配置基本的安全性

关于安全配置

本节提供设置 Cisco Unified Communications Manager 必须执行的基本安全配置任务的相关信息。

安全配置任务

执行以下任务以设置基本安全配置：

为群集启用混合模式

使用此程序可在群集中启用混合模式。

过程

步骤 1 登录到发布方节点上的命令行界面。

步骤 2 运行 **utils ctl set-cluster mixed-mode** CLI 命令。

注释 确保 Communications Manager 已注册到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite，并且从智能帐户或虚拟帐户收到的注册令牌允许在注册此群集时启用导出受控功能。

下载证书

提交 CSR 请求时，使用下载证书任务复制证书或上传证书。

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 指定搜索条件，然后单击**查找**。

步骤 3 选择所需的文件名，然后单击**下载**。

生成证书签名请求

生成证书签名请求 (CSR) 是一块加密的文本，其中包含证书应用程序信息、公钥、组织名称、通用名称、所在地，以及国家/地区。证书颁发机构使用此 CSR 为您的系统生成信任证书。

注释 如果您生成新的 CSR，将覆盖任何现有的 CSR。

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**生成 CSR**。

步骤 3 配置**生成证书签名请求**窗口中的字段。 请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 4 单击**生成**。

下载证书签名请求

下载所生成的 CSR 并准备好将其提交给您的证书颁发机构。

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**下载 CSR**。

步骤 3 从**证书目的**下拉列表中选择证书名称。

步骤 4 单击**下载 CSR**。

步骤 5 （可选） 如果收到提示，请单击**保存**。

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**。

TLS 前提条件

在配置最低 TLS 版本之前，请确保您的网络设备和应用程序都支持 TLS 版本。 此外，请确保您启用了要使用 Unified Communications Manager 和 IM and Presence Service 配置的 TLS。 如果您部署了以下任何产品，请确认它们符合最低 TLS 要求。 如果它们不符合这一要求，请升级这些产品：

- 信令客户端控制协议 (SCCP) 会议桥
- 转码器
- 硬件媒体终结点 (MTP)
- SIP 网关

- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- 思科 Prime 协作部署
- Cisco Unified 边界组件 (CUBE)
- Cisco Expressway
- Cisco TelePresence Conductor

您将无法升级会议桥、媒体终结点 (MTP)、Xcoder、Prime Collaboration Assurance 和 Prime Collaboration Provisioning。

注释 如果您是从较早版本的 Unified Communications Manager 升级，请确保所有设备和应用程序都支持较高版本的 TLS，然后再进行配置。 例如，Unified Communications Manager 和 IM and Presence Service 版本 9.x 仅支持 TLS 1.0。

设置最低 TLS 版本

默认情况下，Unified Communications Manager 支持的最低 TLS 版本为 1.0。 使用此程序可将 Unified Communications Manager 和 IM and Presence Service 支持的最低 TLS 版本重置为较高的版本，例如 1.1 或 1.2。

确保网络中的设备和应用程序支持您要配置的 TLS 版本。 有关详细信息，请参阅TLS 前提条件，第 3 页。

过程

步骤 1 登录到**命令行界面**。

步骤 2 要确认现有 TLS 版本，请运行 **show tls min-version** CLI 命令。

步骤 3 运行 **set tls min-version** <*minimum*> CLI 命令，其中 <*minimum*> 代表 TLS 版本。

例如，运行 **set tls min-version 1.2** 将最低 TLS 版本设置为 1.2。

步骤 4 在所有 Unified Communications Manager 和 IM and Presence Service 服务群集节点上执行步骤 3。

设置 TLS 密码

您可以通过为 SIP 接口选择可用的最强密码来禁用弱密码。 使用此程序配置 Unified Communications Manager 支持用于建立 TLS 连接的密码。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 在**安全参数**中，配置 **TLS 密码**企业参数的值。 有关可用选项的帮助，请参阅企业参数联机帮助。

步骤 3 单击**保存**。

注释 所有 TLS 密码将根据客户端密码首选项进行协商

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。