列表，可查看所配置的 AD 中可用的 AD 组。

如果在无线设置中选择 AD 组，则每个组都映射到 VLAN。如果 AD 组未映射到 VLAN，则用户匹配基本访问策略，该策略允许任何有效的 AD 用户登录。

员工连接至网络

1. **对员工凭证进行身份验证**：Cisco ISE 对照公司活动目录对员工进行身份验证并提供授权策略。
2. **设备重定向到 BYOD 门户**：设备会重定向到 BYOD 门户。系统会填充设备的 MAC 地址字段，用户可以添加设备名称和说明。
3. **配置本地请求方（MacOS、Windows、iOS、Android）**：配置本地请求方；但此过程因设备而异：

- MacOS 和 Windows 设备：员工在 BYOD 门户中点击 **注册** 以下载和安装请求方调配向导。此向导会配置请求方，并安装用于基于 EAP-TLS 证书的身份验证的证书。颁发的证书嵌有设备的 MAC 地址和员工的用户名。

  注释 对于 MacOS，除 Apple 证书外，证书在 MacOS 上显示为“未签名”。这不会影响 BYOD 流。

- iOS 设备：Cisco ISE 策略服务器使用 Apple 的 iOS 空中下载功能向 iOS 设备发送新配置文件，其中包括：
  - 颁发的证书随 IOS 设备的 MAC 地址和员工的用户名一起存储。
  - Wi-Fi 请求方配置文件，其强制使用 MSCHAPv2 或 EAP-TLS 进行 802.1X 身份验证。
- Android 设备 - Cisco ISE 会提示并引导员工从 Google Play 商店下载 Cisco 网络设置助理 (NSA)。安装应用后，员工可以打开 NSA 并启动设置向导。启动向导会生成请求方配置和已使用的颁发证书，用于配置设备。
- **发出授权更改**：用户完成激活流程后，Cisco ISE 会发起授权更改 (CoA)。这会导致 MacOSX、Windows 和 Android 设备使用 EAP-TLS 重新连接到安全 802.1X 网络。对于单 SSID，iOS 设备也会自动连接；但是对于双 SSID，向导会提示 iOS 用户手动连接新网络。

以下操作系统支持本地请求方：

- Android（Amazon Kindle 和 B&N Nook 除外）
- Mac OS（适用于 Apple Mac 计算机）
- Apple iOS 设备（Apple iPod、iPhone 和 iPad）
- Microsoft Windows 7 和 8（RT 除外）、Vista 和 10

通过无线设置流程对 Cisco ISE 和无线控制器进行更改

无线设置会在您逐步执行流程时配置 Cisco ISE 和控制器。无线设置将列出它在每个流程结束时所做的更改。此处列出了每个流程的更改以作参考，帮助您查找无线设置对 Cisco ISE 进行的所有更改，以进行查看或更改。

- **热点**
  - **工作中心 > 访客访问 > 门户和组件 > 访客门户 > 热点门户**
  - **工作中心 > 访客访问 > 策略元素 > 结果 > 授权配置文件**
  - **工作中心 > 访客访问 > 授权策略**
- **自行注册**

- 工作中心 > 访客访问 > 门户和组件 > 访客门户 > 自行注册门户
- 工作中心 > 访客访问 > 门户和组件 > 访客类型 > 访客类型
- 策略 > 策略元素 > 授权 > 授权配置文件
- 工作中心 > 访客访问 > 授权策略
- 管理 > 系统 > 设置 > **SMTP** 服务器
- 管理 > 系统 > 设置 > **SMTP** 网关

- 已发起
  - 工作中心 > 访客访问 > 门户和组件 > 访客门户 > 赞助的热点门户 >
  - 工作中心 > 访客访问 > 门户和组件 > 赞助商门户 > > 赞助商门户 >
  - 策略 > 策略元素 > 授权 > 授权配置文件
  - 工作中心 > 访客访问 > 授权策略
  - 工作中心 > 访客访问 > 门户和组件 > 赞助商 > 赞助商组
  - 工作中心 > 访客访问 > 门户和组件 > 访客类型 > 访客类型
  - 工作中心 > 访客访问 > 外部 **ID** 源 > **Active Directory**

- 自带设备
  - 工作中心 > **BYOD** > 门户和组件 > **BYOD** 门户 > **BYOD** 门户
  - 工作中心 > **BYOD** > 门户和组件 > 我的设备门户 > 我的设备门户
  - 工作中心 > **BYOD** > 策略元素 > 授权 > 授权配置文件
  - 工作中心 > **BYOD** > 授权策略
  - 工作中心 > **BYOD** > 外部 **ID** 源 > **Active Directory**
  - 工作中心 > **BYOD** > 外部 **ID** 源 > **Active Directory**，然后选择您的 AD，随后 **组** 选项卡。

- 安全接入
  - 策略 > 策略元素 > 结果 > 授权 > 授权配置文件
  - 策略 > 策略元素 > 结果 > 授权 > 授权配置文件
  - 策略 **(Policy)** > 策略集 **(Policy Sets)**
  - 工作中心 > 访客访问 > 外部 **ID** 源 > **Active Directory**，然后选择您的 AD，随后 **组** 选项卡。

- 无线 **LAN** 控制器
  - **WLAN**

- **安全** > **访问控制列表**：无线设置创建以下 ACL：
  - 为访客和 BYOD 重定向 ACL
- 无线设置也创建**安全** > **AAA** > **验证统计** 下的条目

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-redirection on port 80/443
ip http secure-server
```

用于综合 RADIUS 事务的本地用户名和密码定义

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
```

用于确保准确日志和记账时间戳的 NTP 服务器配置

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 5
! Update AAA accounting information periodically every 5 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 confiugured 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。

用于启用 RADIUS 授权更改 (CoA) 的命令

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，支持思科 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。
- 共享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。

启用设备跟踪和 DHCP 监听的命令

为了帮助提供思科 ISE 面向安全的可选功能，您可以在交换机端口动态 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
```

启用基于 802.1X 端口的身份验证的命令

输入以下命令可为交换机端口全局开启 802.1X 身份验证：

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

用于为临界身份验证启用 EAP 的命令

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
```

使用恢复延迟限制 AAA 请求的命令

当发生关键身份验证恢复事件时，通过输入以下命令，您可以配置交换机自动引入延迟（以毫秒为单位）以确保思科 ISE 能够在恢复后再次启动服务：

```
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。

```
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-redirection 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 服务器响应之前启用预身份验证访问，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 目前，我们在实验室中使用 ACL-ALLOW，这是因为我们想要启用 802.1X 基于端口的身份验证，却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

用于启用 EPM 日志记录的命令

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
```

支持 SNMP 陷阱的命令

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>
```

为分析启用 SNMP v3 查询的命令

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 context***vlan-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。

启用分析器的 MAC 通知陷阱进行收集的命令

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

交换机上的 RADIUS 空闲超时配置

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，请将无限控制器配置为启用 **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。

在无线 LAN 控制器上配置 ACL 以实现移动设备管理互操作

必须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和证书调配。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 入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 的所有入站流量以执行 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入站 DNS 流量以进行名称解析。

步骤 6 允许从客户端到服务器的入站 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入站流量，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