使用思科身份服务引擎进行通用 NGWC/3850 无线配置

安全访问操作指南系列

作者：Aaron Woland

日期：2012 年 12 月

目录

3850 交换机无线配置

Cisco Catalyst 3850 是首个可堆叠接入交换平台，可在一个基于 Cisco IOS XE 软件的单一平台上提供有线与无线服务。它可提供一系列以无缝方式跨有线与无线工作的丰富功能，如基于堆叠上状态切换 (SSO) 的高可用性、精细 QoS、安全性和 Flexible Netflow (FNF)。此外，有线与无线功能捆绑到单一的 Cisco IOS 软件映像，减少用户在其网络中启用映像前需要确认/证明其资格的软件映像的数量。命令行界面 (CLI) 的单控制台端口管理减少管理无线与有线服务所用的接触点数量，从而降低网络复杂性，简化网络操作，并降低管理基础设施的总体拥有成本。

有线与无线的融合不仅提高整个网络中的无线带宽，还扩大无线部署的规模。每个 48 端口 Cisco Catalyst 3850 都提供 40 Gbps 的无线吞吐量（24 端口型号为 20 Gbps），此无线容量随着堆叠成员数量的增加而增加。此特点能确保网络可以扩展，以支持当前的无线带宽要求（如基于 IEEE 802.11n 的接入点），并支持未来的无线标准（如 IEEE 802.11ac）。此外，Cisco Catalyst 3850 可分配无线控制器功能，能够实现更好的可扩展性。每个 Cisco Catalyst 3850 交换机/堆叠都能在以下两种模式下作为无线控制器工作：

- 移动代理 (MA)：这是 Cisco Catalyst 3850 交换机供货时的默认模式。在此模式下，交换机能够从接入点终止 CAPWAP 隧道，并提供至无线客户端的无线连接。在此模式下，可以执行维护无线客户端数据库、配置和实施无线客户端及接入点的安全性和 QoS 策略。在移动代理模式下，无需在 IP Base 之上使用其他许可。
- 移动控制器 (MC)：在此模式下，Cisco Catalyst 3850 交换机可执行所有移动代理任务，还能在移动子域内进行移动协调、无线资源管理 (RRM) 和 Cisco CleanAir® 协调。可以在交换机命令行界面上启用移动控制器模式。当 Cisco Catalyst 3850 交换机用作移动控制器时，需要 IP Base 许可级别。在较大型的部署中，位于中心的思科 5508 无线局域网控制器 (WLC 5508)、思科无线服务模块 2 (WiSM2)（运行 AireOS 版本 7.3 时）和无线局域网控制器 5760 也可发挥此作用。

总体设计

下图显示组件的整体布局。本设计有两个服务集标识符 (SSID)，其中一个使用 WPA2（Wi-Fi 保护接入 V2）和 802.1x 保护其安全；另一个是开放式 SSID，采用集中式 Web 身份验证 (CWA)。虽然我们不会详细介绍思科身份服务引擎 (ISE) 内不同的自带设备 (BYOD) 策略或安全状况策略，但是此设置将为这些操作提供基准。本文档仅涵盖 3850 交换机上无线配置的基准配置。有关在有线网络或其他 ISE 配置中部署 3850 的信息，请参阅相应的 ISE 操作指南文档。

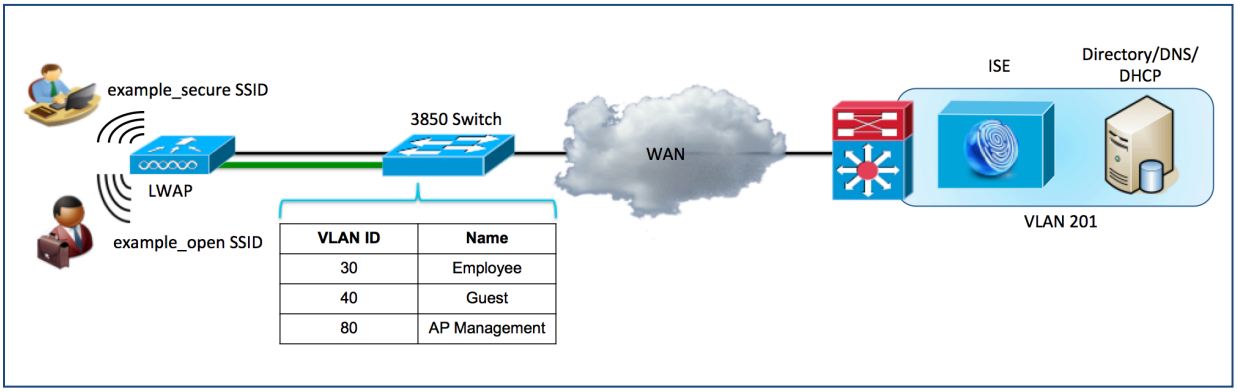

图 1.

使用的组件：

- Cisco ISE 1.2.0.899
- 运行 IOS-XE 版本 03.02.02.SE 的思科 3850
- Cisco LWAP 3602
- 作为 AD/DNS/DHCP 服务器的 Microsoft Windows 2008

有关 NGWC 无线功能的一些注意事项：

- 无线管理接口必须与 AP 接入 VLAN 一样，此布局中不支持 FlexConnect 模式下的 AP
- 客户端空闲超时是全局设置（与最新的 AireOS 相对）
- AP 需要直接连接到 3850 交换机
- 无需使用 DHCP 选项 43 或 DNS 条目的传统 AP 发现方法。借助 CAPWAP 监听，所有直接连接的 AP 只要使用正确的 VLAN 配置，都可以联接 3850。由于采用 CAPWAP 监听，如果在 3850 上配置了无线管理接口，所有直接连接的 AP 都只能与 3850 通信
- 支持 https 重定向，但是用户需要信任 3850 https 的证书，才能继续登录页面
- 借助 IOS-XE 版本 03.02.02.SE，3850 交换机可提供一些基于 GUI 的无线配置功能

注：思科 3850 能够以移动代理 (MA) 模式或移动控制器 (MC) 模式工作。每个移动部署都需要至少一个 MC，而且由于我们的设计包括一个 3850 交换机，所以我们会将此交换机配置为 MC 模式。

3850 交换机无线配置步骤

思科 3850 是一个统一接入平台，可将有线和无线网络融合到一个物理基础设施中。此配置示例显示如何将用于无线身份验证的思科 3850 交换机与 ISE 集成，为 BYOD 和安全状况评估等高级身份功能提供基础。本文档中的示例将主要侧重于 3850 上用于无线配置的命令行界面。

注：借助版本 03.02.02.SE，思科为 3850 引入了通过 GUI 访问无线配置的能力。但是，配置的很多部分仍然依赖于 CLI。本文档仅介绍 CLI 配置。

验证许可

3850 随附标配使用权 (RTU) 许可证方案。RTU 许可允许用户订购和激活特定类型和级别的许可证，以及在交换机上管理许可证使用情况。要激活许可证，用户需要接受最终用户许可协议 (EULA)。对于评估许可证，在 90 天试用期到期之前，系统会通知用户购买永久许可证或停用该评估许可证。用户需要满足以下三个条件，才能在 3850 上启用无线功能：运行 ipbase 或 ipservices 功能包、拥有 RTU 许可证，并且已接受 EULA。如果此交换机用作移动控制器 (MC)，则 RTU 还会管理 AP 计数。

注：配置必备条件：本指南假定交换机具有所需的许可证；以下步骤将侧重于此平台上 RTU 许可证的验证。

步骤 1 验证 RTU 许可证已就绪。

步骤 2 运行以下 show 命令以查看处于可用和使用中状态的许可证：

```
3850#show license right-to-use summary
```

示例输出

```
3850#show license right-to-use summary
  License Name  Type    Count  Period left
-----------------------------------------------
  ipservices  permanent  N/A   Lifetime
  apcount     base       0     Lifetime
  apcount     adder      10    Lifetime

-----------------------------------------------

License Level In Use: ipservices
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 10
AP Count Licenses In-use: 4
AP Count Licenses Remaining: 6


3850#
```

步骤 1 激活支持无线控制器的功能集，同时激活 AP 计数 RTU：

```
3850#license right-to-use activate ipservices slot 1 acceptEULA
3850#license right-to-use activate apcount 10 slot 1 acceptEULA
```

注：激活 AP 计数 RTU 可能需要先启用移动控制器功能 。

在交换机上配置 HTTP 服务器

步骤 1 在交换机上设置 DNS 域名。在设备上定义 DNS 域名之前，Cisco IOS® 软件不允许创建和安装证书或自生成密钥。

步骤 2 输入以下命令：

```
3850(config)#ip domain-name example.com
```

步骤 3 输入以下命令生成用于 HTTPS 的密钥：

```
3850(config)#crypto key generate rsa general-keys modulus 2048
```

注：为避免 Web 重定向期间可能出现证书不匹配错误，我们建议使用受信任证书颁发机构颁发的证书，而不要使用本地证书。此主题不在本文档说明范围之内。

步骤 4 在交换机上启用 HTTP 服务器。

必须在交换机上启用 HTTP 服务器才能执行 HTTP/HTTPS 捕捉和重定向。输入以下命令：

```
3850(config)#ip http server
3850(config)#ip http secure-server
```

注：在执行第 2 步生成密钥之前，请勿运行 **ip http secure-server** 命令。如果您没按照顺序执行命令，那么交换机会自动生成密钥较短的证书。此证书可导致重定向 HTTPS 流量时出现意外。不同于使用 AireOS 的 WLC，3850 系列无线支持重定向 HTTP 请求，但是在重定向期间会提示终端信任交换机的自签名证书。

步骤 5 禁用其他交换机管理功能的 HTPP 和 HTTPS（可选）：

```
3850(config)#ip http active-session-modules none
3850(config)#ip http secure-active-session-modules none
```

注：这将禁用对 3850 无线配置以及从 NCS 主要基础设施执行的配置的管理访问。

配置全局 AAA 命令

步骤 1 在接入交换机上启用身份验证、授权和记帐 (AAA)。

默认情况下会禁用思科交换机的 AAA“子系统”。启用 AAA 子系统之前，配置中所需的任何命令均不可用。输入以下命令：

```
3850(config)#aaa new-model
3850(config)#aaa session-id common
```

注：此命令可启用 AAA 网络安全服务提供的所有服务，例如本地登录身份验证和授权，定义和应用方法列表等。有关详细信息，请参阅《思科 IOS 安全配置指南》。

步骤 2 创建 802.1X 的身份验证方法。

必须通过身份验证方法指示交换机将哪组 RADIUS 服务器用于处理 802.1X 身份验证请求：

```
3850(config)#aaa authentication dot1x default group radius
```

步骤 3 创建 802.1X 的授权方法。

在步骤 2 中创建的方法会使用户/设备身份（用户名/密码或证书）通过 RADIUS 服务器进行验证。但是，只有有效的凭证还不够，还必须获得授权。授权是指用于定义用户或设备是否真正获得网络访问权限的条件以及实际允许的访问级别。

```
3850(config)#aaa authorization network default group radius
```

步骤 4 创建 802.1X 的记帐方法。

RADIUS 记帐数据包非常有用，对许多 ISE 功能都是必需的。这些类型的数据包有助于确保 RADIUS 服务器 (Cisco ISE) 了解接口和终端的确切状态。如果没有记帐数据包，Cisco ISE 将只能了解身份验证和授权通信情况。记帐数据包可提供有关授权会话长度以及客户端带宽使用情况的信息。

```
3850(config)#aaa accounting dot1x default start-stop group radius
```

步骤 5 配置定期 RADIUS 记帐更新。

定期 RADIUS 记帐数据包允许 Cisco ISE 跟踪网络上仍处于活动状态的会话。此命令会每隔 15 分钟定期发送更新。

```
3850(config)#aaa accounting update periodic 15
```

配置全局 RADIUS 命令

我们通过配置主动方法来检查 RADIUS 服务器的可用性。通过此操作，交换机将定期向 RADIUS 服务器 (Cisco ISE) 发送测试身份验证消息，并等待服务器的 RADIUS 响应。并非一定要得到成功消息，身份验证失败的消息也可以，因为这也足以证明服务器处于活动状态。

最佳实践：通过 ISE 1.2，可使用某些条件抑制身份验证。我们将使用该功能抑制任何 RADIUS 保持连接消息。有关说明，请参阅本文档结尾部分。

步骤 1 将 Cisco ISE 服务器添加至 RADIUS 组。

在此步骤中，我们将使用 radius 测试帐户，向交换机配置添加各个思科 ISE 策略服务节点 (PSN)。对各个 PSN 重复这一步骤。

```
3850(config)#radius-server host 192.168.201.88 auth-port 1812 acct-port 1813 test username radius-test idle-time 5 key cisco123
```

注：除了正常流程中执行的所有身份验证或授权之外，每隔 5 分钟会主动进行一次服务器响应检查。对于非 ISE 1.2 部署，由于在更低版本的 ISE 上缺少日志抑制功能，所以此值可能太强，在那种情况下可将此值改为 60 分钟或更高的值。

步骤 2 设置停机条件。

交换机已配置为主动检查 Cisco ISE 服务器的 RADIUS 响应。现在配置交换机上的计数器，以确定服务器是处于活动状态还是处于停机状态。我们的设置为，每 10 秒测试一次 RADIUS 服务器响应，进行 3 次测试尝试后将服务器标记为停机。如果 Cisco ISE 服务器在 30 秒内没有做出有效响应，系统会将其标记为停机。此外，停机时间定义交换机将服务器标记为停机的时间长度，我们将其设置为 15 分钟。

```
3850(config)#radius-server dead-criteria time 10 tries 3
3850(config)#radius-server deadtime 15
```

注：我们会在部署模式部分更加详细地介绍高可用性。

步骤 3 启用授权更改 (CoA)。

之前我们已对 RADIUS 服务器（交换机要将 RADIUS 消息发送到该服务器）的 IP 地址进行了定义。但是，我们还会在其他列表中定义可执行授权更改 (RFC 3576) 操作的服务器，此操作也是在全局配置模式下进行，如下所示：

```
3850(config)#aaa server radius dynamic-author
3850(config-locsvr-da-radius)#client 192.168.201.88 server-key cisco123
3850(config-locsvr-da-radius)#auth-type any
```

步骤 4 将交换机配置为使用思科供应商指定属性。

在此，我们将交换机配置为在身份验证请求和记帐更新过程中将所有已定义的供应商指定属性 (VSA) 发送到 Cisco ISE PSN。

```
3850(config)#radius-server vsa send authentication
3850(config)#radius-server vsa send accounting
```

步骤 5 接下来，我们将启用供应商指定属性 (VSA)。

```
3850(config)#radius-server attribute 6 on-for-login-auth
3850(config)#radius-server attribute 8 include-in-access-req
3850(config)#radius-server attribute 25 access-request include
3850(config)#radius-server attribute 31 mac format ietf upper-case
3850(config)#radius-server attribute 31 send nas-port-detail mac-only
```

步骤 6 对于 RADIUS 请求，请确保交换机始终从正确接口发送流量。

交换机可能经常有多个关联的 IP 地址。因此，最好始终强制所有管理通信均通过一个指定接口执行。此接口 IP 地址必须与 Cisco ISE 网络设备对象中定义的 IP 地址相匹配。

思科最佳实践：网络管理最佳实践为，对所有管理通信使用环回适配器，同时向内部路由协议通告该环回接口。

```
3850(config)#ip radius source-interface vlan 201
```

配置 VLAN 和 SVI

使用轻量级 AP 创建 CAPWAP 隧道需要使用无线管理接口。此外，需要为无线接入要设置的每个 WLAN 创建 VLAN。此外，我们还需要创建将要映射到 WLAN 的所有用户 VLAN。

步骤 1 为无线管理和 WLAN 接口添加以下 VLAN：

```
3850(config)#vlan 80
3850(config-vlan)#name AP_VLAN
3850(config-vlan)#vlan 30
3850(config-vlan)#name WLAN_USER
3850(config-vlan)#vlan 40
3850(config-vlan)#name WLAN_GUEST
```

步骤 2 为无线管理接口创建 SVI。

此接口将用于与 LWAP 通信。LWAP 需要直接连接到 3850 交换机，且需要使用与无线管理 VLAN 相同的 VLAN 配置接口。此外，请配置 IP 帮助程序，将来自 LWAP 的 DHCP 请求转发到 DHCP 服务器。

```
3850(config)#interface Vlan 80
3850(config-if)#ip address 192.168.80.1 255.255.255.0
3850(config-if)#ip helper-address 192.168.201.72
3850(config-if)#no shutdown
```

配置 DHCP 监听（可选）

虽然 3850 无线功能无需 DHCP 监听即可运行，但最佳实践是要求所有终端都通过 DHCP 服务器分配地址。为此，应在 WLAN 配置上全局启用 DHCP 监听并运行 dhcp 所需的选项。

配置 DHCP 监听之前，请确保记下您信任的 DHCP 服务器的位置。配置 DHCP 监听时，交换机会拒绝来自任何未配置为“信任”的端口的 DHCP 服务器应答。输入上行链路接口的接口配置模式，并将其配置为信任端口。

步骤 1 为受信任的端口配置动态主机配置协议 (DHCP) 监听。

```
3850(config)#interface GigabitEthernet x/y/z
3850(config-if)#description Server
3850(config-if)#ip dhcp snooping trust
```

步骤 2 启用 DHCP 监听。

已在全局配置模式下启用 DHCP 监听。启用 DHCP 监听之后，您必须配置应该用于此监听的 VLAN，在我们的示例中为 VLAN 30 和 40。

```
3850(config)#ip dhcp snooping vlan 30, 40
3850(config)#no ip dhcp snooping information option
3850(config)#ip dhcp snooping
```

配置本地访问控制列表

交换机上有些功能需要使用本地配置的访问控制列表 (ACL)，如 URL 重定向。您创建的其中有些 ACL 可以立即使用，而有些则要到部署的后期阶段才能使用。本部分的目标是同时为所有可能的部署模式准备好交换机，并限制重复的交换机配置所带来的运营成本。

步骤 1 添加以下要用于 Web 身份验证 URL 重定向的 ACL：

```
3850(config)#ip access-list extended REDIRECT-ACL
3850(config-ext-nacl)#deny udp any host 192.168.201.72 eq 53
3850(config-ext-nacl)#deny udp any eq bootpc host 192.168.201.72 eq bootps
3850(config-ext-nacl)#deny ip any host 192.168.201.88
3850(config-ext-nacl)#permit ip any any
```

配置全局 802.1X 命令

步骤 1 在交换机上全局启用 802.1X。

在交换机上全局启用 802.1X 实际上不会在任何 WLAN 或端口上启用身份验证。

```
3850(config)#dot1x system-auth-control
```

步骤 2 启用可下载的 ACL 以正常工作。

可下载的访问控制列表 (dACL) 在 Cisco ISE 部署中是一种十分常见的实施机制。要使 dACL 在交换机上正常工作，必须全局启用 IP 设备跟踪，如下所示：

```
3850(config)#ip device tracking
```

注：Windows 7 和不响应 ARP 的设备存在一些需要使用 **ip device tracking use SVI** 命令的特殊情况。

配置全局无线功能

步骤 1 在交换机上启用移动控制器 (MC) 功能。

3850 交换机可以仅用作移动代理 (MA)，也可以同时用作移动控制器 (MC) 和 MA。对于任何 3850 无线部署，都至少需要一个可用于部署的 MC。由于我们只有一个 3850 交换机，所以我们将该 3850 配置为 MC+MA。

```
3850(config)#wireless mobility controller
```

注：3850 交换机始终配置为 MA 。

步骤 2 启用管理接口。

通过使用 3850，所有 AP 都需要位于与管理接口相同的 VLAN 上。这就使得 AP 与 3850 交换机之间可以进行 CAPWAP 隧道传输。

```
3850(config)#wireless management interface Vlan80
```

注：如果有 LWAP 配置为将 CUWN WLC 连接到 3850 交换机，在输入以上命令之后，所有连接到 3850 的 LWAP 都将断开与 CUWN WLC 的连接并开始向 3850 交换机注册。之后，LWAP 将经过代码升级，最终联接 3850 交换机。

步骤 3 启用 fast-ssid-change 功能。

通过 Fast-SSID-Change 功能，客户端可以从一个 SSID 移至另一个 SSID，而不出现延迟。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，而不出现延迟。

```
3850(config)#wireless client fast-ssid-change
```

注：这主要是为满足 Apple iOS 设备在短时间内从一个 SSID 转至另一个 SSID 的需要。

步骤 4 配置客户端空闲超时。

通过空闲超时功能，当在所配置的时间范围内没有来自客户端的流量时，交换机可以删除客户端会话。如果此值太短，则客户端设备在退出独立模式后，将不得不重新进行身份验证。此处我们将其设置为 2 小时。

```
3850(config)#wireless client user-timeout 7200
```

步骤 5 启用限定性门户绕行功能。

Apple 引入了一种 iOS 功能，在存在强制门户时可以促进网络接入。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 http://www.apple.com/library/test/success.html。如果收到回应，则假定存在互联网接入，而且无需进一步交互。如果未收到回应，则假定互联网接入被强制门户阻止，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。以下 CLI 命令将阻止虚拟浏览器弹出。

```
3850(config)#captive-portal-bypass
```

配置 WLAN

步骤 1 添加支持 802.1x 的 WLAN。

以下命令将创建一个 WLAN，以 example_employee 作为配置文件，而且 SSID 使用的 WLAN ID 为 1。如果此 3850 交换机是大规模部署的一部分，请确保所有交换机上 WLAN 设置的所有设置都一致。

```
3850(config)#wlan example_secure 1 example_secure
```

注：虽然我们为 wlan 输入的不是 L2 安全设置，但是对于 802.1x，所有 wlan 的默认设置都是 WPA2/AES 。

步骤 2 将 WLAN 配置为接受来自 RADIUS 服务器的 RADIUS 授权和指令。

WLAN 的 AAA 优先选项让您可以为身份网络连接配置 WLAN。它允许您根据 ISE 返回的 RADIUS 属性向各个客户端应用 VLAN 标记、服务质量 (QoS) 和访问控制列表 (ACL)。此外，nac 指令根据 URL 重定向中的 CWA、DRW、MDM、NSP 和 CPP 等指令实现不同客户端状态。

```
3850(config-wlan)#aaa-override
3850(config-wlan)#nac
```

步骤 3 将 VLAN 映射到 WLAN。

将之前创建的用户 VLAN 分配到 WLAN。

```
3850(config-wlan)#client vlan 30
```

步骤 4 阻止来自使用静态 IP 的客户端的网络接入（可选）。

如果在之前步骤中已为以上 VLAN 配置 DHCP 监听，则此设置会阻止使用静态 IP 地址的客户端设备。

```
3850(config-wlan)#ip dhcp required
```

步骤 5 配置会话超时（重新身份验证计时器）。

此值指定客户端通过 RADIUS 服务器重新进行身份验证的频率。

```
3850(config-wlan)#session-timeout 86400
```

步骤 6 启用 WLAN。

```
3850(config-wlan)#no shutdown
```

注：无论何时需要修改 wlan 配置，都必须关闭 wlan。修改之后可以通过运行以上命令重新启用。请注意，这会断开各个 wlan 上的所有用户。

步骤 7 添加用于 ISE CWA 的开放式 SSID。

```
3850(config)#wlan example_open 2 example_open
```

步骤 8 在 WLAN 上启用 MAC 过滤。

由于这是开放式 SSID，使用默认 RADIUS 列表启用 MAC 过滤将提供将 ISE 用作外部 Web 服务器的 CWA。

```
3850(config-wlan)#mac-filtering default
```

步骤 9 将 WLAN 配置为接受来自 RADIUS 服务器的 RADIUS 授权消息。

```
3850(config-wlan)#aaa-override
3850(config-wlan)#nac
```

步骤 10 将 VLAN 映射到 WLAN。

```
3850(config-wlan)#client vlan 40
```

步骤 11 阻止来自使用静态 IP 的客户端的网络接入（可选）。

```
3850(config-wlan)#ip dhcp required
```

步骤 12 在 WLAN 上禁用 WPA 和 802.1x。

禁用所有 L2 安全功能并将 WLAN 设置为开放式 SSID。

```
3850(config-wlan)#no security wpa
3850(config-wlan)#no security wpa akm dot1x
3850(config-wlan)#no security wpa wpa2
3850(config-wlan)#no security wpa wpa2 ciphers aes
```

步骤 13 配置会话超时（重新身份验证计时器）。

```
3850(config-wlan)#session-timeout 7200
```

注：用于开放式 SSID 的会话超时值设置得比安全 SSID 低，因为 MAB 请求的重新身份验证不会对 ISE 产生像 802.1x 请求那么大的影响 。

步骤 14 启用 WLAN。

```
3850(config)#no shutdown
```

配置用于无线 AP 的接口

步骤 1 确定并配置插入 LWAP 的接口。

```
3850(config)#interface GigabitEthernet x/y/z
3850(config-if)#description AP
```

注：通过使用 3850 交换机，LWAP 需要直接连接到交换机 。

步骤 2 分配无线管理 VLAN。

在交换机上全局启用 802.1X 实际上不会在任何交换机端口上启用身份验证。此时会对身份验证进行配置，但直到配置监控模式时才会启用身份验证。

```
3850(config-if)#switchport mode access
3850(config-if)#switchport access vlan 80
```

注：3850 引入了一种通过使用 CAPWAP 监听功能发现新 LWAP 的新方法。无需为 3850 无线管理 IP 地址配置 DHCP 选项 43 或 DNS 条目。

步骤 3 启用生成树速端口。

```
3850(config-if)#spanning-tree portfast
```

步骤 4 启用接口。

```
3850(config-if)#no shutdown
```

步骤 5 验证 AP 状态。

升级并重新启动 AP 之后，请验证所有 AP 都是在本地模式下运行，并且 Country 设置正确。此外，请确保所有 AP 状态都显示为 Joined。

```
3850#show ap status
3850#show ap join stats summary
```

注：目前 3850 仅在本地、监控器、安全连接和探查器模式下支持 LWAP。如果之前已将 LWAP 配置为 FlexConnect 模式，则运行“ap name {AP_NAME} mode local”命令。

示例输出

```
3850#show ap status
AP Name                                Status     Mode              Country
-------------------------------------------------------------------------
AP4c4e.350d.35f8                       Enabled    Local             US
APd48c.b5e4.3b88                       Enabled    Local             US
AP4c4e.35c7.1572                       Enabled    Local             US
AP44d3.ca42.58cd                       Enabled    Local             US


3850#show ap join stats summary
Number of APs : 4

Base MAC        Ethernet MAC    AP Name                IP Address       Status
-----------------------------------------------------------------------------
20bb.c067.fda0  4c4e.350d.35f8  AP4c4e.350d.35f8       192.168.80.103   Joined
34bd.c890.52f0  d48c.b5e4.3b88  APd48c.b5e4.3b88       192.168.80.101   Joined
5006.046e.f300  4c4e.35c7.1572  AP4c4e.35c7.1572       192.168.80.100   Joined
64d9.8946.b160  44d3.ca42.58cd  AP44d3.ca42.58cd       192.168.80.102   Joined


3850#
```

步骤 6 保存配置。

```
3850#write memory
```

3850 示例配置

```
hostname 3850
!
aaa new-model
aaa session-id common
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa accounting update periodic 15
!
aaa server radius dynamic-author
 client 192.168.201.88 server-key cisco123
 auth-type any
!
vlan 80
 name AP_VLAN
vlan 30
 name WLAN_USER
vlan 40
 name WLAN_GUEST
!
interface vlan 80
 ip address 192.168.80.1
 ip helper 192.168.201.72
 no shut
interface vlan 30
 ip address 192.168.30.1
 ip helper 192.168.201.72
 ip helper 192.168.201.88
 no shut
interface vlan 40
 ip address 192.168.40.1
 ip helper 192.168.201.72
 ip helper 192.168.201.88
 no shut
!
ip device tracking
!
ip dhcp snooping vlan 30, 40
no ip dhcp snooping information option
ip dhcp snooping
!
ip domain-name example.com
!
crypto key generate rsa general-keys modulus 2048
!
dot1x system-auth-control
!
ip http server
ip http secure-server
ip http secure-active-session-modules none
ip http active-session-modules none
!
ip access-list extended REDIRECT-ACL
 deny udp any host 192.168.201.72 eq 53
 deny udp any eq bootpc host 192.168.201.72 eq bootps
 deny ip any host 192.168.201.88
 permit ip any any
!
ip radius source-interface Vlan201
snmp-server community cisco123 RO
radius-server attribute 6 on-for-login-auth
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 10 tries 3
```

```
radius-server host 192.168.201.88 auth-port 1812 acct-port 1813 test username radius-test idle-
time 5 key cisco123
radius-server deadtime 15
radius-server vsa send accounting
radius-server vsa send authentication
!
wireless mobility controller
wireless management interface Vlan80
wireless client fast-ssid-change
wireless mgmt-via-wireless
wireless client user-timeout 7200
captive-portal-bypass
!
wlan example_secure 1 example_secure
 aaa-override
 client vlan 30
 nac
 ip dhcp required
 session-timeout 86400
 no shutdown
!
wlan example_open 2 example_open
 aaa-override
 client vlan 40
 mac-filtering default
 nac
 ip dhcp required
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 session-timeout 7200
 no shutdown
!
interface GigabitEthernet 1/0/17
description Server
switch port mode access
switch port access vlan 201
ip dhcp snooping trust
spanning-tree portfast
no shut
!
interface GigabitEthernet 1/0/9
description AP
switch port mode access
switch port access vlan 80
spanning-tree portfast
no shut
```

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 CWA、BYOD 和状态评估等高级 ISE 功能。虽然本文档涵盖与 BYOD 相关的策略，仍请参阅 BYOD 操作指南以了解如何配置基础服务来启用 BYOD，这包括配置 CA 服务器、外部身份源和请求方调配策略。

创建身份序列

我们将创建一个身份序列来处理安全 SSID 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 ISE 主管理员节点。

步骤 2 导航至 **Administration → Identity Management → Identity Source Sequences**。

步骤 3 点击“Add”。

步骤 4 创建名称为“CAP_AD_Internal”的序列。

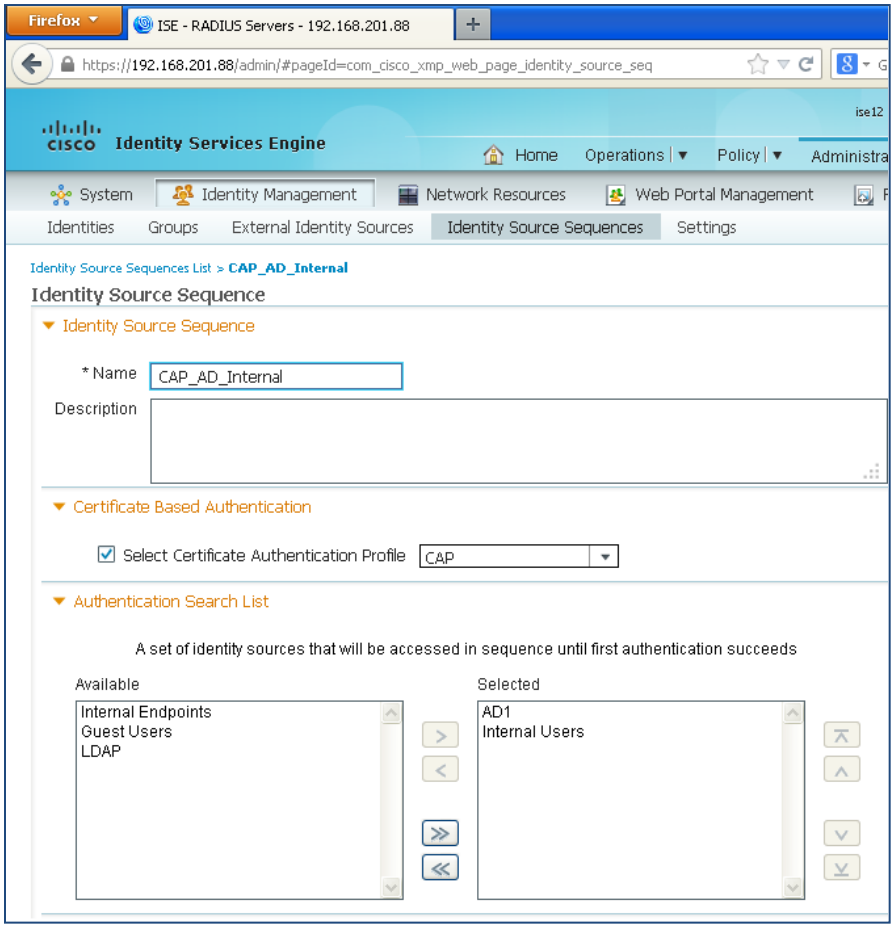

图 2.

步骤 5 点击 **Save**。

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，这将清楚地说明如何向每个 ISE 策略结构使用案例应用策略。

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。

程序 1 创建可下载的 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，使用以下参数创建 NSP 授权配置文件。

名称	INTERNET-ONLY
DACL 目录	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”。

程序 2 配置授权配置文件

此处我们将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，使用以下参数创建 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，使用以下参数创建 WebAuth 授权配置文件。

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

步骤 5 点击“Save”。

步骤 6 点击 Add，使用以下参数创建互联网授权配置文件。

名称	互联网
常见任务	DACL Name
ACL	INTERNET-ONLY

步骤 7 点击“Save”。

配置策略

步骤 1 导航至 Policy → Policy Set。

步骤 2 点击左侧窗格上的“+”号，然后点击“Create Above”。

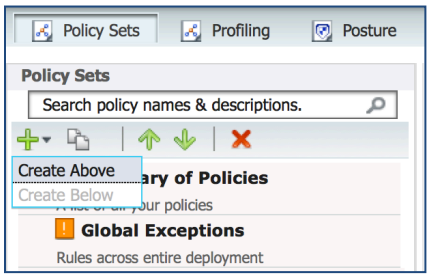

图 3.

步骤 3 使用以下参数将策略集名称定义为“example_secure”。

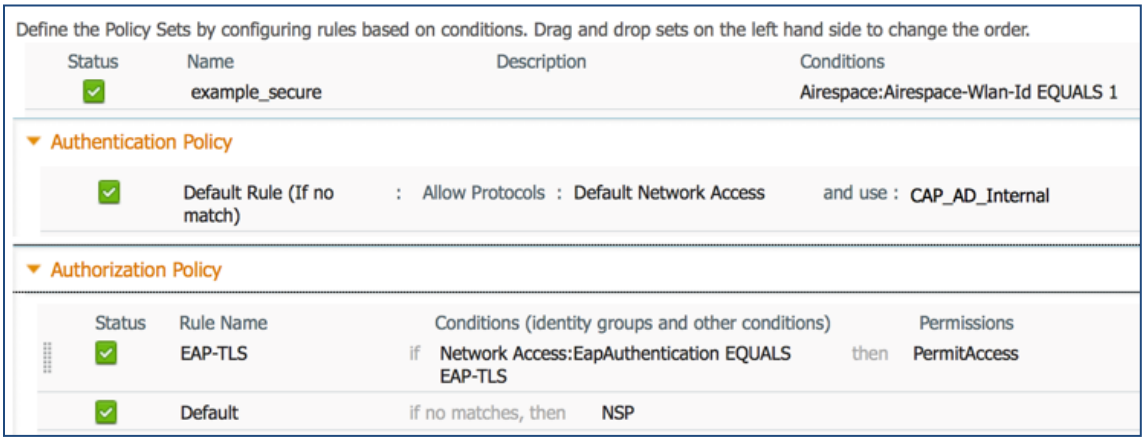

图 4.

步骤 4 点击 **Submit**。

步骤 5 使用以下参数将策略集名称定义为“example_open”。

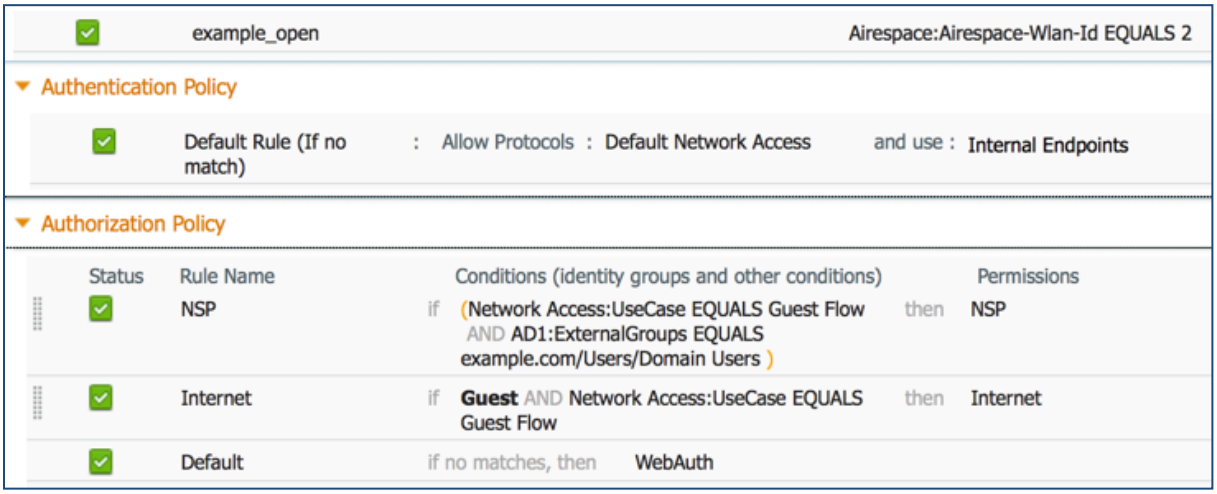

图 5.

步骤 6 点击 **Submit**。

ISE 配置 – 抑制 RADIUS 测试消息

您可以配置收集过滤器禁止发送到监控和外部服务器的日志消息。可以根据不同的属性类型在策略服务节点级别执行抑制，也可以禁用抑制。您可以定义多个具有特定属性类型和对应值的过滤器。

注：建议将收集过滤器数量限制为 20 个。

将 ISE 配置为抑制 RADIUS 测试消息

步骤 1 登录 ISE 主管理员节点。
步骤 2 导航至 **Administration > System > Logging**。
步骤 3 在左侧窗格点击 **Collection Filters**。
步骤 4 在右侧窗格的顶部点击 **Add**。

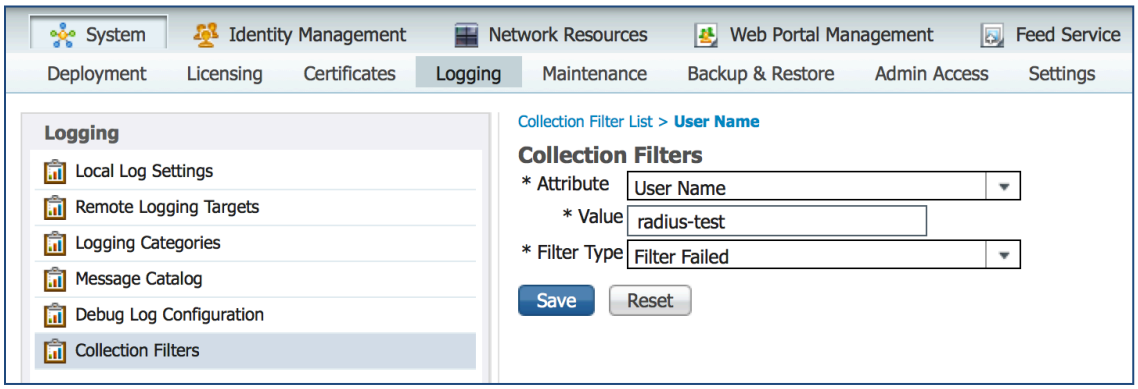

图 6.

步骤 5 从 Attribute 下拉菜单中选择“**User Name**”。
步骤 6 在 Value 中输入“**radius-test**”。
步骤 7 从 Filter Type 下拉菜单中选择“**Filter All**”。
步骤 8 点击 **Save**。