了解无线局域网控制器(WLC)上的Web身份验证

目录

简介

本文档介绍无线局域网控制器(WLC)上的Web身份验证过程。

先决条件

要求

Cisco建议您具备WLC配置的基本知识。

使用的组件

本文档中的信息基于所有WLC硬件型号。

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。

Web身份验证内部进程

作为安全功能的Web身份验证位置

Web身份验证(WebAuth)是第3层安全。它支持用户友好的安全，可在任何运行浏览器的工作站上运行。

它可以与任何预共享密钥(PSK)安全（第2层安全策略）结合使用。

虽然WebAuth和PSK的结合减少了用户友好部分，但它具有加密客户端流量的优势。

WebAuth是一种无加密的身份验证方法。

在同时安装和配置WLC软件版本7.4之前，无法使用802.1x/RADIUS（远程身份验证拨入用户服务）配置WebAuth。

客户端必须通过dot1x和Web身份验证。它旨在为员工（使用802.1x）而非访客添加Web门户。

员工的dot1x或访客的Web门户没有一体化服务集标识符(SSID)。

WebAuth的工作原理

802.11身份验证过程是开放的，因此您可以进行身份验证和关联而不会有任何问题。之后，您会进行关联，但不在WLC中 **RUN** 状态.

启用Web身份验证后，您将被保留在 **WEBAUTH_REQD** 其中无法访问任何网络资源。

您必须在选项中收到DHCP IP地址和DNS服务器地址。

在浏览器中键入有效的URL。客户端通过DNS协议解析URL。然后，客户端将其HTTP请求发送到网站的IP地址。

WLC拦截该请求并返回 **webauth** 登录页面，模仿网站IP地址。使用外部WebAuth时，WLC会以包含您的网站IP地址和页面已移动状态的HTTP响应进行回复。

页面已移动到WLC使用的外部Web服务器。通过身份验证后，您将获得对所有网络资源的访问权，默认情况下会重定向到最初请求的URL（除非在WLC上配置了强制重定向）。

总之，WLC允许客户端解析DNS并自动获得IP地址 **WEBAUTH_REQD** 状态.

要监视另一个端口而不是端口80，请使用 **config network web-auth-port** 在此端口上创建重定向。

例如，访问控制服务器(ACS)Web界面，位于端口2002或其他类似应用上。

有关HTTPS重定向的注意:默认情况下，WLC不会重定向HTTPS流量。这意味着如果您在浏览器中键入HTTPS地址，则不会发生任何情况。您必须键入HTTP地址才能重定向到HTTPS中提供的登录页面。

在版本8.0及更高版本中，您可以使用CLI命令启用HTTPS流量的重定向 **config network web-auth https-redirect enable.**

在发送许多HTTPS请求的情况下，这会为WLC使用大量资源。建议不要在WLC版本8.7之前使用此功能，因为在该版本中此功能增强了可扩展性。另请注意，在这种情况下，证书警告是不可避免的。如果客户端请求任何URL(例如https://www.cisco.com)，则WLC仍提供其自身为虚拟接口IP地址颁发的证书。这始终不匹配客户端请求的URL/IP地址，并且证书不受信任，除非客户端在其浏览器中强制实施例外。

测得的WLC软件版本8.7之前的指示性能下降：

Webauth	实现的速率
3个URL - HTTP	140/秒
第1个URL - HTTP 第2和第3个URL - HTTPS	20/秒
3个URL - HTTPS（大型部署）	<1 /秒
3个URL - HTTPS（最多100个客户端）	10/秒

在此性能表中，3个URL称为：

- 最终用户输入的原始URL
- WLC将浏览器重定向到的URL
- 最终凭证提交

如果所有3个URL都是HTTP，如果所有3个URL都是HTTPS，或者如果客户端从HTTP移动到HTTPS（典型），性能表会提供WLC性能。

如何使内部（本地）WebAuth使用内部页面

要为WLAN配置可运行的动态接口，客户端还会通过DHCP接收DNS服务器IP地址。

在任何 **webauth** 设置，验证WLAN是否正常工作，可以解析DNS请求(**nslookup**)，并且可以浏览网页。

将Web身份验证设置为第3层安全功能。在本地数据库或外部RADIUS服务器上创建用户。

请参阅无线局域网控制器Web身份验证配置示例文档。

如何使用自定义页面配置自定义本地Web身份验证

自定义 **webauth** 可以配置 **redirectUrl** 从 **Security** 选项卡。这会强制重定向到您输入的特定网页。

当用户通过身份验证时，它会覆盖客户端请求的原始URL，并显示为其分配重定向的页面。

自定义功能允许您使用自定义HTML页面而不是默认登录页面。将您的html和图像文件捆绑上传到控制器。

在上传页面中，查找 **webauth bundle** 采用tar格式。PicoZip创建与WLC兼容的标签。

有关WebAuth捆绑包的示例，请参阅无线控制器WebAuth捆绑包的下载软件页。为WLC选择适当的版本。

建议自定义现有的捆绑包；请勿创建新捆绑包。

在以下方面有一些限制 **custom webauth** 因版本和漏洞而异。

- .tar文件大小（不超过5MB）
- .tar中的文件数
- 文件的文件名长度（不超过30个字符）

如果该包不起作用，则尝试创建简单的自定义包。分别添加文件和复杂性以访问用户尝试使用的程序包。这有助于确定问题。

要配置自定义页面，请参阅Cisco无线LAN控制器配置指南7.6版中的部分，创建自定义Web身份验证登录页。

覆盖全局配置技术

使用**override global config**命令配置并为每个WLAN设置WebAuth类型。这将允许内部/默认WebAuth和自定义内部/默认WebAuth用于另一个WLAN。

这允许为每个WLAN配置不同的自定义页面。

合并同一捆绑包中的所有页面并将其上传到WLC。

在每个WLAN上使用**override global config**命令设置自定义页面，并从捆绑包中的所有文件中选择哪个文件是登录页面。

在捆绑包内为每个WLAN选择不同的登录页。

重定向问题

HTML捆绑包内有一个允许重定向的变量。请勿将强制重定向URL放在此处。

对于自定义WebAuth中的重定向问题，思科建议检查捆绑包。

如果在WLC GUI中输入**+=**的重定向URL，这可能会覆盖或添加到捆绑中定义的URL。

例如，在WLC GUI中， **redirectURL** 字段设置为www.cisco.com;但在捆绑包中，它显示：**redirectURL+=** '(网站URL)'。 **+=**会将用户重定向到无效的URL。

如何使外部（本地）Web身份验证与外部页面配合使用

使用外部WebAuth服务器只是登录页面的外部存储库。用户凭证仍由WLC进行身份验证。外部Web服务器仅允许特殊或不同的登录页。

对外部WebAuth执行的步骤：

1. 客户端（最终用户）打开Web浏览器并输入URL。

2. 如果客户端未进行身份验证且使用外部Web身份验证，则WLC会将用户重定向到外部Web服务器URL。WLC向具有模拟IP地址的客户端发送HTTP重定向，并指向外部服务器IP地址。外部Web身份验证登录URL附加了参数，例如 **AP_Mac_Address**,此 **client_url** (**客户端URL地址**)，以及 **action_URL** 需要联系交换机web服务器。

3. 外部Web服务器URL将用户发送到登录页面。用户可以使用预身份验证访问控制列表(ACL)访问服务器。

4. 登录页面将用户凭证请求发送回 **action_URL**例如http://192.0.2.1/login.html。这是作为重定向URL的输入参数提供的，其中192.0.2.1是交换机上的虚拟接口地址。

5. WLC Web 服务器提交用于身份验证的用户名和口令。

6. WLC发起RADIUS服务器请求或使用WLC上的本地数据库，然后对用户进行身份验证。

7. 如果身份验证成功，WLC Web服务器会将用户转发到配置的重定向URL或客户端输入的URL。

8. 如果身份验证失败，则WLC Web服务器会将用户重定向回用户登录URL。

   注意：在本文档中，我们使用192.0.2.1作为虚拟ip的示例。建议将192.0.2.x范围用于虚拟ip，因为它不可路由。旧文档可能指的是“1.1.1.x”，或者仍是WLC中配置的默认设置。但请注意，此ip现在是一个有效的可路由ip地址，因此建议改用192.0.2.x子网。

如果接入点(AP)处于FlexConnect模式， **preauth** ACL不相关。Flex ACL可用于允许未经身份验证的客户端访问Web服务器。

请参阅使用无线局域网控制器的外部Web身份验证配置示例。

Web直通

Web直通是内部Web身份验证的一种变体。它显示带有警告或警告语句的页面，但不提示输入凭证。

然后，用户单击**ok**。启用邮件输入，用户可输入其邮件地址，该地址将成为其用户名。

当用户连接时，检查您的活动客户端列表，并验证用户是否列出其作为用户名输入的邮件地址。

有关详细信息，请参阅无线LAN控制器5760/3850 Web直通配置示例。

有条件的Web重定向

如果启用条件网络重定向，则在802.1x身份验证成功完成之后，有条件地将用户重定向到特定网页。

您可以在您的 RADIUS 服务器上指定重定向页以及发生重定向的条件。

条件可以包括当密码到达到期日期或用户需要支付账单以继续使用/访问时输入密码。

如果RADIUS服务器返回思科AV对 **url-redirect**然后，当用户打开浏览器时，会重定向到指定的URL。

如果服务器还返回Cisco AV对 **url-redirect-acl**然后，指定ACL将作为此客户端的预身份验证ACL安装。

此时，客户端被视为未获得完全授权，只能通过预身份验证ACL允许的流量。在客户端完成指定URL上的特定操作（例如，密码更改或帐单支付）后，客户端必须重新进行身份验证。

当RADIUS服务器不返回 **url-redirect**，客户端被视为完全授权并允许其传递流量。

> **注意**：有条件的Web重定向功能仅适用于为802.1x或WPA+WPA2第2层安全配置的WLAN。

配置RADIUS服务器后，使用控制器GUI或CLI在控制器上配置条件网络重定向。请参阅以下分步指南：配置Web重定向(GUI)和配置Web重定向(CLI)。

启动页Web重定向

如果启用启动页Web重定向，则在802.1x身份验证成功完成之后，会将用户重定向到特定网页。在重定向后，用户具有对网络的完全访问权限。

您可以在RADIUS服务器上指定重定向页面。如果RADIUS服务器返回思科AV对 **url-redirect**然后，当用户打开浏览器时，会重定向到指定的URL。

此时，客户端被视为已完全授权，并且允许传递流量，即使RADIUS服务器不返回 **url-redirect**.

> **注意**：启动页重定向功能仅适用于为802.1x或WPA+WPA2第2层安全配置的WLAN。

配置RADIUS服务器后，使用控制器GUI或CLI在控制器上配置启动页网络重定向。

MAC过滤器上的WebAuth失败

MAC过滤器FaFailure上的WebAuth要求您在第2层安全菜单上配置MAC过滤器。

如果用户使用其MAC地址成功验证，则直接转到 **run** 状态.

如果不是，则转到 **WEBAUTH_REQD** 状态和正常的Web身份验证。

> **注意**：Web传递不支持此功能。有关详细信息，请按照增强请求Cisco Bug ID CSCtw的练习操作73512

集中Web身份验证

集中Web身份验证是指在WLC中不再托管任何服务的场景。客户端直接发送到ISE Web门户，不通过WLC上的192.0.2.1。登录页面和整个门户已外部化。

当在WLAN和MAC过滤器的高级设置中启用RADIUS网络准入控制(NAC)时，将会进行集中网络身

份验证。

WLC向ISE发送RADIUS身份验证（通常用于MAC过滤器），ISE以 **redirect-url** 属性值(AV)对。

然后用户进入 **POSTURE_REQD** 状态，直到ISE发出授权更改授权(CoA)请求。在安全评估或集中网络身份验证中也会发生相同的情况。

中央Web身份验证与WPA-Enterprise/802.1x不兼容，因为访客门户无法像使用可扩展身份验证协议(EAP)那样返回会话密钥以进行加密。

外部用户身份验证(RADIUS)

当WLC处理凭证或启用第3层Web策略时，外部用户身份验证(RADIUS)仅对本地WebAuth有效。在本地或WLC上或通过RADIUS在外部对用户进行身份验证。

WLC按一定的顺序检查用户的凭证。

1. 无论如何，它首先查看自己的数据库。
2. 如果它在该处找不到用户，则会转到在访客WLAN中配置的RADIUS服务器（如果配置了一个）。
3. 然后，它会根据其中的RADIUS服务器检查全局RADIUS服务器列表 **network user** 已选中。

第三点回答了那些没有为该WLAN配置RADIUS的用户的问题，但请注意，当在控制器上找不到用户时，它仍会检查RADIUS。

这是因为 **network user** 会根据全局列表中的RADIUS服务器进行检查。

WLC可以使用密码身份验证协议(PAP)、质询握手身份验证协议(CHAP)或EAP-MD5（消息摘要5）向RADIUS服务器验证用户。

这是一个全局参数，可从GUI或CLI进行配置：

从GUI:导航至 **Controller > Web RADIUS Authentication**

从CLI:输入 **config custom-web RADIUSauth**

> **注**:NAC访客服务器仅使用PAP。

如何设置有线访客WLAN

有线访客WLAN配置类似于无线访客配置。它可以配置一个或两个控制器（仅当有一个是自动锚点时）。

选择一个VLAN作为有线访客用户的VLAN，例如，在VLAN 50上。当有线访客想要访问Internet时，请将笔记本电脑插入配置为VLAN 50的交换机上的端口。

必须允许此VLAN 50并将其存在通过WLC中继端口的路径上。

对于两个WLC（一个锚点和一个外部），此有线访客VLAN必须指向外部WLC（名为WLC1），而不是指向锚点。

然后，WLC1处理通向DMZ WLC（锚点，名为WLC2）的流量隧道，该锚点释放路由网络中的流量。

以下是配置有线访客接入的五个步骤：

1. **为有线访客用户访问配置动态接口(VLAN)。**

   在WLC1上创建动态接口VLAN50。在 **interface configuration** 页面，检查 **Guest LAN** 包装盒.然后，一些字段，例如 **IP address** 和 **gateway** 消失。WLC需要识别从VLAN 50路由的流量。这些客户端是有线访客。

2. **创建访客用户接入的有线LAN。**

   在控制器上，当与WLAN关联时使用接口。接下来，在主办公室控制器上创建WLAN。导航至 **WLANs** 并点击 **New**.在 **WLAN Type**，选择 **Guest LAN**.

   在**配置文件名称**和**WLAN SSID**中，输入标识此WLAN的名称。这些名称可以不同，但不能包含空格。使用术语WLAN，但此网络配置文件与无线网络配置文件无关。

   此 **General** 选项卡提供两个下拉列表： **Ingress** 和 **Egress**.入口是用户来自的VLAN(VLAN 50);出口是您向其发送的VLAN。

   对于 **Ingress**，选择 **VLAN50**.

   对于 **Egress**，情况有所不同。如果只有一个控制器，请创建另一个动态接口， **standard** 一次（不是访客LAN），并将有线用户发送到此接口。在这种情况下，请将它们发送到DMZ控制器。因此，对于 **Egress** 接口，选择 **Management Interface**.

   此 **Security** 此访客LAN“WLAN”的模式是WebAuth，这是可接受的。点击 **Ok** 以便验证。

3. **配置外部控制器（总部）。**

   从 **WLAN list**，单击 **Mobility Anchor** 在 **Guest LAN** 线路，然后选择您的DMZ控制器。这里假设两个控制器相互识别。如果没有，请转至 **Controller** > **Mobility Management** > **Mobility group**并在WLC1上添加**DMZWLC**，然后在DMZ上添加**WLC1**。两个控制器不能位于同一个移动组中。否则，基本安全规则将被破坏。

4. **配置锚点控制器（DMZ控制器）。**

   主办公室控制器已就绪。现在准备您的DMZ控制器。打开与DMZ控制器的Web浏览器会话，并导航至**WLAN**。创建新的WLAN。在 **WLAN Type**，选择 **Guest LAN**.

   在 **Profile Name** 和 **WLAN SSID**，输入标识此WLAN的名称。使用与办公室主控制器上输入的值相同的值。

   此 **Ingress** 此处的接口为 **None**.这无关紧要，因为流量通过IP以太网(EoIP)隧道接收。无需指定任何入口接口。

此 **Egress** 接口是发送客户端的位置。例如， **DMZ VLAN** 是VLAN 9。在DMZWLC上为VLAN 9创建标准动态接口，然后选择 **VLAN 9** 作为出口接口。

配置移动锚点隧道的终端。从WLAN**列表**中选择 **Mobility Anchor for Guest LAN**.将流量发送到本地控制器DMZWLC。两端均已就绪。

5. **微调访客LAN。**

   您还可以微调两端的WLAN设置。两端的设置必须相同。例如，如果您在 **WLAN Advanced** 选项卡， **Allow AAA override** 在WLC1上，选中DMZWLC上的相同复选框。如果两端WLAN有任何差异，隧道将中断。DMZWLC拒绝流量；你可以看到 **run debug mobility**.

   请记住，所有值实际上都是从DMZWLC获得的：IP地址、VLAN值等。以相同方式配置WLC1端，使其将请求中继到WLCDMZ。

登录页的证书

本节提供将您自己的证书放在WebAuth页面上或隐藏192.0.2.1 WebAuth URL并显示命名URL的过程。

上传用于控制器Web身份验证的证书

通过GUI(**WebAuth > Certificate**)或CLI(传输类型 **webauthcert**)您可以在控制器上上传证书。

无论是使用证书颁发机构(CA)创建的证书还是第三方官方证书，都必须采用.pem格式。

在发送之前，还必须输入证书的密钥。

上传后，需要重新启动证书才能生效。重新启动后，转到GUI中的WebAuth证书页面，查找您上传的证书的详细信息（有效性等）。

重要字段是公用名(CN)，这是颁发给证书的名称。此字段在本文档的“控制器上的证书颁发机构和其他证书”部分讨论。

重新启动并验证证书的详细信息后，WebAuth登录页面上会显示新的控制器证书。但是，可能会出现两种情况。

1. 如果您的证书是由每台计算机信任的少数几个主根CA之一颁发，则它是正确的。例如VeriSign，但您通常由Verisign子CA而不是根CA签名。如果看到浏览器证书存储中提到的CA为受信任的，则可以将其签入。

2. 如果您从小型公司/CA获得证书，则所有计算机都不信任它们。同时向客户端提供公司/CA证书，然后其中一个根CA颁发该证书。最后，您有一个链，例如“Certificate has been issued by CA x > CA x certificate has issued by CA y > CA y certificate has been issued by this trusted root CA”。 最终目标是到达客户端信任的CA。

控制器上的证书颁发机构和其他证书

要清除“此证书不受信任”警告，请输入在控制器上颁发控制器证书的CA的证书。

然后，控制器提供两个证书（控制器证书及其CA证书）。 CA证书必须是受信任CA或具有验证CA的资源。您可以实际构建一个CA证书链，在证书上生成一个受信任的CA。

将整个链放在一个文件中。然后，文件包含如下示例的内容：

```
BEGIN CERTIFICATE ------ device certificate*   END CERTIFICATE ------ BEGIN
CERTIFICATE ------ intermediate CA certificate* END CERTIFICATE ------ BEGIN
CERTIFICATE ------ Root CA certificate* END CERTIFICATE ------
```

如何使证书匹配URL

WebAuth URL设置为192.0.2.1以验证您自己并颁发证书（这是WLC证书的CN字段）。

例如，要将网络身份验证URL更改为“myWLC.com”，请转到 **virtual interface configuration** (192.0.2.1接口)，您可以在此处输入 **virtual DNS hostname**，例如myWLC.com。

这将替换URL栏中的192.0.2.1。此名称也必须可解析。嗅探器跟踪显示其全部工作方式，但是当WLC发送登录页时，WLC显示myWLC.com地址，客户端使用其DNS解析此名称。

此名称必须解析为192.0.2.1。这意味着如果您也使用名称来管理WLC，请对WebAuth使用其他名称。

如果使用映射到WLC管理IP地址的myWLC.com，则必须为WebAuth使用其他名称，例如myWLCwebauth.com。

解决证书问题

本节介绍如何检查以及检查什么，以对证书问题进行故障排除。

如何检查

下载OpenSSL（对于Windows，搜索OpenSSL Win32）并安装。无需任何配置，您可以进入bin目录并尝试 **openssl s_client –connect (your web auth URL):443**,

如果此URL是在DNS上链接您的WebAuth页面的URL，请参阅本文档下一部分中的“检查内容”。

如果您的证书使用私有CA，请将根CA证书放置在本地计算机上的目录中，并使用openssl选项 **-CApath**.如果您有中间CA，请将其放入同一目录。

要获取有关证书的一般信息并对其进行检查，请使用：

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

使用openssl转换证书也非常有用：

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

检查的内容

您可以看到客户端连接时向其发送哪些证书。读取设备证书 — CN必须是可访问网页的URL。

阅读设备证书的“颁发者”行。这必须与第二个证书的CN匹配。第二个证书“颁发者”必须与下一个证书的CN匹配，以此类推。否则，它不会形成真正的链。

在此显示的OpenSSL输出中，请注意， **openssl** 无法验证设备证书，因为其“颁发者”与提供的CA证书的名称不匹配。

SSL输出

```
Loading 'screen' into random state - done CONNECTED(00000760) depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=20:unable to get local issuer certificate verify return:1 depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=27:certificate not trusted verify return:1 depth=0 /O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uk verify error:num=21:
unable to verify the first certificate verify return:1 --- Certificate chain
0 s:/O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uki:/C=US/ ST=
Arizona/L=Scottsdale/O=.com/OU=http://certificates.gocompany.com/repository/CN=
Secure Certification Authority/serialNumber=079
692871 s:/C=US/O=Company/OU=Class 2 Certification Authority
i:/C=US/O=Company/OU=Class 2 Certification Authority --- Server certificate

BEGIN CERTIFICATE-----
MIIE/zCCA+egAwIBAgIDRc2iMA0GCSqGSIb3DQEBBQUAMIHKMQswCQYDVQQGEwJV
output cut*
YMaj/NACviEU9J3iot4sfreCQSKkBmjH0kf/Dg1l0kmdSbc=

END CERTIFICATE-----
subject=/O=<company>.ac.uk/OU=Domain Control Validated/CN=<company>c.ac.uk
issuer=/C=US/ST=Arizona/L=Scottsdale/O=.com/OU=http://certificates.
.com/repository/CN=Secure Certification Authority/serialNumber=0
7969287 --- No client certificate CA names sent --- SSL handshake has read
2476 bytes and written 322 bytes --- New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit Compression: NONE Expansion: NONE SSL-Session:

Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: A32DB00A7AB7CD1CEF683980F3696C2BBA31A1453324F711F50EF4B86A4A7F03

Session-ID-ctx:Master-Key: C95E1BDAC7B1A964ED7324955C985CAF186B92EA34CD69E10
5F95D969D557E19
939C6A77C72350AB099B3736D168AB22

Key-Arg : None
Start Time: 1220282986
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

另一个可能的问题是无法向控制器上传证书。在这种情况下，不存在有效性、CA等问题。

要验证这一点，请检查简单文件传输协议(TFTP)连接并尝试传输配置文件。如果您输入 **debug transfer all enable** 命令，请注意问题在于证书的安装。

这可能是由于证书使用的密钥错误。也可能是证书格式错误或损坏。

Cisco建议您将证书内容与已知的有效证书进行比较。这允许您查看是否 **LocalkeyID** 属性显示所有

0（已发生）。 如果是，则必须重新转换证书。

有两个带有OpenSSL的命令允许您从.pem返回到.p12，然后使用您选择的密钥重新发出.pem。

如果收到的.pem中包含证书后跟密钥，请复制/粘贴密钥部分： **----BEGIN KEY ---- until ------- END KEY ------** 从.pem到"key.pem"。

1. **openssl pkcs12 -export -in certificate.pem -inkey key.pem -out newcert.p12** ?系统会提示您输入密钥；输入 **check123**.
2. **openssl pkcs12 -in newcert.p12 -out workingnewcert.pem -passin pass:check123 -passout pass:check123** 这会导致带有密码的可操作.pem **check123**.

需要排除的其他情况

虽然本文档中未讨论**移动锚点**，但如果您处于**锚定访客**状态，请确保移动交换正确发生并且您看到客户端到达锚点。

任何进一步的WebAuth问题都需要对锚点进行故障排除。

以下是您可以排除的一些常见问题：

- **用户无法关联到访客WLAN。**

  这与WebAuth无关。检查客户端配置、WLAN上的安全设置（如果已启用），以及无线电是否处于活动状态且运行正常，等等。

- **用户无法获取IP地址。**

  在访客锚点情况下，这通常是因为外部和锚点的配置方式不完全相同。否则，请检查DHCP配置、连接等。
- 确认其他WLAN是否可以正常使用同一DHCP服务器。这仍然与WebAuth无关。

- **用户不会重定向到登录页面。**

  这是最常见的症状，但更为精确。有两种可能的方案。

  用户未重定向（用户输入URL且从未访问WebAuth页面）。 对于这种情况，请检查：

  已通过DHCP为客户端分配有效的DNS服务器(**ipconfig /all**)，

  DNS可从客户端访问(**nslookup (website URL**)，

  用户输入了有效的URL以便重定向，

  用户访问端口80上的HTTP URL(例如，通过http://localhost:2002访问ACS不会重定向您，因为您发送的是端口2002而不是80)。

用户被正确重定向到192.0.2.1，但页面本身不会显示。

这种情况很可能是WLC问题(bug)或客户端问题。客户端可能具有某些防火墙或软件或策略块。也可能是他们在Web浏览器中配置了代理。

建议：在客户端PC上执行嗅探器跟踪。无需使用特殊的无线软件，只需使用Wireshark即可，Wireshark在无线适配器上运行并显示WLC是否回复并尝试重定向。您有两种可能：WLC没有响应，或者WebAuth页面的SSL握手有问题。对于SSL握手问题，您可以检查用户浏览器是否允许SSLv3（某些只允许使用SSLv2），以及它是否对证书验证过于严格。

手动输入http://192.0.2.1以检查网页是否显示时不带DNS，这是很常见的一步。实际上，您可以键入http://10.0.0.0，获得相同的效果。WLC重定向您输入的任何IP地址。因此，如果输入http://192.0.2.1，则不会让您处理Web重定向。如果输入https://192.0.2.1（安全），则此操作不起作用，因为WLC不会重定向HTTPS流量（默认情况下，这在8.0版及更高版本中实际可行）。 直接加载页面而不重定向的最佳方法是输入https://192.0.2.1/login.html。

- **用户无法进行身份验**证。

  请参阅本文档讨论身份验证的部分。在RADIUS上本地检查凭证。

- **用户可通过WebAuth成功进行身份验证，但之后无法访问Internet。**

  您可以从WLAN的安全性中删除WebAuth，然后拥有一个开放的WLAN。然后，您可以尝试访问Web、DNS等。如果您也遇到问题，请完全删除WebAuth设置并检查您的接口配置。

有关详细信息，请参阅：排除无线局域网控制器(WLC)上的Web身份验证故障。

HTTP代理服务器及其工作原理

可以使用HTTP代理服务器。如果您需要客户端在其浏览器中添加一个例外，即192.0.2.1不会通过代理服务器，则可以使WLC侦听代理服务器（通常为8080）端口上的HTTP流量。

为了理解此场景，您需要了解HTTP代理的作用。它是您在浏览器中的客户端（IP地址和端口）上配置的内容。

当用户访问网站时，通常的场景是使用DNS将名称解析为IP，然后向Web服务器请求网页。该进程始终会向代理发送该页面的HTTP请求。

如果需要，代理会处理DNS并转发到Web服务器（如果尚未在代理上缓存该页面）。 讨论仅限于客户端到代理。代理是否获取实际网页与客户端无关。

以下是网络身份验证过程：

- URL中的用户类型。
- 客户端PC发送到代理服务器。
- WLC拦截和模拟代理服务器IP;它向PC回复重定向至192.0.2.1

在此阶段，如果PC未进行配置，它会向代理请求192.0.2.1 WebAuth页面，使其无法工作。PC必须对192.0.2.1进行例外处理；然后，它会向192.0.2.1发送HTTP请求，并继续执行WebAuth。

通过身份验证后，所有通信将再次通过代理。异常配置通常在浏览器中靠近代理服务器的配置。然后您将看到以下消息："请勿对这些IP地址使用代理"。

在WLC版本7.0及更高版本中， **webauth proxy redirect** 可在全局WLC配置选项中启用。

启用时，WLC检查客户端是否配置为手动使用代理。在这种情况下，它们会将客户端重定向到一个页面，该页面显示它们如何修改代理设置以使所有内容都正常工作。

WebAuth代理重定向可配置为在各种端口上工作并与中央Web身份验证兼容。

有关WebAuth代理重定向的示例，请参阅无线LAN控制器上的Web身份验证代理配置示例。

HTTP而不是HTTPS上的Web身份验证

您可以在HTTP而不是HTTPS上登录Web身份验证。如果登录HTTP，则不会收到证书警报。

对于WLC版本7.2之前的代码，必须禁用WLC的HTTPS管理并退出HTTP管理。但是，这仅允许通过HTTP对WLC进行Web管理。

对于WLC版本7.2代码，请使用 **config network web-auth secureweb disable** 命令禁用。这仅禁用Web身份验证的HTTPS，而不禁用管理。请注意，这需要重新启动控制器！

在WLC版本7.3及更高版本的代码上，只能通过GUI和CLI启用/禁用WebAuth的HTTPS。

相关信息

- **无线局域网控制器 Web 身份验证配置示例**
- **下载无线控制器WebAuth捆绑包的软件**
- **创建自定义Web身份验证登录页**
- **使用无线局域网控制器的外部 Web 身份验证配置示例**
- **无线LAN控制器5760/3850网络直通配置示例**
- **配置Web重定向(GUI)**
- **配置Web重定向(CLI)**
- **对无线 LAN 控制器 (WLC) 上的 Web 身份验证进行故障排除**
- **无线局域网控制器上的Web身份验证代理配置示例**
- **请求注解 (RFC)**
- **技术支持和文档 - Cisco Systems**

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）。