Expressway证书故障排除

目录

简介

本文档介绍证书的工作方式以及Expressway服务器中证书的最常见问题和提示。

先决条件

要求

Cisco 建议您了解以下主题：

- Expressway和视频通信服务器(VCS)服务器
- 安全套接字层(SSL)
- 证书
- 网真设备
- 移动和远程访问
- 协作部署

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Expressway x14

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

SSL和证书是标准，在其他设备和品牌间使用相同。本文档重点介绍Expressway中的证书用途。

定义

证书用于在两台设备之间创建安全连接。它们是验证服务器或设备身份的数字签名。某些协议(如安全超文本传输协议(HTTPS)或会话发起协议(SIP)传输层安全(TLS))需要使用证书才能正常工作。

谈论证书时使用的不同术语：

- 证书签名请求(CSR)：使用标识设备的名称创建的模板，以便稍后签名并转换为客户端或服务器证书
- 证书：已签名的CSR。这些是身份的一种类型，安装在设备上用于SSL协商。它们可以由自己或证书颁发机构签名。
- 证书签名：验证相关证书合法性的身份；这些证书以其他证书的形式显示。
- 自签名证书：由自己签名的客户端或服务器证书
- 证书颁发机构(CA)：签署证书的实体
    - 中间证书：CA证书不是由自身签名，而是由另一个CA证书签名，通常由根证书签名，但也可以由另一个中间证书签名
    - 根证书：由自身签名的CA证书

基本原则

当客户端与服务器对话并开始SSL会话时，它们会交换证书，稍后会使用这些证书来加密设备之间的流量。在交换过程中，设备还会确定证书是否受信任。必须满足多个条件才能确定证书是否受信任，其中一些条件为：

- 最初用于联系服务器的完全限定域名(FQDN)与服务器提供的证书内部的名称匹配。
    - 例如，当您在浏览器上打开网页时，cisco.com解析了提供证书的服务器的IP，该服务器必须包含cisco.com作为名称才能受信任。

- 对服务器提供的服务器证书（或自签名时的同一服务器证书）签名的CA证书存在于设备的CA受信任证书列表中。
    - 设备具有受信任的CA证书列表，计算机通常包含具有已知公共证书颁发机构的预建列表。

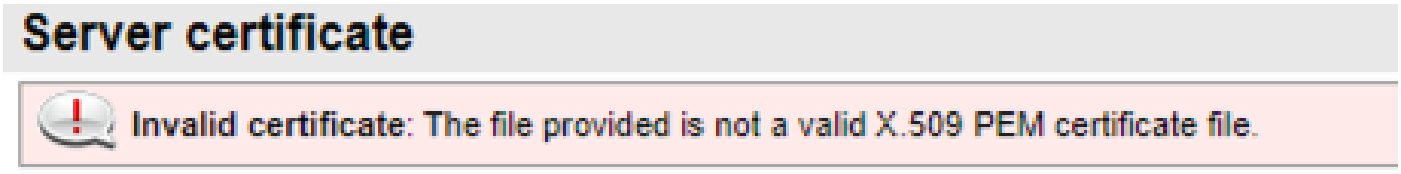
- 当前日期和时间在证书的有效期限内。
    - 证书颁发机构仅在设定的时间内签署CSR，这由CA确定。

- 证书未吊销。
    - 公共证书颁发机构通常在证书中包含证书撤销列表URL。这样，接收证书的参与方可以确认该证书未被CA撤销。

常见问题

Expressway证书上传失败

导致此问题的原因有两个。它们会导致不同的描述性错误。



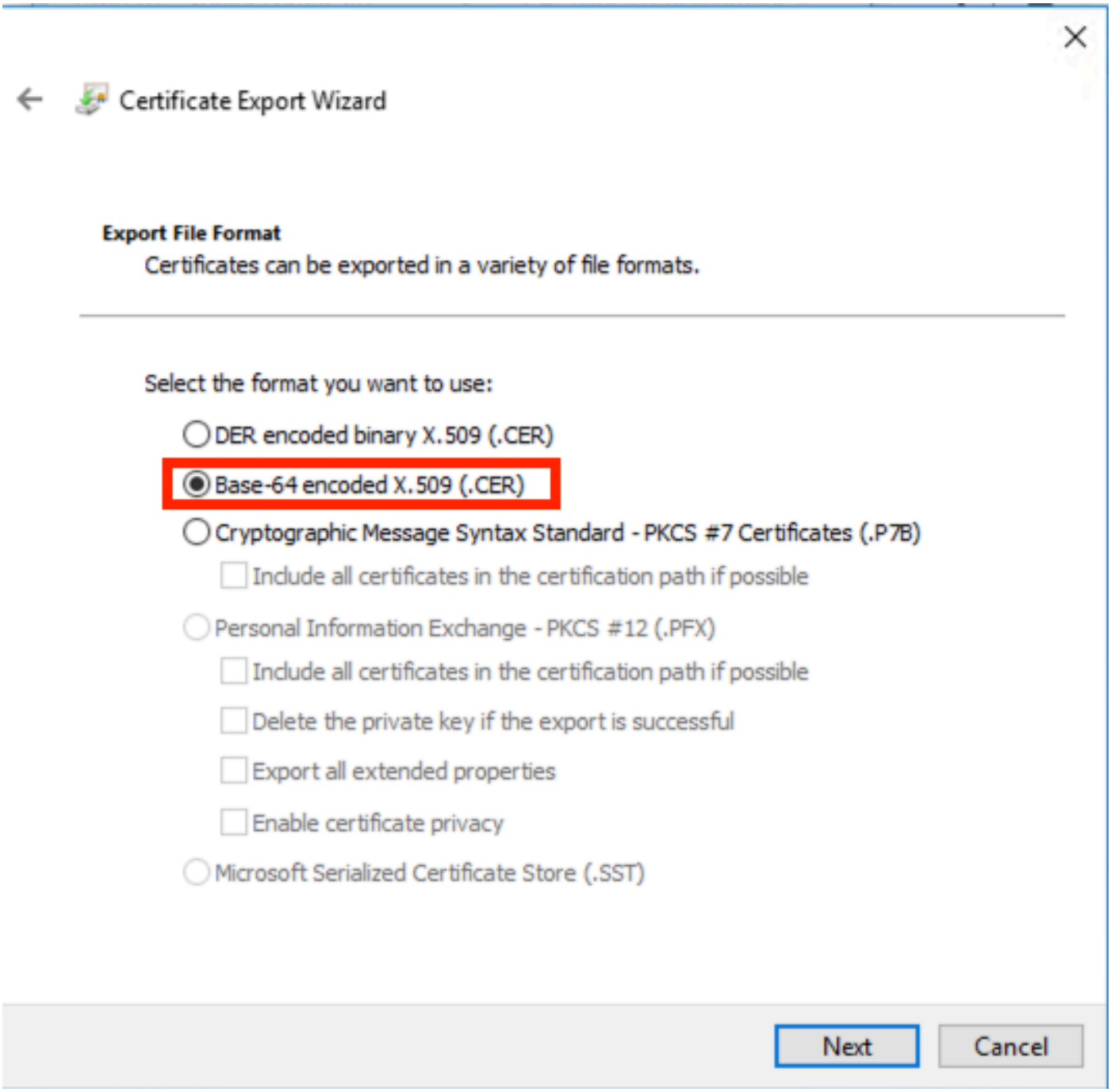
证书格式无效

当证书的格式无效时，会发生第一个错误。文件扩展名并不重要。

如果证书未打开，可以从CA以正确的格式请求新证书

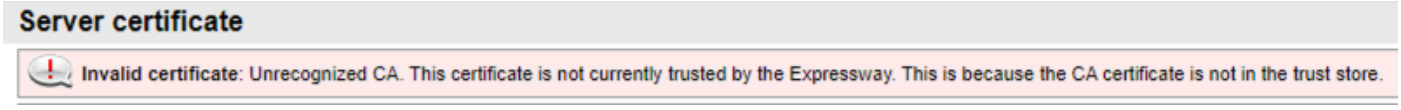
如果证书打开，请执行以下步骤：

步骤1:打开证书并导航到Details选项卡。
第二步：选择复制到文件。
第三步：按照向导操作，确保已选择Base-64 encoded。



证书格式选择

第四步：保存后，将新文件上传到Expressway。



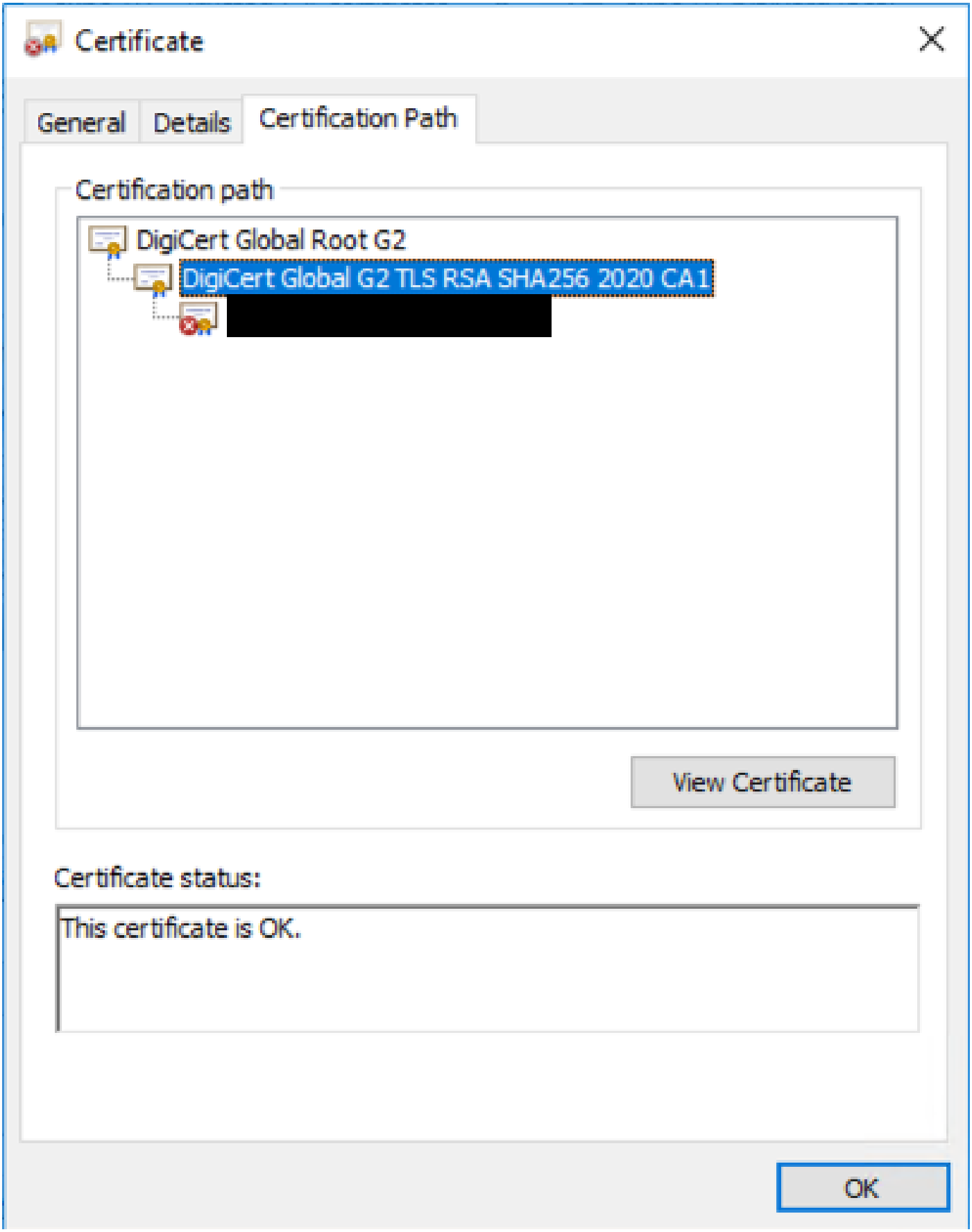
不受信任的CA证书链

当签署服务器证书的CA证书不受信任时会发生此错误。在上传服务器证书之前，服务器必须信任链中的所有CA证书。

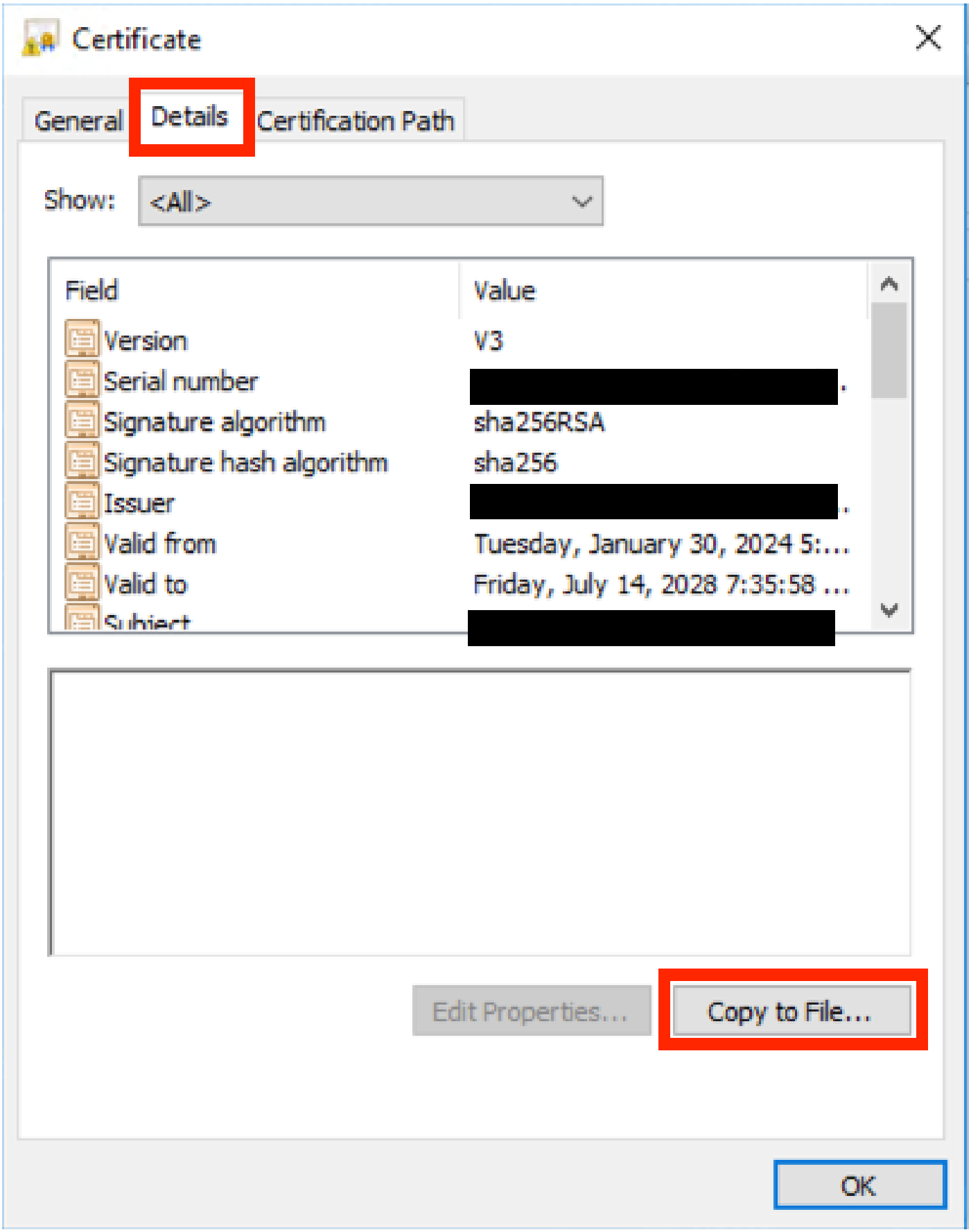
通常，CA会提供CA证书以及已签名的服务器证书。如果可用，请跳至下面的步骤6。

如果CA证书不可用，可从服务器证书获取这些证书。执行下列步骤：

步骤1:打开服务器证书。
第二步：导航到Certification Path选项卡。排名靠前的证书被视为根CA证书。底部一个是服务器证书，中间的所有证书都被视为中间CA证书。
第三步：选择CA证书并选择查看证书。



第四步：导航到Details选项卡，然后按照前面的步骤将证书保存到单独的文件中。
第五步：对存在的所有CA证书重复这些步骤。



证书详细信息选项卡

所有CA证书可用后，将其上传到Expressway Trusted CA Certificate列表：

第六步：在Expressway服务器上导航到维护>安全>受信任CA证书。

步骤 7.选择Choose File并上传。
步骤 8对每个CA证书重复步骤7。
步骤 9在信任列表中上传所有CA证书后，在服务器上上传服务器证书。

遍历区域关闭，错误为TLS协商错误

当Expressway-C和Expressway-E之间的SSL交换未成功完成时，会发生此错误。导致此问题的几个示例：

- 主机名与提供的证书中的名称不匹配。
  - 确保Expressway-C遍历区域上配置的对等体地址至少与Expressway-E服务器证书上的其中一个名称匹配
- TLS验证名称与提供的证书中的名称不匹配。
  - 确保在Expressway-E遍历区域上配置的TLS验证名称与Expressway-C服务器证书上的某个名称匹配。如果是集群配置，建议将Expressway-C集群FQDN配置为TLS。验证该名称，因为此名称必须存在于群集的所有节点上。
- 服务器不信任CA证书
  - 正如每台服务器在上传服务器证书之前必须信任自己的CA证书一样，其它服务器也必须信任这些CA证书才能信任服务器证书。为此，请确保来自两个Expressway服务器的证书路径的所有CA证书都存在于所有相关服务器的受信任CA列表中。CA证书可通过本文档前面提供的步骤提取。

证书续订后，遍历区域打开，但SSH隧道关闭

SSH隧道故障

当一个或多个中间CA证书不受信任、根CA证书信任启用穿越区域连接时，通常会在证书续订后发生此错误，但SSH隧道是更详细的连接，当整个链不受信任时可能会失败，中间CA证书经常由证书颁发机构更改，因此证书的续订可能会触发此问题。确保所有中间CA证书都上传到所有Expressway信任列表。

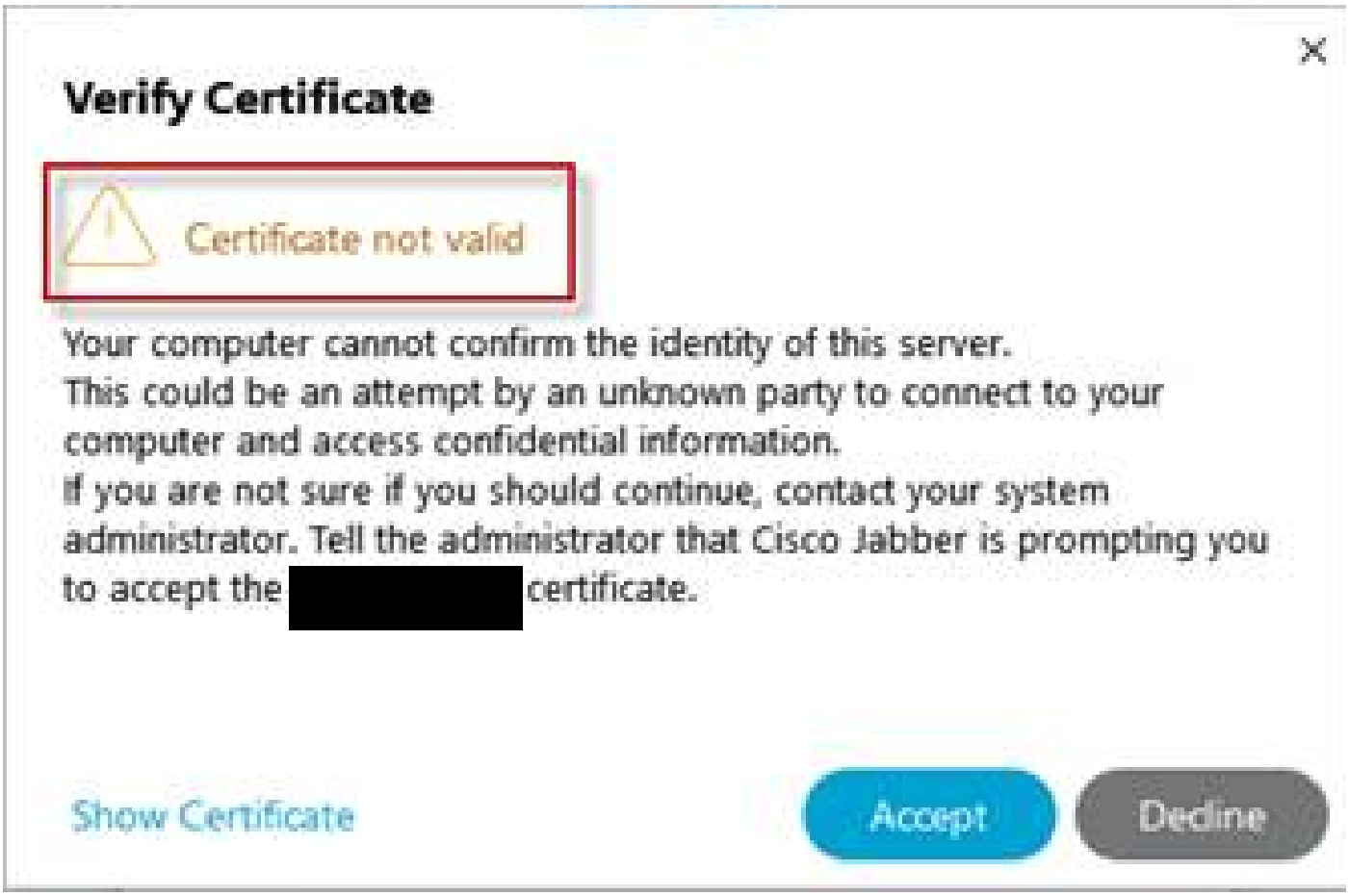
升级或证书续订后，移动和远程访问登录失败

登录可能会因证书原因而失败，但在Expressway软件的较新版本中，由于安全原因，已实施了一些软件更改，这些更改会强制进行以前未执行的证书验证。

此处对此有更好的解释：流量服务器实施证书验证

如解决方法所述，确保Expressway-C CA证书作为tomcat-trust和callmanager-trust上传到Cisco Unified Communications Manager上，然后重新启动所需的服务。

移动和远程访问登录时Jabber上的证书警报



Jabber不可信证书警告

当应用程序上使用的域与Expressway E服务器证书上的主题备用名称不匹配时，会发生此行为。确保example .com或备用collab-edge.example .com是证书上存在的主题备用名称之一。

相关信息

思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。