

配置802.1X在无线访问接入点的请求方设置

客观

802.1X标准被开发提供在开放式系统互联(OSI)型号的第2层的安全。它包括以下组件：请求方、证明人和认证服务器。请求方是连接到网络的客户端或软件，以便能访问其资源。它需要提供证件或证书获得IP地址和是该特定网络的一部分。请求方不能访问网络资源，直到验证。

配置802.1X在您的无线访问接入点(WAP)的请求方设置是有用允许在您的WAP后的被核准的设备是网络的一部分和访问其资源。同时，它也添加安全层到网络。

此条款将显示您如何配置802.1X在您的无线访问接入点的请求方设置。

可适用的设备

- WAP100系列
- WAP300系列
- WAP500系列

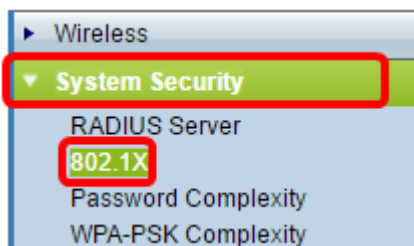
软件版本

- 1.0.1.2 – WAP150 , WAP361
- 1.0.6.2 – WAP121 , WAP321
- 1.0.2.2 – WAP131 , WAP351
- 1.2.1.3 – WAP551 , WAP561 , WAP371
- 1.0.0.17 – WAP571 , WAP571E

配置802.1X在WAP的请求方设置

步骤1.登陆到接入点的基于Web的工具并且选择系统Security>802.1X。

Note:基于Web的工具菜单可能根据您的WAP型号变化。下面的镜像从WAP361被采取。



Note:如果使用WAP其他型号，然后请选择系统安全> 802.1X请求方跳到第3步。

Step 2.检查您希望配置端口号的机箱然后点击请编辑。

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details

Edit

第 3 步：检查Enable复选框从下拉列表然后选择请求方。这是默认选项。

Note:对于WAP其他型号，请检查Enable复选框管理模式然后跳到第5步。

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant Authenticator	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details

Edit

步骤4.点击enable (event)的显示详细资料链路您编辑设置。

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details

Edit

步骤5.从EAP方法下拉列表选择可扩展的认证协议(EAP)方法正确的类型。

EAP Method: MD5 ▼

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

选项是：

- MD5 — MD5是用于加密所有大小数据到128位的算法。MD5算法使用一公共加密系统加密数据。
- PEAP — Protected Extensible Authentication Protocol (PEAP)通过服务器发行的数字证书验证无线局域网(LAN)客户端通过创建在客户端和认证服务器之间的一条被加密的安全套接字协议层(SSL)或传输层安全(TLS)隧道。
- TLS — TLS是为在互联网的通信提供安全和数据完整性的协议。它保证第三方不篡改原始消息。

Note:在本例中，使用MD5。

步骤6.输入您的首选用户名在用户名字段。这，当回应802.1X证明人时，将使用。它长期是64个字符，可能包括大写和小写字母、编号和特殊字符除了双引号。

EAP Method: MD5 ▼

Username: Username (Range: 1 - 64 Characters)

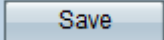
Password: (Range: 1 - 64 Characters)

步骤7.输入您的首选密码在密码字段。此MD5密码，当回应802.1X证明人时，使用。密码长期是64个字符，可能包括大写和小写字母、编号和特殊字符除了引号。

EAP Method: MD5 ▼

Username: Username (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

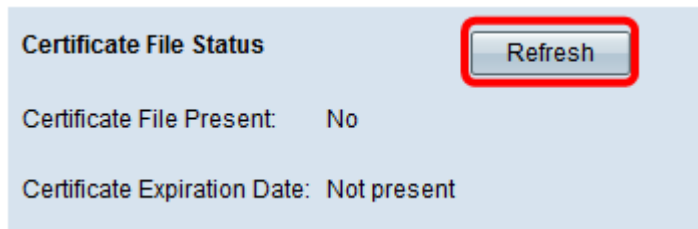
步骤8.点击  按钮。

您应该当前配置了在您的WAP的802.1X请求方设置。

查看证书文件设置

证书文件状态地区显示是否证书文件存在。SSL认证是一个数字式地签名的证书由允许Web浏览器有安全通信用Web服务器的认证机关。

第 1 步：要查看证书文件的当前状态，请点击**刷新**。



Certificate File Status

Refresh

Certificate File Present: No

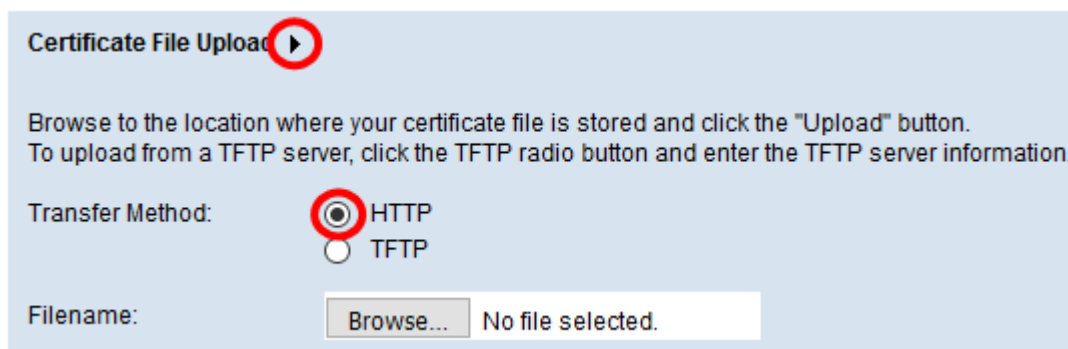
Certificate Expiration Date: Not present

证书文件状态地区有以下字段：

- 当前证书文件-显示是否证书文件存在。
- 证书到期到期日-显示当前证书文件的有效期。

加载证书文件

步骤1.点击在证书文件加载旁边的箭头然后从转移方法选择期望单选按钮。



Certificate File Upload ▶

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Transfer Method: HTTP TFTP

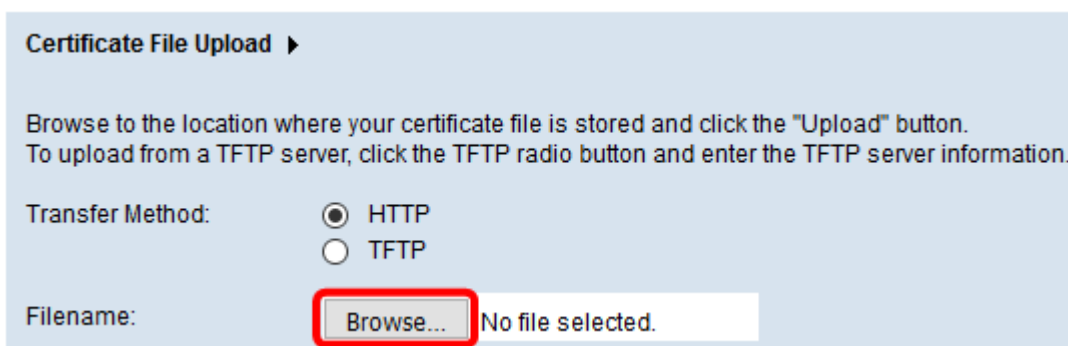
Filename: No file selected.

有在加载文件的两个转移方法：

- 超文本传输协议(HTTP)
- 简单文件传输协议 (TFTP)

Note:在本例中， HTTP被选择。

第2.步(可选)，如果HTTP被选择，点击访问从您的计算机选择证书文件然后跳到第5.步。



Certificate File Upload ▶

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Transfer Method: HTTP TFTP

Filename: No file selected.

第3.步(可选)，如果选择了在Step1的TFTP，在 *Filename* 字段输入证书文件的名称。TFTP server用于自动地调用在设备内的引导程序文件并且是非常简单的。

Note:在本例中， *mini_httpd.pem*使用作为文件名。

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename: (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

步骤4.输入TFTP server的IP地址在 *TFTP server IPv4*地址域。

Note:在本例中，10.10.10.11使用作为TFTP server IPv4地址。

Transfer Method: HTTP
 TFTP

Filename: (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

步骤5.点击**更新**。

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename: (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

Note:如果使用WAP其他型号，请点击**加载**。

步骤6.点击 按钮保存您的设置。

您应该顺利地当前加载了在您的WAP的证书文件。