



# Cisco IP 会议电话安全性

- [Cisco IP 电话安全性概述，第 1 页](#)
- [电话网络安全增强功能，第 2 页](#)
- [支持的安全功能，第 3 页](#)

## Cisco IP 电话安全性概述

安全功能可防范多种威胁，包括对电话身份或数据的威胁。这些功能会建立和维持电话与 Cisco Unified Communications Manager 服务器之间经验证的通讯流，并确保电话只使用数字签名的文件。

默认情况下，Cisco Unified Communications Manager 8.5(1) 版及更高版本包括安全性，这可为 Cisco IP 电话提供以下安全功能（无需运行 CTL 客户端）：

- 电话配置文件签名
- 电话配置文件加密
- Tomcat 和其他 Web 服务的 HTTPS



**注释** 安全信令和媒体功能仍需您运行 CTL 客户端和使用硬件电子令牌。

有关安全功能的详细信息，请参阅特定 Cisco Unified Communications Manager 版本的文档。

本地有效证书 (LSC) 会在您执行与证书权限代理功能 (CAPF) 关联的必要任务后安装在电话上。您可使用 Cisco Unified Communications Manager Administration 来配置 LSC。有关详细信息，请参阅特定 Cisco Unified Communications Manager 版本的文档。

LSC 无法用作使用 WLAN 验证的 EAP-TLS 的用户证书。

或者，您可在电话上从“安全设置”菜单启动 LSC 的安装。此菜单还可用于更新或移除 LSC。

Cisco 8832 IP 会议电话符合联邦信息处理标准 (FIPS) 的规定。在 FIPS 模式下，需要使用 2048 位或更高的 RSA 密钥，电话才可以正常工作。如果 RSA 服务器证书大小未达到 2048 位或更高，则电话将无法在 Cisco Unified Communications Manager 上注册，并且电话的状态消息中会显示电话注册失败。在电话的状态消息中显示的证书密钥大小不符合 FIPS 标准。

您无法在 FIPS 模式下使用私钥（LSC 或 MIC）。

如果电话的现有 LSC 低于 2048 位，您需要更新 LSC 密钥大小为 2048 位或更高，方可启用 FIPS。

#### 相关主题

[设置本地有效证书](#)，第 5 页

[Cisco Unified Communications Manager 文档](#)

## 电话网络安全增强功能

您可以启用 Cisco Unified Communications Manager 11.5(1) 和 12.0(1) 以在增强的安全环境下运行。这些增强功能可以使您的电话网络在严格的安全和风险管理控制下运行，以保障您和用户的安全。

Cisco Unified Communications Manager 12.5(1) 不支持增强的安全环境。在升级到 Cisco Unified Communications Manager 12.5(1) 之前禁用 FIPS，否则您的 TFTP 和其他服务将无法正常工作。

增强的安全环境包括以下功能：

- 联系人搜索身份验证。
- 使用 TCP 作为远程审计日志记录的默认协议。
- FIPS 模式。
- 经过改进的凭证策略。
- 支持数字签名使用 SHA-2 系列哈希值。
- 支持 512 和 4096 位的 RSA 密钥大小。

使用 Cisco Unified Communications Manager 版本 14.0 以及 Cisco IP 电话固件版本 14.0 和更高版本时，电话支持 SIP OAuth 验证。

具有 Cisco Unified Communications Manager 14.0(1)SU1 或更高版本以及 Cisco 14.1(1) 版 IP 电话固件的代理简单文件传输协议 (TFTP) 支持 OAuth。Mobile Remote Access (MRA) 不支持代理 TFTP 以及适用于代理 TFTP 的 OAuth。

有关安全的其他信息，请参阅以下文档：

- 《Cisco Unified Communications Manager 系统配置指南》版本 14.0(1) 或更高版本 (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>)。
- 《Cisco Unified Communications Manager 安全指南》(<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>)
- SIP OAuth：《Cisco Unified Communications Manager 功能配置指南》(<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>)



**注释** Cisco IP 电话只能存储有限数量的身份信任列表 (ITL) 文件。ITL 文件在电话上不能超出 64K 限制，因此应限制 Cisco Unified Communications Manager 发送到电话的文件数。

## 支持的安全功能

安全功能可防范多种威胁，包括对电话身份或数据造成的威胁。这些功能会建立和维持电话与 Cisco Unified Communications Manager 服务器之间经验证的通讯流，并确保电话只使用数字签名的文件。

默认情况下，Cisco Unified Communications Manager 8.5(1) 版及更高版本包括安全性，这可为 Cisco IP 电话提供以下安全功能（无需运行 CTL 客户端）：

- 电话配置文件签名
- 电话配置文件加密
- Tomcat 和其他 Web 服务的 HTTPS



**注释** 安全信令和媒体功能仍需您运行 CTL 客户端和使用硬件电子令牌。

在 Cisco Unified Communications Manager 系统中实施安全性，防止电话和 Cisco Unified Communications Manager 服务器的身份被窃、防止数据被篡改以及防止呼叫信令和媒体流被篡改。

要减轻这些威胁，Cisco IP 电话网络在电话与服务器之间建立和维护安全（加密的）通信流，以数字方式签名这些文件，然后将其传输到电话，并加密 Cisco IP 电话媒体流和呼叫信令。

本地有效证书 (LSC) 会在您执行与证书权限代理功能 (CAPF) 关联的必要任务后安装在电话上。您可使用 Cisco Unified Communications Manager Administration 来配置 LSC，如《Cisco Unified Communications Manager 安全指南》中所述。或者，您可在电话上从“安全设置”菜单启动 LSC 的安装。此菜单还可用于更新或删除 LSC。

LSC 无法用作使用 WLAN 验证的 EAP-TLS 的用户证书。

电话使用电话安全性配置文件，该文件定义设备为不安全还是安全。有关将安全性配置文件应用到电话的信息，请参阅特定 Cisco Unified Communications Manager 版本的文档。

如果您在 Cisco Unified Communications Manager Administration 中配置了安全相关的设置，电话配置文件将包含敏感信息。为确保配置文件的私密性，您必须将其配置为加密。有关详细信息，请参阅特定 Cisco Unified Communications Manager 版本的文档。

在 Cisco Unified Communications Manager 系统中实施安全性，防止电话和 Cisco Unified Communications Manager 服务器的身份被窃、防止数据被篡改以及防止呼叫信令和媒体流被篡改。

下表列出了 Cisco 8832 IP 会议电话支持的安全功能。如需了解关于这些功能、Cisco Unified Communications Manager 和 Cisco IP 电话安全性的更多信息，请参阅特定 Cisco Unified Communications Manager 版本的文档。

表 1: 安全功能概述

功能	说明
图像验证	签名的二进制文件（带扩展名 .sbn）可以防止固件映像在的映像。
客户现场证书的安装	每部电话都需要具有唯一的证书才能进行设备验证。电话 Communications Manager Administration 中指定使用证书权安装本地有效证书 (LSC)。
设备验证	当每个实体都接受了其他实体的证书时，在 Cisco Unified Communications Manager 之间是否进行了安全的连接。非电话通过了 Cisco Unified Communications Manager 的验证。
文件身份验证	验证电话下载的数字签名文件。电话验证该签名以确保文件不会拒绝此类文件，并且不会再进行进一步的处理。
信令验证	使用 TLS 协议验证传输期间信令信息包未发生篡改。
厂商预装证书	每部电话都包含唯一的厂商预装证书 (MIC) 用于进行设备验证。Cisco Unified Communications Manager 对电话进行验证。
安全的 SRST 参考	当您配置用于保证安全性的 SRST 参考并在 Cisco Unified Communications Manager 中配置 SRST 证书，然后将该文件添加到电话 cnf.xml 文件中添加 SRST 证书，然后将该文件发布到电话。
媒体加密	使用 SRTP 确保支持的设备之间的媒体流以证明安全性，并交付密钥给设备以及传输密钥期间确保安全交付密钥。
CAPF（证书权限代理功能）	实施对于电话而言处理太密集的证书生成程序，并与电话的证书颁发机构要求证书，或将其配置为本地生成证书。
安全性配置文件	定义电话是不安全、已验证还是已加密。
加密配置文件	让您确保电话配置文件的隐私性。
可以选择禁用电话的 Web 服务器功能	您可以阻止访问电话网页，该网页上显示电话的各种运行信息。
电话强化	<p>额外的安全性选项，您可以从 Cisco Unified Communications Manager 配置电话强化。</p> <ul style="list-style-type: none"> <li>禁止访问电话网页</li> </ul> <p>注释 进入电话“配置”菜单，查看“GARP 已启用”。</p>
802.1x 验证	电话可以使用 802.1X 验证来要求并获取网络访问权限。

功能	说明
AES 256 加密	<p>连接至 Cisco Unified Communications Manager 版本 10.5 和媒体加密的 SIP。这样，电话就可以使用符合 SHA-256 密码，发起并支持 TLS 1.2 连接。新密码为：</p> <ul style="list-style-type: none"> <li>• 对于 TLS 连接： <ul style="list-style-type: none"> <li>• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</li> <li>• TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</li> </ul> </li> <li>• 对于 sRTP： <ul style="list-style-type: none"> <li>• AEAD_AES_256_GCM</li> <li>• AEAD_AES_128_GCM</li> </ul> </li> </ul> <p>有关详细信息，请参阅 Cisco Unified Communications Manager 11.5 及更高版本的文档。</p>
椭圆曲线数字签名算法 (ECDSA) 证书	<p>作为通用标准 (CC) 认证的一部分，Cisco Unified Communications Manager 11.5 及更高版本的所有设备都支持 ECDSA 证书。</p>

#### 相关主题

[Cisco Unified Communications Manager 文档](#)

## 设置本地有效证书

此任务适用于使用验证字符串方法设置 LSC。

#### 开始之前

确保相应的 Cisco Unified Communications Manager 和证书权限代理功能 (CAPF) 安全性配置都已完成：

- CTL 或 ITL 文件具有 CAPF 证书。
- 在 Cisco Unified Communications 操作系统管理中，确认已安装 CAPF 证书。
- CAPF 正在运行且已配置。

有关这些设置的详细信息，请参阅特定 Cisco Unified Communications Manager 版本的文档。

#### 过程

**步骤 1** 获取在配置 CAPF 时设置的 CAPF 验证代码。

**步骤 2** 在电话上，选择设置。

**步骤 3** 选择管理设置 > 安全设置。

**注释** 您可通过使用 Cisco Unified Communications Manager Administration “电话配置” 窗口中的 “设置访问权限” 字段，控制对 “设置” 菜单的访问权限。

**步骤 4** 选择 **LSC** 并按 **选择或更新**。

电话会提示输入验证字符串。

**步骤 5** 输入验证代码并按 **提交**。

电话会开始安装、更新或移除 LSC，具体取决于配置 CAPF 的方式。在此程序期间，“安全性配置” 菜单中的 LSC 选项字段中会出现一系列消息，因此您可监视进度。当此程序完成后，电话上会显示 “已安装” 或 “未安装”。

LSC 安装、更新或移除过程需要较长时间才能完成。

如果电话安装过程成功，则会显示已安装的消息。如果电话显示未安装，则可能是授权字符串不正确，也可能是电话升级未启用。如果 CAPF 操作删除了 LSC，电话会显示未安装来标识该操作已成功。CAPF 服务器会记录错误消息。请参阅 CAPF 服务器文档，以查找日志并理解错误消息的含义。

---

#### 相关主题

[Cisco Unified Communications Manager 文档](#)

## 启用 FIPS 模式

### 过程

---

**步骤 1** 在 Cisco Unified Communications Manager Administration 中，依次选择 **设备 > 电话**，然后找到相应电话。

**步骤 2** 导航至 “产品特定配置” 区域。

**步骤 3** 将 **FIPS 模式** 字段设置为启用。

**步骤 4** 选择 **应用配置**。

**步骤 5** 选择 **保存**。

**步骤 6** 重新启动电话。

---

## 电话呼叫安全性

当为电话实施安全性时，可通过电话屏幕上的图标来识别安全电话呼叫。如果在呼叫开始时播放安全音，则也可确定连接的电话是否安全并获得保护。

在安全呼叫中，所有呼叫信令和媒体流都会加密。安全呼叫提供高级安全性，确保呼叫的完整性和私密性。如果进行中呼叫已加密，则电话屏幕中的呼叫持续时间计时器右侧的呼叫进度图标会变为以下图标：。



**注释** 如果呼叫通过非 IP 呼叫分支（例如 PSTN）路由，则呼叫可能不安全，即使其已在 IP 网络内加密并且具有与之关联的锁定图标也不例外。

在安全的呼叫中，呼叫开始时播放安全音，表示其他连接的电话也会接收和传输安全音。如果您的呼叫连接到不安全的电话，则不会播放安全音。



**注释** 支持两个电话之间的安全呼叫。可通过安全会议桥配置安全会议、Cisco 分机移动和共享线路。

电话在 Cisco Unified Communications Manager 中配置为安全（加密和信任）时，可以指定为“受保护”状态。然后，如需要，受保护电话可以配置为在呼叫的开头播放提示音：

- **受保护设备：**要将安全电话的状态更改为受保护，请在 Cisco Unified Communications Manager 管理（**设备 > 电话**）中的“电话配置”窗口中选中“受保护设备”复选框。
- **播放安全提示音：**要使受保护电话播放安全或不安全提示音，请将“播放安全提示音”设置设为“真”。默认情况下，“播放安全提示音”设置为“假”。您可在 Cisco Unified Communications Manager 管理中设置此选项（**系统 > 服务参数**）。选择此服务器，然后选择 Unified Communications Manager 服务。在“服务参数配置”窗口中，选择“功能 - 安全音”区域中的选项。默认值为“假”。

## 安全会议呼叫标识

您可启动安全电话会议并监控参加者的安全性级别。使用此过程建立安全电话会议：

1. 用户从安全电话启动会议。
2. Cisco Unified Communications Manager 将安全会议桥分配给呼叫。
3. 在添加参加者后，Cisco Unified Communications Manager 会验证每个电话的安全模式，并为会议维持安全级别。
4. 电话会显示电话会议的安全性级别。安全会议会在电话屏幕上的会议右侧显示安全图标 。



**注释** 支持两个电话之间的安全呼叫。对于受保护的电话，在配置安全呼叫后，部分功能（例如电话会议、共享线路和分机移动）将不可用。

下表提供有关根据发起者电话安全性级别、参加者的安全性级别以及安全会议桥的可用性更改会议安全性级别的信息。

表 2: 电话会议的安全性限制

发起者电话安全性级别	使用的功能	参与者的安全性级别	行动结果
不安全	会议	安全	不安全的会议桥 不安全的会议
安全	会议	至少一个成员不安全。	安全会议桥 不安全的会议
安全	会议	安全	安全会议桥 安全加密级别的会议
不安全	Meet Me	最低安全性级别已加密。	发起者接收消息“不满足安全级别，呼叫”
安全	Meet Me	最低安全性级别为不安全。	安全会议桥 会议接受所有呼叫。

## 安全电话呼叫标识

当您的电话与另一端的电话已配置为安全呼叫时，才可建立安全呼叫。另一个电话可以位于相同的 Cisco IP 网络中或位于 IP 网络以外的网络。安全呼叫只可以在两个电话之间进行。在建立会议桥后，电话会议应支持安全呼叫。

遵照以下过程建立安全呼叫：

1. 用户从安全电话（受保护的安全模式）启动呼叫。
2. 电话会在电话屏幕上显示安全图标 。此图标表示电话已配置为安全呼叫，但这不表示其他连接的电话也会受保护。
3. 如果呼叫连接至另一个安全电话，用户会听到一声安全音，表示对话两端已加密并受保护。如果呼叫连接至不安全的电话，用户不会听到安全音。



**注释** 支持两个电话之间的安全呼叫。对于受保护的电话，在配置安全呼叫后，部分功能（例如电话会议、共享线路和分机移动）将不可用。

只有受保护的电话才会播放这些安全或不安全的提示音。不受保护的电话从不会播放提示音。如果在呼叫过程中整个呼叫状态发生了变化，则提示音会改变并且受保护的电话会播放相应的提示音。

在以下情况下，受保护电话会播放提示音，但也可能不会播放：

- 当“播放安全提示音”选项启用后：

- 建立端到端安全媒体并且呼叫状态为安全时，电话会播放安全提示音（三声较长的哔声，中间停顿）。
- 建立端到端非安全媒体并且呼叫状态为不安全时，电话将播放不安全提示音（六声短哔声并简短暂停）。

如果“播放安全提示音”选项禁用，不会播放任何提示音。

## 提供插入加密

Cisco Unified Communications Manager 在建立会议时检查电话安全状态，然后更改会议的安全指示或阻止呼叫完成以保持系统中的完整性和安全性。

如果用于插入的电话没有配置为加密，则用户无法插入到加密的呼叫中。在此情况下插入失败时，将在发起插入的电话上播放重拨提示音（急促的忙音）。

如果发起方电话配置为加密，则插入发起方可以从加密的电话插入到不安全的呼叫中。进行插入后，Cisco Unified Communications Manager 将呼叫归类为不安全。

如果发起方电话配置为加密，则插入发起方可以插入到加密的呼叫中，并且电话指示呼叫已加密。

## WLAN 安全

由于范围内的所有 WLAN 设备均可接收所有其他 WLAN 流量，因此安全语音通信在 WLAN 中至关重要。为确保入侵者不会操纵或拦截语音通信，Cisco SAFE 安全体系结构支持 Cisco IP 电话和 Cisco Aironet AP。有关网络中安全性的详细信息，请参阅

[http://www.cisco.com/en/US/netsol/ns744/networking\\_solutions\\_program\\_home.html](http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html)。

Cisco 无线 IP 电话解决方案提供无线网络安全，通过使用无线 Cisco IP 电话支持的以下验证方法，阻止未经授权的登录和有危害的通信：

- 开放式验证：任何无线设备均可在开放式系统中请求验证。收到请求的 AP 可允许任何请求方或仅允许用户列表中的请求方进行验证。无线设备与 AP 之间的通信可以是非加密通信，或者设备可使用有线等效加密 (WEP) 密钥来提供安全性。使用 WEP 的设备仅尝试通过使用 WEP 的 AP 进行验证。
- 通过安全隧道的可扩展验证协议灵活验证 (EAP-FAST) 验证：此客户端服务器安全体系结构在 AP 与 RADIUS 服务器（例如，Cisco 访问控制服务器 (ACS)）之间的传输层安全 (TLS) 隧道内加密 EAP 事务。

TLS 隧道使用受保护的访问凭证 (PAC) 进行客户端（电话）与 RADIUS 服务器之间的验证。服务器将授权 ID (AID) 发送给客户端（电话），后者会选择适当的 PAC。客户端（电话）将返回 PAC - 对 RADIUS 服务器不透明。服务器通过主密钥解密 PAC。现在，两个终端均包含 PAC 密钥，且 TLS 隧道已创建。EAP-FAST 支持自动 PAC 部署，但您必须在 RADIUS 服务器上启用该功能。



**注释** 在 Cisco ACS 中，默认情况下，PAC 将在一周后过期。如果电话有过期的 PAC，则电话获取新 PAC 时，与 RADIUS 服务器的验证要花较长的时间。为避免 PAC 部署延迟，在 ACS 或 RADIUS 服务器上，将 PAC 过期期限设置为 90 天或更长时间。

- 可扩展身份验证协议-传输层安全 (EAP-TLS) 验证：EAP-TLS 需要客户端证书用于身份验证和网络访问。对于有线 EAP-TLS，客户端证书可以是电话的 MIC 或 LSC。LSC 是有线 EAP-TLS 的建议客户端身份验证证书。
- 受保护的可扩展验证协议 (PEAP)：客户端（电话）与 RADIUS 服务器之间 Cisco 专有的、基于密码的相互验证方案。Cisco IP 电话可以使用 PEAP 与无线网络进行验证。仅支持 PEAP-MSCHAPV2。不支持 PEAP-GTC。

以下验证方案使用 RADIUS 服务器管理验证密钥：

- WPA/WPA2：使用 RADIUS 服务器信息生成唯一的密钥进行验证。由于这些密钥在中央 RADIUS 服务器生成，因此 WPA/WPA2 提供比存储在 AP 和电话上的 WPA 预共享密钥更高的安全性。
- 快速安全漫游：使用 RADIUS 服务器和无线域服务器 (WDS) 信息管理和验证密钥。WDS 为启用 CCKM 的客户端设备创建安全凭证缓存以快速安全地重新验证。Cisco 8800 系列 IP 电话支持 802.11r (FT)。同时支持 11r (FT) 和 CCKM 以便快速安全漫游。但思科强烈建议使用空中 802.11r (FT) 方法。

使用 WPA/WPA2 和 CCKM 时，加密密钥不在电话上输入，而是在 AP 和电话之间自动获得。但必须在每部电话上输入用于验证的 EAP 用户名和密码。

为确保语音通信安全，Cisco IP 电话支持 WEP、TKIP 和高级加密标准 (AES) 进行加密。这些机制用于加密时，信令 SIP 信息包和语音实时传输协议 (RTP) 信息包在 AP 与 Cisco IP 电话之间加密。

## WEP

在无线网络中使用 WEP 时，使用开放或共享密钥验证在 AP 进行验证。电话上设置的 WEP 密钥必须与在 AP 配置的 WEP 密钥匹配，方可成功连接。Cisco IP 电话支持使用 40 位加密或 128 位加密的 WEP 密钥并在电话与 AP 之间保持静态。

EAP 和 CCKM 验证可以使用 WEP 密钥用于加密。RADIUS 服务器管理 WEP 密钥并在验证后将唯一的密钥传递给 AP 用于加密所有语音信息包；因此，这些 WEP 密钥可以通过每次验证进行更改。

## TKIP

WPA 和 CCKM 使用相对于 WEP 有一些改进的 TKIP 加密。TKIP 提供每个信息包的密钥加密和更长的初始化向量 (IV) 来强化加密。此外，消息完整性检查 (MIC) 可确保加密的信息包不会被更改。TKIP 消除了有助于入侵者解密 WEP 密钥的 WEP 可预测性。

## AES

用于 WPA2 验证的加密方法。此国家加密标准使用对称算法，加密和解密具有相同的密钥。AES 使用大小为 128 位最小值的密码阻止链 (CBC) 加密，其支持的密钥大小为 128、192 和 256 位。Cisco IP 电话支持 256 位密钥大小。



**注释** Cisco IP 电话不支持具有 CMIC 的 Cisco 密钥完整性协议 (CKIP)。

验证和加密方案在无线 LAN 内设置。VLAN 在网络和 AP 中配置，指定验证和加密的不同组合。SSID 与 VLAN 以及特定验证和加密方案关联。要使无线客户端设备成功验证，必须配置与 AP 和 Cisco IP 电话上其验证和加密方案相同的 SSID。

某些验证方案需要特定类型的加密。通过开放式验证，您可以使用静态 WEP 进行加密以实现增强的安全性。但如果您使用共享密钥验证，则必须设置静态 WEP 用于加密，且必须在电话上配置 WEP 密钥。



- 注释**
- 使用 WPA 预共享密钥或 WPA2 预共享密钥时，预共享密钥必须在电话上静态设置。这些密钥必须与 AP 上的密钥匹配。
  - Cisco IP 电话不支持自动 EAP 协商；要使用 EAP-FAST 模式，您必须指定它。

下表提供 Cisco IP 电话支持的 Cisco Aironet AP 上配置的验证和加密方案列表。该表显示对应 AP 配置的电话的网络配置选项。

表 3: 验证和加密方案

Cisco IP 电话配置	AP 配置			
	安全	密钥管理	加密	快速漫游
安全模式	安全	密钥管理	加密	快速漫游
无	无	无	无	不适用
WEP	静态 WEP	静态	WEP	不适用
PSK	PSK	WPA	TKIP	无
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM
EAP-TLS	EAP-TLS	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM

Cisco IP 电话配置	AP 配置			
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1X	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM

有关在 AP 上配置验证和加密方案的详细信息，请参阅适用于您的型号和版本的《Cisco Aironet 配置指南》，位于以下 URL：

<http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243>

## 无线 LAN 的安全性

支持的 Wi-Fi 的 Cisco 电话有更多安全性要求，并且需要进行额外配置。这些额外的步骤包括在电话和 Cisco Unified Communications Manager 上安装证书以及设置安全性。

有关详细信息，请参阅《Cisco Unified Communications Manager 安全指南》。

### Cisco IP 电话管理页面

支持 Wi-Fi 的 Cisco 电话拥有与其他电话页面不同的特殊网页。简单证书注册协议 (SCEP) 不可用时，您可使用这些特殊网页进行电话安全配置。使用这些页面可在电话上手动安装安全证书、下载安全证书或手动配置电话日期和时间。

这些网页还显示与其他电话网页上显示相同的信息，包括设备信息、网络设置、日志和统计信息。

#### 配置电话的管理页面

管理网页在电话出厂时为启用状态，且密码设置为 Cisco。但如果电话要在 Cisco Unified Communications Manager 上进行注册，则必须启用管理网页，并配置新的密码。

在注册电话后第一次使用网页之前，必须先启用该网页，并设置登录凭证。

启用网页后，可通过 HTTPS 端口 8443 访问管理网页（<https://x.x.x.x:8443>，其中 x.x.x.x 是电话的 IP 地址）。

#### 开始之前

先确定密码，然后再启用管理网页。密码可以是字母或数字的任意组合，但长度必须介于 8 到 127 个字符之间。

您的用户名设置为 admin，且永久有效。

#### 过程

**步骤 1** 在 Cisco Unified Communications Manager Administration 中，选择设备 > 电话。

**步骤 2** 找到您的电话。

- 步骤 3 在产品特定配置布局中，将 **Web 管理** 参数设为启用。
- 步骤 4 在管理员密码字段中输入密码。
- 步骤 5 选择**保存**，然后单击**确定**。
- 步骤 6 选择**应用配置**，然后单击**确定**。
- 步骤 7 重新启动电话。

---

## 访问电话管理网页

当您想要访问管理网页时，您需要指定管理端口。

### 过程

---

步骤 1 获取电话的 IP 地址：

- 在 Cisco Unified Communications Manager Administration 中，依次选择**设备 > 电话**，然后找到相应电话。在 Cisco Unified Communications Manager 中注册的电话会在**查找和列出电话**窗口中以及**电话配置**窗口的顶部显示 IP 地址。

步骤 2 打开 Web 浏览器并输入以下 URL，其中 *IP\_address* 为 Cisco IP 电话的 IP 地址：

**https://<IP\_address>:8443**

步骤 3 在“密码”字段中输入密码。

步骤 4 单击**提交**。

---

## 从电话管理网页安装用户证书

如果简单证书注册协议 (SCEP) 不可用，您可以在电话上手动安装用户证书。

厂商预装证书 (MIC) 可用作 EAP-TLS 用户证书。

用户证书安装完毕后，您需要将其添加到 RADIUS 服务器信任列表。

### 开始之前

在为电话安装用户证书之前，您必须拥有：

- 保存到您 PC 上的用户证书。证书必须是 PKCS #12 格式。
- 证书的提取密码。

### 过程

---

步骤 1 在电话管理网页中选择**证书**。

步骤 2 浏览至您 PC 上的证书。

**步骤 3** 在提取密码字段中，输入证书提取密码。

**步骤 4** 单击上传。

**步骤 5** 上传完毕后需重新启动电话。

---

## 从电话管理网页安装验证服务器证书

如果简单证书注册协议 (SCEP) 不可用，您可以在电话上手动安装验证服务器证书。

必须为 EAP-TLS 安装用于颁发 RADIUS 服务器证书的根 CA 证书。

### 开始之前

在电话上安装证书之前，您必须将验证服务器证书保存到您的 PC 上。证书必须采用 PEM (Base 64) 或 DER 编码格式。

### 过程

---

**步骤 1** 在电话管理网页中选择证书。

**步骤 2** 找到验证服务器 CA（管理网页）字段，然后单击安装。

**步骤 3** 浏览至您 PC 上的证书。

**步骤 4** 单击上传。

**步骤 5** 上传完毕后需重新启动电话。

如果您要安装多个证书，则您需在所有证书都安装完成后重新启动电话。

---

## 从电话管理网页手动删除安全证书

如果简单证书注册协议 (SCEP) 不可用，您可以从电话中手动删除安全证书。

### 过程

---

**步骤 1** 在电话管理网页中选择证书。

**步骤 2** 在证书页面找到证书。

**步骤 3** 单击删除。

**步骤 4** 在删除过程完成后，重新启动电话。

---

## 手动设置电话日期和时间

如果使用基于证书的验证，则电话必须显示正确的日期和时间。验证服务器会对照证书有效期检查电话的日期和时间。如果电话和服务器的日期和时间不匹配，电话将停止工作。

如果电话无法从您的网络接收正确的信息，则使用此程序手动设置电话上的日期和时间。

## 过程

---

**步骤 1** 在电话管理网页中，滚动至日期和时间。

**步骤 2** 执行下列选项之一：

- 单击将电话设为本地日期和时间以使电话与本地服务器同步。
  - 在指定日期和时间字段中，通过菜单选择月、日、年、小时、分钟和秒，然后单击将电话设为指定日期和时间。
- 

## SCEP 设置

简单证书注册协议 (SCEP) 是用于自动配置和续订证书的一种标准。它无需在您的电话上手动安装证书。

### 配置 SCEP 产品的特定配置参数

您需要在电话网页上配置以下 SCEP 参数

- RA IP 地址
- SCEP 服务器根 CA 证书的 SHA-1 或 SHA-256 指纹

Cisco IOS 注册颁发机构 (RA) 可充当 SCEP 服务器的代理。电话上的 SCEP 客户端使用从 Cisco Unified Communication Manager 下载的参数。配置完这些参数后，电话会向 RA 发送 SCEP getcs 请求，然后设备使用定义的指纹验证根 CA 证书。

## 过程

---

**步骤 1** 在 Cisco Unified Communications Manager Administration 中，选择设备 > 电话。

**步骤 2** 找到此电话。

**步骤 3** 滚动至 **Product Specific Configuration Layout**（产品特定配置布局）区域。

**步骤 4** 选中 **WLAN SCEP 服务器** 复选框以激活 SCEP 参数。

**步骤 5** 选中 **WLAN 根 CA 指纹 (SHA256 或 SHA1)** 复选框以激活 SCEP QED 参数。

---

### 支持简单证书注册协议服务器

如果您使用简单证书注册协议 (SCEP) 服务器，服务器会自动可以保持您的用户和服务器证书。在 SCEP 服务器上，将 SCEP 注册座席 (RA) 配置为：

- 充当 PKI 信任点
- 充当 PKI RA

- 通过 RADIUS 服务器执行设备验证

有关详细信息，请参阅您的 SCEP 服务器文档。

## 802.1x 验证

Cisco IP 电话支持 802.1X 验证。

Cisco IP 电话和 Cisco Catalyst 交换机过去使用 Cisco Discovery Protocol (CDP) 来识别彼此并确定 VLAN 分配和线内电源要求等参数。

对 802.1X 验证的支持需要多个组件：

- Cisco IP 电话：电话会发起访问网络的请求。电话包含 802.1X 请求方。网络管理员可以通过此请求方控制 IP 电话至 LAN 交换机端口的连接。电话 802.1X 请求方的最新版本使用 EAP-FAST 和 EAP-TLS 选项进行网络验证。
- Cisco Catalyst 交换机（或其他第三方交换机）：交换机必须支持 802.1X，因此可以充当验证器，并在电话和验证服务器之间传递消息。在交换完成后，交换机会授予或拒绝电话访问网络的权限。

您必须执行以下操作来配置 802.1X。

- 在电话上启用 802.1X 验证前配置其他组件。
- 配置语音 VLAN — 由于 802.1X 标准不考虑 VLAN，应根据交换机支持来配置此设置。
  - 启用 — 如果您使用的是支持多域验证的交换机，可以继续使用语音 VLAN。
  - 禁用 — 如果交换机不支持多域验证，则禁用语音 VLAN 并考虑将此端口分配给本机 VLAN。

### 相关主题

[Cisco Unified Communications Manager 文档](#)

## 当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。