配置 CAPF

证书权限代理功能 (CAPF) 概述

Cisco 证书权限代理功能 (CAPF) 是颁发当地有效证书 (LSC) 和验证 Cisco 终端的 Cisco 专有服务。CAPF 服务在 Unified Communications Manager 上运行并执行以下任务：

- 颁发 LSC 给受支持的 Cisco Unified IP 电话。
- 在启用混合模式时验证电话。
- 升级电话的现有 LSC。
- 检索电话证书进行查看和故障排除。

CAPF 运行模式

您可以配置 CAPF 在以下模式下运行：

- Cisco 权限代理功能—Unified Communications Manager 上的 CAPF 服颁发由 CAPF 服务本身签名的 LSC。 该模式为默认模式。
- 在线 CA—使用此选项可让外部在线 CA 签名电话的 LSC。 CAPF 服务会自动连接到外部 CA。提交 CSR 后，CA 将会签名并自动返回 CA 签名的 LSC。
- 离线 CA—如果要使用离线外部 CA 为电话签名 LSC，则使用此选项。 此选项要求您手动下载 LSC，将其提交到 CA，然后在就绪后上传 CA 签名的证书。

注释 如果您想要使用第三方 CA 签名 LSC，Cisco 建议使用**在线 CA**选项而不是**离线 CA**，因为该流程已自动化，所以要快得多并且不容易遇到问题。

CAPF 服务证书

安装 Unified Communications Manager 后，CAPF 服务将自动安装，并且生成 CAPF 特定的系统证书。应用安全性后，Cisco CTL 客户端会将证书复制到所有群集节点。

电话证书类型

Cisco 为电话使用以下 X.509v3 证书类型：

- 本地有效证书 (LSC)—在您执行与 Cisco 证书权限代理功能 (CAPF) 关联的必要任务后安装在受支持的电话上的证书。将设备安全模式配置为验证或加密后，LSC 保护 Unified Communications Manager 和电话之间的连接安全。

注释 对于在线 CA，LSC 有效性基于 CA，并且只要 CA 允许，就可以使用。

- 厂商预装证书 (MIC) — Cisco 厂商自动安装 MIC 到支持的电话型号中。 厂商预装证书向 Cisco 证书权限代理功能 (CAPF) 验证以进行 LSC 安装。 您不能覆盖或删除厂商预装证书。

注释 Cisco 建议您仅针对 LSC 安装使用厂商预装证书 (MIC)。 Cisco 支持 LSC 验证与 Unified Communications Manager 的 TLS 连接。 由于 MIC 根证书可能受损，配置电话使用 MIC 进行 TLS 验证或进行其他操作的客户要自行承担风险。 思科不承担 MIC 受损产生的任何责任。

通过 CAPF 生成 LSC

配置 CAPF 后，在电话上添加所配置的身份验证字符串。 密钥和证书交换在电话和 CAPF 之间进行，并会发生以下情况：

- 电话使用所配置的身份验证方法向 CAPF 验证自身身份。
- 电话生成公钥-私钥对。
- 电话通过签名消息前转公钥给 CAPF。
- 私钥仍在电话中，并且绝不会外泄。
- CAPF 签名电话证书，然后通过签名消息将证书发送给电话。

注释 请注意，电话用户可以退出电话上的证书操作或查看操作状态。

注释 设置于低优先级的密钥生成可让电话在进行该操作的同时正常运行。 虽然证书生成期间电话功能正常，但增加的TLS流量会导致电话出现微小的呼叫处理中断； 例如，在安装结束将证书写入闪存时可能出现音频卡顿。

CAPF 前提条件

在配置用于生成 LSC 的证书权限代理功能之前，请执行以下操作：

- 如果想要使用第三方 CA 签署您的 LSC，请在外部配置您的 CA。
- 计划如何验证您的电话。
- 在生成 LSC 之前，请确保拥有以下各项：
  - Unified Communications Manager 版本 12.5 或更高版本。
  - 对证书使用 CAPF 的终端（包括 Cisco IP 电话和 Jabber）。
  - Microsoft Windows Server 2012 和 2016。
  - 已配置域名服务 (DNS)。
- 此备注适用于 14 SU2 及更高版本。

注释 任何 CAPF 证书都应包含以下默认 X509 扩展名：

X509v3 Basic Constraints:

CA:TRUE, pathlen:0

X509v3 Key Usage:

Digital Signature, Certificate Sign

如果 CAPF 证书中缺少这些扩展名，TLS 连接将失败。

- 在生成 LSC 之前，必须上传 CA 根证书和 HTTPS 证书。 在安全的 SIP 连接期间，HTTPS 证书通过 CAPF-trust，而 CA 根证书则通过 CAPF-trust 和 CallManager 信任。 互联网信息服务 (IIS) 会托管 HTTPS 证书。 CA 根证书用于签署证书签名请求 (CSR)。

  出现以下情况时，必须上传证书：

表 *1:* 上传证书的情况

场景	结果
CA 根证书和 HTTPS 证书相同。	上传 CA 根证书。
CA 根证书和 HTTPS 证书不同，且 HTTPS 证书由同一 CA 根证书颁发。	上传 CA 根证书。
中间 CA 和 HTTPS 证书不同，且由 CA 根证书颁发。	上传 CA 根证书。
CA 根证书和 HTTPS 证书不同，且由同一 CA 根证书颁发。	上传 CA 根证书和 HTTPS 证书。

注释 Cisco 强烈建议您在计划的维护窗口期间使用 CAPF，因为同时生成很多证书可能导致呼叫处理中断。

证书权限代理功能配置任务流程

完成这些任务以配置证书权限代理功能 (CAPF) 服务来为终端颁发 LSC：

注释 在重新生成或上传新的 CAPF 证书后，您无需重新启动 CAPF 服务。

过程

	命令或操作	目的
步骤 1	上传第三方 CA 的根证书	如果想要 LSC 经过第三方 CA 签名，请将 CA 根证书链上传到 CAPF-trust 存储区。 否则，您可以跳过此任务。
步骤 2	上传证书颁发机构 (CA) 根证书 ， 第 6 页	上传 CA 根证书到 Unified Communications Manager 信任存储区。
步骤 3	配置在线证书颁发机构设置 ， 第 6 页	使用此程序生成电话 LSC 证书。
步骤 4	配置离线证书颁发机构设置	使用此程序可通过离线 CA 生成电话 LSC 证书。
步骤 5	激活或重新启动 CAPF 服务	在配置 CAPF 系统设置后，激活基本 CAPF 服务。

	命令或操作	目的
步骤 6	使用以下程序之一在 Unified Communications Manager 中配置 CAPF 设置： • 在通用设备模板中配置 CAPF 设置，第 9 页 • 通过批量管理更新 CAPF 设置，第 10 页 • 配置电话的 CAPF 设置，第 11 页	使用以下选项之一将 CAPF 设置添加到电话配置： • 如果尚未同步 LDAP 目录，请将 CAPF 设置添加到通用设备模板，并通过初始 LDAP 同步应用设置。 • 使用批量管理工具可在一次操作中将 CAPF 设置应用到多部电话。 • 您可以逐个电话应用 CAPF 设置。
步骤 7	设置保持连接计时器，第 11 页	（可选）设置CAPF终端连接的保持连接值，以使其不会被防火墙超时。 默认值为 15 分钟。

上传第三方 CA 的根证书

将 CA 根证书上传到 CAPF-trust 存储区，Unified Communications Manager 信任存储区使用外部 CA 签名 LSC 证书。

注释 如果您不想使用第三方 CA 签名 LSC，请跳过此任务。

过程

步骤 1 从 Cisco Unified OS 管理中，选择**安全** > **证书管理**。

步骤 2 单击**上传证书/证书链**。

步骤 3 从**证书用途**下拉列表，选择 **CAPF-trust**。

步骤 4 输入证书**说明**。 例如，**适用于外部 LSC 签名 CA 的证书**。

步骤 5 单击**浏览**，导航至文件，然后单击**打开**。

步骤 6 单击**上传**。

步骤 7 重复此任务，将证书上传到 **callmanager-trust证书用途**。

上传证书颁发机构 (CA) 根证书

注释 确保中间CA或根CA证书的通用名称中不包含“CAPF-”子字符串。“CAPF-”通用名称是为CAPF证书保留的。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 单击**上传证书/证书链**。

步骤 3 从**证书用途**下拉列表，选择 **callmanager-trust**。

步骤 4 输入证书**说明**。 例如，**适用于外部 LSC 签名 CA 的证书**。

步骤 5 单击**浏览**，导航至文件，然后单击**打开**。

步骤 6 单击**上传**。

重要事项 此备注适用于 14 SU2 及更高版本。

注释 对于任何根或中间 CA 证书，它应包括以下默认 X509 扩展名：

X509v3 Basic Constraints:

CA:TRUE, pathlen:0

X509v3 Key Usage:

Digital Signature, Certificate Sign

如果证书中缺少这些扩展名，TLS 连接将失败。

重要事项 此备注适用于 14 SU3 及更高版本，并且仅适用于 IPSec 证书。

注释 对于任何 CA 签名的 IPSec 证书，不应包括以下扩展名：

X509v3 Basic Constraints:

CA:TRUE

配置在线证书颁发机构设置

在 Unified Communications Manager 中使用此程序以通过在线 CAPF 生成电话 LSC。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **服务参数**。

步骤 2 从**服务器**下拉列表中，选择您要在其中激活 Cisco 证书权限代理功能（活动）服务的节点。

步骤 3 从**服务**下拉列表中，选择**Cisco 证书权限代理功能（活动）**。确认服务名称旁边显示“活动”一词。

步骤 4 从**证书颁发者到终端**下拉列表中，选择**在线 CA**。 对于 CA 签名的证书，我们建议使用在线 CA。

步骤 5 在**证书有效的持续时间（日）**字段中，输入介于 1 到 1825 之间的数字以表示 CAPF 颁发的证书的有效天数。

步骤 6 在**在线 CA 参数**部分，设置以下参数，以便创建到“在线 CA”部分的连接。

- 在线 CA 主机名—主题名称或通用名称 (CN) 应与 HTTPS 证书的完全限定域名 (FQDN) 相同。

  注释 主机名配置为与 Microsoft CA 上运行的 Internet Information Services (IIS) 托管的 HTTPs 证书通用名称 (CN) 相同。

- 在线 CA 端口—输入在线 CA 的端口号。例如，443
- 在线 CA 模板—输入模板的名称。 Microsoft CA 将创建模板。

  注释 仅当在线 CA 类型为 Microsoft CA 时，才会启用此字段。

- 在线 CA 类型—为终端证书的自动注册选择 Microsoft CA 或 EST 支持的 CA。
  - Microsoft CA - 当 CA 是 Microsoft CA 时，使用此选项向设备分配数字证书。

    注释 Microsoft CA 不支持 FIPSS 启用模式。

    - **重要事项** 从 14SU2 版开始支持。

    EST 支持的 CA – 当 CA 支持自动注册的内置 EST 服务器模式时，使用此选项。

- 在线 CA 用户名—输入 CA 服务器的用户名。
- 在线 CA 密码—输入 CA 服务器用户名的密码。
- 证书注册配置文件标签—使用有效字符输入 EST 支持的 CA 的数字标识。

  注释 仅当在线 CA 类型为 EST 支持的 CA 时，才会启用此字段。

步骤 7 完成其余的 CAPF 服务参数。 单击参数名称可查看服务参数帮助系统。

步骤 8 单击**保存**。

步骤 9 重新启动 **Cisco 证书权限代理功能**以使更改生效。 即会自动重新启动 Cisco 证书登记服务。

当前在线 CA 限制

- 如果 CA 服务器使用除英语之外的任何其他语言，则在线 CA 功能不工作。 CA 服务器只能以英语响应。
- 在线 CA 功能不支持使用 CA 的 mTLS 验证。
- 使用在线 CA 进行 LSC 操作时，如果没有为 LSC 证书提供“数字签名”和“密钥加密”密钥使用情况，设备安全注册将失败。

- 使用在线 CA 进行 LSC 操作时，如果没有为 LSC 证书提供“数字签名”和“密钥加密”，设备安全注册将失败。

配置离线证书颁发机构设置

如果您决定使用离线 CA 生成电话 LSC 证书，请遵循此高级流程。

注释 离线 CA 选项比在线 CA 更费时，涉及许多手动步骤。如果在证书生成和传输过程中出现任何问题（例如，网络中断或电话重置），请重新启动此过程。

过程

步骤 1 从第三方证书颁发机构下载根证书链。

步骤 2 将根证书链上传到 Unified Communications Manager 中要求的信任（CallManager 信任 CAPF 信任）。

步骤 3 通过将**证书颁发给终端**服务参数设置为“离线 CA”，配置 Unified Communications Manager 使用离线 CA。

步骤 4 为您的电话 LSC 生成 **CSR**。

步骤 5 发送 **CSR** 到证书颁发机构。

步骤 6 从 **CSR** 那里获取签名的证书 。

有关如何使用离线 CA 生成电话 LSC 的详细示例，请参阅 CUCM 第三方 CA 签名 LSC 生成和导入配置。

激活或重新启动 CAPF 服务

在配置 CAPF 系统设置后激活必要的 CAPF 服务。 如果 CAPF 服务已激活，则重新启动。

过程

步骤 1 从 Cisco Unified 功能配置，选择**工具** > **服务激活**。

步骤 2 从**服务器**下拉列表中，选择发布方节点并单击**前往**。

步骤 3 从**安全服务**窗格中，选中适用的服务：

- **Cisco 证书登记服务**—如果您使用的是在线 CA，则选中此服务，否则请不要选中。
- **Cisco 证书权限代理功能** —如果未选中（已取消激活），则选中此服务。 如果服务已激活，则重新启动。

步骤 4 如果您修改了任何设置，请单击**保存**。

步骤 5 如果 **Cisco 证书权限代理功能**服务已选中（已激活），则重新启动：

a) 从**相关链接**下拉列表中，选择**控制中心 - 功能服务**并单击**前往**。

b) 在**安全设置**窗格中，选中 **Cisco 证书权限代理功能**服务，然后单击**重新启动**。

步骤 6 完成以下程序，配置针对个别电话的 CAPF 设置。

a) 在通用设备模板中配置 CAPF 设置，第 9 页

b) 通过批量管理更新 CAPF 设置，第 10 页

c) 配置电话的 CAPF 设置，第 11 页

在通用设备模板中配置 CAPF 设置

使用此程序将 CAPF 设置配置为通用设备模板 通过功能组模板配置将模板应用于 LDAP 目录同步。模板中的 CAPF 设置适用于使用此模板的所有同步设备。

注释 您只能将通用设备模板添加到尚未同步的 LDAP 目录中。 如果初始 LDAP 同步已进行，请使用批量管理来更新电话。 有关详细信息，请参阅通过批量管理更新 CAPF 设置，第 10 页。

过程

步骤 1 从 Cisco Unified CM 管理，选择**用户管理 > 用户/电话添加 > 通用设备模板**。

步骤 2 执行以下任一操作：

- 单击**查找**并**选择**现有模板。
- 单击**新增**。

步骤 3 展开**证书权限代理功能 (CAPF) 设置**区域

步骤 4 在**证书操作**下拉列表中，选择**安装/升级**。

步骤 5 从**身份验证模式**下拉列表菜单中，为设备选择一个选项以验证自身身份。

步骤 6 如果选择使用身份验证字符串，请在文本框中输入**身份验证字符串**，或单击**生成字符串**以让系统为您生成字符串。

注释 如果设备本身未配置此字符串，身份验证会失败。

步骤 7 从其余字段，配置密钥信息。 有关这些字段的帮助，请参阅联机帮助。

步骤 8 单击**保存**。

注释 确保您已使用在此程序中分配的相同身份验证方法配置了使用此模板的设备。 否则，设备身份验证会失败。 有关如何为电话配置身份验证的详细信息，请参阅电话文档。

步骤 9 将模板设置应用到使用此配置文件的设备。

a) 将通用设备模板添加到功能组模板配置。
b) 将功能组模板添加到未同步的 LDAP 目录配置。
c) 完成 LDAP 同步。 CAPF 设置会应用到所有已同步的设备。

有关配置功能部件组模板和 LDAP 目录的详细信息，请参阅Cisco Unified Communications Manager 系统配置指南的“配置最终用户”一节。

通过批量管理更新 CAPF 设置

使用批量管理的**更新电话**查询在一次操作中为许多现有电话配置 CAPF 设置和 LSC 证书。

注释 如果您尚未预配置电话，请使用批量管理的**插入电话**菜单，使用 CSV 文件中的 CAPF 设置预配置新电话。 有关如何从 CSV 文件插入电话的详细信息，请参阅Cisco Unified Communications Manager 批量管理指南的“电话插入”一节了解详细信息。

确保使用您计划在此程序中添加的相同字符串和身份验证方法配置了您的电话。 否则，您的电话将不会向 CAPF 进行验证。 有关如何在电话上配置身份验证的详细信息，请参阅您的电话文档。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**批量管理** > **电话** > **更新电话** > **查询**。

步骤 2 使用过滤器选项将搜索限制为您要更新的电话，然后单击**查找**。

例如，使用**查找电话位置**下拉列表选择所有电话，其中 LSC 在特定日期之前或特定设备池中过期。

步骤 3 单击**下一步**。

步骤 4 从**注销/重置/重新启动**部分，选择**应用配置**单选按钮。 当作业运行时，CAPF 更新将应用到所有更新了的电话。

步骤 5 在**证书权限代理功能 (CAPF) 信息**下，选中**证书操作**复选框。

步骤 6 从**证书操作**下拉列表中，选择**安装/升级**以使 CAPF 在电话上安装新的 LSC 证书。

步骤 7 从**身份验证模式**下拉列表中，选择您希望电话在 LSC 安装期间验证自身身份的方式。

注释 在电话上应配置相同的身份验证方法。

步骤 8 如果您选择**按验证字符串** 作为 **验证模式**，请完成以下步骤之一：

- 如果要对每个设备使用唯一的验证字符串，请选中**为每个设备生成唯一的验证字符串**。
- 在**验证字符串**文本框中输入字符串，如果想要对所有设备使用相同的验证字符串，则单击**生成字符串**。

步骤 9 完成**更新电话**窗口的**证书权限代理功能 (CAPF) 信息**部分中其余字段的设置。 有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 10 从**作业信息**部分，选择**立即运行**。

注释 如果想要在计划的时间运行作业，则选择**稍后运行**。 有关计划作业的详细信息，请参阅 Cisco Unified Communications Manager 批量管理指南中的“管理计划作业”一节 。

步骤 11 单击**提交**。

注释 如果在此程序中没有选择**应用配置**选项，则为所有更新了的电话应用**电话配置**窗口中的配置。

配置电话的 CAPF 设置

使用此程序可为个人电话上的 LSC 证书配置 CAPF 设置。

注释 使用批量管理或同步 LDAP 目录将 CAPF 设置应用到大量电话。

使用您计划在此程序中添加的相同字符串和身份验证方法配置您的电话。 否则，电话不会向 CAPF 验证自身身份。 有关如何在电话上配置身份验证的详细信息，请参阅您的电话文档。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**设备** > **电话**。

步骤 2 单击**查找**并选择现有电话。 **电话配置**页面将会显示。

步骤 3 导航至**证书权限代理功能 (CAPF) 信息**窗格。

步骤 4 从**证书操作**下拉列表中，选择**安装/升级** CAPF 以在电话上安装新的 LSC 证书。

步骤 5 从**身份验证模式**下拉列表中，选择您希望电话在 LSC 安装期间验证自身身份的方式。

注释 电话应配置为使用相同的身份验证方法。

步骤 6 如果您选择了**按验证字符串**，则输入文本字符串或单击**生成字符串**以为您生成字符串。

步骤 7 在**电话配置**页的**证书权限代理功能 (CAPF) 信息**窗格的其余字段中输入详细信息。 有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 8 单击**保存**。

设置保持连接计时器

使用此程序设置 CAPF - 终端连接的群集范围保持连接计时器，以使该连接不会被防火墙超时。 计时器默认值为 15 分钟。 在每个间隔后，CAPF 服务会发送保持连接信号给电话以使该连接保持接通状态。

过程

步骤 1 使用命令行界面以登录发布方节点。

步骤 2 运行 `utils capt keep_alive` CLI 命令。

步骤 3 输入 5 到 60（分钟）之间的数字，然后单击 **Enter**。

CAPF 管理任务

在配置 CAPF 并颁发 LSC 证书后，可以使用以下任务来定期管理 LSC 证书。

证书状态监控

您可将系统配置为自动监控证书状态。 当证书接近到期时，系统将向您发送电子邮件，然后在过期后吊销证书。

有关如何配置证书监控检查的详细信息，请参阅 “管理证书”一章中的证书监控和吊销任务流程。

运行过时的 LSC 报告

使用此程序从 Cisco Unified 报告运行过时的 LSC 报告。 过时的 LSC 是为响应终端 CSR 而生成但从未安装的证书，因为在安装过时的 LSC 之前，终端生成了新的 CSR。

注释 您还可以通过 `在发布方节点上运行 utils capf stale-lsc list CLI 命令获取过时 LSC 证书的列表 。`

过程

步骤 1 从 Cisco Unified 报告，选择**系统报告**。

步骤 2 在左侧导航栏中，选择**过时的 LSC**。

步骤 3 单击**生成新报告**。

查看待处理的 CSR 列表

使用此程序可查看待处理的 CAPF CSR 文件列表。 所有 CSR 文件都有时间戳。

过程

步骤 1 使用命令行界面以登录发布方节点。

步骤 2 运行 `utils capf csr list` CLI 命令。
有时间戳的待处理 CSR 文件列表将会显示。

删除过时的 LSC 证书

使用此程序从系统中删除过时的 LSC 证书。

过程

步骤 1 使用命令行界面以登录发布方节点。

步骤 2 运行 `utils capf stale-lsc delete all` CLI 命令
系统将删除所有过时的 LSC 证书。

CAPF 系统相互作用和限制

功能	互动
验证字串	电话的 CAPF 验证方式，操作后在电话上必须输入相同的验证字符串，否则操作将失败。如果启用了 TFTP 已加密配置企业参数，并且您没有输入验证字符串，电话将出现故障并且无法恢复，直至在电话上输入匹配的验证字符串。
群集服务器凭证	Unified Communications Manager 群集中的所有服务器必须使用相同的管理员用户名和密码，以便 CAPF 能够验证群集中的所有服务器。
迁移安全电话	如果安全的电话被移至另一个群集，Unified Communications Manager 将不信任电话发送的 LSC 证书，因为它是由另一 CAPF 颁发的，而其证书不在 CTL 文件中。 要启用安全的电话以注册，请删除现有CTL文件。然后，您可以使用安装/升级选项来安装使用新的 CAPF 的新证书，并重置电话以使用新的 CTL 文件（或使用 MIC）。 在移动电话之前，使用电话配置窗口 CAPF 部分的删除选项删除现有 LSC。

功能	互动
Cisco Unified 6900 系列、7900 系列、8900 系列和 9900 系列 IP 电话	Cisco 建议升级 Cisco Unified 6900 系列、7900 系列、8900 系列和 9900 系列 IP 电话以使用 LSC 进行至 Unified Communications Manager 的 TLS 连接，并从 CallManager 信任存储区中删除 MIC 根证书以避免今后出现兼容性问题。 请注意有些使用MIC进行至 Unified Communications Manager 的 TLS 连接的电话型号可能无法注册。 管理员应该从 CallManager 信任存储区中删除以下 MIC 根证书： • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048
电源故障	发生通信或电源故障时，以下信息适用。 • 如果在证书安装期间电话发生通信故障，电话将以30秒为间隔尝试获取证书三次。 您无法更改这些值。 • 如果在电话尝试与 CAPF 进行会话期间发生电源故障，电话将使用存储在闪存中的验证模式，亦即，电话重新启动后，不能从 TFTP 服务器加载新的配置文件。 证书操作完成后，系统将清除闪存中的值。
证书加密	从 Unified Communications Manager 版本 11.5 (1) SU1 开始，CAPF 服务颁发的所有 LSC 证书都使用 SHA-256 算法签名。 因此，IP 电话 7900/8900/9900 系列型号支持 SHA-256 签名的 LSC 证书和外部 SHA2 身份证书（Tomcat、CallManager、CAPF、TVS 等等）。 对于需要验证签名的任何其他加密操作，仅支持 SHA-1。 **注释** 如果您使用的电话型号软件维护终止或寿命结束，我们强烈建议您使用 11.5 (1) SU1 版本之前的 Unified Communications Manager。

7942 和 7962 电话的 CAPF 示例

用户或 Unified Communications Manager 重置电话时，请考虑以下 CAPF 如何与 Cisco Unified 7962 和 7942 IP 电话交互的相关信息。

注释 在以下示例中，如果电话中尚不存在 LSC 且为“CAPF 验证模式”选中**按现有证书**，CAPF 证书操作将失败。

示例 — 不安全设备安全模式

在本例中，在您将“设备安全模式”配置为**不安全**，将“CAPF 验证模式”配置为**按空字符串**或**按现有证书 (优先于...)**后，电话将重置。 电话重置后，它将立即向主 Cisco Unified Communications Manager 注册并接收配置文件。 然后，电话将自动发起与 CAPF 的会话以下载 LSC。 电话安装 LSC 后，将设备安全模式配置为“已验证”或“已加密”。

示例 — 已验证/已加密设备安全模式

本例中，在您将**设备安全模式**配置为**已验证**或**已加密**，将“CAPF 验证模式”配置为**按空字符串**或**按现有证书 (优先于...)**后，电话将重置。 电话不会向主 Unified Communications Manager 注册，直至 CAPF 会话结束并且电话安装了 LSC。 会话结束后，电话注册并立即在已验证或已加密模式下运行。

本例中，您不能配置**按验证字符串**，因为电话不会自动联系 CAPF 服务器；如果电话没有有效的 LSC，注册将失败。

CAPF 与 IPv6 寻址的相互作用

CAPF 可以发行和升级证书给使用 IPv4、IPv6 或同时使用两类地址的电话。 要颁发或升级运行 SCCP 的使用 IPv6 地址的电话的证书，您必须在 Unified Communications Manager 管理中将“启用 IPv6”服务参数设置为**真**。

电话连接至 CAPF 获取证书时，CAPF 使用“启用 IPv6”(Enable IPv6) 企业参数中的配置确定是发行还是升级证书到电话。 如果该企业参数设为“假”(**False**)，CAPF 会忽略/拒绝来自使用 IPv6 地址的电话的连接，该电话不会收到证书。

下表介绍使用 IPv4、IPv6 或同时使用两类地址的电话如何连接到 CAPF。

表 *2: IPv6* 或 *IPv4* 电话如何连接到 *CAPF*

IP 电话模式	电话上的 **IP** 地址	**CAPF IP** 地址	电话如何连接到 **CAPF**
双堆栈	IPv4 和 IPv6 可用	IPv4，IPv6	电话使用 IPv6 地址连接 CAPF。如果电话无法通过 IPv6 地址连接，将尝试使用 IPv4 地址连接。
双堆栈	IPv4	IPv4，IPv6	电话使用 IPv4 地址连接 CAPF。
双堆栈	IPv6	IPv4，IPv6	电话使用 IPv6 地址连接 CAPF。 如果尝试失败，电话将使用 IPv4 地址连接 CAPF。
双堆栈	IPv4	IPv4	电话使用 IPv4 地址连接 CAPF。
双堆栈	IPv4 和 IPv6 可用	IPv6	电话使用 IPv6 地址连接 CAPF。
双堆栈	IPv4 和 IPv6 可用	IPv4	电话使用 IPv4 地址连接 CAPF。
双堆栈	IPv4	IPv6	电话无法连接 CAPF。

IP 电话模式	电话上的 IP 地址	CAPF IP 地址	电话如何连接到 CAPF
双堆栈	IPv6	IPv4	电话无法连接 CAPF。
双堆栈	IPv6	IPv6	电话使用 IPv6 地址连接 CAPF。
IPv4 堆栈	IPv4	IPv4，IPv6	电话使用 IPv4 地址连接 CAPF。
IPv6 堆栈	IPv6	IPv4，IPv6	电话使用 IPv6 地址连接 CAPF。
IPv4 堆栈	IPv4	IPv4	电话使用 IPv4 地址连接 CAPF。
IPv4 堆栈	IPv4	IPv6	电话无法连接 CAPF。
IPv6 堆栈	IPv6	IPv6	电话使用 IPv6 地址连接 CAPF。
IPv6 堆栈	IPv6	IPv4	电话无法连接 CAPF。

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。