Cisco IP 电话安全性

域和互联网设置

配置域受限访问域

您可以将电话配置为仅使用指定的服务器注册、设置、进行固件升级和发送报告。 不能在电话上执行不使用指定服务器的注册、设置、升级和报告。 如果您指定要使用的服务器，请确保在以下字段中输入的服务器包含在列表中：

- **设置**选项卡上的**配置文件规则**、**配置文件规则 B**、**配置文件规则 C** 和**配置文件规则 D**
- **设置**选项卡上的**升级规则**和 **Cisco 头戴式耳机升级规则**
- **设置**选项卡上的**报告规则**
- **设置**选项卡上的**自定义 CA 规则**
- **分机 (n)** 选项卡上的**代理**和**出站代理**

开始之前

访问电话 Web 界面.

过程

步骤 1 选择语音 > 系统。

步骤 2 在 **System Configuration** 部分的 **Restricted Access Domains** 字段中，输入每台服务器的完全限定域名 (FQDN)。 用逗号分隔 FQDN。

示例：

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

您可以通过输入以下格式的字符串，在电话配置 XML 文件 (cfg.xml) 中配置此参数：

```
<Restricted_Access_Domains ua="na">voiceip.com, voiceip1.com</Restricted_Access_Domains>
```

步骤 3 单击 **Submit All Changes**。

配置 DHCP 选项

您可以设置您的电话使用 DHCP 选项的顺序。 有关 DHCP 选项的帮助，请参阅 DHCP 选项支持，第 3 页。

开始之前

访问电话 Web 界面.

过程

步骤 1 选择语音 > 部署。

步骤 2 在 **Configuration Profile** 部分，如 DHCP 选项配置参数，第 3 页表中所述设置 **DHCP Option To Use** 和 **DHCPv6 Option To Use** 参数。

步骤 3 单击 **Submit All Changes**。

DHCP 选项配置参数

下表定义了电话 Web 界面中 Voice > Provisioning 选项卡下 Configuration Profile 部分中 DHCP Options Configuration 参数的功能和用法。 它还定义了电话配置文件中添加的字符串的语法，其中包含用于配置参数的 XML(cfg.xml) 代码。

表 *1: DHCP* 选项配置参数

参数	说明
使用的 DHCP 选项	DHCP 选项用逗号分隔，用于检索固件和配置文件。 执行下列操作之一： • 在包含 XML(cfg.xml) 的电话配置文件中，输入以下格式的字符串： `<DHCP_Option_To_Use ua="na">66,160,159,150,60,43,125</DHCP_Option_To_Use>` • 在电话网页上，输入以逗号分隔的 DHCP 选项。 **示例**：66,160,159,150,60,43,125 默认值：66,160,159,150,60,43,125
DHCPv6 Option To Use	DHCPv6 选项，用逗号分隔，用于检索固件和配置文件。 执行下列操作之一： • 在包含 XML(cfg.xml) 的电话配置文件中，输入以下格式的字符串： `<DHCPv6_Option_To_Use ua="na">17,160,159</DHCPv6_Option_To_Use>` • 在电话网页上，输入以逗号分隔的 DHCP 选项。 **示例**：17,160,159 默认值：17,160,159

DHCP 选项支持

下表列出了多业务平台电话支持的 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
DHCP 选项 3	路由器
DHCP 选项 6	域名服务器
DHCP 选项 15	域名

网络标准	说明
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 INVITE 消息质询

您可以将电话设置为在会话中质询 SIP INVITE（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。 这种做法可防止电话遭受恶意攻击。 启用此功能后，由 SIP 代理发来的初始 INVITE 请求需要授权。

您还可以使用 XML(cfg.xml) 代码配置电话配置文件中的参数。

开始之前

访问电话 Web 界面.

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 **Auth INVITE** 列表选择**是**以启用此功能，或者选择**否**将其禁用。

您可以通过输入以下格式的字符串，在电话配置 XML 文件 (cfg.xml) 中配置此参数：

```
<Auth_INVITE_1>Yes</Auth_INVITE_1_>
```

默认值：**No**。

步骤 3 单击 **Submit All Changes**。

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 信令消息进行加密。

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

下表说明了两个 TLS 层。

表 *2: TLS* 层

协议名称	说明
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。

使用基于 TLS 的 SIP 加密信令

在使用基于 TLS 的 SIP 加密信令消息时，您可以配置额外的安全功能。

开始之前

访问电话 Web 界面. 请参阅传输层安全 ，第 5 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 Settings** 部分，从 **SIP Transport** 列表框中选择 **TLS**。

您可以通过输入以下格式的字符串，在电话配置 XML 文件 (cfg.xml) 中配置此参数：

```
<SIP_Transport_1_ ua="na">TLS</SIP_Transport_1_>
```

.

可用选项：

- UDP
- TCP
- TLS

- 自动

默认值：**UDP**。

步骤 3 单击 **Submit All Changes**。

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。

您还可以使用 XML(cfg.xml) 代码配置电话配置文件中的参数。

开始之前

访问电话管理网页。 请参阅：访问电话 Web 界面。

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。

您也可以通过输入以下格式的字符串，在电话配置 XML 文件 (cfg.xml) 中配置此参数：

```
<LDAP_Server ua="na">ldaps://10.45.76.79</LDAP_Server>
```

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

其中：

- **ldaps://**= 服务器地址字符串的开头。
- **ldaps_server** = IP 地址或域名
- **port** = 端口号。 默认值：636

步骤 3 单击 **Submit All Changes**。

配置 StartTLS

您可以为电话与 LDAP 服务器之间的通信启用启动传输层安全 (StartTLS)。 它对安全和不安全的通信使用相同的网络端口（默认 389）。 如果 LDAP 服务器支持 StartTLS，TLS 将对通信进行加密。否则，通信将为纯文本形式。

开始之前

- 访问电话管理网页。 请参阅：访问电话 Web 界面。

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 `ldap://<ldap_server>[:port]`。

其中：

- **`ldap://`** = 服务器地址字符串的开头，URL 的方案
- **`ldap_server`** = IP 地址或域名
- **`port`** = 端口号

您也可以通过输入以下格式的字符串，在电话配置 XML 文件 (cfg.xml) 中配置此参数：

```
<LDAP_Server ua="na">ldap://<ldap_server>[:port]</LDAP_Server>
```

步骤 3 将 **StartTLS Enable** 字段设置为 **Yes**。

您也可以通过输入以下格式的字符串，在电话配置 XML 文件 (cfg.xml) 中配置此参数：

```
<LDAP_StartTLS_Enable ua="na">是</LDAP_StartTLS_Enable>
```

步骤 4 单击 **Submit All Changes**。

相关主题

LDAP 目录参数

HTTPS 设置

电话支持 HTTPS 用于设置，以提高管理远程部署设备的安全性。 除 Sipura CA 服务器根证书之外，每部电话携带唯一的 SLL 客户端证书（以及关联的专用密钥）。 后者可让电话识别授权的设置服务器，并拒绝未经授权的服务器。 另一方面，客户端证书可让设置服务器识别出发出请求的单个设备。

要使服务提供商使用 HTTPS 管理部署，必须为电话使用 HTTPS 重新同步的每个设置服务器生成服务器证书。 服务器证书必须由 Cisco 服务器 CA 根密钥签名，所有部署的设备都会携带其证书。 为获得签名的服务器证书，服务提供商必须将证书签名请求转发给思科，思科将签名并返回服务器证书以供在设置服务器上安装。

设置服务器证书必须包含公用名称 (CN) 字段以及在主题中运行服务器的主机的 FQDN。 主机 FQDN 后可能包含信息，以斜线 (/) 字符分隔。 以下示例为电话接受的有效 CN 条目：

```
CN=sprov.callme.com
CN=pv.telco.net/mailto:admin@telco.net
CN=prof.voice.com/info@voice.com
```

除验证服务器证书，电话将依据针对服务器证书中指定的服务器名称的 DNS 查找，测试服务器 IP 地址。

获取签名的服务器证书

OpenSSL 实用程序可以生成证书签名请求。 以下示例显示了生成 1024 位 RSA 公共/专用密钥对和证书签名请求的 **openssl** 命令：

```
openssl req -new -out provserver.csr
```

此命令会在 **privkey.pem** 中生成服务器专用密钥，并在 **provserver.csr** 中生成对应的证书签名请求。 服务提供商会保留 **privkey.pem** 密钥并将 **provserver.csr** 提交给思科签名。 收到 **provserver.csr** 文件之后，思科会生成签名的服务器证书 **provserver.crt**。

过程

步骤 1 导航到 https://software.cisco.com/software/cda/home并使用 CCO 凭证登录。

注释 电话第一次连接到网络时或恢复出厂设置后，如果没有设置 DHCP 选项，它会联系设备激活服务器以执行零接触设置。 新电话将使用 “activate.cisco.com” 而不是 “webapps.cisco.com” 进行设置。 如果固件为 11.2 (1) 之前的版本，电话将继续使用 “webapps.cisco.com”。 我们建议您允许这两个域名通过防火墙。

步骤 2 选择**证书管理**。

在**签名 CSR** 选项卡上，将上传之前步骤中的 CSR 供签名。

步骤 3 从**选择产品**下拉列表框中，选择 **SPA1xx 固件 1.3.3 和更高版本/SPA232D 固件 1.3.3 和更高版本/SPA5xx 固件 7.5.6 和更高版本/CP-78xx-3PCC/CP-88xx-3PCC**。

步骤 4 在 **CSR 文件**字段中，单击**浏览**并选择 CSR 供签名。

步骤 5 选择加密方法：

- MD5
- SHA1

- SHA256

思科建议您选择 SHA256 加密。

步骤 6 从**登录持续时间**下拉列表框选择适用的持续时间（例如 1 年）。

步骤 7 单击**登录证书请求**。

步骤 8 选择以下选项之一接收签名的证书：

- **输入收件人的电子邮件地址**—如果您想要通过电子邮件接收证书，在此字段中输入您的电子邮件地址。
- **下载**—如果想要下载签名的证书，请选择此选项。

步骤 9 单击**提交**。

会下载签名的服务器证书，或者通过电子邮件将其发送给之前提供的电子邮件地址。

多业务平台电话 CA 客户端根证书

思科还为服务提供商提供多业务平台电话客户端根证书。 此根证书验证每部电话携带的客户端证书的可靠性。 多业务平台电话还支持第三方签名的证书，例如 Verisign、Cybertrust 等提供的证书。

要确定电话是否携带个性化的证书，请使用 $CCERT 设置宏变量。 视乎是否存在唯一的客户端证书而定，变量值将扩展为“已安装”或“未安装”。 如果采用通用的证书，可能要从“用户-代理”字段的 HTTP 请求标头中获取设备的序列号。

可将 HTTPS 服务器配置为从连接的客户端请求 SSL 证书。 如果启用，服务器可以使用思科提供用以验证客户端证书的多业务平台电话客户端根证书。 服务器然后可以向 CGI 提供证书信息以供进一步处理。

证书存储位置可能不尽相同。 例如，在 Apache 安装中，存储设置服务器签名证书的文件路径、其关联的专用密钥以及多业务平台电话 CA 客户端根证书如下所示：

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.crt

# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/provserver.key

# Certificate Authority (CA):
SSLCACertificateFile /etc/httpd/conf/spacroot.crt
```

有关详细信息，请参阅 HTTPS 服务器文档。

思科客户端证书根颁发机构会在每个唯一的证书上签名。 相应的根证书可供服务提供商用于验证客户端。

冗余设置服务器

设置服务器可以指定为 IP 地址或者为完全限定域名 (FQDN)。 使用 FQDN 可加快冗余设置服务器的部署。 通过 FQDN 确定设置服务器后，电话将尝试通过 DNS 将 FQDN 解析为 IP 地址。 仅支持将 DNS A 记录用于设置；DNS SRV 地址解析对设置不适用。 在服务器响应之前，电话将继续处理 A 记录。 如果没有与 A 记录关联的服务器响应，电话将向系统日志服务器记录一个错误。

系统日志服务器

如果使用 <Syslog Server> 参数在电话上配置系统日志服务器，执行重新同步和升级操作时会发送消息到系统日志服务器。 消息可在远程文件请求开始（配置文件或固件负载）和操作结束（指示成功或失败）时生成。

记录的消息在以下参数中配置，并宏扩展到实际的系统日志消息：

启用防火墙

我们通过强化操作系统来增强电话的安全性。 强化可确保电话具有防火墙，可保护其免受恶意传入流量的侵害。 防火墙会跟踪传入和传出数据的端口。 它会检测来自意外来源的传入流量并阻止访问。 您的防火墙允许所有传出流量。

防火墙可能会动态取消阻止通常阻止的端口。 传出 TCP 连接或 UDP 流会取消阻止端口以返回和继续传输流量。 在流处于活动状态时，端口将保持畅通。 当流终止或超时时，端口将恢复为阻止状态。

在旧版设置中，IPv6 多播 Ping **语音** > **系统** > **IPv6 设置** > **Broadcast Echo** 继续独立于新的防火墙设置工作。

防火墙配置更改通常不会导致电话重新启动。 电话软重启通常不会影响防火墙的运行。

防火墙默认启用。 如果其被禁用，您可以从电话网页启用。

开始之前

访问电话 Web 界面

过程

步骤 1 选择 **Voice** > **System** > **Security Settings**。

步骤 2 在 **Firewall** 下拉列表中，选择 **Enabled**。

您也可以通过输入以下格式的字符串，在配置文件 (cfg.xml) 中配置此参数：

```
<Firewall ua="na">Enabled</Firewall>
```

允许的值包括：Disabled|Enabled。 默认值为 Enabled。

步骤 3 单击 **Submit All Changes**。

这样可让防火墙使用其默认的开放 UDP 和 TCP 端口。

步骤 4 如果想要您的网络恢复为其之前的行为，可选择 **Disabled** 以禁用防火墙。

下表说明了默认的开放 UDP 端口。

表 *3:* 防火墙默认的开放 *UDP* 端口

默认开放的 **UDP** 端口	说明
DHCP/DHCPv6	DHCP 客户端端口 68 DHCPv6 客户端端口 546
SIP/UDP	当**启用线路**设置为**是**、**SIP 传输**设置为 **UDP** 或**自动**时，在**语音** > **分机<n>** > **SIP 设置** > **SIP 端口**中配置端口（示例：5060）。
RTP/RTCP	UDP 端口范围为 **RTP 最小端口号**到 **RTP 最大端口号+1**
PFS（对等固件共享）	当**启用升级**和**对等固件共享**设置为**是**时，端口 4051。
TFTP 客户端	端口 53240-53245。 如果远程服务器使用标准 TFTP 端口 69 以外的端口，则需要此端口范围。如果服务器使用标准端口 69，则可以将其关闭。请参阅通过其他选项配置防火墙 ， 第 11 页。
TR-069	当**启用 TR-069**设置为**是**时，UDP/STUN 端口 7999。

下表说明了默认的开放 TCP 端口。

表 *4:* 防火墙默认的开放 *TCP* 端口

默认开放的 **TCP** 端口	说明
Web 服务器	当**启用 Web 服务器**设置为**是**时，通过 Web 服务器端口配置的端口（默认为 80）。
PFS（对等固件共享）	当**启用升级**和**对等固件共享**都设置为**是**时，端口 4051 和 6970。
TR-069	当**启用 TR-069** 设置为**是**时，TR-069 连接请求 URL 中的 HTTP/SOAP 端口。 端口从 8000-9999 范围中随机选择。

通过其他选项配置防火墙

您可以在**防火墙选项**字段中配置其他选项。 在字段中键入每个选项的关键字，然后用逗号 (,) 分隔关键字。 有些关键字有值。 将值以冒号 (:) 隔开。

开始之前

访问电话 Web 界面

过程

步骤 1 转至 **Voice** > **System** > **Security Settings**。

步骤 2 为 **Firewall** 字段选择 **Enabled**。

步骤 3 在 **Firewall Options** 字段中，输入关键字。 端口列表同时适用于 IPv4 和 IPv6 协议。

当您输入关键字时，

- 使用逗号 (,) 将关键字隔开。
- 使用冒号 (:) 将关键字值隔开。

表 5: 防火墙可选设置

防火墙选项关键字	说明
字段为空。	防火墙使用默认的开放端口运行。
NO_ICMP_PING	防火墙会阻止传入的 ICMP/ICMPv6 **Echo** 请求 (Ping)。 此选项可能会中断对电话的某些类型的 traceroute 请求。 Windows **tracert** 是一个示例。 带选项组合的**防火墙选项**条目示例： NO_ICMP_PING,TCP:12000,UDP:8000:8010 防火墙使用默认设置和以下附加选项运行： • 丢弃传入 ICMP/ICMPv6 **Echo** (Ping) 请求。 • 为传入连接打开 TCP 端口 12000（IPv4 和 IPv6）。 • 为传入请求打开 UDP 端口范围 8000-8010（IPv4 和 IPv6）。
NO_ICMP_UNREACHABLE	对于 UDP 端口，电话不会发送 ICMP/ICMPv6 `Destination Unreachable`。 **注释** 例外情况是，对于 RTP 端口范围内的端口，始终会发送 `Destination Unreachable`。 此选项可能会中断到设备的某些类型的 **traceroute** 请求。例如，Linux **traceroute** 可能会中断。

防火墙选项关键字	说明
NO_CISCO_TFTP	• 电话未打开 TFTP 客户端端口范围 (UDP53240:53245)。 • 对非标准（非 69）TFTP 服务器端口的请求失败。 • 对标准 TFTP 服务器端口 69 的请求正常。
当电话运行可处理传入请求的自定义应用程序时，以下关键字和选项适用。	
UDP：<xxx>	打开 UDP 端口 <xxx>。
UDP：<xxx:yyy>	打开 UDP 端口范围，<xxx to yyy>，包括在内。 最多可以有 5 个 UDP 端口选项（单一端口和端口范围）。 例如，您可以有 3 个 UDP：<xxx> 和 2 个 UDP：<xxx:yyy>。
TCP：<xxx>	打开 TCP 端口 <xxx>。
TCP：<xxx:yyy>	打开 TCP 端口范围 <xxx to yyy>，包括在内。 最多可以有 5 个 TCP 端口选项（单一端口和端口范围）。 例如，您可以有 4 个 TCP：<xxx> 和一个 TCP：<xxx:yyy>。

您也可以通过输入以下格式的字符串，在配置文件 (cfg.xml) 中配置此参数：

```
<Firewall_Config ua="na">NO_ICMP_PING</Firewall_Config>
```

步骤 4 单击 **Submit All Changes**。

配置密码列表

您可以指定电话 TLS 应用程序使用的密码套件。 指定的密码列表适用于使用 TLS 协议的所有应用程序。 您的电话上的 TLS 应用包括：

- 客户 CA 设置
- E911 地理位置
- 固件/思科头戴式耳机升级
- LDAPS
- LDAP (StartTLS)
- 图片下载
- 徽标下载

- 词典下载
- 设置
- 报告上传
- PRT 上传
- 通过 TLS 的 SIP
- TR-069
- WebSocket API
- XML 服务
- XSI 服务

您还可以使用 TR-069 参数 (`Device.X_CISCO_SecuritySettings.TLSCipherList`) 或通过配置文件 (cfg.xml) 指定加密套件。 在配置文件中输入一个以下格式的字符串：

```
<TLS_Cipher_List ua="na">RSA:!aNULL:!eNULL</TLS_Cipher_List>
```

开始之前

访问电话管理网页，请参阅访问电话 Web 界面。

过程

步骤 1 选择**语音** > **系统**。

步骤 2 在 **Security Settings** 部分的 **TLS Cipher List** 字段中输入密码套件或密码套件组合。

示例：

```
RSA:!aNULL:!eNULL
```

支持使用 RSA 验证的密码套件，但不包括不提供加密和验证的密码套件。

注释 有效密码列表必须遵循以下网址规定的格式：https://www.openssl.org/docs/man1.1.1/man1/ciphers.html。 您的电话不支持 OpenSSL 网页上所列的所有密码字符串。 有关支持的字符串，请参阅支持的密码字符串 ， 第 15 页。

如果 **TLS Cipher List** 字段的值为空或者无效，则所用的密码套件将因应用程序而异。 请参阅以下列表，以了解当此字段为空或值无效时应用程序所用的套件。

- Web 服务器 (HTTPS) 应用程序使用以下密码套件：
  - **ECDHE-RSA-AES256-GCM-SHA384**
  - **ECDHE-RSA-AES128-GCM-SHA256**
  - **AES256-SHA**
  - **AES128-SHA**

- **DES-CBC3-SHA**

- XMPP 使用密码列表 **HIGH:MEDIUM:AES:@STRENGTH**。
- 使用 curl 库的 SIP、TR-069 和其他应用程序使用**默认**密码列表。 **默认**密码字符串包含电话支持的以下密码套件：

```
DEFAULT Cipher Suites (28 suites):
        ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        ECDHE_RSA_WITH_AES_256_GCM_SHA384
        DHE_RSA_WITH_AES_256_GCM_SHA384
        ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
        ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        ECDHE_RSA_WITH_AES_128_GCM_SHA256
        DHE_RSA_WITH_AES_128_GCM_SHA256
        ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
        ECDHE_RSA_WITH_AES_256_CBC_SHA384
        DHE_RSA_WITH_AES_256_CBC_SHA256
        ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
        ECDHE_RSA_WITH_AES_128_CBC_SHA256
        DHE_RSA_WITH_AES_128_CBC_SHA256
        ECDHE_ECDSA_WITH_AES_256_CBC_SHA
        ECDHE_RSA_WITH_AES_256_CBC_SHA
        DHE_RSA_WITH_AES_256_CBC_SHA
        ECDHE_ECDSA_WITH_AES_128_CBC_SHA
        ECDHE_RSA_WITH_AES_128_CBC_SHA
        DHE_RSA_WITH_AES_128_CBC_SHA
        RSA_WITH_AES_256_GCM_SHA384
        RSA_WITH_AES_128_GCM_SHA256
        RSA_WITH_AES_256_CBC_SHA256
        RSA_WITH_AES_128_CBC_SHA256
        RSA_WITH_AES_256_CBC_SHA
        RSA_WITH_AES_128_CBC_SHA
        EMPTY_RENEGOTIATION_INFO_SCSV
```

步骤 3 单击 **Submit All Changes**。

支持的密码字符串

下面列出的支持的密码字符串基于 OpenSSL 1.1.1d 标准。

表 *6:* 支持的密码字符串 *(OpenSSL 1.1.1d)*

字符串	字符串	字符串
DEFAULT	kECDHE、kEECDH	CAMELLIA128、CAMELLIA256、CAMELLIA
COMPLEMENTOFDEFAULT	ECDHE、EECDH	CHACHA20
ALL	ECDH	SEED
COMPLEMENTOFALL	AECDH	MD5

字符串	字符串	字符串
HIGH	aRSA	SHA1、SHA
MEDIUM	aDSS、DSS	SHA256、SHA384
eNULL、NULL	aECDSA、ECDSA	SUITEB128、SUITEB128ONLY、SUITEB192
aNULL	TLSv 1.2、TLSv1、SSLv3	
kRSA、RSA	AES128、AES256、AES	
kDHE、kEDH、DH	AESGCM	
DHE、EDH	AESCCM、AESCCM8	
ADH	ARIA128、ARIA256、ARIA	

为基于 TLS 的 SIP 启用主机名验证

如果您使用 TLS，可以在电话线路上启用增强的电话安全性。 电话线路可以验证主机名以确定连接是否安全。

通过 TLS 连接，电话可以验证主机名以检查服务器身份。 电话可以检查主题备选名称 (SAN) 和主题通用名 (CN)。 如果有效证书上的主机名与用于同服务器通信的主机名匹配，TLS 连接即会建立。 否则，TLS 连接会失败。

电话始终验证以下应用程序的主机名：

- LDAPS
- LDAP (StartTLS)
- XMPP
- 基于 HTTPS 的映像升级
- 基于 HTTPS 的 XSI
- 基于 HTTPS 的文件下载
- TR-069

当电话线路基于 TLS 传输 SIP 消息时，您可以通过**分机 (n)** 选项卡的 **TLS 名称验证**字段配置线路以启用或绕过主机名验证。

开始之前

- 访问电话管理网页。 请参阅：访问电话 Web 界面。

- 在 **Ext(n)** 选项卡上，将 **SIP Transport** 设置为 **TLS**。

过程

步骤 1 转至 **Voice** > **Ext(n)**。

步骤 2 在 **Proxy and Registration** 部分，将 **TLS Name Validate** 字段设置为 **Yes** 启用主机名验证，或设置为 **No** 绕过主机名验证。

您也可以通过输入以下格式的字符串，在配置文件 (cfg.xml) 中配置此参数：

```
<TLS_Name_Validate_1_ ua="na">Yes</TLS_Name_Validate_1_>
```

允许的值包括 Yes 和 No。默认设置为 Yes。

步骤 3 单击 **Submit All Changes**。

为媒体平面安全协商启用客户端启动的模式

要保护媒体会话，您可以配置电话以发起与服务器的媒体平面安全协商。 安全机制遵循 RFC 3329 及其扩展草案媒体安全机制名称中所述的标准（请参阅 https://tools.ietf.org/html/draft-dawes-sipcore-mediasec-parameter-08#ref-2）。 电话与服务器之间的协商传输可以通过 UDP、TCP 和 TLS 使用 SIP 协议。 您可以限制为，仅当信令传输协议为 TLS 时，才应用媒体平面安全协商。

您还可以在配置文件 (cfg.xml) 中配置参数。 要配置各个参数，请参阅媒体平面安全协商的参数，第 18 页中的字符串语法。

开始之前

访问电话管理网页。 请参阅：访问电话 Web 界面。

过程

步骤 1 选择**语音** > **分机 (n)**。

步骤 2 在 **SIP Settings** 部分，如媒体平面安全协商的参数，第 18 页中所述设置 **MediaSec Request** 和 **MediaSec Over TLS Only** 字段

步骤 3 单击 **Submit All Changes**。

媒体平面安全协商的参数

下表定义了电话 Web 界面中**语音** > **分机 (n)** 选项卡下**SIP 设置**部分呼叫功能设置部分中媒体平面安全协商参数的功能和用法。它还定义了电话配置文件 (cfg.xml) 中添加的字符串的语法，其中包含用于配置参数的 XML 代码。

表 *7:* 媒体平面安全协商的参数

参数	说明
MediaSec Request	指定电话是否向服务器发起媒体平面安全协商。 执行下列操作之一： • 在包含 XML(cfg.xml) 的电话配置文件中，输入以下格式的字符串： `<MediaSec_Request_1_ ua="na">Yes</MediaSec_Request_1_>` • 在电话 Web 界面中，根据需要将此字段设置为 **Yes** 或 **No**。 允许的值：是|否 • **Yes** — 客户端发起的模式。 电话发起媒体平面安全协商。 • **No** — 服务器发起的模式。服务器发起媒体平面安全协商。 电话不发起协商，但可以处理来自服务器的协商请求以建立安全呼叫。 默认值：No
MediaSec Over TLS Only	指定通过其应用媒体平面安全协商的信令传输协议。 在将此字段设置为 **Yes** 之前，请确保信令传输协议为 TLS。 执行下列操作之一： • 在包含 XML(cfg.xml) 的电话配置文件中，输入以下格式的字符串： `<MediaSec_Over_TLS_Only_1_ ua="na">No</MediaSec_Over_TLS_Only_1_>` • 在电话 Web 界面中，根据需要将此字段设置为 **Yes** 或 **No**。 允许的值：是|否 • **Yes** — 仅当信令传输协议为 TLS 时，电话才会发起或处理媒体平面安全协商。 • **No** — 无论信令传输协议如何，电话都会发起并处理媒体平面安全协商。 默认值：No

802.1x 验证

Cisco IP 电话使用思科发现协议 (CDP) 来识别 LAN 交换机并确定 VLAN 分配和线内电源要求等参数。 CDP 不识别本地连接的工作站。 Cisco IP 电话提供 EAPOL 传递机制。 利用此机制，连接至 Cisco IP 电话的工作站会将 EAPOL 消息传递给 LAN 交换机处的 802.1X 验证器。 该传递机制可确保，在访问网络前 IP 电话不会充当 LAN 交换机来验证数据终端。

Cisco IP 电话还提供代理 EAPOL 注销机制。 如果本地连接的 PC 与 IP 电话断开，LAN 交换机看不到物理链路失效，因为保持了 LAN 交换机与 IP 电话之间的链路。 为了避免损害网络完整性，IP 电话会代表下游 PC 向交换机发送一则 EAPOL 注销的消息，这会触发 LAN 交换机清除下游 PC 的验证条目。

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。 Cisco IP 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 安全访问控制服务器 (ACS)（或其他第三方验证服务器）：验证服务器和电话必须均使用验证电话的共享密钥进行配置。
- LAN 交换机支持 802.1X：交换机充当验证器，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 PC 端口：802.1X 标准不会考虑 VLAN，因此建议只验证连接至特定交换机端口的单个设备。 但是，某些交换机支持多域验证。 交换机配置决定是否可以将 PC 连接至电话的 PC 端口。
  - 是：如果您使用的是支持多域验证的交换机，可以启用 PC 端口并将 PC 连接至该端口。 在此情况下，Cisco IP 电话支持代理 EAPOL 注销，来监控交换机与所连 PC 之间的验证交换。
  - 否：如果交换机不支持同一端口上的多个符合 802.1X 的设备，应在启用 802.1X 验证后禁用 PC 端口。 如果不禁用此端口，后来又尝试将 PC 连接至该端口，交换机会拒绝对电话和 PC 的网络访问。
- 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。

启用 802.1X 验证

您可以在电话上启用 802.1X 验证。 802.1 X 验证启用后，电话将使用 802.1 X 验证请求网络访问。 802.1 X 验证关闭后，电话将使用 CDP 获取 VLAN 和网络访问。 您还可以在电话屏幕菜单中查看事务状态。

过程

步骤 1 执行以下操作之一以启用 802.1 X 验证：

- 在电话 Web 界面中，选择 **Voice** > **System**，然后将 **Enable 802.1X Authentication** 字段设置为 **Yes**。 然后，单击 **Submit All Changes**。
- 在配置文件 (cfg.xml) 中，输入一个以下格式的字符串：

```
<Enable_802.1X_Authentication ua="rw">Yes</Enable_802.1X_Authentication>
```

- 在电话上，按**应用程序** > **网络配置** > **以太网配置** > **802.1X 验证**。 然后，使用**选择**按键将**设备验证**字段设置为**开**并按**提交**。

步骤 2 （可选）选择**事务状态**以查看以下各项：

- **事务状态**：显示 802.1x 验证的状态。 状态可为
  - 正在验证：指示验证过程正在进行中。
  - 已验证：指示电话已验证完成。
  - 禁用：指示在电话上禁用了 802.1x 验证。
- **协议**：显示用于 802.1x 验证的 EAP 方法。 协议可以是 EAP-FAST 或 EAP-TLS。

步骤 3 按**返回**退出菜单。

设置代理服务器

您可以将电话配置为使用代理服务器以增强安全性。 代理服务器充当电话和互联网之间的防火墙。 配置成功后，电话通过代理服务器连接到互联网，代理服务器保护电话免受网络攻击。

您可以通过使用自动配置脚本或手动配置主机服务器（主机名或 IP 地址）和代理服务器的端口来设置代理服务器。

配置后，HTTP 代理特性将应用于所有使用 HTTP 协议的应用程序。 应用程序包括以下内容：

- GDS（激活码加入）
- EDOS 设备激活
- 加入 Webex 云（通过 EDOS 和 GDS）

- 证书验证
- 设置
- 固件升级
- 电话状态报告
- PRT 上传
- XSI 服务
- Webex 服务

开始之前

访问电话管理网页。 请参阅：访问电话 Web 界面。

过程

步骤 1 选择 **Voice** > **System**。

步骤 2 在**HTTP 代理设置**部分中，根据您的要求配置参数**代理模式**和其他方式。 以下步骤提供了详细的程序。

步骤 3 执行下列操作之一：

- **代理模式**为**自动**：
  - 如果**使用自动发现 (WPAD)**为**是**，则不需要进一步的操作。 电话将通过 Web 代理自动发现协议自动检索代理自动配置 (PAC) 文件。
  - 如果**使用自动发现 (WPAD)**为**否**，请在 **PAC URL** 中输入一个有效的 URL。
- **代理模式**为**手动**：
  - 如果**代理服务器要求验证**为**否**，则在**代理主机**中输入代理服务器，在**代理端口**中输入代理端口。
  - 如果**代理服务器要求验证**为**是**，则在**代理主机**中输入代理服务器，在**代理端口**中输入代理端口。 并在**用户名**中输入用户名，在**密码**中输入密码。
- **代理模式**为**关**，电话上的 HTTP 代理功能被禁用。

您还可以在电话配置文件 (cfg.xml) 中配置参数。 要配置各个参数，请参阅 HTTP 代理设置的参数，第 22 页 中的字符串语法。

步骤 4 单击 **Submit All Changes**。

HTTP 代理设置的参数

下表定义了电话 Web 界面中**语音** > **系统**选项卡下 **HTTP 代理设置**部分中 HTTP 代理参数的功能和用法。 它还定义了电话配置文件 (cfg.xml) 中添加的字符串的语法，其中包含用于配置参数的 XML 代码。

表 *8: HTTP* 代理设置的参数

参数	描述和默认值
代理模式	指定电话使用的 HTTP 代理模式，或禁用 HTTP 代理功能。 • 自动 电话会自动检索代理自动配置 (PAC) 文件以选择代理服务器。 在这种模式下，您可以决定是使用 Web 代理自动发现 (WPAD) 协议来检索 PAC 文件，还是手动输入 PAC 文件的有效 URL。 有关参数的详细信息，请参阅使用自动发现 (WPAD) 和 PAC URL。 • 手动 您必须手动指定服务器（主机名或 IP 地址）和代理服务器的端口。 有关参数的详细信息，请参阅代理主机和代理端口。 • 关 您禁用了电话上的 HTTP 代理功能。 执行下列操作之一： • 在包含 XML(cfg.xml) 的电话配置文件中，输入以下格式的字符串： `<Proxy_Mode ua="rw">Off</Proxy_Mode>` • 在电话 Web 界面上，选择代理模式或禁用该功能。 允许的值：自动、手动和关 默认值：关

参数	描述和默认值
使用自动发现 (WPAD)	确定电话是否使用 Web 代理自动发现 (WPAD) 协议来检索 PAC 文件。 WPAD 协议使用 DHCP 或 DNS 或两种网络协议来自动定位代理自动配置 (PAC) 文件。 PAC 文件用于为给定的 URL 选择代理服务器。 此文件可以在本地或网络上托管。 • 当**代理模式**设置为**自动**时，参数配置生效。 • 如果将参数设置为**否**，则必须指定一个 PAC URL。 有关该参数的详细信息，请参阅 PAC URL。 执行下列操作之一： • 在包含 XML(cfg.xml) 的电话配置文件中，输入以下格式的字符串： `<Use_Auto_Discovery__WPAD_ ua="rw">Yes</Use_Auto_Discovery__WPAD_>` • 在电话 Web 界面上，根据需要选择是或否。 允许的值：Yes 和 No 默认值：Yes
PAC URL	PAC 文件的 URL。 例如，`http://proxy.department.branch.example.com` 支持 TFTP、HTTP 和 HTTPS。 如果将**代理模式**设置为**自动**并将**使用自动发现 (WPAD)** 设置为**否**，则必须配置此参数。 执行下列操作之一： • 在包含 XML(cfg.xml) 的电话配置文件中，输入以下格式的字符串： `<PAC_URL ua="rw">http://proxy.department.branch.example.com/pac</PAC_URL>` • 在电话 Web 界面上，输入一个定位到 PAC 文件的有效 URL。 默认值：空

参数	描述和默认值

代理主机	电话要访问的代理主机服务器的 IP 地址或主机名。 例如：
	`proxy.example.com`
	不需要该方案 (`http://` or `https://`)。
	如果将**代理模式**设置为**手动**，则必须配置此参数。
	执行下列操作之一：
	• 在包含 XML(cfg.xml) 的电话配置文件中，输入以下格式的字符串：
	`<Proxy_Host ua="rw">proxy.example.com</Proxy_Host>`
	• 在电话 Web 界面上，输入代理服务器的 IP 地址或主机名。
	默认值：空

代理服务器端口	代理主机服务器的端口号。 如果将**代理模式**设置为**手动**，则必须配置此参数。 执行下列操作之一： • 在包含 XML(cfg.xml) 的电话配置文件中，输入以下格式的字符串： `<Proxy_Port ua="rw">3128</Proxy_Port>` • 在电话 Web 界面上，输入服务器端口。 缺省：3128
代理服务器需要验证	确定用户是否需要提供代理服务器所需的验证凭据（用户名和密码）。 此参数是根据代理服务器的实际行为配置的。 如果将参数设置为**是**，则必须配置**用户名**和**密码**。 有关参数的详细信息，请参阅用户名和密码。 当**代理模式**设置为**手动**时，参数配置生效。 执行下列操作之一： • 在包含 XML(cfg.xml) 的电话配置文件中，输入以下格式的字符串： `<Proxy_Server_Requires_Authentication ua="rw">No</Proxy_Server_Requires_Authentication>` • 在电话 Web 界面上，根据需要设置此字段“是”或“否”。 允许的值：Yes 和 No 默认值：No

参数	描述和默认值
用户名	代理服务器上凭据用户的用户名。 如果**代理模式**设置为**手动**，并且**代理服务器要求验证**设置为**是**，则必须配置该参数。 执行下列操作之一： • 在包含 XML(cfg.xml) 的电话配置文件中，输入以下格式的字符串： `<Proxy_Username ua="rw">Example</Proxy_Username>` • 在电话 Web 界面上，输入用户名。 默认值：空
密码	用于代理验证目的的指定用户名的密码。 如果**代理模式**设置为**手动**，并且**代理服务器要求验证**设置为**是**，则必须配置该参数。 执行下列操作之一： • 在包含 XML(cfg.xml) 的电话配置文件中，输入以下格式的字符串： `<Proxy_Password ua="rw">Example</Proxy_Password>` • 在电话 Web 界面上，为用户的代理验证输入有效密码。 默认值：空

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。