管理证书

证书概述

您的系统使用自签证书和第三方签名证书。 证书在您系统中的设备之间使用，以安全地验证设备、加密数据，并对数据进行散列，以确保其从源到目的地的完整性。 证书允许安全传输带宽、通信以及操作。

证书最重要的部分在于您知道并定义您的数据如何加密，并与诸如预期网站、电话或 FTP 服务器等实体共享。

当您的系统信任一个证书时，意味着您的系统上有一个预安装的证书，该证书声明它完全相信它与正确的目的地共享信息。 否则，它会终止这些点之间的通信。

为了信任证书，必须已经与第三方证书颁发机构 (CA) 建立信任。

您的设备必须知道，它们可以首先信任 CA 和中间证书，然后才能信任由称为安全套接字层 (SSL) 握手的消息交换提供的服务器证书。

注释 支持基于 EC 的 Tomcat 证书。此新证书称为 tomcat-ECDSA。有关详细信息，请参阅在 *Cisco Unified Communications Manager* 上的 *IM and Presence Service* 配置和管理“IM and Presence Service 部分”的增强型 TLS 加密。

默认情况下，Tomcat 接口上的 EC 密码处于禁用状态。您可以使用 Cisco Unified Communications Manager 或 IM and Presence Service 上的 **HTTPS 密码**企业参数启用它们。如果您更改此参数，必须在所有节点上重新启动 Cisco Tomcat 服务。

有关基于 EC 的证书的详细信息，请参阅 Cisco Unified Communications Manager 和 IM and Presence Service 发行说明中的“对认证解决方案通用标准的 ECDSA 支持”。

第三方签名证书或证书链

上传为应用程序证书签名的证书颁发机构的证书颁发机构根证书。如果次级证书颁发机构为应用程序证书签名，您必须上传次级证书颁发机构的证书颁发机构根证书。您还可以上传所有证书颁发机构证书的 PKCS#7 格式的证书链。

您可以使用相同的**上传证书**对话框上传证书颁发机构根证书和应用程序证书。当上传证书颁发机构根证书或仅包含证书颁发机构证书的证书链时，选择格式为“证书类型-信任”的证书名称。当上传应用程序证书或包含应用程序证书和证书颁发机构证书的证书链时，选择仅包含证书类型的证书名称。

例如，当上传 Tomcat 证书颁发机构证书或证书颁发机构证书链时，选择 **tomcat-信任**；当上传 Tomcat 应用程序证书或包含一个应用程序证书和证书颁发机构证书的证书链时，选择 **tomcat** 或 **tomcat-ECDSA**。

当上传 CAPF 证书颁发机构根证书时，该证书会被复制到 CallManager-信任存储库中，因此您无需单独为 CallManager 上传证书颁发机构根证书。

注释 成功上传第三方证书颁发机构签名的证书，会删除最近生成的用于获取签名证书的 CSR，并且会覆盖现有证书，包括第三方签名证书（如果已上传）。

注释 系统会自动将“tomcat-信任”、“CallManager-信任”和“电话-SAST-信任”证书复制到群集中的每个节点。

注释 您可以将目录信任证书上传到 tomcat-信任，这是 DirSync 服务在安全模式下工作所必需的。

第三方证书颁发机构的证书

若要使用第三方证书颁发机构颁发的应用程序证书，您必须向证书颁发机构或 PKCS#7 证书链（可辨别编码规则 [DER]，其中包含应用程序证书和证书颁发机构的证书）获取签署的应用程序证书和证书颁发机构根证书。请检索有关向您的证书颁发机构获取这些证书的信息。证书颁发机构之间的流程各不相同。 签名算法必须使用 RSA 加密。

Cisco Unified Communications 操作系统以隐私增强邮件 (PEM) 编码格式生成 CSR。 系统接受 DER 和 PEM 编码格式的证书和 PEM 格式的 PKCS#7 证书链。 对于除证书权限代理功能 (CAPF) 之外的所有证书类型，您必须获取和上传证书颁发机构根证书和每个节点上的应用程序证书。

对于CAPF，获取并上传证书颁发机构根证书和仅在第一个节点上的应用程序证书。 CAPF 和Unified Communications ManagerCSR 中包含的扩展必须包括在向证书颁发机构申请应用程序证书的请求中。如果您的证书颁发机构不支持扩展请求机制，则您必须启用 X.509 扩展，如下所述：

- CAPF CSR 使用以下扩展：

```
X509v3 Extended Key Usage: TLS Web Server Authentication X509v3 Key Usage:
Digital Signature, Certificate Sign
```

- 适用于 Tomcat 的 CSR 和 Tomcat-ECDSA 使用以下扩展：

注释 Tomcat 或 Tomcat-ECDSA 不要求密钥协议或 IPsec 终端系统密钥用法。

```
X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client
Authentication, IPSec End System X509v3 Key Usage: Digital Signature, Key
Encipherment, Data Encipherment, Key Agreement
```

- 适用于 IPsec 的 CSR 使用以下扩展：

```
 X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client
Authentication, IPSec End System X509v3 Key Usage: Digital Signature, Key
Encipherment, Data Encipherment, Key Agreement
```

- 适用于 Unified Communications Manager 的 CSR 使用以下扩展：

```
X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client
Authentication X509v3 Key Usage: Digital Signature, Key Encipherment, Data
Encipherment, Key Agreement
```

- IM and Presence Service cup 和 cup-xmpp 证书的 CSR 使用以下扩展名：

```
X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client
Authentication, IPSec End System X509v3 Key Usage: Digital Signature, Key
Encipherment, Data Encipherment, Key Agreement,
```

注释 您可以为您的证书生成CSR并让具有SHA256签名的第三方证书颁发机构对其进行签名。然后，您可以将该签名证书上传回Unified Communications Manager，允许Tomcat和其他证书支持SHA256。

证书签名请求密钥使用情况扩展

下表显示了Unified Communications Manager和IM and Presence Service CA证书的证书签名请求(CSR)的密钥使用扩展。

***表 1: Cisco Unified Communications Manager CSR* 密钥使用扩展**

	多服务器	扩展密钥使用			密钥使用				
		服务器身份验证 **(1.3.6.1.5.5.7.3.1)**	客户端验证 **(1.3.6.1.5.5.7.3.2)**	**IP** 安全端系统 **(1.3.6.1.5.5.7.3.5)**	数字签名	密钥加密	数据加密	密钥证书签名	密钥协议
CallManager CallManager-ECDSA	Y	Y	Y		Y	Y	Y		
CAPF（仅发布方）	N	Y			Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		
TVS	N	Y	Y		Y	Y	Y		

***表 2: IM and Presence Service CSR* 密钥使用扩展**

	多服务器	扩展密钥使用			密钥使用				
		服务器身份验证 **(1.3.6.1.5.5.7.3.1)**	客户端验证 **(1.3.6.1.5.5.7.3.2)**	**IP** 安全端系统 **(1.3.6.1.5.5.7.3.5)**	数字签名	密钥加密	数据加密	密钥证书签名	密钥协议
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

注释 确保“数据加密”位未作为 CA 签名证书过程的一部分进行更改或删除。

显示证书

使用“证书列表”页上的过滤器选项，可以根据证书的通用名称、到期日期、密钥类型和使用来排序和查看证书列表。 这样，过滤选项可让您有效地对数据进行排序、查看和管理。

从 Unified Communications Manager 版本 14 中，您可以选择使用选项来排序和查看身份或信任证书列表。

过程

步骤 1 从 Cisco Unified OS 管理中，选择**安全** > **证书管理**。
“证书列表”页将会显示。

步骤 2 从**查找证书列表位置**下拉列表中，选择所需的过滤器选项，在**查找**字段中输入搜索项目，然后单击**查找**按钮。

例如，要仅查看身份证书，请从**查找证书列表位置**下拉列表中选择**使用**，在**查找**字段中输入身份，然后单击**查找**按钮。

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**。

安装中间证书

要安装中间证书，您必须首先安装根证书，然后上传签名证书。 仅当证书颁发机构在证书链中提供了签名证书及多个证书时，才需要执行此步骤。

过程

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

步骤 2 单击**上传证书 / 证书链**。

步骤 3 从**证书目的**下拉列表中选择适当的信任存储库以安装根证书。

步骤 4 输入所选证书用途的说明。

步骤 5 通过执行以下操作之一选择要上传的文件：

- 在**上传文件**文本框中，输入文件的路径。
- 单击**浏览**并导航至文件，然后单击**打开**。

步骤 6 单击**上传**。

步骤 7 安装客户证书后，使用 FQDN 访问 Cisco Unified Intelligence Center URL。 如果使用 IP 地址访问 Cisco Unified Intelligence Center，即使成功安装了自定义证书，您也会看到消息“单击此处以继续”。

注释
- 上传 Tomcat 证书时，应重新启动 TFTP 服务。 否则 TFTP 会继续提供缓存的旧自签 tomcat 证书。
- 从电话边缘信任库上传证书的操作应由发布方完成。

删除信任证书

信任的证书是您可以删除的唯一一种证书类型。 您无法删除由您的系统生成的自签证书。

⚠

注意 删除证书可能会影响您的系统操作。 如果证书是现有证书链的一部分，也可能会破坏证书链。 通过**证书列表**窗口中相关证书的用户名和主题名称来验证此关系。 您无法撤销此操作。

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 使用**查找**控件过滤证书列表。

步骤 3 选择证书的文件名。

步骤 4 单击**删除**。

步骤 5 单击**确定**。

注释

- 如果您删除 “CAPF-trust”、“tomcat-trust”、“CallManager-trust” 或 “Phone-SAST-trust” 证书类型，证书将跨群集中的所有服务器删除。
- 从电话边缘信任库删除证书的操作应由发布方完成。
- 如果您将证书导入到CAPF-trust中，它将仅在该特定节点上启用，并且不会跨群集复制。

重新生成证书

建议您在证书到期之前重新生成证书。 当证书即将到期时，您将在 RTMT（系统日志查看器）和电子邮件通知中收到警告。

不过，您也可以重新生成过期的证书。 在下班时间执行此任务，因为您必须重新启动电话并重启服务。 您只能重新生成在 Cisco Unified 操作系统管理中被列为“cert”类型的证书。

注意 重新生成证书可能影响您的系统操作。 重新生成证书会覆盖现有证书，包括第三方签名证书（如果已上传）。

过程

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

输入搜索参数以查找证书并查看其配置详细信息。 系统会在**证书列表**窗口中显示与所有条件匹配的记录。

单击证书详细信息页面中的**重新生成**按钮，此时将会重新生成具有相同密钥长度的自签证书。

注释 重新生成证书时，**证书说明**字段将不会更新，直到您关闭**重新生成**窗口并打开新生成的证书。

单击**生成自签证书**以重新生成密钥长度为 3072 或 4096 的自签证书。

步骤 2 配置**生成新的自签名证书**窗口中的字段。 有关这些字段及其配置选项的更多信息，请参阅联机帮助。

步骤 3 单击**生成**。

步骤 4 重新启动受重新生成的证书影响的所有服务。 有关详细信息，请参阅证书名称和说明，第 8 页。

步骤 5 重新生成 CAPF、ITLRecovery 证书或 CallManager 证书之后，更新 CTL 文件（如配置有）。

注释 重新生成证书后，您必须执行系统备份，以使最新备份包含重新生成的证书。 如果您的备份不包含重新生成的证书，而您要执行系统恢复任务，则您必须手动解锁系统中的每部电话，以使电话可以注册。

重要事项 在重新生成/续订 CallManager、CAPF 和 TVS 证书后，电话将自动重设以接收更新的 ITL 文件。

证书名称和说明

下表说明您可以重新生成的系统安全证书，以及必须重新启动的相关服务。有关重新生成 TFTP 证书的信息，请参阅《*Cisco Unified Communications Manager* 安全指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

表 *3:* 证书名称和说明

名称	说明	相关服务
tomcat tomcat-ECDSA	此证书由 WebServices、Cisco DRF 服务和 Cisco CallManager 服务在 SIP Oauth 模式启用时使用。	Cisco Tomcat 服务、CallManager 服务。
CallManager CallManager-ECDSA	此功能用于 SIP、SIP 干线、SCCP、TFTP 等。	CallManager - 不可用 CallManager-ECDSA CallManager 服务
CAPF	由运行在 Unified Communications Manager 发布方上的 CAPF 服务使用。此证书用于颁发 LSC 到终端（在线和离线 CAPF 模式除外）	不适用
TVS	此功能由信任验证服务使用，可用作电话在服务器证书更改时的辅助信任验证机制。	不适用

注释 在“安全参数”部分的“证书更新”下，引入了新的企业参数“电话相互作用”，用于在 TVS、CAPF 或 TFTP 证书中的任意一个更新时手动或自动重置电话。此参数默认设置为自动重置电话。

重新生成 OAuth 刷新登录的密钥

使用此程序以使用命令行界面重新生成加密密钥和签名密钥。 仅当 Cisco Jabber 用来在 Unified Communications Manager 中进行 OAuth 验证的加密密钥或签名密钥已经被入侵时，才完成此任务。签名密钥是一种不对称密钥，基于 RSA，而加密秘钥是一种对称密钥。

完成此任务后，使用这些秘钥的当前访问和刷新令牌将失效。

我们建议您在非高峰时段完成此任务，以将对最终用户的影响降至最低。

加密密钥仅可通过下面的 CLI 重新生成，但您也可以使用发布方的 Cisco Unified 操作系统管理 GUI 重新生成签名密钥。 选择**安全** > **证书管理**，然后选择 **AUTHZ** 证书，并单击**重新生成**。

过程

步骤 1 从 Unified Communications Manager 发布方节点登录到**命令行**界面。

步骤 2 如果想要重新生成加密密钥：

a) 运行 `set key regen authz encryption` 命令。

b) 输入 `yes`。

步骤 3 如果想要重新生成签名密钥：

a) 运行 `set key regen authz signing` 命令。

b) 输入 `yes`。
Unified Communications Manager 发布方节点会重新生成密钥并将新密钥复制到所有 Unified Communications Manager 群集节点，包括任何本地 IM and Presence Service 节点。

您必须重新生成新密钥并在所有 UC 群集上同步：

- IM and Presence 中心群集 — 如果您有一个 IM and Presence 集中式部署，您的 IM and Presence 节点会运行在与您的电话分离的群集上。 在这种情况下，在 IM and Presence Service 中心群集的 Unified Communications Manager 发布方节点上重复此程序。
- Cisco Expressway 或 Cisco Unity Connection — 同样在那些群集上重新生成秘钥。 有关详细信息，请参阅您的 Cisco Expressway 和 Cisco Unity Connection 文档。

注释 重新分配密钥后，在群集中的所有节点上重新启动 Cisco CallManager 服务。

上传证书或证书链

上传您希望您的系统信任的任何新证书或证书链。

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**证书目的**下拉列表中选择证书名称。

步骤 4 通过执行以下操作之一选择要上传的文件：

- 在**上传文件**文本框中，输入文件的路径。
- 单击**浏览**，导航至文件，然后单击**打开**。

步骤 5 要将文件上传到服务器，请单击**上传文件**。

注释　上传证书后，重新启动受影响的服务。 当服务器恢复时，您可以访问 CCMAdmin 或 CCMUser GUI，检验是否在使用您新添加的证书。

管理第三方证书颁发机构的证书

此任务流程提供第三方证书流程的概述，以及对序列中每个步骤的参考。 您的系统支持由第三方证书颁发机构使用 PKCS # 10 证书签名请求 (CSR) 签发的证书。

过程

	命令或操作	目的
步骤 1	生成证书签名请求， 第 11 页	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。
步骤 2	下载证书签名请求， 第 11 页	下载所生成的 CSR 并准备好将其提交给您的证书颁发机构。
步骤 3	请参阅您的证书颁发机构文档。	向您的证书颁发机构获取应用程序证书。
步骤 4	请参阅您的证书颁发机构文档。	向您的证书颁发机构获取根证书。
步骤 5	将证书颁发机构签名的 CAPF 根证书添加到信任存储库 ， 第 11 页	将根证书添加到信任存储库中。当使用证书颁发机构签名的 CAPF 证书时，请执行此步骤。
步骤 6	上传证书或证书链， 第 9 页	将证书颁发机构根证书上传到节点。
步骤 7	如果您更新了 CAPF 或 Cisco Unified Communications Manager 的证书，请生成新的 CTL 文件。	请参阅《*Cisco Unified Communications Manager* 安全指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。 上传第三方签名的 CAPF 或 CallManager 证书之后，重新运行 CTL 客户端（如配置有）。
步骤 8	重新启动服务， 第 12 页	重新启动受新证书影响的服务。对于所有证书类型，重新启动相应的服务（例如，如果您更新了 Tomcat 或 Tomcat-ECDSA 证书，则重新启动 Cisco Tomcat 服务）。

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**。

将证书颁发机构签名的 CAPF 根证书添加到信任存储库

当使用证书颁发机构签名的 CAPF 证书时，请将根证书添加到 Unified Communications Manager 信任存储库。

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 在**上传证书/证书链**弹出窗口中，从**证书用途**下拉列表中选择 **CallManager-trust** 并浏览至证书颁发机构签名的 CAPF 根证书。

步骤 4 证书出现在**上传文件**字段中后，单击**上传**。

重新启动服务

如果您的系统需要您在群集中的特定节点上重新启动任何功能或网络服务，请使用此程序。

过程

步骤 1 根据您要重新启动的服务类型，执行以下任务之一：

- 选择**工具** > **控制中心 - 功能服务**。
- 选择**工具** > **控制中心 - 网络服务**。

步骤 2 从**服务器**下拉列表中选择您的系统节点，然后单击**前往**。

步骤 3 单击要重新启动的服务旁边的单选按钮，然后单击**重新启动**。

步骤 4 看到重新启动需要一些时间的消息之后，单击**确定**。

通过在线证书状态协议吊销证书

Unified Communications Manager 预配置了用于监控证书吊销的 OCSP。 系统将检查证书状态以确认在预定时间间隔的有效性，并且每次都有上传的证书。

在线证书状态协议 (OCSP) 可帮助管理员管理其系统的证书要求。 OCSP 配置后，它将提供简单、安全和自动的方法来检查证书的有效性并实时吊销过期的证书。

对于启用 Common Criteria 模式的 FIPS 部署，OCSP 还可帮助确保您的系统符合 Common Criteria 要求。

验证检查

Unified Communications Manager 会检查证书状态并确认有效性。

证书按以下方式进行验证：

- Unified Communications Manager 使用委托的信任模型 (DTM) 并检查根 CA 或中间 CA 的 OCSP 签名属性。 根 CA 或中间 CA 必须对 OCSP 证书签名，才能检查状态。 如果委托的信任模型失败，Unified Communications Manager 会退回到信任响应者模型 (TRP)，并使用来自 OCSP 服务器的指定 OCSP 响应签名证书来验证证书。

注释 OCSP 响应器必须运行以检查证书的吊销状态。

- 在**证书吊销**窗口中启用 OCSP 选项，以提供最安全的方式实时检查证书吊销。 从选项中选择以使用来自证书或者所配置 OCSP URI 的 OCSP URI。 有关手动 OCSP 配置的详细信息，请参阅配置通过 OCSP 吊销证书。

注释 对于叶证书，TLS 客户端（例如 syslog、FileBeat、SIP、ILS、LBM 等）会将 OCSP 请求发送到 OCSP 响应器，并从 OCSP 响应器实时接收证书吊销响应。

执行验证并且 Common Criteria 模式设为“开”后，系统将为证书返回以下状态之一。

- **良好**--状态为**良好**表示对状态查询的响应积极。 此积极响应至少表示证书未被吊销，但不一定意味着证书曾被颁发，或者响应的生成时间在证书的有效期内。 响应分机可用于传达响应器就证书状态所做的断言的其他信息，例如关于发行、有效期等的肯定声明。
- **已吊销**--状态为**已吊销**表示证书已被吊销（永久或临时（保留））。
- **未知**--状态为**未知**表示 OCSP 响应器不知道所请求的证书。

注释 在 Common Criteria 模式下，如果状态为**已吊销**和**未知**，连接将失败；未启用 Common Criteria 时，如果状态为**未知**，连接将成功。

证书监控任务流程

完成以下任务可将系统配置为自动监控证书状态和到期时间。

- 证书即将到期时通过电子邮件通知您。
- 吊销到期的证书。

过程

	命令或操作	目的
步骤 1	配置证书监控通知 ， 第 14 页	配置自动证书监控。 当证书即将到期时，系统会定期检查证书状态并向您发送电子邮件。
步骤 2	配置通过 OCSP 吊销证书 ， 第 14 页	配置OCSP，以便系统自动吊销到期的证书。

配置证书监控通知

为 Unified Communications Manager 或 IM and Presence Service 配置自动证书监控。 当证书即将到期时，系统会定期检查证书状态并向您发送电子邮件。

注释 **Cisco 证书到期监控**网络服务必须运行。 此服务默认启用，但您也可以在 Cisco Unified 功能配置中手动确认该服务是否在运行，方法是选择**工具 > 控制中心 - 网络服务**，然后验证 **Cisco 证书到期监控服务**状态是否是**正在运行**。

过程

步骤 1 登录到 Cisco Unified 操作系统管理（适用于 Unified Communications Manager 证书监控）或 Cisco Unified IM and Presence 管理（适用于 IM and Presence Service 证书监控）。

步骤 2 选择**安全性 > 证书监控**。

步骤 3 在**通知开始时间**字段中输入一个数值。 此值表示证书到期前系统开始通知您即将到期的天数。

步骤 4 在**通知频率**字段中，输入通知的频率。

步骤 5 可选。 选中**启用电子邮件通知**复选框以让系统发送证书即将到期的电子邮件通知。

步骤 6 选中**启用 LSC 监控**复选框以在证书状态检查种包含 LSC 证书。

步骤 7 在**电子邮件 ID** 字段中，输入您希望系统将通知发送到的电子邮件地址。 您可以输入多个电子邮件地址，用分号分隔。

步骤 8 单击**保存**。

注释 默认情况下，证书监控服务每 24 小时运行一次。 当重新启动证书监控服务时，它将启动服务，然后计算下一个计划，仅在 24 个小时后运行。 即使证书接近七天的到期日期，间隔也不会改变。 当证书已经过期或将在一天内过期时，服务会每 1 小时运行一次。

下一步做什么

配置在线证书状态协议 (OCSP)，以便系统自动吊销到期的证书。 有关详细信息，请参阅配置通过 OCSP 吊销证书，第 14 页

配置通过 OCSP 吊销证书

启用在线证书状态协议 (OCSP) 定期检查证书状态并自动吊销到期的证书。

开始之前

确保您的系统具有是 OCSP 检查所需的证书。 您可以使用通过 OCSP 响应属性配置的根证书或中间 CA 证书，也可以使用已上传到 tomcat-trust 的指定 OCSP 签名证书。

过程

步骤 1 登录到 Cisco Unified 操作系统管理（适用于 Unified Communications Manager 证书吊销）或 Cisco Unified IM and Presence 管理（适用于 IM and Presence Service 证书吊销）。

步骤 2 选择**安全性** > **证书吊销**。

步骤 3 选中**启用 OCSP** 复选框，然后执行以下任务之一：

- 如果要为 OCSP 检查指定 OCSP 响应器，选择**使用配置的 OCSP URI** 按键并在 **OCSP 配置的 URI** 字段中输入响应器的 URI。
- 如果采用 OCSP 响应器 URI 配置证书，选择**使用来自证书的 OCSP URI** 按键。

步骤 4 选中**启用吊销检查**复选框。

步骤 5 使用吊销检查的间隔时间填写**检查间隔**字段。

步骤 6 单击**保存**。

步骤 7 可选。 如果您有 CTI、IPsec 或 LDAP 链接，除上述步骤之外，还必须完成以下操作，以便为这些长期连接启用 OCSP 吊销支持：

a) 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。
b) 在**证书撤消和过期**下，将**证书有效性检查**参数设置为**真**。
c) 配置**有效性检查频率**参数的值。

注释 **证书吊销**窗口中**启用吊销检查**参数的时间间隔值优先于**有效性检查频率**企业参数的值。

d) 单击**保存**。

对证书错误进行故障诊断

开始之前

如果您在尝试从 IM and Presence Service 节点或来自 Unified Communications Manager 节点的 IM and Presence Service 功能访问 Unified Communications Manager 服务时遇到错误，问题的根源在于 tomcat-trust 证书。 错误消息 `Connection to the Server cannot be established (unable to connect to Remote Node)`（无法建立与服务器的连接（无法连接到远程节点））出现在以下功能配置界面窗口中：

- **服务激活**
- **控制中心 - 功能服务**
- **控制中心 - 网络服务**

使用此程序帮助您解决证书错误。从第一个步骤开始，如有必要，继续后面的步骤。有时，您可能只需要完成第一个步骤便可解决错误；有时则必须完成所有步骤。

过程

步骤 1 从 Cisco Unified 操作系统管理中，确认存在必需的 tomcat-信任证书：**安全** > **证书管理**。

如果所需的证书不存在，请等待 30 分钟，然后再次检查。

步骤 2 选择要查看其信息的证书。 确认内容与远程节点上的相应证书匹配。

步骤 3 从 CLI 中，重新启动 Cisco 群集间同步代理服务：**utils service restart Cisco Intercluster Sync Agent**。

步骤 4 Cisco 群集间同步代理服务重新启动后，重新启动 Cisco Tomcat 服务：**utils service restart Cisco Tomcat**。

步骤 5 等待 30 分钟。 如果前面的步骤不能解决证书错误，而 tomcat-信任证书存在，请删除该证书。 删除证书后，您必须通过以下方法手动交换证书：下载用于每个节点的 Tomcat 和 Tomcat-ECDSA 证书并将其作为 tomcat 信任证书上传到其对等机。

步骤 6 证书交换完成后，重新启动每台受影响服务器上的 Cisco Tomcat：**utils service restart Cisco Tomcat**。

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。