Cisco IP Phone 安全性

安全功能

安全功能可确保呼叫安全且经过验证。

域和互联网设置

配置域受限访问域

如果您输入域，Cisco IP Phone 仅响应来自所标识服务器的 SIP 消息。

开始之前

访问电话管理网页。请参阅访问电话网页。

过程

步骤 1 选择**语音** > **系统**。

步骤 2 在**系统配置**部分的**受限访问域**字段中，输入您希望电话响应的每台 SIP 服务器的完全限定域名 (FQDN)。用逗号分隔 FQDN。

示例：

```
voiceip.com, voiceip1.com
```

步骤 3 单击**提交所有更改**。

配置 Internet 连接类型

您可以将连接类型设置为以下值之一：

- 动态主机配置协议 (DHCP) — 电话能够从网络 DHCP 服务器接收 IP 地址。Cisco IP Phone 通常在 DHCP 服务器向设备分配 IP 地址的网络中运行。由于 IP 地址是有限资源，因此 DHCP 服务器会定期更新 IP 地址上的设备租约。如果电话出于任何原因丢失了 IP 地址，或者网络上的其他设备被分配了相同的 IP 地址，则 SIP 代理与电话之间的通信将被切断或降级。每当在相应 SIP 命令发送后的可编程时长内没有收到预期的 SIP 响应时，DHCP 续订超时参数会致使设备请求更新其 IP 地址。如果 DHCP 服务器返回其原来分配给电话的 IP 地址，则认为 DHCP 分配在正常运行。否则，电话将重置以尝试修复问题。
- 静态 IP — 电话的静态 IP 地址。

开始之前

访问电话管理网页。请参阅访问电话网页。

过程

步骤 1 选择**语音** > **系统**。

步骤 2 在 **IPv4 设置**部分，使用**连接类型**下拉列表框选择连接类型：

- 动态主机配置协议 (DHCP)
- 静态 IP

步骤 3 在 **IPv6 设置**部分，使用**连接类型**下拉列表框选择连接类型：

- 动态主机配置协议 (DHCP)
- 静态 IP

步骤 4 如果您选择静态 IP，则在**静态 IP 设置**部分配置这些设置：

- **静态 IP** — 电话的静态 IP 地址
- **网络掩码** — 电话的网络掩码
- **网关** — 网关的 IP 地址

步骤 5 单击**提交所有更改**。

DHCP 选项支持

下表列出了 Cisco IP Phone 支持的 DHCP 选项。

网络标准	说明
DHCP 选项 1	子网掩码
DHCP 选项 2	时间偏移量

网络标准	说明
DHCP 选项 3	路由器
DHCP 选项 6	域名服务器
DHCP 选项 15	域名
DHCP 选项 41	IP 地址租用时间
DHCP 选项 42	NTP 服务器
DHCP 选项 43	供应商特定信息 可用于发现 TR.69 自动配置服务器 (ACS)。
DHCP 选项 56	NTP 服务器 使用 IPv6 的 NTP 服务器配置
DHCP 选项 60	供应商类别标识符
DHCP 选项 66	TFTP 服务器名称
DHCP 选项 125	供应商识别供应商特定信息 可用于发现 TR.69 自动配置服务器 (ACS)。
DHCP 选项 150	TFTP 服务器
DHCP 选项 159	设置服务器 IP
DHCP 选项 160	设置 URL

配置 SIP 邀请消息质询

在会话中，电话可以质询 SIP 邀请（起始）消息。该质询限制允许与服务提供商网络上的设备进行交互的 SIP 服务器。这种做法可防止设备受到恶意攻击，大大提高了 VoIP 网络的安全性。

开始之前

访问电话管理网页。请参阅访问电话网页。

过程

步骤 1 选择**语音** > **分机(n)**，其中 n 是分机号码。

步骤 2 在 **SIP 设置**部分，从**授权邀请**下拉列表框中选择**是**。

步骤 3 单击**提交所有更改**。

传输层安全

传输层安全 (TLS) 是用于确保能通过 Internet 进行安全通信并验证通信的标准协议。基于 TLS 的 SIP 会对服务提供商 SIP 代理和最终用户之间的 SIP 消息进行加密。基于 TLS 的 SIP 仅对信令消息进行加密，不对媒体进行加密。

TLS 有两层：

- TLS 记录协议 — 该层建立在 SIP 或 TCH 等可靠的传输协议上，采用对称数据加密，能确保连接的私有性和可靠性。
- TLS 握手协议 — 验证服务器和客户端，并在应用程序协议传输或接收数据之前协商加密算法和密钥。

Cisco IP Phone 使用 UDP 作为 SIP 传输标准，同时还支持基于 TLS 的 SIP 以增强安全性。

配置基于 TLS 的 SIP 信令加密

开始之前

访问电话管理网页。请参阅访问电话网页。

过程

步骤 1 选择**语音** > **分机(n)**，其中 n 是分机号码。

步骤 2 在 **SIP 设置**部分，从 **SIP 传输**下拉列表框中选择 **TLS**。

步骤 3 单击**提交所有更改**。

配置基于 TLS 的 LDAP

您可以配置基于 TLS 的 LDAP (LDAPS) 以启用服务器与特定电话之间的安全数据传输。

注意 Cisco 建议保留验证方法的默认值**无**。验证字段在服务器字段旁边，使用值**无**、**简单**或 **DIGEST MD5**。没有任何用于验证的 **TLS** 值。软件将从服务器字符串的 ldaps 协议确定验证方法。

开始之前

访问电话管理网页。请参阅访问电话网页。

过程

步骤 1 选择**语音** > **电话**。

步骤 2 在 **LDAP** 部分的**服务器**字段中输入服务器地址。

例如，输入 **ldaps://<ldaps_server>[:port]**。

其中：

- **ldaps://**= 服务器字符串以 **ldaps://** 开头，然后再输入 IP 地址或域名
- **ldaps_server** = IP 地址或域名
- **port** = 端口号。默认值：636

步骤 3 单击**提交所有更改**。

思科产品安全概述

本产品包含加密功能，在进出口、运输和使用方面受美国和当地国家/地区法律约束。交付思科加密产品并不表示第三方拥有进出口、分发或使用加密的权利。进口商、出口商、分销商和用户应遵守美国和所在国家/地区法律法规。使用本产品，即表示同意遵守适用的法律法规。如果不能遵守美国以及当地法律，请立即退回本产品。

有关美国出口条例的详细信息，请查阅 https://www.bis.doc.gov/policiesandregulations/ear/index.htm。