目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[配置](#)
[概略的配置步骤](#)
[详细配置示例](#)
[相关信息](#)

简介

许多网络管理员选择实现Cisco Unified Communications Manager Express (CME)以安全。而不是内置的IOS认证机关(IOS-CA)，网络管理员能选择集成与他们的现有公共密钥基础设施(PKI)基础设施的安全CME。本文描述如何配置安全CME运行与安全信令和媒体，通过第三方证书。

先决条件

要求

本文假设， Cisco Unified Communications Manager Express (CME)在您的环境运行和功能完备的。 一定是可操作的在Secure Cisco Unified CME的所有电话需要能成功首先注册到CME。 关于如何配置CME的信息，参考Cisco Unified Communications Manager Express系统管理员指南。

本文也假设，语音和安全功能启用。

使用的组件

本文档中的信息根据Cisco Unified Communications Manager Express (CME)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的信息，请参阅 Cisco 技术提示规则。

配置

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

概略的配置步骤

1. 创建IOS-CA实例。
2. 创建信任点有第三方CA证书。
3. 生成证书签名请求(CSR)从信任点。
4. 签署与服务器验证使用情况的CSR，并且获取CA证明。
5. 验证与CA证书的信任点，并且导入各自身份证书。
6. 验证第三方证书信任点。
7. 创建IOS CA CME信任点。
8. 配置证书信任列表(CTL)客户端。
9. 配置认证机关代理功能(CAPF)服务器。
10. 配置电话服务。
11. 配置测试电话。
12. 验证。

详细配置示例

1. 创建IOS-CA实例。IOS-CA实例生产使用签署电话的局部重要的证书的自签名证书(LSC)。
2. 创建将生成第三方签字的CSR的信任点。 这些信任点最终有第三方CA证书，以及身份证书，是CSR的结果。

3. 生成从信任点的CSR。**crypto pki登记**提供给第三方CA签字的命令生产CSR。

   示例 1：
   示例 2：
4. 请使用两CSR为了生成与服务器验证权限的证书。
   注意： 重要的是全双工证书链为两证书之一得到从CA。 证书链提供CA和身份证书从签署的CA。保证证书在base64格式下载。按该顺序重要的是非常CA证书使用每信任点的验证，并且身份证书导入到每信任点。
5. 验证与CA证书的信任点，并且导入SAST身份证书。

   示例 1：

   示例 2：
6. 一旦CA和身份证书装载到各自信任点，请验证每信任点的证书链。此步骤保证上一个步骤顺利地完成。

7. 创建IOS CA CME信任点。

   由于IOS-CA信任点不可能用于客户端验证(传输级安全性(TLS)连接用电话)，您在它必须创建另一信任点和放置IOS-CA证书。

此信任点用于只授权IP电话的要求TLS连接(因此他们能适当地注册)。

8. 配置CTL客户端。

   注意：保证CTL文件顺利地创建：
9. 配置CAPF服务器。

10. 配置电话服务。

11. 配置测试电话(ephone)为了升级其证书和使用加密的模式。 一旦配置完成，重置电话并且等待它注册。

    注意：在电话重置前，请保证已经没有安全配置存在。如果安全配置存在，必须手工删除或在注册之前完成测试电话的出厂重置获取Cisco Unified CME。

    要重置电话，请执行这些命令：一旦电话接收更新LSC， CERT**操作升级验证模式空字符串**命令删除。
12. 验证电话注册与验证和加密。

安全Cisco Unified CME应该是功能完备的与第三方证书。

相关信息

- Cisco Unified Communications Manager Express 系统管理员指南
- 在Cisco TAC维基的安全语音
- 技术支持和文档 - Cisco Systems