DCYK WLAN 配置手册

目录

修订记录

本文档修订内容列表.

修订	修订说明
Rev 01	初始发布

配置 WLAN

基本 WLAN 配置工作流程

创建新 WLAN 配置的推荐方法是通过新建 WLAN 向导，但高级用户也可以通过 DCYKOS WebUI 和 CLI 手动配置 WLAN。

使用 WLAN 向导创建 WLAN

要启动“新建 WLAN”向导，请在“托管网络”节点层次结构中导航到“配置>任务”，然后选择“创建新 WLAN”。向导将打开并提示您输入以下信息：

配置设置	描述
常规	
名称 （SSID）	分配给新 WLAN 的名称。
主要用途	选择 WLAN 是主要支持员工还是访客用户。
播出时间	选择 WLANSSID 是否应在与受管设备或移动主机配置关联的所有 AP 上进行广播，或者 WLAN 是否应在所选 AP 组中的 AP 上进行广播。如果选择“选择 AP 组”选项，系统会提示您选择一个或多个 AP 组。
转发方式	如果转发模式设置为隧道，则使用 GRE 将数据通过隧道传输到受管设备。当 WLAN 配置为使用解密隧道转发模式时，该 AP 解密和解封装来自客户端的所有 802.11 帧，并通过 GRE 隧道将 802.3 帧发送到受管设备，然后受管设备将防火墙策略应用于用户流量。当受管设备向客户端发送流量时，受管设备通过 GRE 隧道将 802.3 流量发送到 AP，然后 AP 将其转换为加密的 802.11 并转发到客户端。
VLAN	

VLAN	将用户放入其中以获取 IP 地址的 VLAN。如果要创建访客 WLAN，请记住，访客用户必须通过网络中的 VLAN 与员工用户分开。
命名 VLAN	单击显示 VLAN 详细信息以查看在受管设备或移动主机上配置的命名 VLAN 列表。 要添加新的 VLAN，请单击“命名 VLAN”表中的“+”，然后在以下字段中输入相应的值： VLAN 名称：新 VLAN 的名称 VLAN ID/范围：指定以连字符分隔的开始和结束 VLAN ID。例如，55-58。 要编辑命名 VLAN，请从表中选择 VLAN，然后单击铅笔按钮。您可以编辑 VLAN 名称和 VLAN ID/范围参数。
VLAN ID	从“命名 VLAN”表中选择一个 VLAN，以查看在受管设备或移动主机上配置的 VLAN ID 列表。 要添加新的 VLAN ID，请单击 VLAN ID 表中的 +，然后在以下字段中输入/选择适当的值： VLAN ID：VLAN 的标识号 管理员状态：启用或禁用 VLAN 接口。 要编辑 VLAN ID，请从 VLAN ID 表中选择 VLAN，然后单击铅笔按钮。您可以编辑 VLAN ID 和管理状态设置。
安全性（员工 WLAN 专用）	
企业	此选项支持以下配置参数： 密钥管理：使用此设置选择要在此 WLANSSID 上使用的第 2 层加密类型。选择“WPA-3 Enterprise”（默认）、“WPA-2 Enterprise”或“WPA Enterprise”。 使用 CNSA 套件：将商业国家安全算法 （CNSA） 用于企业网络。 身份验证服务器：要添加现有服务器，请单击 + 打开“添加现有服务器”窗口，然后从服务器列表中选择预配置的服务器。要定义新服务器，请单击“添

	加现有服务器”窗口中的“+”，然后定义新的 LDAP 或 RADIUS 服务器。有关详细信息，请参阅配置身份验证服务器 重新身份验证间隔：定义重新身份验证尝试之间的间隔（以秒或分钟为单位），以分钟或秒为单位。 MAC 身份验证：选择此选项可在用户身份验证之前强制执行计算机身份验证。如果选中，则会将 machine-default-role 或 user-default-role 分配给用户，具体取决于哪个身份验证成功。 黑名单：如果身份验证失败的次数达到指定次数，则将客户端列入黑名单。 最大身份验证失败次数：如果启用了黑名单，则此参数定义用户可以尝试使用错误凭据登录的次数，之后该用户将被列入安全威胁黑名单。
个人	此选项支持以下配置参数： 密钥管理：使用此设置选择要在此 WLANSSID 上使用的第 2 层加密类型。选择“WPA-3 个人版”（默认）、“WPA-2 个人版”或“WPA 个人版”。 密码：输入 WLAN 的密码。 重新键入：重新键入密码。 MAC 身份验证：选择此选项可在用户身份验证之前强制执行计算机身份验证。如果选中，则会将 machine-default-role 或 user-default-role 分配给用户，具体取决于哪个身份验证成功。 黑名单：如果身份验证失败的次数达到指定次数，则将客户端列入黑名单。 最大身份验证失败次数：如果启用了黑名单，则此参数定义用户可以尝试使用错误凭据登录的次数，之后该用户将被列入安全威胁黑名单。
开放	此选项支持以下配置参数： MAC 身份验证：选择此选项可在用户身份验证之前强制执行计算机身份验证。如果选中，则会将 machine-default-role 或 user-default-role 分配给用户，具体取决于哪个身份验证成功。
安全性（访客 WLAN）	

ClearPass 或其他外部强制网络门户	此选项支持以下配置参数： 身份验证服务器：单击“+”打开“添加现有服务器”窗口，然后从服务器列表中选择预配置的服务器。要定义新服务器，请单击“添加现有服务器”窗口中的“+”，然后定义新的 LDAP 或 RADIUS 服务器。有关详细信息，请参阅配置身份验证服务器 CPPM 主机：ClearPass Policy Manager 主机的 IPv4 地址。 CPPM 页面：为用户登录显示的页面的 URL。这可以设置为任何 URL。默认值：/auth/index.html。 重定向 URL：经过身份验证的用户将被定向到的 URL。此参数必须是以 http:// 或 https:// 开头的绝对 URL。
具有身份验证的内部强制网络门户	此选项支持以下配置参数： 模板：定义强制门户登录页面的标题、文本、横幅图标和横幅颜色。 重定向 URL：经过身份验证的用户将被定向到的 URL。此参数必须是以 http:// 或 https:// 开头的绝对 URL。 自定义 HTML：单击此链接可浏览并选择初始登录页和欢迎页的 HTML 文件。
具有电子邮件注册的内部强制网络门户	此选项支持以下配置参数： 模板：定义强制门户登录页面的标题、文本、横幅图标和横幅颜色。 重定向 URL：经过身份验证的用户将被定向到的 URL。此参数必须是以 http:// 或 https:// 开头的绝对 URL。 自定义 HTML：单击此链接可浏览并选择初始登录页和欢迎页的 HTML 文件。
内部强制网络门户，无需身份验证或注册	此选项支持以下配置参数： 模板：定义强制门户登录页面的标题、文本、横幅图标和横幅颜色。 重定向 URL：经过身份验证的用户将被定向到的 URL。此参数必须是以 http:// 或 https:// 开头的绝对 URL。 自定义 HTML：单击此链接可浏览并选择初始登录页和欢迎页的 HTML 文件。

没有强制门户	访客无需强制门户即可访问。
访问	
默认角色	选择要分配给成功向 WLAN 进行身份验证的员工的用户角色。 如果要创建员工 WLAN，请单击“默认角色”下拉列表，然后选择现有用户角色，或通过单击“显示角色”并单击“角色”表中的“+”来定义 WLAN 的新角色。 如果要创建访客 WLAN，则 WLAN 向导会自动为已成功通过 WLAN 身份验证的访客用户创建默认角色，名为 <WLAN-name>-guest-logon。若要配置此角色，请在“托管网络”节点层次结构中，导航到“配置”>“角色和策略”>“角色”选项卡，然后选择创建的角色。在配置访客角色时，请记住访客 WLAN 的以下准则： 来宾不仅要限制他们要去的地方，还要限制他们可以使用哪些网络协议和端口来访问资源。 应仅允许来宾访问 IP 连接所需的本地资源。这些资源包括 DHCP，如果外部 DNS 服务器不可用，则可能包括 DNS。在大多数情况下，公共 DNS 始终可用。 所有其他内部资源都应禁止访客使用。此限制通常是通过拒绝访客用户的任何内部地址空间来实现的。 应使用时间限制策略，允许客人仅在正常工作时间访问网络，因为他们应仅在执行公务时使用网络。还可以对每个访客用户设置速率限制，以防止用户使用有限的无线带宽。帐户应设置为在本地工作完成时过期，通常在每个工作日结束时过期。 注意：有关创建用户角色以及为角色分配规则和策略的完整信息，请参阅。
服务器派生角色	（适用于使用企业安全的员工 WLAN）启用此选项可配置服务器派生规则，这些规则可以基于服务器在身份验证期间返回的一个或多个属性，也可以基于客户端属性（如 SSID）（即使服务器未返回该属性）。服务器派生规则在客户端身份验证后执行。
推导方法	（适用于使用企业安全的员工 WLAN）选择派生方法。如果您的用户将通过 ClearPass Policy Manager 或其他类型的身份验证服务器向 WLAN 进行身份验

	证，请选择使用从 ClearPass 或其他身份验证服务器返回的值，或选择下表中定义的用户规则以定义基于 RADIUS 服务器 VSA 的自定义角色。单击“角色派生规则”（Role Derivations Rules） 表格中的“+”（+），然后定义以下值： 属性：RADIUSVSA 类型 条件：包含、等于、不等于、开头或值 操作数：与 VSA 条件比较的文本字符串 角色：如果 VSA 条件和操作数匹配，则分配的角色。 注意：有关当前在受管设备上运行的 DCYKOS 版本中可用的所有 RADIUS VSA 的当前和完整列表，请访问命令行界面并发出命令 show aaa radius attributes。另请参阅配置身份验证服务器

您可以使用 WebUI 或 CLI 手动创建 WLAN。

在 WebUI 中

以下工作流列出了手动配置使用 802.1X 身份验证的 WLAN 的任务。单击下面的任何链接，了解有关该任务的配置过程的详细信息。

此配置 WLAN 的方法仅建议高级用户使用。

1. 配置身份验证服务器。
2. 创建一个身份验证服务器组，并将您在步骤 1 中配置的身份验证服务器分配给该服务器组。
3. 为一组用户配置防火墙访问策略
4. 创建一个用户角色，并将您在步骤 3 中创建的防火墙访问策略分配给该用户角色。
5. 为配置节点配置 AAA 配置文件。
   a.将步骤 4 中定义的用户角色分配给与 AAA 配置文件关联的 802.1X 身份验证默认角色。
   b.将您在步骤 2 中创建的服务器组关联到 AAA 配置文件。
6. 配置配置节点的 SSID 配置文件
7. 配置配置节点的 virtual AP 配置文件，配置节点的 virtual AP 配置文件将自动关联到步骤

5 中配置的 AAA 配置文件以及步骤 6 中配置的 SSID 配置文件。

在 CLI 中

以下示例遵循建议的步骤顺序，使用 CLI 配置 WLAN。

```
(host)[node](config) #aaa server-group "THR-DOT1X-SERVER-GROUP-WPA2"
auth-server Internal
!
ip access-list session THR-POLICY-NAME-WPA2
user any any permit
!
(host)[node](config) #user-role THR-ROLE-NAME-WPA2
session-acl THR-POLICY-NAME-WPA2
!
(host)[node](config) #aaa server-group "THR-DOT1X-SERVER-GROUP-WPA2"
auth-server Internal
!
(host)[node](config) #aaa profile "THR-AAA-PROFILE-WPA2"
dot1x-default-role "THR-ROLE-NAME-WPA2"
dot1x-server-group "THR-DOT1X-SERVER-GROUP-WPA2"
!
(host)[node](config) #wlan ssid-profile "THR-SSID-PROFILE-WPA2"
essid "THR-WPA2"
opmode wpa2-aes
!
(host)[node](config) #wlan virtual-ap "THR-VIRTUAL-AP-PROFILE-WPA2"
ssid-profile "THR-SSID-PROFILE-WPA2"
aaa-profile "THR-AAA-PROFILE-WPA2"
vlan 60
!
(host)[node](config) #ap-group "THRHQ1-STANDARD"
virtual-ap "THR-VIRTUAL-AP-PROFILE-WPA2"
```

WLAN 配置文件

您可以配置 WLAN，以便为同一物理网络上的用户提供不同的网络访问或服务。例如，您可以将一个 WLAN 配置为通过相同的 AP 为访客用户提供访问权限，将另一个 WLAN 设置为为员工用户提供访问权限。您还可以配置一个 WLAN，该 WLAN 提供开放身份验证和强制网络门户访问，数据速率为 1 Mbps 和 2 Mbps，另一个 WLAN 需要 WPA 身份验证，数据速率高达 11 Mbps。您可以将两个 virtual AP 配置应用于同一 AP 或 AP 组。

当您使用移动主机或独立控制器 WebUI 的“配置>任务”页面上的“新建 WLAN”向导定义 WLAN 时，向导会自动创建与 WLAN 同名的新 virtual AP 配置文件、AAA 配置文件、802.1X、服务器组配置文件和 SSID 配置文件，并使用通过向导定义的配置设置和值。这些配置文件还支持其他高级功能，这些功能无法通过“配置>任务”页面上的 WLAN 向导进行配置。

下表描述了构成 DCYKOS WLAN 配置设置的配置文件，以及指向本文档中更详细描述这些配置文件的部分的链接。

配置文件	描述
virtual AP 配置文件	这是顶级 WLAN 配置文件。virtual AP 配置文件允许您配置 WLAN 设置，例如广播/组播设置、转发模式和 RF 频段，但它也可以识别该 WLAN 要使用的单个 802.11k、AAA、Anyspot、Hotspot 2.0、SSID 和 WWM 流量管理配置文件。 默认配置文件名称：<WLAN 名称> 使用 WLAN 向导创建 WLAN 时，DCYKOS 会自动创建与 WLAN 同名的新 virtual AP 配置文件。
802.11k 配置文件	802.11k 协议为 AP 和客户端提供了动态测量可用无线电资源的机制。每个 802.11k 配置文件还引用以下每个附加配置文件类型的一个实例。 信标报告请求配置文件：定义信标报告请求设置。信标报告请求仅发送到符合 802.11k 的客户端，这些客户端在其启用无线电资源管理的功能 IE 中通告信标报告功能。 无线资源管理 IE 配置文件：为启用了 802.11k 支持的 WLAN 定义无线资源管理信息元素。 流量流测量报告请求配置文件：定义流量流测量报告请求。这些报告请求仅发送到通告流量流报告功能的符合 802.11k 的客户端。 默认配置文件名称：default
AAA 型材	AAA 配置文件定义与 WLAN 关联的客户端使用的身份验证类型。每个 AAA 配置文件还引用以下每个附加配置文件类型的一个实例： 802.1X 身份验证配置文件：定义 802.1X 身份验证设置。

	802.1X 身份验证服务器组配置文件：为用于 802.1X 身份验证的一组服务器定义故障传递和负载平衡设置。 MAC 身份验证配置文件：定义 MAC 身份验证设置。 MAC 身份验证服务器组配置文件：为用于 MAC 身份验证的一组服务器定义故障通过和负载平衡设置。 RADIUS 记帐服务器组配置文件：为用于 RADIUS 记帐的一组服务器定义故障通过和负载平衡设置。 RFC 3576 服务器配置文件：定义 RADIUS 服务器以发送用户断开连接、CoA 和会话超时消息，如 RFC 3576 中所述。 XML API 服务器配置文件：为 XMLAPI 服务器定义身份验证密钥，以使用 XMLAPI 接口执行自定义的外部强制网络门户用户管理。 默认配置文件名称：<WLAN 名称> 使用 WLAN 向导创建 WLAN 时，DCYKOS 会自动创建与 WLAN 同名的新 AAA 配置文件。
AnySpot 配置文件	Anyspot 客户端探测抑制功能通过抑制来自试图定位和连接到其他已知网络的客户端的探测请求来减少网络流量。默认情况下，virtual AP 不与 Anyspot 配置文件关联，因此必须先定义 Anyspot 配置文件，然后手动关联到 virtual AP。 默认配置文件名称：N/A
Hotspot 2.0 配置文件	Hotspot 2.0 是基于 802.11u 协议的 WFA Passpoint 规范，它为无线客户端提供了一种简化的机制来发现合适的网络并对其进行身份验证，并允许移动用户能够在合作伙伴网络之间漫游，而无需额外的身份验证。WLAN 的热点配置文件引用热点通告配置文件，而热点通告配置文件又引用定义各个热点功能设置的其他几个配置文件。 热点广告配置文件 ANQP 场地名称简介 ANQP 网络身份验证配置文件 ANQP 域名配置文件

	ANQP IP 地址可用性配置文件 ANQP NAI 领域配置文件 ANQP 漫游联盟配置文件 ANQP 3GPP 蜂窝网络配置文件 H2QP 连接能力配置文件 H2QP 操作员友好名称配置文件 H2QP 操作等级指示配置文件 H2QP WAN 指标配置文件 默认配置文件名称：<WLAN 名称> 使用 WLAN 向导创建 WLAN 时，DCYKOS 会自动创建与 WLAN 同名的新 Hotspot 2.0 配置文件。
SSID 配置文件	SSID 配置文件定义网络的名称、网络的身份验证类型、基本速率、传输速率、SSID 隐藏以及网络的某些 WMM 设置。每个 SSID 配置文件还引用以下每个附加配置文件类型的一个实例： 802.11r 配置文件：快速 BSS 转换 （802.11r） 机制可最大限度地减少语音客户端在同一 ESS 内从一个 BSS 过渡到另一个 BSS 时的延迟。 EDCA 参数 （AP） 配置文件：DCYKOS 支持通过 EDCA 确定媒体访问优先级，EDCA 定义了四个 AC 来确定流量优先级。此配置文件定义 AP 的 EDCA 设置。 EDCA 参数（站点）配置文件：DCYKOS 支持通过 EDCA 确定媒体访问优先级，EDCA 定义了四个 AC 来确定流量优先级。此配置文件定义客户端的 EDCA 设置。 高吞吐量 SSID 配置文件：定义 5 GHz 频段的 802.11ac 超高吞吐量设置，以及 5 GHz 和 2.4 GHz 频段的高吞吐量 （802.11n） 设置。 高效 SSID 配置文件：定义 2.4 GHz 和 5 GHz 频段上的 802.11ax 频谱效率和区域吞吐量。 默认配置文件名称：<WLAN 名称>

	使用 WLAN 向导创建 WLAN 时，DCYKOS 会自动创建与 WLAN 同名的新 SSID 配置文件。

配置 virtual AP 配置文件

创建新 WLAN 配置的推荐方法是通过新建 WLAN 向导，但高级用户也可以通过 DCYKOS WebUI 和命令行界面手动配置 WLAN。

手动配置 virtual AP 配置文件

您可以使用 WebUI 或 CLI 手动配置 virtual AP 配置文件。

在 WebUI 中

执行以下任务以配置 virtual AP 配置文件：

1. 在“托管网络”节点层次结构中，导航到“配置>系统>配置文件”选项卡。
2. 从“所有配置文件”列表中，选择无线局域网>virtual AP。
3. 要编辑现有 virtual AP 配置文件，请选择要编辑的 virtual AP 配置文件。要创建新的 virtual AP 配置文件，请单击 +，然后在配置文件名称字段中输入新 virtual AP 配置文件的名称。virtual AP 配置文件设置分为四个部分：常规、射频、高级和广播/组播。
4. 配置 virtual AP 设置，virtual AP 配置文件参数中介绍了每个部分中的配置文件参数。
5. 单击提交。
6. 单击“挂起的更改”（Pending Changes）。
7. 在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

参数	描述
常规	
虚拟 AP 使能	选中虚拟 AP 启用复选框以启用或禁用虚拟 AP。
VLAN	将用户放入其中以获取 IP 地址的 VLAN。 注： 您必须将现有 VLAN ID 添加到虚拟 AP 配置文件。

前进模式	此参数控制数据是使用 GRE 通过隧道传输到受管设备，还是桥接到本地 EthernetLAN（对于远程 AP），还是根据目的地（公司流量转到受管设备，Internet 访问保持本地）的组合。所有转发模式都支持频段控制、TSPEC/TCLAS 执行、802.11k 和电台黑名单。 单击下拉列表以选择以下转发模式之一： 隧道：AP 处理所有 802.11 关联请求和响应，但通过 GRE 隧道将所有 802.11 数据包、操作帧和 EAPOL 帧发送到受管设备进行处理。受管设备删除或添加 GRE 标头，解密或加密 802.11 帧，并像往常一样将防火墙规则应用于用户流量。远程 AP 和园区 AP 都可以配置为隧道模式。 网桥：802.11 帧桥接到本地 EthernetLAN。当远程 AP 或园区 AP 处于桥接模式时，AP（而不是受管设备）处理所有 802.11 关联请求和响应、加密/解密过程和防火墙实施。802.11e 和 802.11k 操作帧也由 AP 处理，然后根据需要发送响应。 网桥模式下的 AP 不支持强制门户身份验证。远程 AP 和园区 AP 都可以配置为桥接模式。请注意，在网桥模式下配置园区 AP 之前，您必须在受管设备上启用控制平面安全功能。 注意： 在网桥模式下，即使 AP 部署为园区 AP，与远程 AP 的本地 DHCP 服务器具有相同 IP 地址的有线或无线客户端也无法与其他设备通信。如果要使用默认远程 AP 的 IP 地址作为客户端 IP 地址，则需要将远程 AP 的 DHCP 服务器 IP 地址更改为其他 IP 地址。要更改远程 AP 的 DHCP 服务器 IP 地址，请参阅启用远程 AP 高级配置选项。 拆分隧道：802.11 帧通过隧道或桥接，具体取决于目标（公司流量将转到受管设备，并且 Internet 访问仍为本地）。 处于拆分隧道转发模式的远程 AP 处理所有 802.11 关联请求和响应、加密/解密和防火墙实施。802.11e 和 802.11k 操作帧也由远程 AP 处理，然后根据需要发送响应。 Decrypt-Tunnel：远程 AP 和校园 AP 都可以配置为解密隧道模式。当 AP 使用解密隧道转发模式时，该 AP 解密和解封装来自客户端的所有 802.11 帧，

	并通过 GRE 隧道将 802.3 帧发送到受管设备，然后受管设备将防火墙策略应用于用户流量。 当受管设备向客户端发送流量时，受管设备通过 GRE 隧道将 802.3 流量发送到 AP，然后 AP 将其转换为加密的 802.11 并转发到客户端。这种转发模式允许网络利用 AP 的加密/解密容量，同时减少对受管设备上处理资源的需求。 处于解密隧道转发模式的 AP 还管理所有 802.11 关联请求和响应，并处理所有 802.11e 和 802.11k 操作帧。使用解密隧道模式的 AP 确实存在一些常规隧道转发模式下的 AP 所没有的限制。 在解密隧道转发模式下配置园区 AP 之前，您必须在受管设备上启用控制平面安全功能。 注意：使用静态 WEP 的网桥或拆分隧道模式下的虚拟 AP 应使用受管设备上的密钥插槽 2-4。密钥插槽 1 只能用于处于隧道模式的虚拟 AP。
RF	
允许的频段	使用虚拟 AP 的频段： g—仅 802.11b/g 频段 （2.4 Ghz）。 a—仅 802.11aband （5 Ghz）。 全部 — 802.11a 和 802.11b/g 频段（5 GHz 和 2.4 GHz）。这是默认设置。
带式转向	ARM 的频段控制功能鼓励支持双频段的客户端在双频段 AP 上保持 5 GHz 频段。这样可以释放 2.4 Ghz 频段上的资源，用于 VoIP 电话等单频段客户端。 频带控制可减少同信道干扰并增加双频客户端的可用带宽，因为 5 Ghz 频段上的信道比 2.4 Ghz 频段上的信道更多。支持双频 802.11n 的客户端可能会看到更大的带宽改进，因为频段控制功能将在 802.11n 网络中自动在 40MHz 或 20 Mhz 信道之间进行选择。默认情况下，此功能处于禁用状态，必须在虚拟 AP 配置文件中启用。 频段控制功能支持将虚拟 AP 配置文件设置为隧道、拆分隧道或桥接转发模式的园区 AP 和远程 AP。但请注意，如果园区或远程 AP 在网桥或拆分隧道

	转发模式下配置了虚拟 AP 配置文件，但在隧道模式下没有虚拟 AP，则这些 AP 将独立收集有关支持 5G 的客户端的信息，并且不会仅与具有网桥或拆分隧道虚拟 AP 的其他 AP 交换此信息。
转向模式	频段转向支持以下三种不同的频段转向模式。 平衡带：在这种频段控制模式下，AP 尝试在两个无线电之间平衡客户端，以便最好地利用可用的 2.4G 带宽。此功能考虑了以下事实：5 Ghz 频段的信道比 2.4 Ghz 频段多，并且 5 Ghz 信道的工作频率为 40 Mhz，而 2.5 Ghz 频段的工作频率为 20 MHz。 首选 5GHz（默认）：如果将 AP 配置为使用 首选 5GHz 频段控制模式，则 AP 将尝试将客户端引导至 5G 频段（如果客户端支持 5G），但如果客户端坚持进行 2.4 G 关联尝试，则允许客户端在 2.4G 频段上连接。 Force-5GHz：当 AP 配置为 force-5GHz 频段转向模式时，AP 将尝试强制支持 5Ghz 的 AP 使用该无线电频段。
高级	
蜂窝切换辅助	当同时启用客户端匹配和蜂窝切换辅助功能时，蜂窝切换辅助功能可以帮助支持 Wi-Fi 网络末端的双模 3G 或 4G Wi-Fi 设备（如 iPhone、iPad 或 Android 客户端）从 Wi-Fi 切换到备用 3G 或 4G 无线电，从而提供更好的网络访问。此功能仅受 iOS 和 Android 设备支持。
身份验证失败黑名单时间	时间（以秒为单位），如果客户端未通过重复身份验证，则会阻止客户端。 默认设置为 3600 秒（1 小时）。值为 0 将无限期阻止客户端。
黑名单时间	客户端被列入黑名单后与网络隔离的秒数。 默认值：3600 秒（1 小时）
拒绝用户间流量	选中此复选框可拒绝使用此虚拟 AP 配置文件的客户端之间的流量。 “配置”>高级服务>状态防火墙>全局“窗口中显示的全局防火墙还包括一个选项，用于拒绝所有用户间流量，而不考虑这些客户端使用的虚拟 AP 配置文件。 如果启用了拒绝用户间流量的全局设置，则无论虚拟 AP 配置文件中配置的设置如何，客户端之间的所有用户间流量都将被拒绝。如果在单个虚拟 AP

	上全局禁用了拒绝用户间流量的设置，则只会阻止不受信任的用户与该特定虚拟 AP 上的客户端之间的流量。 注意：此字段不适用于控制器，即使它们位于同一集群中也是如此。
拒绝时间范围	单击下拉列表，然后选择 AP 将拒绝访问的已配置时间范围。如果尚未配置时间范围，请导航到“配置>安全”>“访问控制”>“时间范围”以定义时间范围，然后再在虚拟 AP 配置文件中配置此设置。
DoS 预防	如果启用，AP 将忽略来自客户端的取消身份验证帧。这样可以防止对 AP 执行成功的取消授权攻击。这不会影响第三方 AP。 默认值：禁用
HA 发现 **关联**	如果启用，则在客户端关联时触发家乡代理发现，而不是基于来自客户端的流量触发家乡代理发现。关联上的移动性可以加快漫游速度并改善不发送许多上行链路数据包来触发移动性的客户端（VoIP 客户端）的连接性。最佳做法是禁用此参数，因为它会增加同一移动域中受管设备之间的 IP 移动控制流量。仅当在 VoIP 客户端中观察到语音问题时，才启用此参数。 默认值：禁用 注意：ha-disc-onassoc 参数仅在受管设备上启用和配置 IP 移动性时才有效。有关此参数的详细信息，请参阅关联时的 Home Agent 发现
移动 IP	启用或禁用此虚拟 AP 的 IP 移动性。 默认值：已启用
保留客户端 VLAN	如果选中此复选框，则如果客户端与 AP 解除关联，然后立即与同一 AP 或同一受管设备上的另一个 AP 重新关联，则客户端将保留其以前的 VLAN 分配。
远程 AP 操作	配置虚拟 AP 在远程 AP 上运行的时间： standard（默认值）— 当远程 AP 连接到受管设备时启用虚拟 AP。此选项可用于任何（网桥/拆分隧道/隧道/d-tunnel）虚拟 AP。 persistent — 在远程 AP 最初连接到受管设备后永久启用虚拟 AP（仅限网桥模式）。此选项可用于任何 （Open/PSK/802.1X） 桥接 VAP。

	backup — 如果远程 AP 无法连接到受管设备（仅限网桥模式），则启用虚拟 AP。此选项可用于非 802.1X 桥接 VAP。 always — 永久启用虚拟 AP（仅限网桥模式）。此选项可用于非 802.1X 桥接 VAP。
车站黑名单	选中此复选框可启用对不是欺骗性取消授权攻击的 DoS 攻击（如 ping 或 SYN 泛洪）的检测。 默认值：已启用
严格遵守	如果启用，则在 AP 和客户端工作站未定义通用速率时，AP 将拒绝客户端关联请求。某些不完全符合 802.11 的旧客户端工作站可能未在其关联请求中包含其配置的速率。除非禁用严格合规，否则此类不合规的站点可能难以与 AP 关联。 默认值：禁用
VLAN 移动性	启用或禁用 VLAN（第 2 层）移动性。 默认值：禁用
广域网操作模式	此功能可与 WAN 运行状况检查管理器和上行链路管理器配合使用。当所有上行链路都关闭时，上行链路管理器会根据配置进行所需的更改，并将这些更改推送到 AP。 如果操作模式设置为主要模式，VAP 将被禁用。 如果操作模式设置为备份，则将启用 VAP。 如果操作模式设置为始终，则 VAP 不会更改。
FDB Assoc 更新	此参数可为静默客户端启用无缝故障转移，从而允许它们重新关联。如果选择此选项，控制器将代表客户端生成第 2 层更新，以更新桥接设备中的转发表。 默认值：禁用
广播/组播	
动态组播优化（DMO）	启用/禁用动态组播优化。默认情况下，此参数处于禁用状态，如果没有 PEFNG 许可证，则无法启用。

动态组播优化（DMO） 阈值	组播组中超过该组将停止动态组播优化的高通量站的最大数量。 范围：2-255 站 默认值：6 个站点。
掉线广播和组播	选中“丢弃广播和组播”复选框以过滤掉空中的广播和组播流量。 请勿为在网桥转发模式下配置的虚拟 AP 启用此选项。此配置参数仅适用于隧道模式下的虚拟 AP。在隧道模式下，所有数据包都传输到控制器，因此控制器能够丢弃所有广播流量。当虚拟 AP 配置为使用桥接转发模式时，大多数数据流量都保留在 AP 本地，控制器无法过滤掉该广播流量。 重要说明：如果启用此选项，则还必须在虚拟 AP 配置文件上启用将广播 ARP 请求转换为单播参数，以防止丢弃 ARP 请求。
将广播 ARP 请求转换为单播	如果启用，则所有广播 ARP 请求都将转换为单播并直接发送到客户端。您可以使用 show ap active 和 show datapath tunnel 命令检查此选项的状态。如果启用，输出将在 flags 列中显示字母 a。 此配置参数仅适用于隧道模式下的虚拟 AP。在隧道模式下，所有数据包都传输到控制器，因此控制器能够将定向到广播地址的 ARP 请求转换为单播。 当虚拟 AP 配置为使用网桥转发模式时，大多数数据流量都保留在 AP 本地，控制器无法转换该广播流量。 默认情况下，此参数处于启用状态。升级到 DCYKOS 6.1.3.2 时，将启用与这些设置关联的行为。如果您的控制器支持无线网桥后面的客户端或 VMware 设备上的虚拟客户端，则必须禁用此设置以允许这些客户端获取 IP 地址。在 DCYKOS 的早期版本中，虚拟 AP 配置文件包含两个唯一的广播过滤器参数; 丢弃广播和组播参数，用于过滤除 DHCP 响应帧（这些帧转换为单播帧并发送到相应的客户端）之外的所有广播和组播流量，以及将广播 ARP 请求转换为单播参数，该参数将广播 ARP 请求转换为直接发送到客户端的单播消息。“将广播 ARP 请求转换为单播”设置包括广播过滤所有参数的附加功能，其中 DHCP 响应帧作为单播发送到相应的客户端。这可能会影响无线网桥后面的客户端和 VMware 设备上的虚拟客户端的 DHCP 发现/请求的数据包。禁用此

	选项可解决此问题，并允许无线网桥或 VMware 设备后面的客户端接收 IP 地址。 默认值：已启用

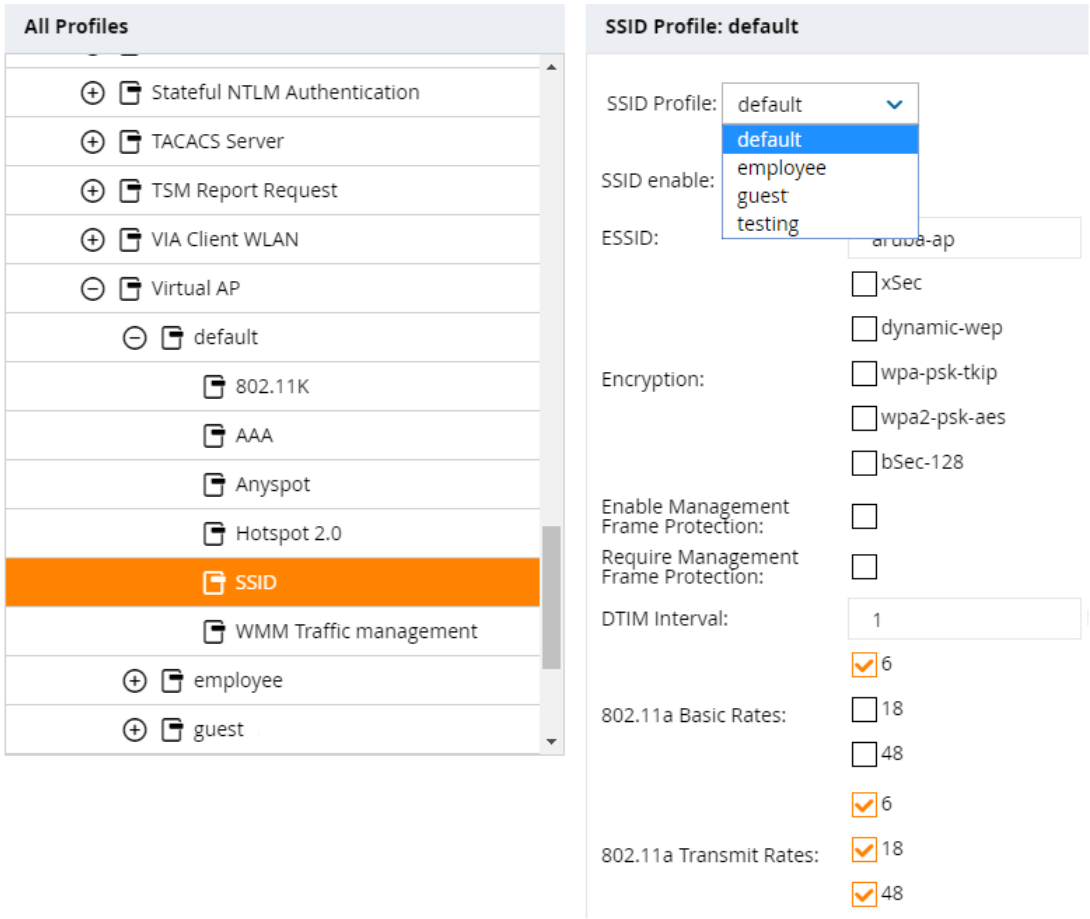
虚拟 AP 配置文件直接引用以下每种配置文件类型之一。

- 802.11k
- AAA
- AnySpot
- HotSpot 2.0
- SSID WWM 流量管理

要更改与虚拟 AP 配置文件关联的配置文件，请执行以下操作:

1. 在“托管网络”节点层次结构中，导航到“配置>系统>配置文件”选项卡。
2. 从“所有配置文件”列表中，选择无线局域网>虚拟 AP。
3. 选择要编辑的虚拟 AP 配置文件。“All Profiles”（所有配置文件）窗口显示该虚拟 AP 的关联配置文件列表。
4. 在列表中选择任何关联的配置文件。
5. 右窗格顶部会出现一个下拉列表，允许您为该类型选择另一个配置文件。
6. 单击提交。
7. 单击“挂起的更改”。
8. 在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

图 1 配置文件关联虚拟 AP



在 CLI 中

执行以下命令以配置虚拟 AP 配置文件:

(host)[node](config) #wlan virtual-ap <profile>

(host)[node] (Virtual AP profile "profile")aaa-profile <profile>

(host)[node] (Virtual AP profile "profile")anyspot-profile <profile>

(host)[node] (Virtual AP profile "profile")dot11k-profile <profile>

(host)[node] (Virtual AP profile "profile")hs2-profile <profile>

(host)[node] (Virtual AP profile "profile")ssid-profile <profile>

(host)[node] (Virtual AP profile "profile")wmm-traffic-management-profile <profile>

修改 AP 组关联的配置文件和参数

从 DCYKOS 8.0.1.0 开始，您可以使用 WebUI 修改与 AP 组关联的配置文件和参数。

执行以下任务以修改与 AP 组关联的配置文件和参数:

1. 在“托管网络”节点层次结构中，导航到“配置> AP 组”页面。
2. 在“AP 组”表中选择一个 AP 组，然后单击“配置文件”选项卡。
3. 在“配置文件”下选择一个配置文件 <AP 组>。
4. 单击<NAME>配置文件下拉列表，然后选择一个配置文件。
5. 对配置文件进行必要的更改，然后单击提交。
6. 单击“挂起的更改”（Pending Changes）。
7. 在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

选择性组播流

选择性组播组仅基于通过 Internet 组管理协议 （IGMP） 获知的数据包。

在虚拟 AP 配置文件中启用丢弃广播和组播设置后，仅当满足以下条件时，受管设备才允许转发组播数据包:

- 来自有线端的数据包的目标地址范围为 225.0.0.0 - 239.255.255.255
- 射频已订阅组播组。

如果在虚拟 AP 配置文件中启用了 DMO 设置，则数据包将使用 802.11 单播报头发送。

禁用 IGMP 监听/代理时，受管设备不会知道 IGMP 成员身份并丢弃组播流。

如果启用了 AirGroup，则 mDNS （SSDP） 数据包将发送到 AirGroup 应用程序。mDNS 的通用地址为 224.0.0.251，SSDP 为 239.255.255.250。

更改虚拟 AP 转发模式

当您更改主动为客户端提供服务的虚拟 AP 的转发模式时，除非手动清除这些用户的条目，否则用户表将不会反映准确的客户端信息。使用以下过程更改为有线或无线客户端提供服务的虚拟 AP 上的转发模式。

更改有线用户的转发模式

要更改连接到 AP 上有线端口的有线用户的转发模式:

1. 通过发出 CLI 命令 ap wired-port-profile shutdown 来禁用端口<ap-wired-port-profile>。这将断开使用该端口的任何有线客户端的连接。

2. 发出命令 aaa user delete {<ipaddr>|all|mac <macaddr>|name <username>|role <role>}, 使用 <ap-wired-port-profile>.

3. 发出命令 ap wired-ap-profile <profile> forward-mode，<mode>其中<mode>是有线端口的新转发模式

4. 使用命令 ap wired-port-profile no shutdown 重新启用端口<ap-wired-port-profile>。

Open 更改无线用户的转发模式

要更改与 AP 无线电关联的无线用户的转发模式:

1. 发出命令 ap-name <group> no virtual-ap <vap-profile> 或 ap-group <group> no virtual-ap，<vap-profile>以取消 AP 或 AP 组与虚拟 AP 配置文件的关联。

2. 发出命令 aaa user delete {<ipaddr>|all|mac <macaddr>|name <username>|role <role>}, 从用户表中删除与上一步中指定的 virtual-ap 关联的用户。

3. 发出命令 wlan virtual-AP <vap-profile> forward-mode，<mode>其中<mode>是虚拟 AP 的新转发模式。

4. 发出命令 ap-name <group> virtual-ap <vap-profile> 或 ap-group <group> virtual-ap <vap-profile> 以将 AP 或 AP 组与虚拟 AP 配置文件重新关联。

WLAN SSID 配置文件

SSID 是任何客户端看到的网络或 WLAN。SSID 配置文件定义网络的名称、网络的身份验证类型、基本速率、传输速率、SSID 隐藏以及网络的某些 WMM 设置。

本节介绍以下主题:

SSID 配置文件概述

DCYKOS 支持不同类型的 AES、TKIP 和 WEP 加密。AES 是最安全且推荐的加密方法。大多数现代设备都支持 AES，并且 AES 应该是默认加密方法。仅当网络包含不支持 AES 的设备时，才使用 TKIP。在这些情况下，请对仅支持 TKIP 的设备使用单独的 SSID。

Suite-B 加密

Suite-B （bSec） 协议是向 IEEE802.11 委员会提出的前标准协议，作为 802.11i 的替代方案。bSec 和标准 802.11i 之间的主要区别在于 bSec 尽可能实现 Suite-B 算法。值得注意的是，AES-CCM 被 AES-GCM 取代，802.11i 的密钥派生函数 （KDF） 升级为支持 SHA-256 和 SHA-384。为了提供与标准 Wi-Fi 软件驱动程序的互操作性，bSec 作为标准 802.11Wi-Fi 和第 3 层协议（如 IP）之间的垫片层实现。配置为通告 bSec SSID 的托管设备将通告开放网络，但网络上只允许 bSec 帧。

bSec 协议要求您在客户端设备上使用 VIA 2.1.1 或更高版本。有关配置和安装威盛的更多信息，请参阅威盛文档。

bSec 协议提供 128 位模式和 256 位模式。位数指定 AES-GCM 加密密钥的长度。使用美国国防部的分类术语，bSec-128 适用于保护最高 SECRET 级别的信息，而 bSec-256 适用于保护最高 TOP SECRET 级别的信息。

DCYKOS 硬件支持 Suite-B AES-128-GCM 和 AES-256-GCM 加密。

Wi-Fi 多媒体保护

Wi-Fi 多媒体™ （WMM®） 是基于 IEEE802.11e 修正案的 Wi-Fi 联盟®认证计划。WMM 确保空中延迟敏感流量的 QoS。WMM 将流量分为四个队列或访问类别:

- 声音
- 视频
- 尽力而为
- 背景

管理帧保护

DCYKOS 支持 IEEE 802.11w 标准，也称为管理帧保护 （MFP）。管理帧保护使攻击者难以通过欺骗 Deauth 和 Disassoc 管理帧来拒绝服务。管理帧保护使用 802.11i（可靠的安全网络）框架在客户端和 AP 之间建立加密密钥。

管理帧保护在虚拟 AP 上配置为 wlan ssid-profile 的一部分。支持 WPA2 操作模式的 SSID 在除隧道模式之外的所有转发模式下都支持 MFP。支持 WPA3 操作模式的 SSID 仅支持隧道模式下的 MFP。两个与 MFP 相关的参数（支持 mfp 和需要 mfp）无法通过 CLI 或 WebUI 进行配置。DCYKOS 会根据操作模式自动配置这些参数。

HE WLAN（HEW）

DCYKOS 8.4.0.0 支持 IEEE 802.11ax 标准，也称为高效 WLAN （HEW）。HEW 在室内外环境下，在 AP 或基站密集部署场景下，提高了频谱效率和区域吞吐量。HEW 增强了 2.4 GHz 和 5 GHz 频段上的 802.11 PHY 和 MAC 通道。

HEW 包括以下功能：

向后兼容 802.11a/b/g/n/ac。

更好的电源管理，延长电池寿命。

HEW 作为 WLANSSID 配置文件的一部分在虚拟 AP 上配置。您可以从 WebUI 配置高效 SSID 配置文件。有关详细信息，请参阅第 1 页的“高效 （HE） AP”。

配置 SSID 配置文件

按照以下步骤创建新的 SSID 配置文件，并使用 WebUI 或 CLI 将该配置文件关联到您的虚拟 AP。

Open 在 WebUI 中

执行以下任务以配置 SSID 配置文件：

1. 在“托管网络”节点层次结构中，导航到“配置>系统>配置文件”选项卡。
2. 从“所有配置文件”列表中，选择无线局域网> SSID。
3. 要编辑现有 SSID 配置文件，请选择要编辑的 SSID 配置文件。要创建新的 SSID 配置文件，请单击 + 并在配置文件名称字段中输入新 SSID 配置文件的名称。
4. 配置您的 SSID 设置。SSID 配置文件参数中介绍了配置参数。
5. 单击提交。
6. 单击“挂起的更改”（Pending Changes）。
7. 在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

SSID 配置文件参数

参数	描述
SSID 启用	单击此复选框可启用或禁用 SSID。默认情况下，SSID 处于启用状态。
ESSID	唯一标识无线网络的名称。网络名称或 ESSID 最多可以是 32 个 ASCII 字符，如果它包含 unicode，则最大字符数会有所不同。例如，ESSID 最多可以有 10 个汉字。如果 ESSID 包含空格，则必须将其括在引号中。
WPA 密码	输入 WPA 密码。 如果加密类型为 wpa2-psk-aes，请输入 WPA 密码、WPA 十六进制密钥或 MPSK 密码之一。MPSK 密码短语要求对 ClearPass Policy Manager 服务器进行 MAC 身份验证。 如果输入了 WPA 密码短语、WPA 十六进制密钥和 MPSK 密码短语，则 MPSK 密码短语优先，客户端必须使用从 ClearPass Policy Manager 服务器接收的 MPSK 密码短语。MPSK 密码短语要求对 ClearPass Policy Manager 服务器进行 MAC 身份验证。 如果配置了 WPA 密码和 WPA 十六进制，即加密类型不是 mpsk-aes，则只考虑 WPA 十六进制。
加密	选择以下加密类型之一：
xSec 的	控制器与有线或无线客户端之间或控制器之间的第 2 层流量的加密和隧道。 若要使用 xSec 加密，必须使用 RADIUS 身份验证服务器。对于客户端，您必须安装 Funk Odyssey 客户端软件。 需要安装 xSec 许可证。对于托管设备之间的 xSec，必须在每个托管设备中安装 xSec 许可证。
增强型开放	增强的开放加密，带或不带 PMK 缓存。
WPA3-SAE-AES 型	使用 Simultaneous 进行 AES 加密的 WPA3 等等身份验证 （SAE）。
WPA3-AES-CCM-128 型	WPA3 具有 AES CCM 加密和使用 802.1X 的动态密钥。
wpa3-cnsa	使用 CNSA（192 位）的 AES GCM-256 加密的 WPA3。

静态-WEP	带有静态键的 WEP。
动态-WEP	带有动态键的 WEP。
WPA-TKIP 型	使用 802.1X 的 TKIP 加密和动态密钥的 WPA。
WPA-AES 公司	使用 802.1X 的 AES 加密和动态密钥的 WPA。
wpa-psk-tkip	使用预共享密钥进行 TKIP 加密的 WPA。
wpa-psk-aes	使用预共享密钥进行 AES 加密的 WPA。
wpa2-aes	使用 802.1X 的 AES 加密和动态密钥的 WPA2。
WPA2-PSK-AES 的	使用预共享密钥进行 AES 加密的 WPA2。
WPA2-PSK-TKIP 系列	使用预共享密钥进行 TKIP 加密的 WPA2。
WPA2-TKIP 型	使用 802.1X 的 TKIP 加密和动态密钥的 WPA2。
MPSK-AES 的	具有 AES 加密的 MPSK。
Opmode 转换	启用向后兼容性 增强型开口/WPA3-SAE-AES 操作模式。
启用管理帧保护	选择后，SSID 支持支持 MFP 的客户端和传统客户端。 只能在支持 WPA2 的 SSID 上启用管理帧保护。
需要管理帧保护	选择后，SSID 仅支持支持管理帧保护的客户端。 只能在支持 WPA2 的 SSID 上启用管理帧保护。
DTIM 间隔	指定在信标中发送 DTIM 之间的间隔（以毫秒为单位）。这是刷新未确认的网络广播之前的最大信标周期数。使用采用电源管理功能的无线客户端进入睡眠状态时，客户端必须在 DTIM 期间至少恢复一次才能接收广播
802.11a 基本费率	选择在信标帧和探测响应中通告的受支持的 802.11a 速率集（以 Mbps 为单位）。
802.11a 传输速率	选择允许 AP 发送数据的一组 802.11a 速率。实际传输速率取决于客户端能够处理的内容、关联时发送的信息以及客户端的当前错误/丢失率。
802.11g 基本费率	选择在信标帧和探测响应中通告的一组受支持的 802.11b/g 速率。
802.11g 传输速率	选择允许 AP 发送数据的 802.11b/g 速率集。实际传输速率取决于客户端能够处理的内容、关联时发送的信息以及客户端的当前错误/丢失率。

站点老化时间	允许客户端在老化之前保持空闲的时间（以秒为单位）。
最大传输尝试次数	AP 发送帧允许的最大重试次数。
RTS 阈值	传输大于此阈值的帧的无线客户端必须发出 RTS 并等待 AP 使用 CTS 进行响应。这有助于防止不在无线对等范围内且无法检测到其他无线客户端何时传输的无线客户端发生空中碰撞。 默认值：2333
简短的序言	单击此复选框可启用或禁用 802.11b/g 无线电的短前导码。启用短前导码时，网络性能可能会更高。在混合无线电环境中，某些 802.11b 无线客户端电台可能难以使用短前导码与 AP 关联。若要仅使用长前导码，请禁用短前导码。通常可以更新仅使用长前导码的旧版客户端设备以支持短前导码。
最大关联数	SSID 的每个无线电的最大无线客户端数（受每个无线电 255 个客户端的 AP 限制）。 默认值：64
无线多媒体（WMM）	启用或禁用 WMM，也称为 IEEE802.11e 增强型配电协调功能。WMM 提供相对于网络中其他流量的特定流量的优先级。
无线多媒体 U-APSD（WMM-UAPSD） 省电	启用 WMM UAPSD 电源保存。
WMMTSPEC 最小不活动间隔	指定 WMM 流量的最小非活动超时阈值。此设置在播发低非活动间隔超时的环境中非常有用，这可能会导致不必要的超时。 支持的范围为 0-3,600,000 毫秒，默认值为 0 毫秒。
WMM 语音 AC 的 DSCP 映射 （0-63）	用于映射 WMM 语音流量的 DSCP。 支持的范围为 0-63。
WMM 视频 AC 的 DSCP 映射 （0-63）	选择用于映射 WMM 视频流量的 DSCP。 支持的范围为 0-63。
WMM 尽力而为 AC 的 DSCP 映射 （0-63）	选择用于映射 WMM 尽力而为流量的 DSCP 值。 支持的范围为 0-63。

WMM 后台 AC 的 DSCP 映射 （0-63）	选择用于映射 WMM 后台流量的 DSCP。 支持的范围为 0-63。
隐藏 SSID	选中此复选框可启用或禁用在信标帧中隐藏 SSID 名称。请注意，隐藏 SSID 对提高安全性几乎没有作用。
Deny_Broadcast 探测	当客户端发送广播探测请求帧以搜索所有可用的 SSID 时，此选项控制系统是否响应此 SSID。启用后，不会发送任何响应，客户端必须知道 SSID 才能与 SSID 关联。禁用后，将为此 SSID 发送探测响应帧。
本地探测请求阈值（dB）	输入 SNR 阈值，低于该阈值的传入探测请求将被忽略。支持的值范围为 0-100 dB。值为 0 将禁用此功能。
禁用探测重试	单击此复选框可启用或禁用探测响应帧的电池 MAC 级别重试。默认情况下，此参数处于启用状态，这意味着对探测响应帧的 MAC 级别重试处于禁用状态。 注意：200 系列接入点不支持此参数。
Battery Boost	在传送到客户端之前将组播流量转换为单播，从而允许您设置更长的 DTIM 间隔。较长的间隔可防止关联的无线客户端激活其无线电以进行组播指示和传输，从而使它们处于省电模式的时间更长，从而延长电池寿命。 此参数需要 PEFNG 许可证。
WEP 密钥 1	与密钥索引关联的第一个静态 WEP 密钥。长度可以是 10 或 26 个十六进制字符。
WEP 密钥 2	与密钥索引关联的第二个静态 WEP 密钥。长度可以是 10 或 26 个十六进制字符。
WEP 密钥 3	与密钥索引关联的第三个静态 WEP 密钥。长度可以是 10 或 26 个十六进制字符。
WEP 键 4	与密钥索引关联的第四个静态 WEP 密钥。长度可以是 10 或 26 个十六进制字符。
WEP 传输密钥索引	指定要使用的静态 WEP 密钥的密钥索引。可以是 1、2、3 或 4。
WPA 六角形	WPAPSK 的。
WPA 密码	用于生成 PSK 的 WPA 密码。

最大传输失败次数	AP 假定客户端已离开，当 AP 检测到由于已超过最大重试阈值而未传送此数量的连续帧时，应取消授权。
BC/MC 速率优化	单击此复选框可启用或禁用当前与 AP 关联的所有活动电台的扫描，以选择广播和组播帧的最低传输速率。此选项仅适用于广播和组播数据帧;802.11 管理帧以最低配置的速率传输。 注意：除非 DCYK 技术支持代表指示，否则请勿启用此参数。
用于交付 EAPOL 帧的速率优化	单击此复选框可使用更保守的速率，以便更可靠地交付 EAPOL 帧。 默认值：已启用
严格的 Spectralink 语音协议 （SVP）	单击此复选框可启用 Strict SVP
802.11g 信标率	单击此下拉列表以选择 802.11g 的信标速率（仅用于 DAS）。在正常操作中使用此参数可能会导致连接问题。
802.11a 信标率	单击此下拉列表以选择 802.11a 的信标速率（仅用于 DAS）。在正常操作中使用此参数可能会导致连接问题。
视频组播速率优化	配置后，受管设备会选择视频多播帧的速率。您也可以配置 MCS 费率。MCS 是一个重要的设置，因为它提供了潜在的更高吞吐量。 注意： 如果启用或禁用高吞吐量 SSID 配置文件中的 20 MHz 模式下的短保护间隔设置，则以下信息显示 MCS 速率： MCS 流 20 MHz 20 MHz SGI --- ------- ------ ---------- 0 1 6.5 7.2 1 1 13.0 14.4 2 1 19.5 21.7 3 1 26.0 28.9 4 1 39.0 43.3 5 1 52.0 57.8 6 1 58.5 65.0 7 1 65.0 72.2

	8 2 13.0 14.4 9 2 26.0 28.9 10 2 39.0 43.3 11 2 52.0 57.8 12 2 78.0 86.7 13 2 104.0 115.6 14 2 117.0 130.0 15 2 130.0 144.4 注意：所有支持 802.11n 的 AP 都支持视频组播的 MCS 速率。320 系列 AP 不支持此功能。
播发 QBSS Load IE	单击此复选框可使 AP 通告 QBSS 负载元素。该元素包括以下参数，这些参数提供有关交通状况的信息： 站数：与 QBSS 关联的站总数。 通道利用率：检测到通道繁忙的时间百分比（归一化为 255）。接入点使用物理或虚拟载波检测机制来检测繁忙信道。 可用入场容量：通过显式入场控制为电台可用的剩余介质时间量（以 32us/s 的数量衡量）。 QAP 使用这些参数来决定是否接受准入控制请求。无线站使用这些参数来选择适当的接入点。 注意：确保为旧版 AP 启用 WMM 以通告 QBSS 负载元素。对于 802.11n AP，请确保启用 WMM 或高吞吐量。
宣传位置信息	启用此选项后，AP 将在 Beacon 帧和 Probe Response 帧中传输的 IE 中广播其位置。AP 的纬度、经度和海拔高度可以在受管设备 WebUI >无线配置>AP 安装页面中配置，也可以在受管设备命令行界面中使用 provision-ap 命令进行配置。
通告 AP 名称	如果开启该参数，AP 将广播 ap-name 命令配置的 AP 名称。 默认值：禁用

对开放的工作站强制实施用户 VLAN	选择此选项可将数据流量从打开的工作站限制到分配给用户的 VLAN。默认情况下，此选项处于禁用状态。
启用 OKC	OKC 是一种类似的技术，未由 802.11i 定义，可用于网络中多个 AP 之间的身份验证，这些 AP 处于公共管理控制之下。在单个受管设备的控制下具有多个 AP 的 DCYK 部署就是这样一个例子。使用 OKC，漫游到网络中任何 AP 的站不必完成完整的身份验证交换，而只需执行 4 次握手即可建立暂时性加密密钥。

在 CLI 中

执行以下命令以配置 SSID 配置文件:

（config） #wlan ssid-profile <profile>

WLAN 认证

WLAN 向导允许您定义与 WLAN 关联的客户端使用的身份验证类型。WLAN 向导是定义 WLAN 设置的推荐方法，但高级用户也可以通过 WebUI 或 CLI 中的 AAA 配置文件手动定义身份验证设置。

Open 在 WebUI 中

执行以下任务以配置 WLAN 身份验证:

1. 在“托管网络”节点层次结构中，导航到“配置>身份验证”>“AAA 配置文件”选项卡。
2. 从“AAA 配置文件”列表中，选择无线局域网> AAA.
3. 要编辑现有的 AAA 配置文件，请选择要编辑的 AAA 配置文件。要创建新的 AAA 配置文件，请单击 +，然后在配置文件名称字段中输入新 AAA 配置文件的名称。
4. 配置表 1 中描述的 AAA 配置文件参数。
5. 单击提交。
6. 单击“挂起的更改”（Pending Changes）。
7. 在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

AAA 配置文件参数

参数	描述

初始角色	单击“初始角色”下拉列表，然后为未经身份验证的用户选择一个角色。未经身份验证的用户的默认角色是登录。
MAC 身份验证默认角色	单击“MAC 身份验证默认角色”下拉列表，然后选择设备通过 MAC 身份验证时分配给用户的角色。MAC 身份验证的默认角色是访客用户角色。如果存在派生规则，则通过这些规则分配给客户端的角色优先于默认角色。 此功能需要 PEFNG 许可证。
802.1X 身份验证默认角色	单击 802.1X 身份验证默认角色下拉列表，然后选择在 802.1X 身份验证后分配给客户端的角色。802.1X 身份验证的默认角色是来宾用户角色。如果存在派生规则，则通过这些规则分配给客户端的角色优先于默认角色。 此功能需要 PEFNG 许可证。
用户空闲超时	指定客户端的空闲超时值（以秒为单位）。值为 0 时，在与无线网络解除关联后立即删除用户。有效范围为 30-15300，以 30 秒的倍数表示。
RADIUS 记账更新	启用此选项后，RADIUS 记帐功能允许受管设备定期向服务器发送包含当前用户统计信息的临时更新消息。默认情况下，此选项处于禁用状态，允许受管设备仅向 RADIUS 记帐服务器发送启动和停止消息。
用户派生规则	单击用户派生规则下拉列表，然后指定从中派生用户角色或 VLAN 的用户属性配置文件。
有线到无线漫游	启用此功能可在用户从网络的有线端漫游时保持用户身份。默认情况下，此功能处于启用状态。
在 VLAN 更改时重新验证有线用户	当有线用户在 VLAN 之间移动时，将创建一个触发器来重新验证此用户。
设备类型分类	选择此选项时，受管设备将解析用户代理字符串，并尝试识别连接到 AP 的设备类型。启用设备类型分类后，如果可以识别客户端设备，则“监控>网络>所有 WLAN 客户端”窗口中显示的全局客户端表将显示每个客户端的设备类型。
强制实施 DHCP	选择此选项时，客户端必须先使用 DHCP 获取 IP，然后才能与 AP 关联。在创建根据客户端设备类型分配特定角色或 VLAN 的用户规则时，请启用此选项。有关详细信息，请参阅使用用户派生的 VLAN。

	如果客户端通过“登录用户生存期”AAA 计时器从用户表中删除，则该客户端将无法发送流量，直到它续订其 DHCP。 强制实施 DHCP 在受管设备上仅适用于配置为隧道或解密隧道转发模式的 AP。
PAN 防火墙集成	需要 Palo Alto Networks 防火墙的 IP 映射。有关详细信息，请参阅第 1 页的“ ”。
打开 SSID RADIUS 记帐	一旦用户关联到 Open SSID，无需任何身份验证，就会启动 RADIUS 记帐。 请勿为有线用户启用此参数。如果启用，受管设备会为未经身份验证的有线用户发送 RADIUS 记帐数据包。

在 CLI 中

执行以下命令配置 WLAN 认证:

(host)[node](config) #aaa authentication dot1x <profile>

(host)[node](config) #aaa profile <profile>