了解移动和远程访问证书要求和ATS历史记录

目录

简介

本文档介绍CUCM上用于移动和远程访问的证书上传要求。

背景信息

Cisco Expressway使用Apache Traffic Server(ATS)。流量服务器是遍历解决方案中非常重要的组件，主要用于以下功能：

- 证书验证：它对Cisco Unified Communications Manager(CUCM)、IM & Presence和Unity服务器节点执行MRA服务的证书验证。
- 代理和缓存：它充当HTTP/HTTPS流量的快速、可扩展缓存代理服务器。

在Expressway版本14.0.2上

流量服务器(ATS)在MRA调配期间与CUCM通信时，会开始看到轻微的“证书验证”实施。

要求记录在CSCvz45074下，其中签署Expressway核心服务器证书的根证书必须作为Tomcat-Trust和Callmanager Trust上载到CUCM:https://cdetsng.cisco.com/summary/#/defect/CSCvz45074。

- 流量服务器实施证书验证。
- 升级到X14.0.2版本之前，请确保满足此证书要求。

要求 — 必须向CUCM的tomcat-trust和CallManager-trust列表中添加签署Expressway-C证书的证书颁发机构(CA)链（根+中介），即使Unified Communications Manager(UCM)处于非安全模式。

原因 — 每当服务器UCM请求证书时，Expressway中的流量服务器服务都会发送其证书。这些请求适用于除8443之外的端口（例如，端口6971、6972等）上运行的服务。 即使UCM处于非安全模式

，这也会执行证书验证。有关详细信息，请参阅通过Expressway进行移动和远程访问部署指南。

早于14.0.8版本的行为

处理Expressway-C和统一通信节点之间的安全HTTPS双向连接的Expressway-C上的流量服务器未验证远程端提供的证书。在MRA配置下，如果在Configuration > Unified Communications > Unified CM servers/IM and Presence Service nodes/Unity Connection servers下添加了CUCM、IM&P或Unity服务器，则可以通过将TLS验证模式配置为“On”来进行TLS证书验证。配置选项显示在下一个屏幕截图中，表示它验证了SAN中的FQDN或IP、证书的有效性以及证书是否由受信任CA签名。

还存在一个已知问题，无法在Expressway信任存储上加载两个具有相同CN名称的证书。此限制导致两个问题：

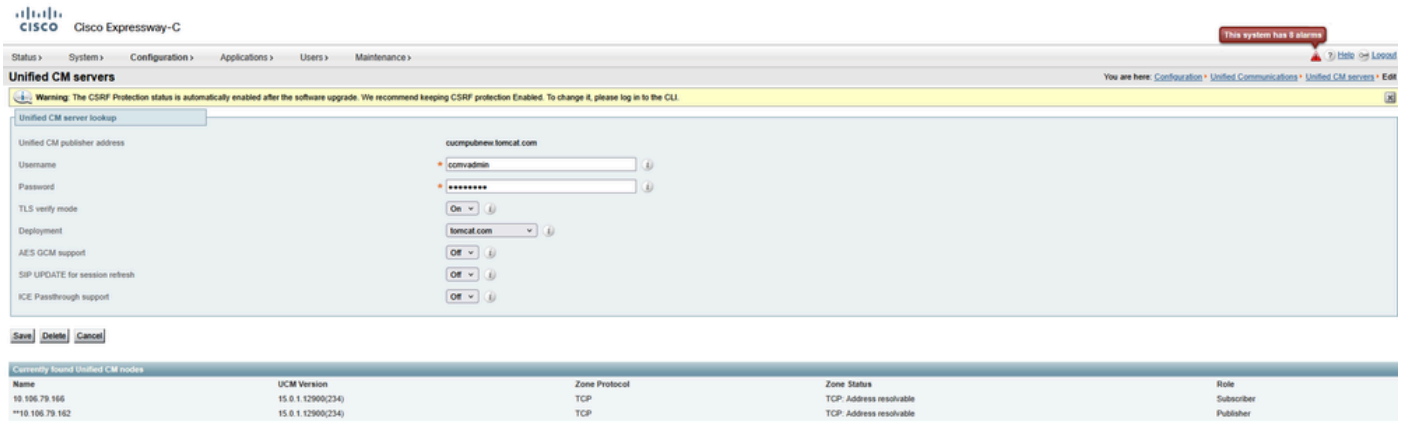
1.如果选择在Expressway信任存储上加载呼叫管理器证书，则添加CUCM时，TLS验证“打开”将失败。

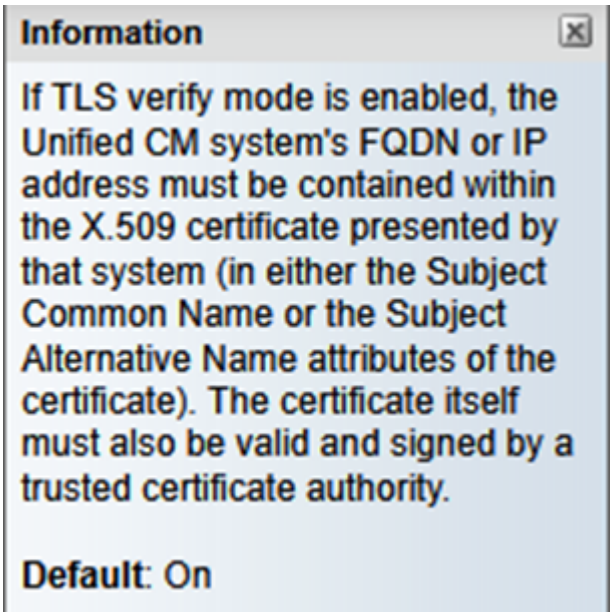
2:如果选择在Expressway信任存储上加载Tomcat证书，则5061上的安全SIP注册将失败。

此行为记录在CSCwa12894中。

此外，此TLS证书验证检查仅在发现CUCM/IM&P/Unity服务器时完成，而不是在MRA客户端调配期间完成。

此配置的缺点是它仅验证您添加的发布者地址。它不会验证订用服务器节点上的证书是否设置正确，因为它从发布服务器节点的数据库中检索订用服务器节点信息（FQDN或IP）。





版本14.0.8及更高版本上的行为

从X14.0.8版本开始，Expressway服务器对通过流量服务器发出的每个HTTPS请求执行TLS证书验证。这意味着，在发现CUCM/IM&P/Unity节点期间，当TLS验证模式设置为“关闭”时，它也会执行此操作。如果验证失败，则TLS握手不会完成，并且请求失败，这可能导致功能丢失，例如冗余、故障切换问题或完全登录失败。此外，当TLS验证模式设置为“打开”时，它并不保证所有连接都能正常运行（如后面的示例所述）。

Expressway向CUCM/IM&P/Unity节点检查的确切证书如MRA指南部分所示。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-0/mra/exwy_b_mra-deployment-guide-x150.pdf

部分

Certificate Requirements > Certificate Exchange Requirements

由于Expressway-Core和CUCM之间的通信方式发生了这些变化，必须确保：

1.建议将CA签名的证书用于移动和远程访问。

2.每个Unified CM集群必须信任Expressway-C证书。对于每个群集，请确保：

- 如果启用混合模式 — 必须将Expressway-C证书安装到Unified CM上的CallManager-trust和Tomcat-trust存储区。
- 如果禁用混合模式 — 必须将Expressway-C证书签名的根CA证书安装到Unified CM上的CallManager-trust和Tomcat-trust存储区。然后，重新启动以下内容：· Tomcat服务· CallManager服务· HA代理服务（如果在Tomcat上使用TLS）。

在Expressway — 核心上，确保采取以下措施：

- Expressway-C必须信任每个Unified CM和IM and Presence服务集群提供的证书。

Expressway-C的信任存储必须包括根CA证书，用于签署所有UC集群的Unified CM和IM and Presence Service证书。

注意：确保将所有用于签署Expressway-C证书的根和中间CA证书或完整CA链添加到Cisco Unified Communications Manager(UCM)的Tomcat-trust和CallManager-trust列表中，即使UCM在非安全模式下运行。

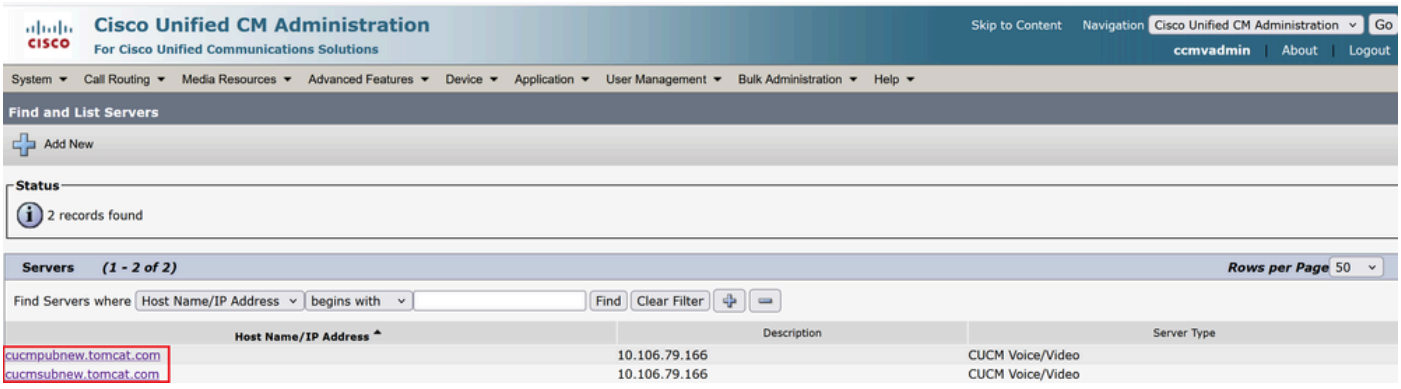
原因 — 每当服务器(UCM)请求证书时，Expressway中的流量服务器服务就会发送其证书。这些请求适用于除8443之外的端口（例如，端口6971、6972等）上运行的服务。 即使UCM处于非安全模式，这也会执行证书验证。

在System > Server下添加CUCM地址的方式在Configuration > Unified Communications > Unified CM servers/IM and Presence Service nodes下添加Expressway核心上的CUCM/IMP时起着非常重要的作用。

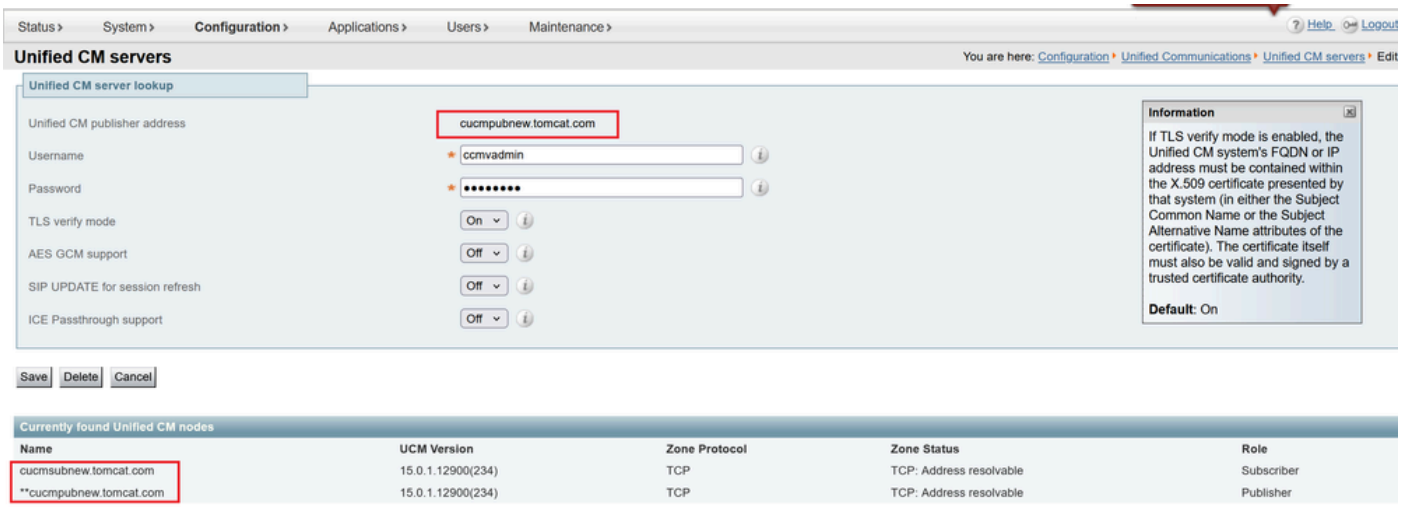
必须始终使用FQDN添加CUCM，而不是主机名或IP地址。如果发现在System > Server下添加了CUCM作为主机名/IP地址

在TLS握手期间，TLS验证“打开”将失败，并且不会在Expressway-Core上添加CUCM集群。

此图显示添加为主机名的CUCM:



此图显示使用TLS验证模式=打开(ON)的FQDN在Expressway-Core上添加的CUCM:

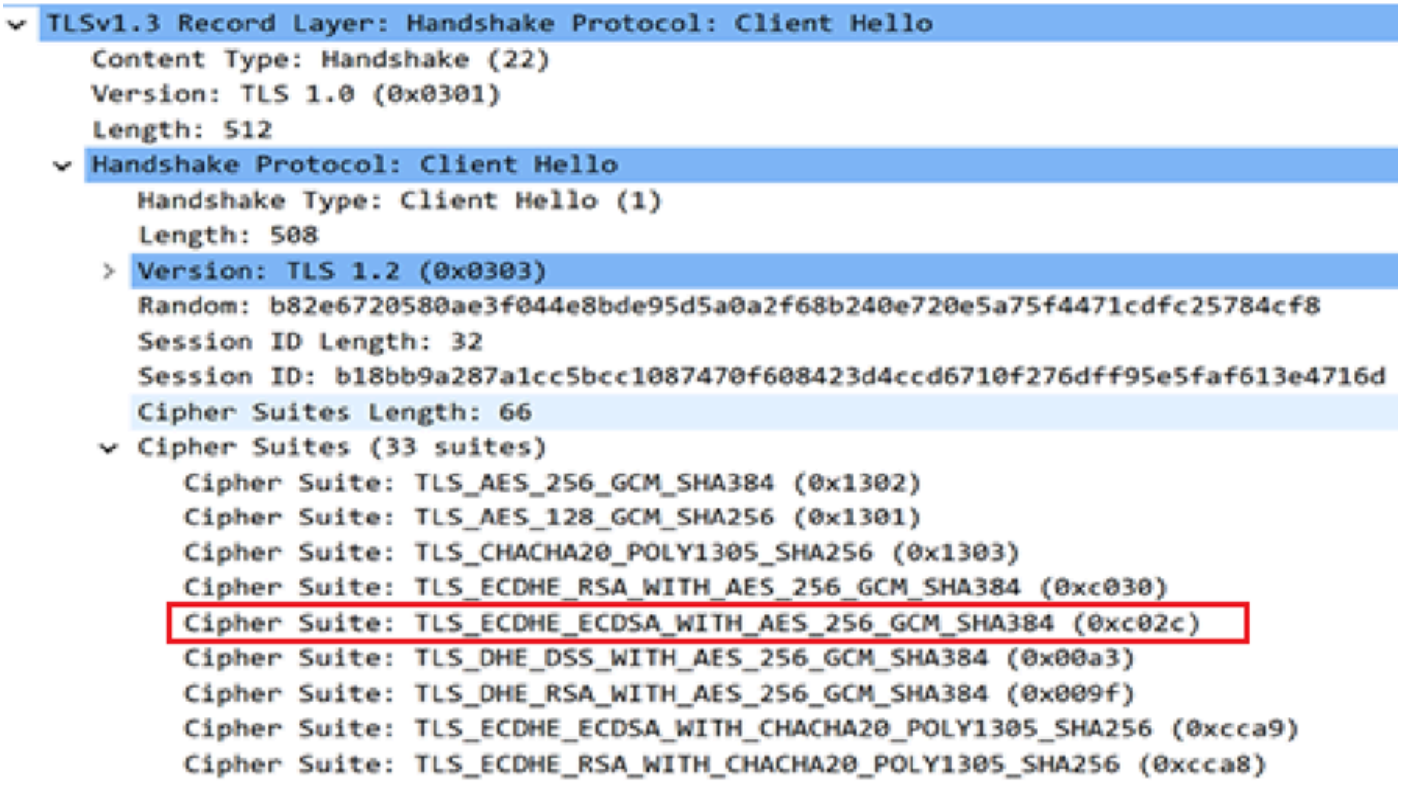


X14.2中还引入了一个更改，该更改将在TLS握手（客户端呼叫）期间以不同的首选顺序显示密码。这取决于升级路径，并且在软件升级后导致意外的TLS连接。可能是，在TLS握手期间升级之前，它请求从CUCM获取Cisco Tomcat或Cisco CallManager证书。但是，升级后，它请求ECDSA变体（比RSA更安全的密码变体）。 Cisco Tomcat-ECDSA或Cisco CallManager-ECDSA证书可以由其他CA签名，也可以仅由自签名证书签名（默认）。

此密码首选项顺序更改并非始终与您相关，因为它取决于Expressway X14.2.1版本说明中所示的升级路径。简而言之，您可以从Maintenance > Security > Ciphers中查看每个密码列表是否预置了ECDHE-RSA-AES256-GCM-SHA384。如果没有，则它首选更新的ECDSA密码而不是RSA密码。如果是，则您有与前面一样的行为，其中RSA具有更高的优先级。

下一个屏幕截图显示在客户端Hello中TLS协商消息期间Expressway核心通告的ECDSA加密中，#IF TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384由远程响应器(CUCM)在服务器Hello中选择，那么TLS协商将在以下情况下失败：

ROOT CA证书或来自响应器的实际ECDSA证书，即在这种情况下，CUCM未安装在Expressway信任存储上。



或者，您也可以修改Expressway密码，以便ECDSA不优先。

1.通过附加GCM-Sha384开放式SSL字符串修改SIP密码。

"ECDHE-RSA-AES256-GCM-SHA384:EECDH:EDH:HIGH:.....:!MD5:!PSK:!eNULL:!aNULL:!aDH”

2.添加+以便最后移动密码首选项，或添加!以永久禁用ECDSA。

密码："EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH:+ECDSA"

3.在CUCM上添加签名ECDSA证书的根和中间CA证书，或在Expressway信任存储上添加Tomcat-ECDSA证书（某些情况下）。

但是，由于密码优先级的更改、升级后，MRA部署可能会中断，因此TAC必须执行前面提到的解决方法，才能重新正常工作。

随着TLS 1.3的引入，在Wireshark中检查交换的证书变得更加困难。

x15.3版本上的行为

仅对于SIP接口，您可以选择使用RSA或ECDSA密码。

X15.x TLS 1.3已实施。如现场所示，RSA算法主要优于ECDSA。现在升级到x15.2的客户可以选择

RSA和ECDSA算法之间使用此命令集：

xConfiguration SIP Advanced TlsSignatureAlgoPrefRsa:开/关

TlssignatureAlgoPrefRSA仅在SIP接口具有TLS 1.3时有效

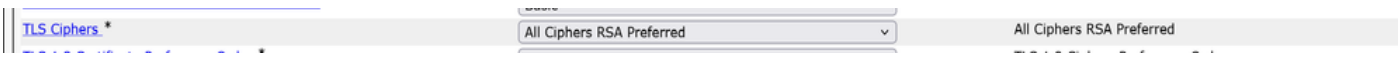
xConfiguration SIP Advanced SipTlsVersions:"TLSv1.3"

注意：从现在起，这仅适用于SIP接口。8443上的流量服务器和Tomcat注意事项保持不变，如前文所述。

选择RSA时，Expressway在“客户端呼叫”期间向CUCM发送的密码套装将显示为下图。

- 签名算法：rsa_pss_rsae_sha512(0x0806)
- 签名算法：rsa_pss_rsae_sha384(0x0805)
- 签名算法：rsa_pss_rsae_sha256(0x0804)
- 签名算法：ecdsa_secp521r1_sha512(0x0603)
- 签名算法：ecdsa_secp384r1_sha384(0x0503)
- 签名算法：ecdsa_secp256r1_sha256(0x0403)

早期的配置将在Enterprise Parameters > Security Parameters下与您在CUCM上选择的TLS密码配置协同工作。



此外，必须注意的是，在Expressway-C和CUCM之间通过TLS 1.3进行中断的TLS握手期间，诊断日志或PCAP中打印的错误不是非常有用。使用TAC时，值得启用这些调试，以便组件打印出清晰的错误以进行故障排除。

xConfiguration Logger Developer developer.trafficserver.http级别："调试"
xConfiguration Logger Developer developer.trafficserver.http_trans级别："调试"
xConfiguration Logger Developer developer.trafficserver.iocore级别："调试"

xConfiguration Logger Developer developer.trafficserver.ssl级别："调试"

当Callmanager与多个服务共享一个证书时的预期结果

在CUCM上重复使用证书后，情况略有变化。

从CUCM 14.0开始，您可以将Tomcat和Tomcat ECDSA证书重新用作Call manager和Call manager ECDSA。

Tomcat证书可以作为Callmanager证书重复使用。

Tomcat-ECDSA证书可重用为Callmanager-ECDSA证书。

这让生活变得轻松。

1. CUCM上的多个服务现在使用一个证书，这会降低证书的成本。

2.减少证书管理。

3.如果您需要在Expressway-Core信任存储上上传Tomcat/Callmanager或Tomcat-ECDSA/Callmanager-ECDSA证书（出于任何原因），它将只是您需要上传的一个证书。不存在相同的CN名称问题（本文档前面已讨论）。

注意：只有当Tomcat和Tomcat-ECDSA是多存储区证书时，才会重复使用证书。

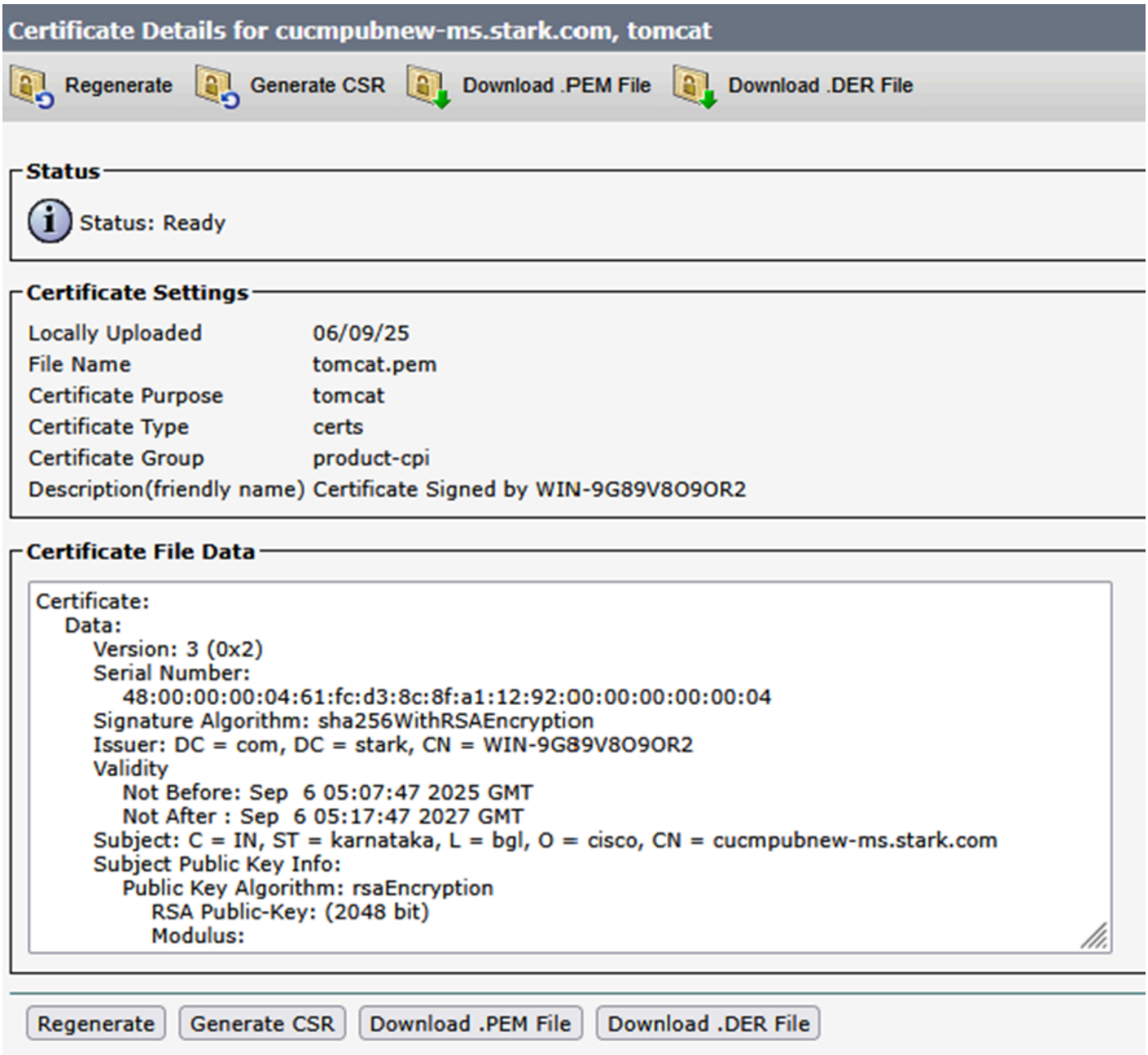
Post Reuse、Callmanager和Callmanager ECDSA服务器证书在CUCM信任存储上不可见。您可以通过运行以下命令从CLI验证证书重复使用：

show cert own CallManager

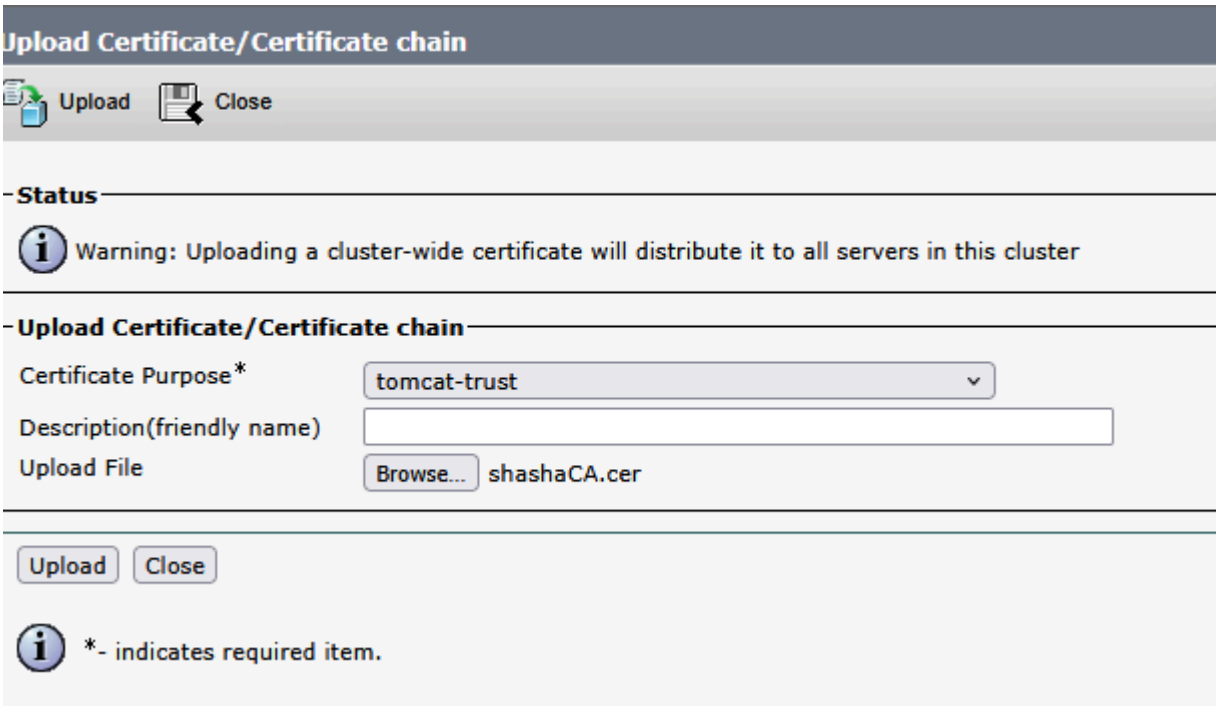
show cert own tomcat

重新使用证书的步骤

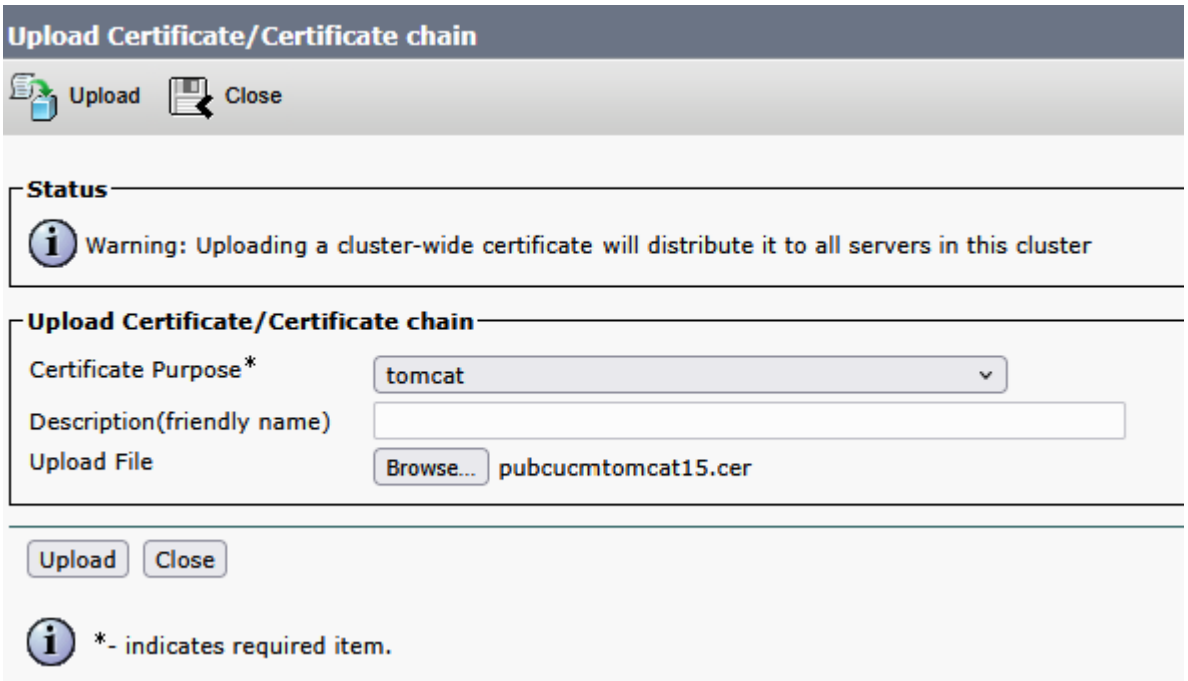
正在生成Tomcat CSR pub add。



上传CA证书，该证书将作为Tomcat-trust在CUCM上签署Tomcat证书。



签署Tomcat证书后，在发布服务器上传。根据提示重新启动相关服务。



签署Tomcat证书后，在发布服务器上传。根据提示重新启动相关服务。

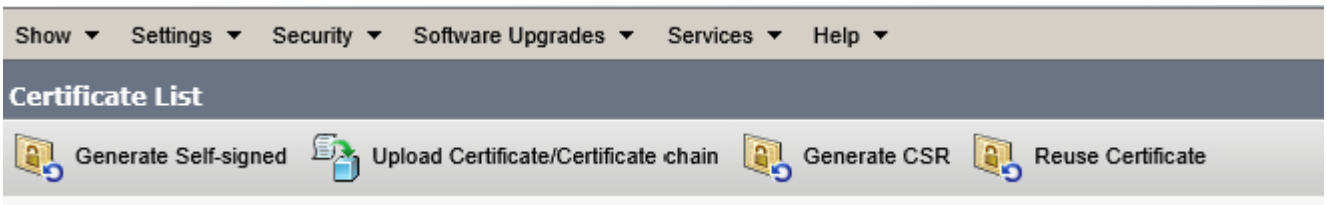
成功：已上传证书。执行灾难恢复备份，以便最新备份包含上传的证书。
在所有群集节点(UCM/IMP)上使用CLI“utils service restart Cisco Tomcat”重新启动Cisco Tomcat Web服务。 在所有UCM群集节点上使用CLI“utils service restart Cisco UDS Tomcat and utils service restart Cisco UDS Tomcat”重新启动Cisco UDS Tomcat和Cisco AXL Tomcat Web服务。此外，在发布方节点上重新启动Cisco DRF Master和Cisco DRF Local服务。仅重启用户节点上的Cisco DRF本地服务。

Tomcat证书现在由CA签名。

		signed					
tomcat	cucmpubnew-ms.stark.com_51dc40f400000000000b	IdentityCA-signed	RSA	Multi-server(SAN)	RICKY200-TMS-CA	10/23/2027	Certificate Signed by RICKY200-TMS-CA

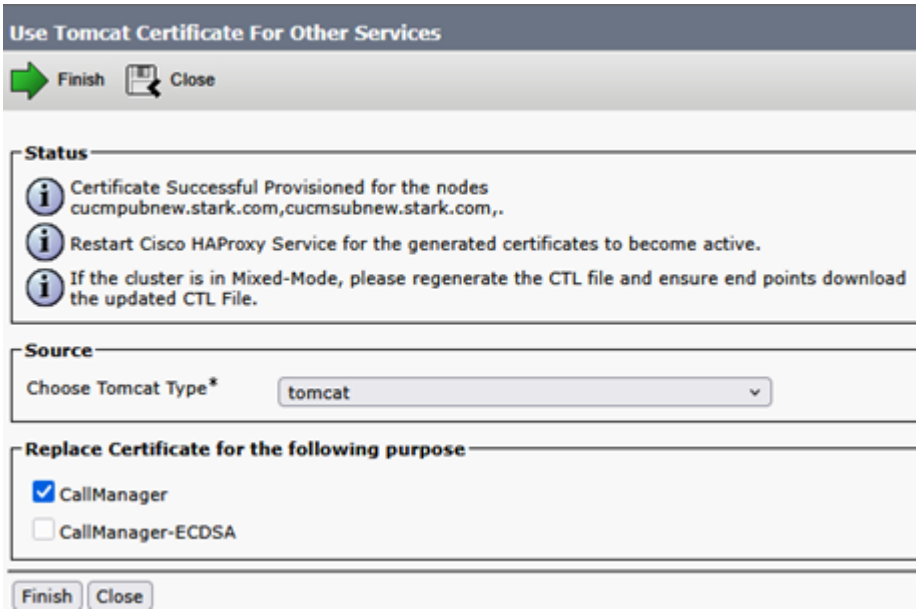
以便立即将Tomcat证书重新用作Callmanager证书。

单击Reuse Certificate。



在下拉列表中选择Tomcat并检查Callmanager证书。

单击 完成。



Tomcat证书现在被重用为Callmanager证书。这可以通过CLI进行验证。

Callmanager证书序列号(SN):56:ff:6c:71:00:00:00:00:00:0d

```
admin:show cert own CallManager
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:ff:6c:71:00:00:00:00:00:0d
        Signature Algorithm: sha384WithRSAEncryption
        Issuer: DC = com, DC = RICKY200, CN = RICKY200-TMS-CA
        Validity
            Not Before: Oct 24 08:44:34 2025 GMT
            Not After : Oct 24 08:54:34 2027 GMT
        Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-ms.
tomcat.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b4:a6:fa:8f:9a:c3:32:02:74:fa:e9:92:30:de:
                    6e:3b:70:cd:d7:4e:64:e4:71:04:fe:17:80:0d:5b:
                    44:d1:7f:00:63:69:4a:5c:1a:1b:75:0c:1a:d6:ce:
                    10:3f:01:e2:d0:f1:75:33:57:b7:0a:71:e1:60:d1:
                    89:3c:e8:a4:8c:3e:30:69:4d:4e:98:da:b8:5d:dd:
                    23:8c:4d:69:90:69:9d:43:74:84:20:a8:9f:45:dc:
                    5a:aa:7b:c8:d1:d0:6f:05:13:d8:99:58:0e:49:7b:
Press <enter> for 1 line, <space> for one page, or <q> to quit
```

Tomcat证书SN:56:ff:6c:71:00:00:00:00:00:0d

```
admin:show cert own tomcat
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:ff:6c:71:00:00:00:00:00:0d
        Signature Algorithm: sha384WithRSAEncryption
        Issuer: DC = com, DC = RICKY200, CN = RICKY200-TMS-CA
        Validity
            Not Before: Oct 24 08:44:34 2025 GMT
            Not After : Oct 24 08:54:34 2027 GMT
        Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-ms.tomcat.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b4:a6:fa:8f:9a:c3:32:02:74:fa:e9:92:30:de:
                    6e:3b:70:cd:d7:4e:64:e4:71:04:fe:17:80:0d:5b:
                    44:d1:7f:00:63:69:4a:5c:1a:1b:75:0c:1a:d6:ce:
                    10:3f:01:e2:d0:f1:75:33:57:b7:0a:71:e1:60:d1:
                    89:3c:e8:a4:8c:3e:30:69:4d:4e:98:da:b8:5d:dd:
                    23:8c:4d:69:90:69:9d:43:74:84:20:a8:9f:45:dc:
                    5a:aa:7b:c8:d1:d0:6f:05:13:d8:99:58:0e:49:7b:
Press <enter> for 1 line, <space> for one page, or <q> to quit
```

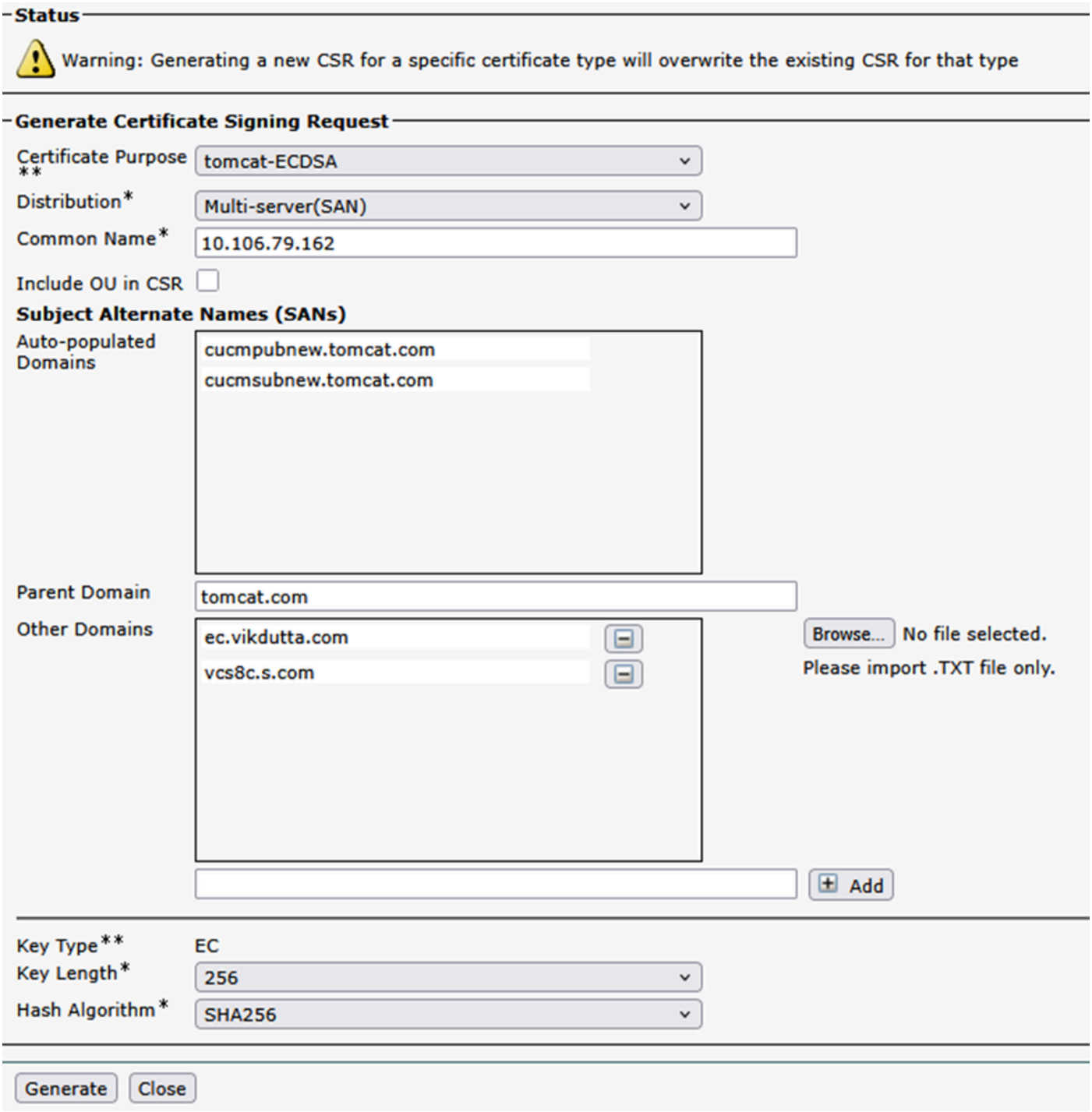
对用户执行相同的步骤。

让我们立即签署ECDSA证书，以便可以将其重用为Callmanager-ECDSA。

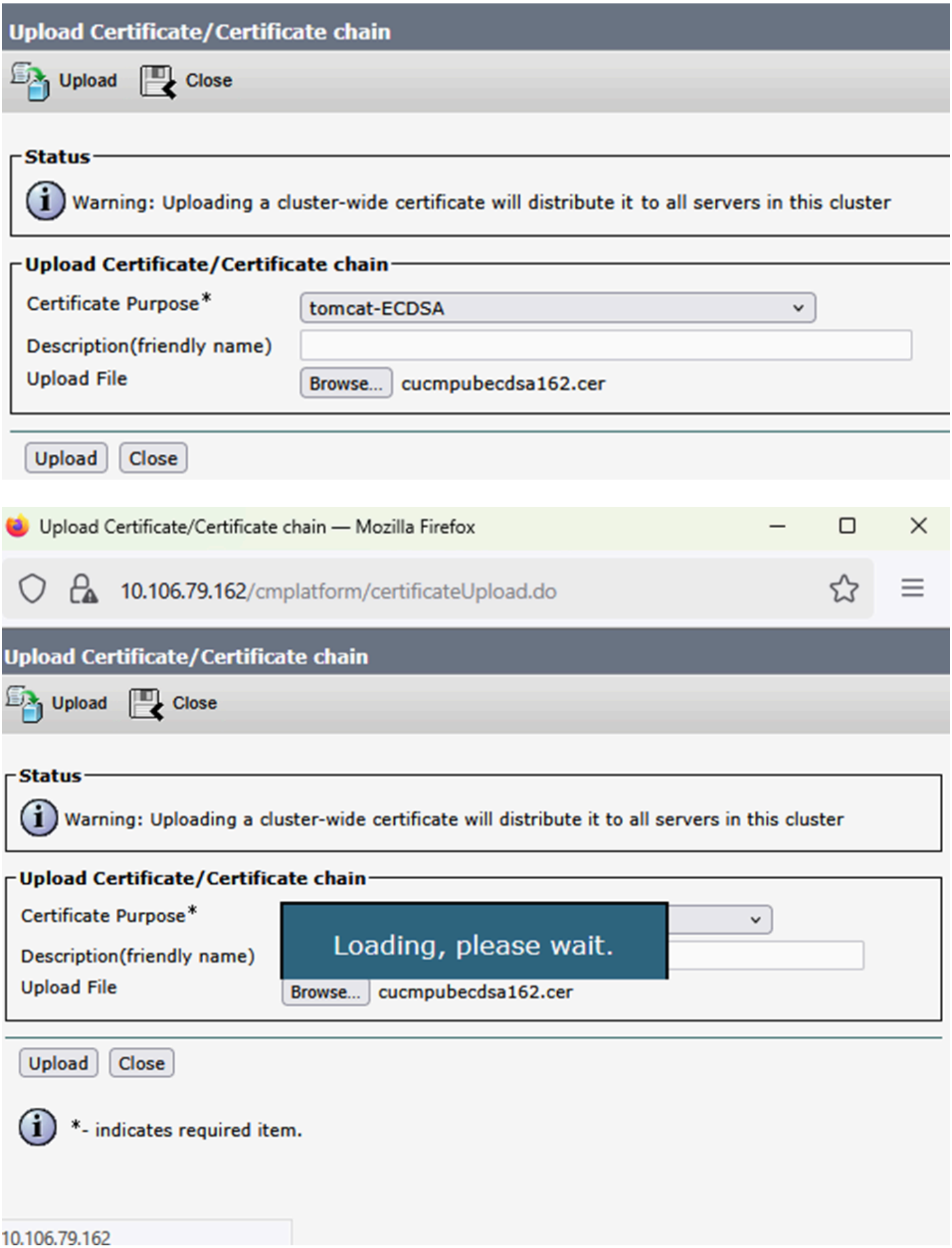
当前Tomcat-ECDSA证书是自签名的。

tomcat	10.106.79.162_5aceb67f00000000000f	Identity	CA-signed	RSA	Multi-server(SAN)	RICKY200-TMS-CA	10/25/2027	Certificate Signed by RICKY200-TMS-CA
tomcat-ECDSA	cucmpubnew-EC.tomcat.com_4b404cd202f54fcabf8abdb8fc715d4b	Identity	self-signed	EC	cucmpubnew.tomcat.com	cucmpubnew-EC.tomcat.com	10/23/2030	Self-signed certificate generated by system

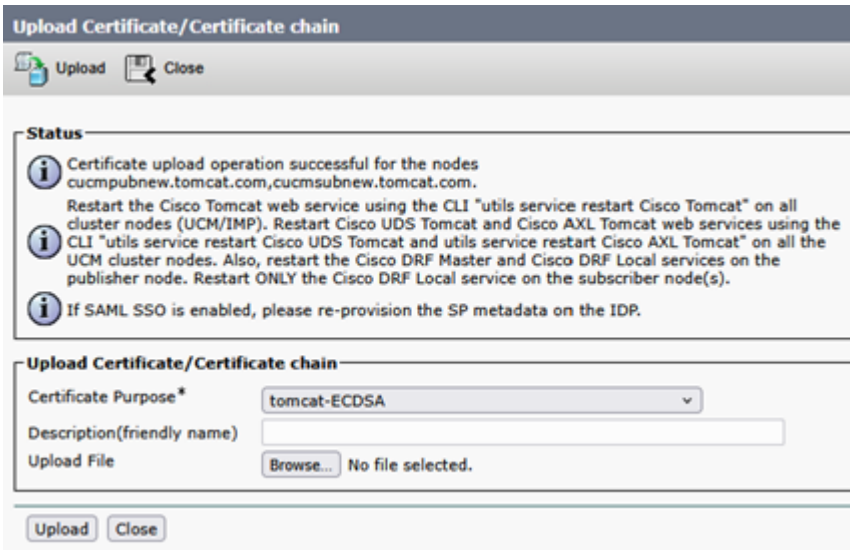
为Tomcat-ECDSA证书签署multisan CSR。



使用CSR签署证书并上传。



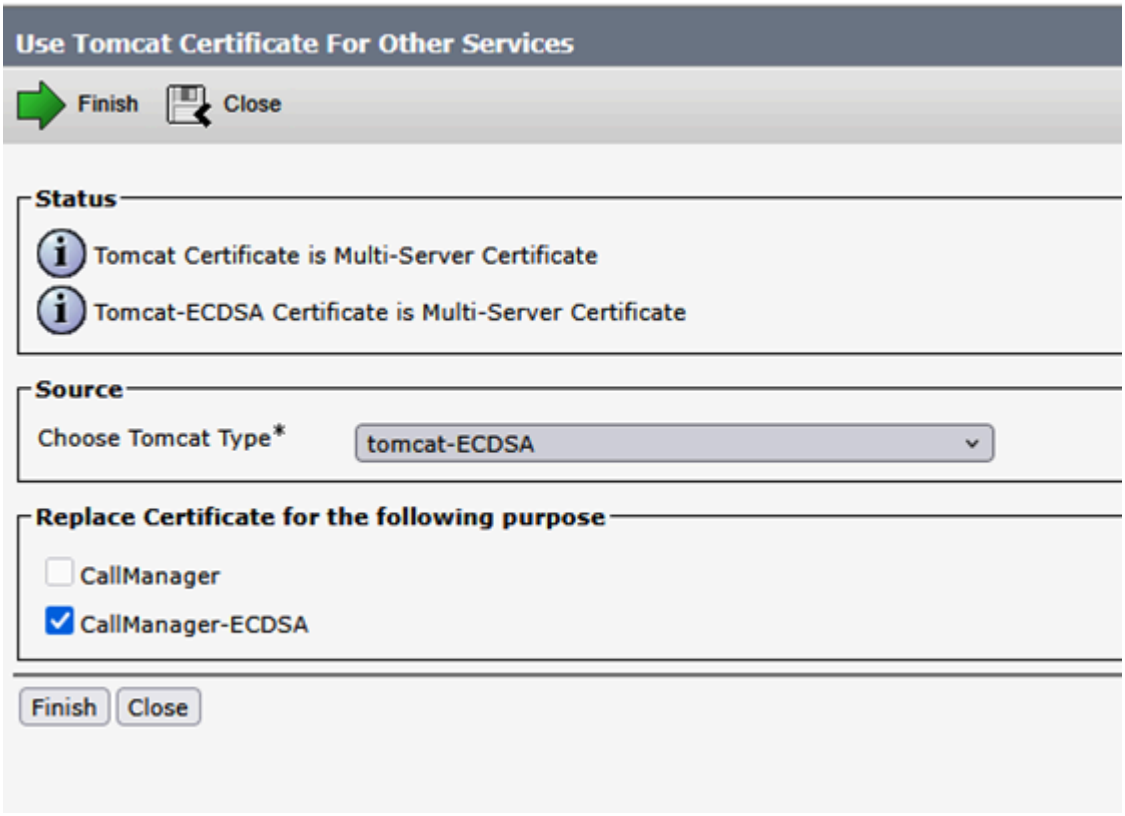
上载成功.根据提示重新启动相关服务。



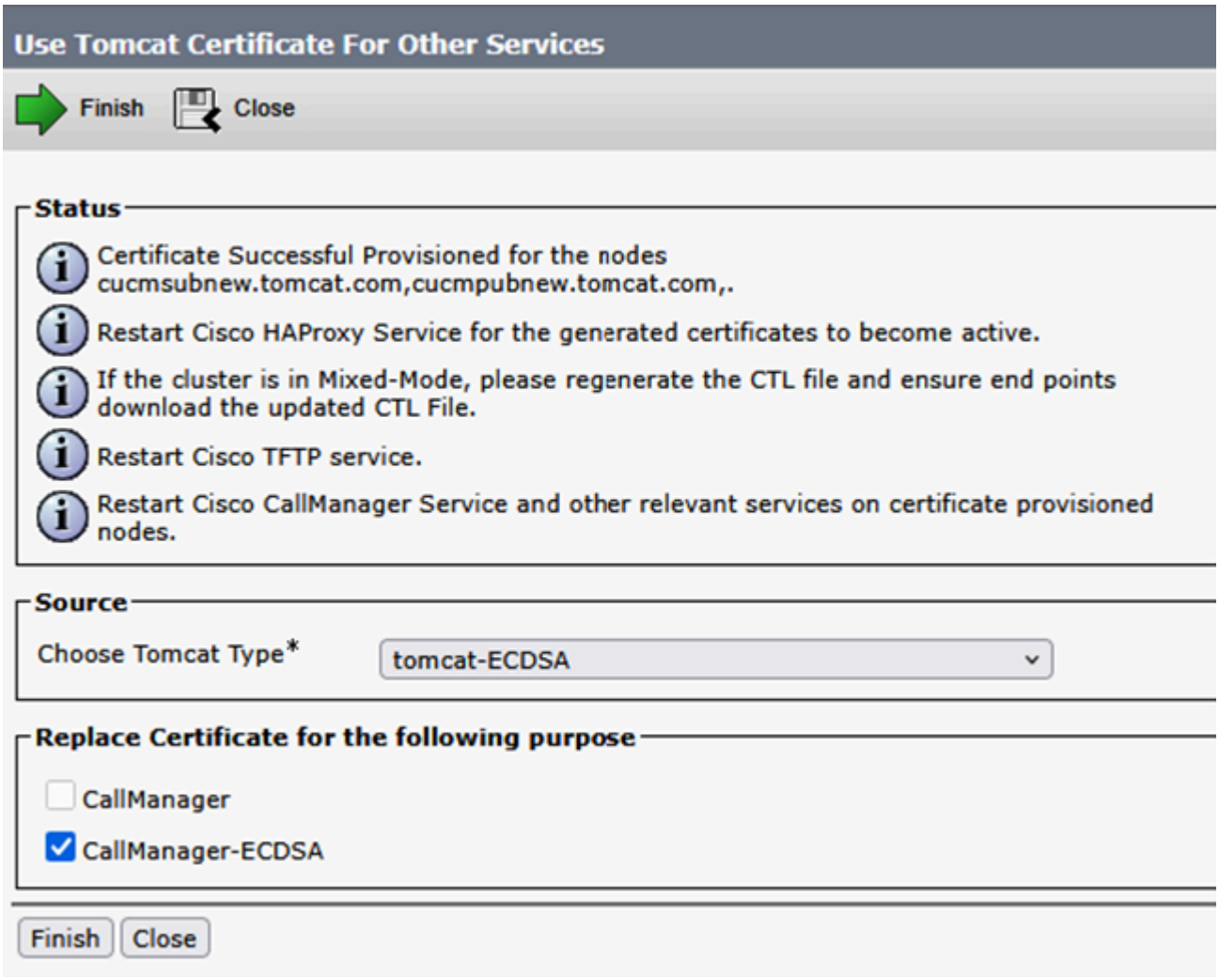
由CA签名的Tomcat和Tomcat-ECDSA。

tomcat	10.106.79.162_5aceb67f00000000000f	Identity	CA-signed	RSA	Multi-server(SAN)	RICKY200-TMS-CA	10/25/2027 Certificate Signed by RICKY200-TMS-CA
tomcat-ECDSA	cucmpubnew-EC-ms.tomcat.com_2f0000003880becca8a18e8f23000000000038	Identity	CA-signed	EC	Multi-server(SAN)	bgluclab-WIN-DC-01-CA	10/25/202GCertificate Signed by bgluclab-WIN-DC-01-CA

现在将Tomcat-ECDSA重用为Callmanager-ECDSA证书。



上载成功.根据提示重新启动相关服务。



从CLI验证证书。

Callmanager-ECDSA证书SN:2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38

```
admin:show cert own CallManager-ecdsa
Invalid Certificate Name. Certificate Not Found.

admin:show cert own CallManager-Ecdsa
Invalid Certificate Name. Certificate Not Found.

admin:show cert own tomcat-ECDSA
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = com, DC = bgluclab, CN = bgluclab-WIN-DC-01-CA
        Validity
            Not Before: Oct 25 06:46:37 2025 GMT
            Not After : Oct 25 06:46:37 2026 GMT
```

Tomcat-ECDSA证书SN:2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38。

```
admin:show cert own tomcat-ECDSA
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = com, DC = bgluclab, CN = bgluclab-WIN-DC-01-CA
        Validity
            Not Before: Oct 25 06:46:37 2025 GMT
            Not After : Oct 25 06:46:37 2026 GMT
        Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-EC-ms.tomcat.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
```

由于您现在对两项服务（即Tomcat和Callmanager服务的Tomcat证书，以及Tomcat-ECDSA和Callmanager-ECDSA服务的Tomcat-ECDSA）使用一个证书，因此在Expressway信任存储上上传证书变得不那么麻烦（如果需要上传）。

在MRA的expressway-core上添加UCM时，使TLS验证“开启”，比以往任何时候都更容易。只需添加一个Tomcat证书CA或服务器证书即可执行该操作（因为证书现在在Callmanager和Tomcat服务之间共享）。

如果升级到x14.2或更高版本导致移动远程访问中断，您还可以参阅此综合文档以排除此问题。

Apache流量服务器版本历史记录

要检查服务器上的版本，请登录到root并运行~ # /apache2/bin/httpd -v。

Expressway x8.11.4
服务器版本：Apache/2.4.34(Unix)
服务器构建：2018年11月12日19:04:23

Expressway x12.6

服务器版本：Apache/2.4.43(Unix)
服务器构建：2020年5月26日18:27:21

Expressway x14.0.8

服务器版本：Apache/2.4.53(Unix)
服务器构建：2022年5月4日08:52:57

Expressway x15.3

服务器版本：Apache/2.4.62(Unix)
服务器构建：2025年7月16日12:10:19

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）。