Entender os requisitos do certificado de acesso móvel e remoto e o histórico ATS

Contents

Introdução

Informações de Apoio

No Expressway versão 14.0.2

Comportamento em versões anteriores à 14.0.8

Comportamento nas versões 14.0.8 e posteriores

- Seção

Comportamento nas versões x15.3

O que esperar quando o Callmanager compartilha um certificado com vários serviços

- Etapas para reutilizar o certificado

Histórico de Versão do Apache Traffic Server

Introdução

Este documento descreve os requisitos de carregamento de certificado no CUCM para acesso móvel e remoto.

Informações de Apoio

O Cisco Expressway usa o Apache Traffic Server (ATS). O servidor de tráfego é um componente muito importante em soluções transversais, usado principalmente para estes recursos:

- Verificação do certificado: Ele executa a verificação de certificado do Cisco Unified Communications Manager (CUCM), IM & Presence e nós de servidor Unity para serviços MRA.
- Proxying e cache: Ele atua como um servidor proxy de cache rápido e escalável para tráfego HTTP/HTTPS.

No Expressway versão 14.0.2

O servidor de tráfego (ATS) começa a ver uma pequena aplicação de 'verificação de certificado' quando se comunica com o CUCM durante o provisionamento de MRA.

O requisito foi documentado em CSCvz45074, onde os certificados raiz que assinaram os certificados do servidor Expressway Core devem ser carregados no CUCM como Tomcat-Trust e Callmanager Trust: https://cdetsng.cisco.com/summary/#/defect/CSCvz45074.

- O Servidor De Tráfego Impõe A Verificação De Certificado.

- Antes de atualizar para a versão X14.0.2, certifique-se de que este requisito de certificado seja atendido.

Requisito - A cadeia de Autoridade de Certificação (CA) (Raiz + Intermediário) que assinou o certificado Expressway-C deve ser adicionada à lista tomcat-trust e CallManager-trust do CUCM, mesmo se o Unified Communications Manager (UCM) estiver no modo não seguro.

Motivo - o serviço de servidor de tráfego no Expressway envia seu certificado sempre que um servidor UCM o solicita. Essas solicitações são para serviços executados em portas diferentes de 8443 (por exemplo, portas 6971, 6972 e assim por diante). Isso reforça a verificação de certificado mesmo se o UCM estiver no modo não seguro. Para obter mais informações, consulte Guia de implantação do Mobile and Remote Access Through Expressway.

Comportamento em versões anteriores à 14.0.8

O servidor de tráfego no Expressway-C que lida com conexões bidirecionais HTTPS seguras entre os nós Expressway-C e Unified Communication não verificou o certificado apresentado pela extremidade remota. Na configuração MRA, há uma opção para ter a verificação de certificado TLS pela configuração do modo de verificação TLS como 'Ativado' quando servidores CUCM, IM&P ou Unity forem adicionados em Configuração > Comunicações Unificadas > servidores Unified CM/nós de serviço IM e Presence/servidores Unity Connection. A opção de configuração é mostrada na próxima captura de tela, que indica que ele verifica o FQDN ou o IP na SAN, bem como a validade do certificado e se ele está assinado por uma CA confiável.

Houve também um problema conhecido em que dois certificados com o mesmo nome CN não podem ser carregados no repositório de confiança do Expressway. Essa limitação causou dois problemas:

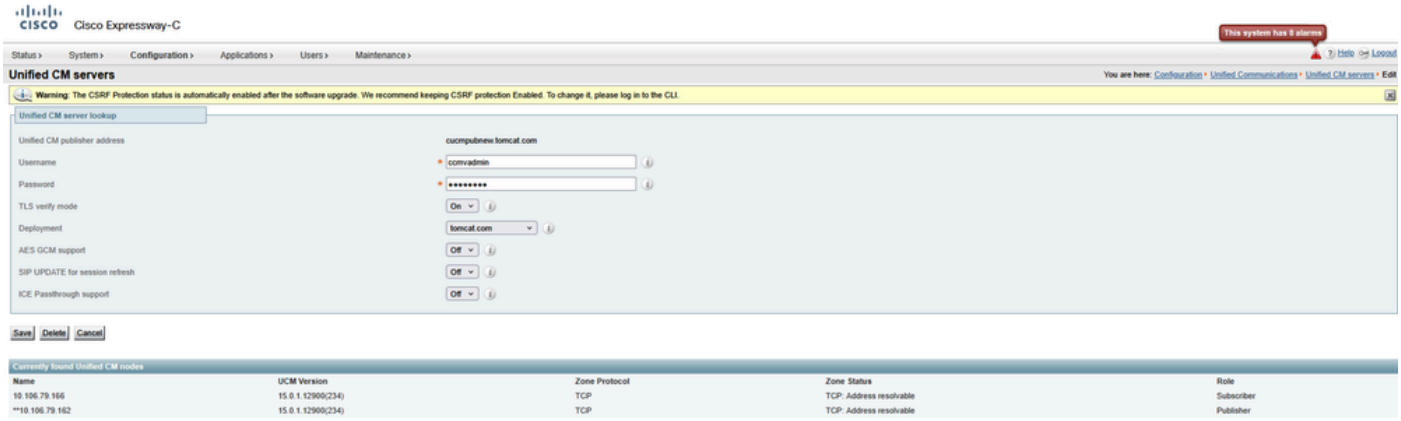
1. Se você optar por carregar o certificado do gerenciador de chamadas no repositório Expressway Trust, a verificação TLS de 'Ativado' falhará ao adicionar CUCMs.

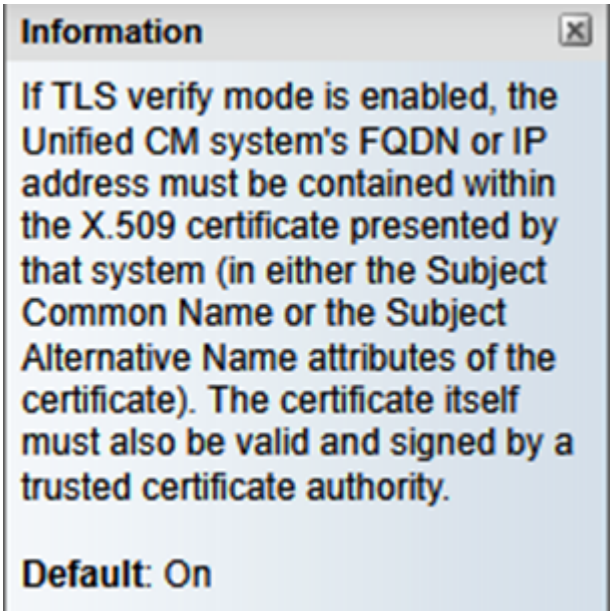
2: Se você optar por carregar o certificado Tomcat no repositório Expressway Trust, os registros sip seguros no 5061 falharão.

Esse comportamento é documentado no CSCwa12894.

Além disso, essa verificação de certificado TLS só é feita na descoberta dos servidores CUCM/IM&P/Unity e não no momento do provisionamento do cliente MRA.

A desvantagem dessa configuração é que ela apenas verifica o endereço do publicador adicionado. Ele não valida se o certificado nos nós do assinante foi configurado corretamente, pois recupera as informações do nó do assinante (FQDN ou IP) do banco de dados do nó do publicador.





Comportamento nas versões 14.0.8 e posteriores

A partir da versão X14.0.8, o servidor Expressway executa a verificação de certificado TLS para cada solicitação HTTPS feita através do servidor de tráfego. Isso significa que ele também executa isso quando o Modo de verificação TLS está definido como 'Desligado' durante a descoberta dos nós CUCM/IM&P/Unity. Quando a verificação não é bem-sucedida, o handshake TLS não é concluído e a solicitação falha, o que pode levar à perda de funcionalidade, como redundância, problemas de failover ou falhas de login completo, por exemplo. Além disso, com o Modo de verificação TLS definido como 'Ativado', ele não garante que todas as conexões funcionem bem, como abordado no exemplo mais adiante.

Os certificados exatos que o Expressway verifica em relação aos nós CUCM/IM&P/Unity são como mostrado na seção do guia MRA.

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

Seção

Requisitos de Certificado > Requisitos de Troca de Certificado

Devido a essas mudanças na forma como a comunicação ocorre entre o Expressway-Core e o CUCM, deve-se garantir que:

1. É recomendável usar certificados assinados pela CA para acesso móvel e remoto.

2. Cada cluster do Unified CM deve confiar no certificado Expressway-C. Para cada cluster, assegure-se de:

- Se o modo Misto estiver ativado — O certificado Expressway-C deverá ser instalado no armazenamento CallManager-trust e Tomcat-trust no Unified CM.
- Se o modo Misto estiver desativado — O certificado raiz de CA que assina o certificado Expressway-C deve ser instalado no armazenamento CallManager-trust e Tomcat-trust no Unified CM. Em seguida, reinicie: · Serviço Tomcat · Serviço CallManager · Serviço de proxy HA (se estiver usando TLS no Tomcat).

No Expressway - Core, certifique-se de que estas ações sejam executadas:

- O Expressway-C deve confiar nos certificados apresentados por cada cluster do Unified CM e do Serviço IM e Presence.

O repositório de confiança do Expressway-C deve incluir o certificado de CA raiz que assina os certificados do Unified CM e do Serviço IM e Presence para todos os clusters de UC.

Note: Certifique-se de adicionar todos os certificados CA raiz e intermediários ou a cadeia CA completa usada para assinar o certificado Expressway-C à lista Tomcat-trust e CallManager-trust do Cisco Unified Communications Manager (UCM), mesmo que o UCM esteja operando no modo não seguro.

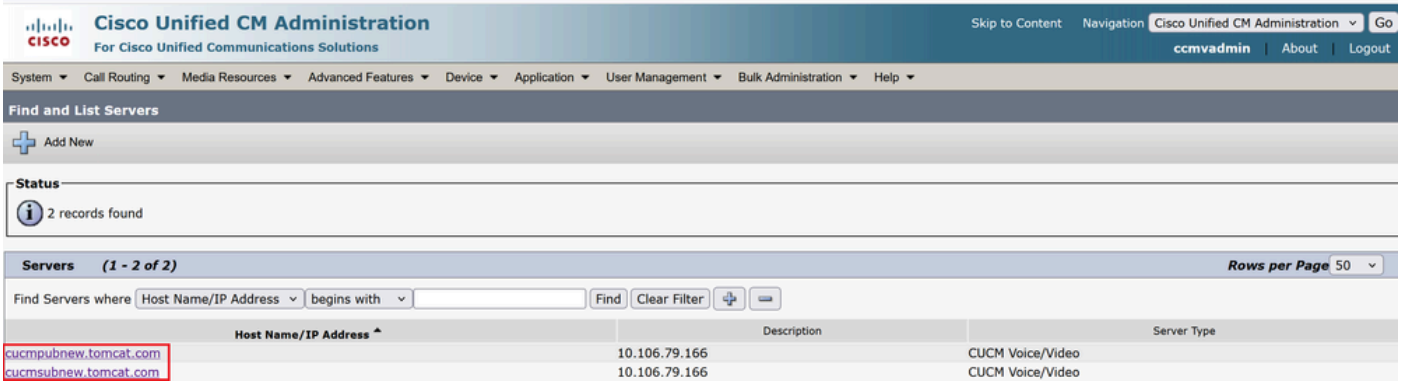
Motivo - o serviço de servidor de tráfego no Expressway envia seu certificado sempre que um servidor (UCM) o solicita. Essas solicitações são para serviços executados em portas diferentes de 8443 (por exemplo, portas 6971, 6972 e assim por diante). Isso reforça a verificação de certificado mesmo se o UCM estiver no modo não seguro.

A forma como o endereço do CUCM é adicionado em Sistema > Servidor desempenha um papel muito importante na adição de CUCM/IMP no núcleo do Expressway em Configuração > Comunicações Unificadas > Servidores Unified CM/IM e nós de serviço de presença.

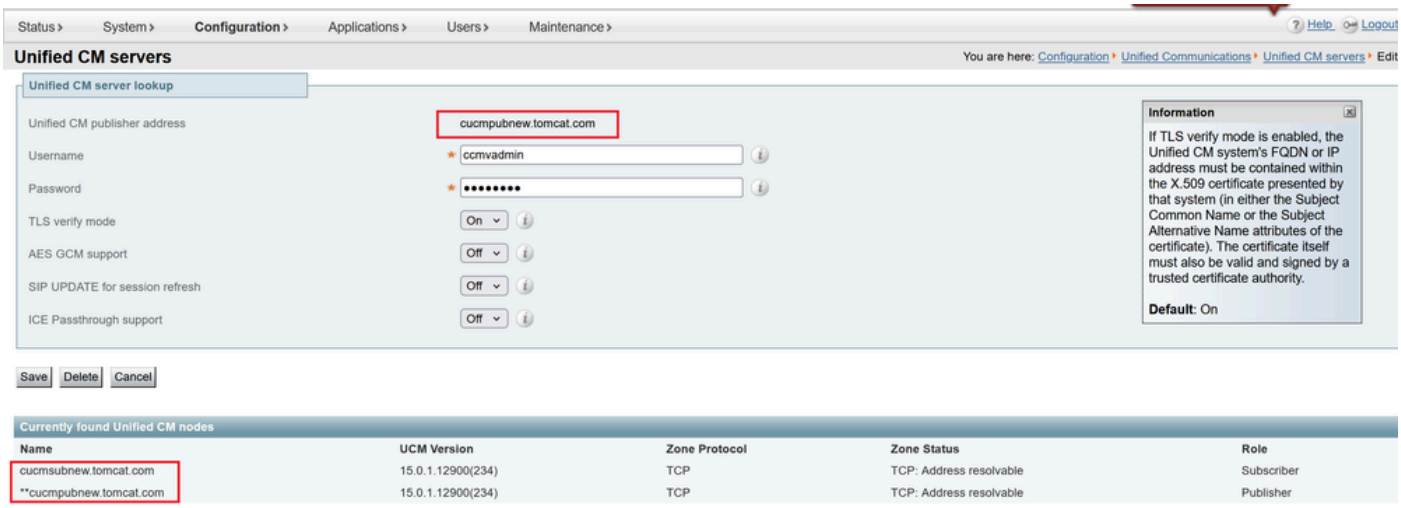
O CUCM sempre deve ser adicionado com FQDN e não com nome de host ou endereço IP. Se perceber que o CUCM foi adicionado em System > Server como Hostname/IP address

durante o handshake TLS, a verificação TLS 'On' falhará e o cluster CUCM não será adicionado no Expressway-Core.

Esta figura mostra o CUCM adicionado como nome de host:



Esta figura mostra o CUCM adicionado no Expressway-Core com FQDN com TLS verify Mode = ON:

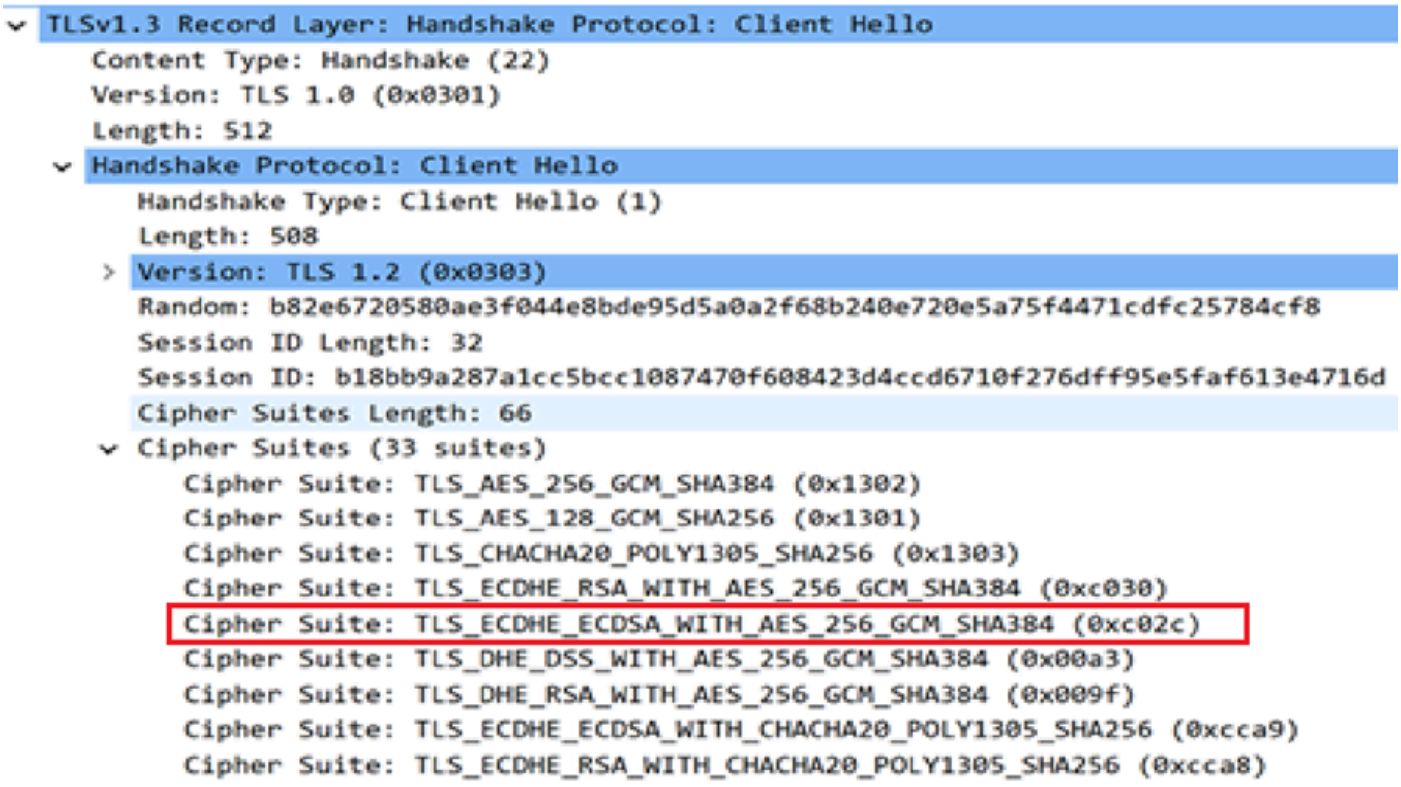


Houve também uma alteração introduzida no X14.2 que apresentará cifras durante um handshake TLS (hello do cliente) em ordem de preferência diferente. Isso dependia do caminho de atualização e causava conexões TLS inesperadas após uma atualização de software. Pode ser que, antes da atualização durante o handshake TLS, ele tenha solicitado o certificado Cisco Tomcat ou Cisco CallManager do CUCM. Mas que após a atualização, ele solicitou para a variante ECDSA (que é a variante de cifra mais segura do que RSA). Os certificados Cisco Tomcat-ECDSA ou Cisco CallManager-ECDSA podem ser assinados por uma CA diferente ou apenas certificados ainda autoassinados (o padrão).

Essa alteração de ordem de preferência de codificação nem sempre é relevante para você, pois depende do caminho de atualização, conforme mostrado nas notas de versão do Expressway X14.2.1. Resumindo, você pode ver em Manutenção > Segurança > Cifras para cada uma das listas de cifras se ela contém ou não o prefixo ECDHE-RSA-AES256-GCM-SHA384. Caso contrário, ele prefere a cifra ECDSA mais recente em vez da cifra RSA. Se tiver, você terá o comportamento anterior com RSA que tem a preferência mais alta.

A próxima captura de tela mostra em caixa vermelha a cifra ECDSA anunciada pelo núcleo do Expressway durante a mensagem de negociação TLS na saudação do cliente, #IF TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 é escolhida pelo respondente remoto (CUCM) na saudação do servidor, então a negociação TLS falhará se:

Certificados de CA RAIZ ou certificados ECDSA reais do Respondente, ou seja, o CUCM não está instalado no armazenamento Expressway Trust nesse caso.



Como alternativa, você também pode modificar as Cifras do Expressway para que o ECDSA não tenha precedência.

1. Modifique a cifra SIP anexando a string SSL aberta GCM-Sha384.

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

2. Adicione + para mover a cifra na última preferência ou adicione ! para desabilitar permanentemente o ECDSA.

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

3. Adicione o certificado de CA raiz e intermediário que assinou o certificado ECDSA no CUCM ou adicione o certificado Tomcat-ECDSA no armazenamento de confiança do Expressway (em alguns casos).

No entanto, devido à alteração na precedência da cifra, após a atualização, as implantações de MRA podem ser interrompidas, de modo que o TAC terá que executar a solução alternativa mencionada anteriormente para fazer as coisas funcionarem novamente.

Com a introdução do TLS 1.3, fica ainda mais difícil verificar quais certificados estão sendo trocados no Wireshark.

Comportamento nas versões x15.3

Somente para a interface SIP, você pode optar por ter cifras RSA ou ECDSA.

Com X15.x, o TLS 1.3 foi aplicado. Como visto no campo, o algoritmo RSA é escolhido principalmente sobre o ECDSA. Os clientes que fizerem upgrade para o x15.2 agora podem escolher

entre o algoritmo RSA e ECDSA com este conjunto de comandos:

TlsSignatureAlgoPrefRsa Avançado SIP do xConfiguration: Ligado/Desligado

TlssignatureAlgoPrefRSA só funcionará se a interface SIP tiver TLS 1.3

Versões avançadas do SipTls do SIP xConfiguration: "TLSv1.3"

Note: Isso está qualificado para a interface SIP somente a partir de agora. As considerações do servidor de tráfego e do Tomcat no 8443 permanecem inalteradas conforme documentado anteriormente.

Os trajes de cifra enviados durante a saudação do cliente pelo Expressway para o CUCM serão como mostrado quando RSA é escolhido.

- Algoritmo de assinatura: rsa_pss_rsae_sha512 (0x0806)
- Algoritmo de assinatura: rsa_pss_rsae_sha384 (0x0805)
- Algoritmo de assinatura: rsa_pss_rsae_sha256 (0x0804)
- Algoritmo de assinatura: ecdsa_secp521r1_sha512 (0x0603)
- Algoritmo de assinatura: ecdsa_secp384r1_sha384 (0x0503)
- Algoritmo de assinatura: ecdsa_secp256r1_sha256 (0x0403)

A configuração anterior funcionará em tandem na configuração que você escolheu em CUCM para cifras TLS em Parâmetros empresariais > Parâmetros de segurança.

Além disso, é importante observar que durante um handshake TLS sobre TLS 1.3 interrompido entre o Expressway-C e o CUCM, os erros impressos nos logs de diagnóstico ou no PCAP não são muito úteis. Vale a pena habilitar essas depurações ao trabalhar com o TAC, para que o componente imprima erros claros para solucionar problemas.

Desenvolvedor do Agente de Log xConfiguration.trafficServer.http Nível: "DEBUG"
xConfiguration Logger Developer developer.trafficServer.http_trans Nível: "DEBUG"
xConfiguration Logger Developer developer.traffic server.iocore Nível: "DEBUG"
xConfiguration Logger Developer developer.traffic server.ssl Nível: "DEBUG"

O que esperar quando o Callmanager compartilha um certificado com vários serviços

As coisas mudam um pouco com a reutilização do certificado no CUCM.

A partir do CUCM 14.0, você pode reutilizar os certificados ECDSA Tomcat e Tomcat como Call manager e Call manager ECDSA.

O certificado Tomcat pode ser reutilizado como certificado do Callmanager.

O certificado Tomcat-ECDSA pode ser reutilizado como certificado Callmanager-ECDSA.

Isso facilita a vida.

1. Vários serviços no CUCM agora usam um certificado, o que reduz o custo do certificado.

2. Menos gerenciamento de certificados.

3. Se você precisar carregar o certificado Tomcat/Callmanager ou Tomcat-ECDSA/Callmanager-ECDSA (por qualquer motivo) no repositório de confiança Expressway-Core, ele será apenas um certificado que você precisará carregar. Não haverá problema em ter o mesmo problema de nome CN (mencionado anteriormente neste documento).

Note: A reutilização do certificado só ocorrerá quando o Tomcat e o Tomcat-ECDSA forem certificados de multisserviço.

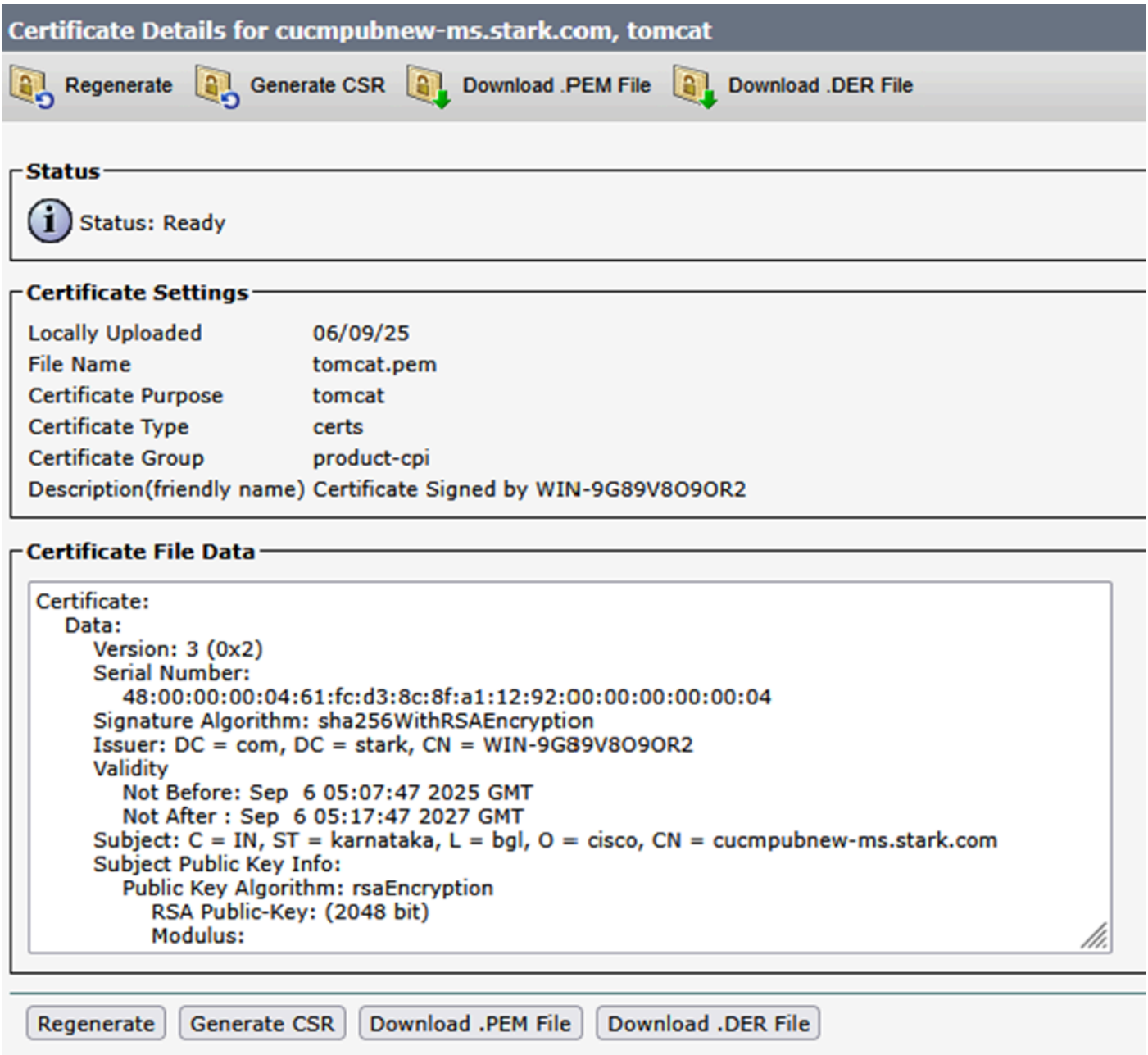
Os certificados de servidor ECDSA Post Reuse, Callmanager e Callmanager não são visíveis no armazenamento confiável do CUCM. Você pode validar a reutilização de certificado do CLI executando comandos:

show cert own CallManager

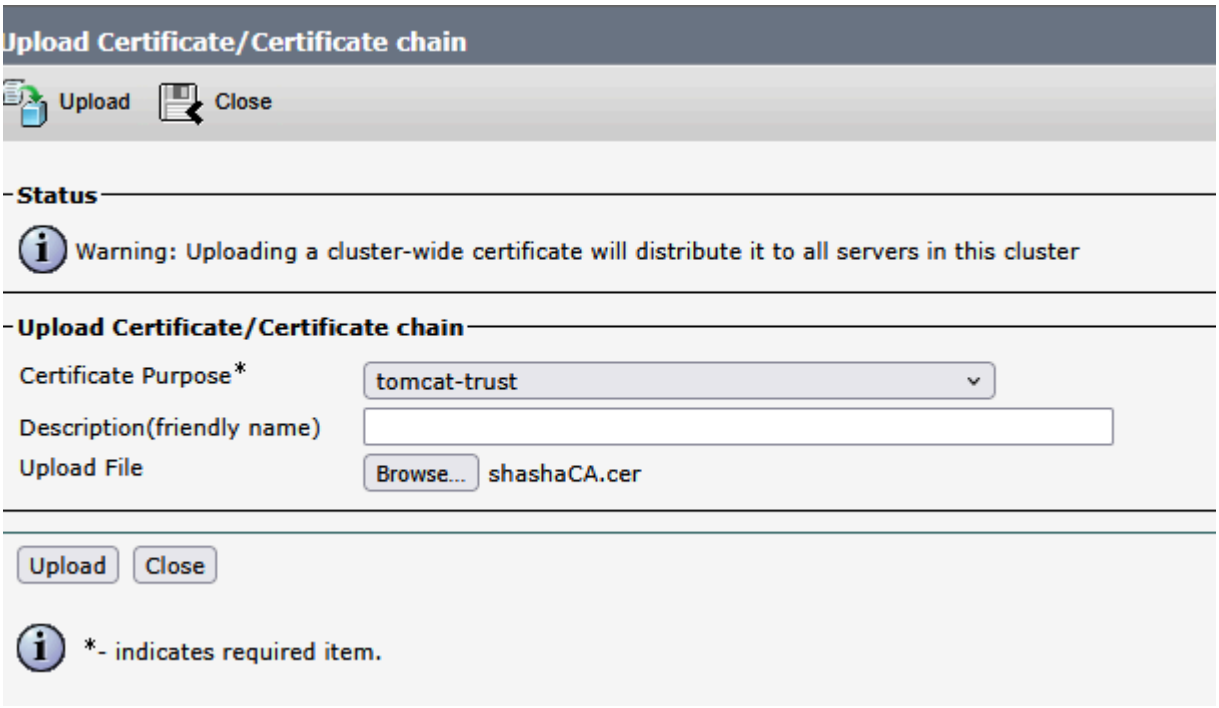
show cert own tomcat

Etapas para reutilizar o certificado

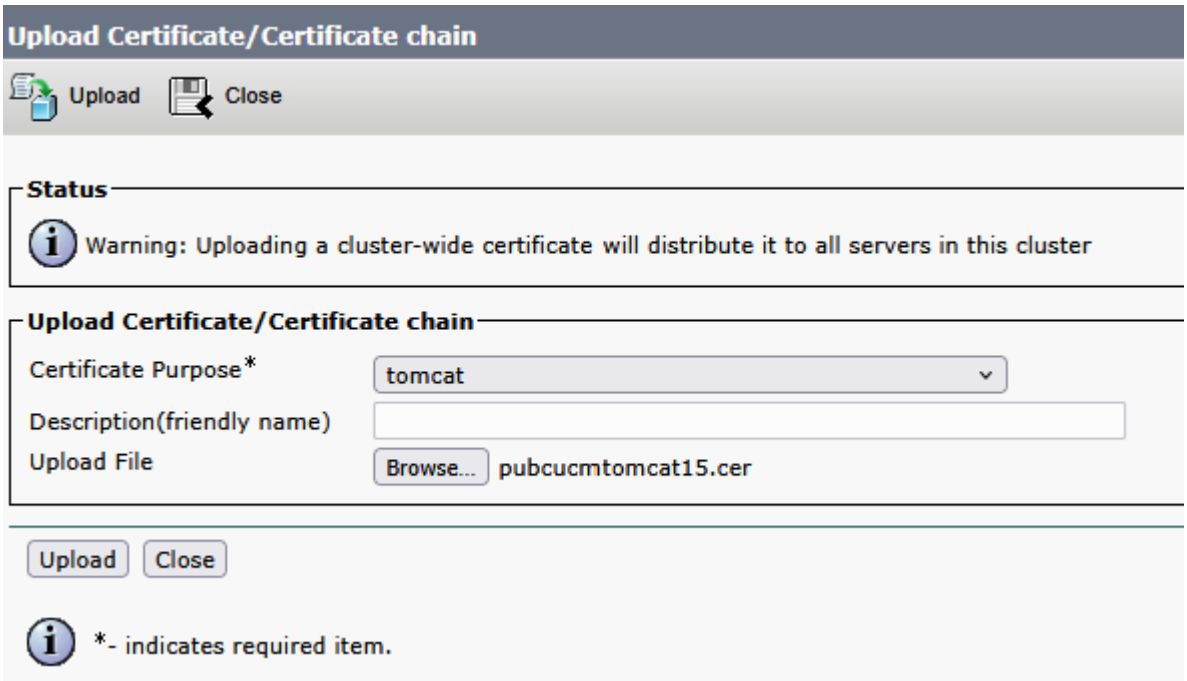
Gerando adição Tomcat CSR.



Carregue o certificado CA que assinará o certificado Tomcat no CUCM como Tomcat-trust.



Quando o certificado Tomcat estiver assinado, carregue no editor. Reinicie os serviços relevantes conforme solicitado.



Quando o certificado Tomcat estiver assinado, carregue no editor. Reinicie os serviços relevantes conforme solicitado.

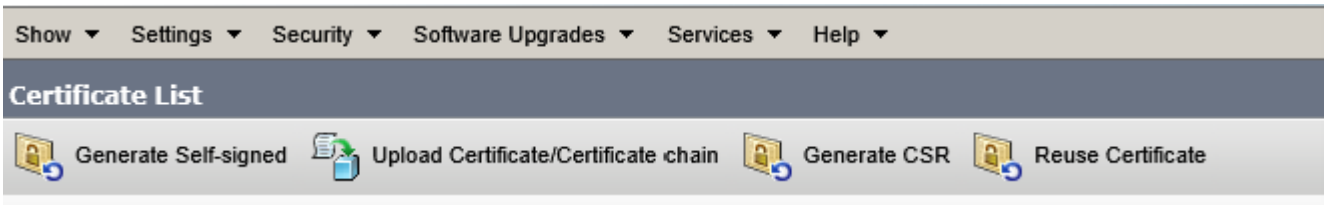
Sucesso: Certificado carregado. Execute um backup da Recuperação de desastres para que o backup mais recente contenha o certificado carregado.
Reinicie o serviço Web Cisco Tomcat usando o comando CLI 'utils service restart Cisco Tomcat' em todos os nós do cluster (UCM/IMP). Reinicie os serviços Web Cisco UDS Tomcat e Cisco

AXL Tomcat usando o comando CLI 'utils service restart Cisco UDS Tomcat and utils service restart Cisco AXL Tomcat' em todos os nós de cluster UCM. Além disso, reinicie os serviços Cisco DRF Master e Cisco DRF Local no nó do editor. Reinicie somente o serviço Cisco DRF Local no(s) nó(s) do assinante.

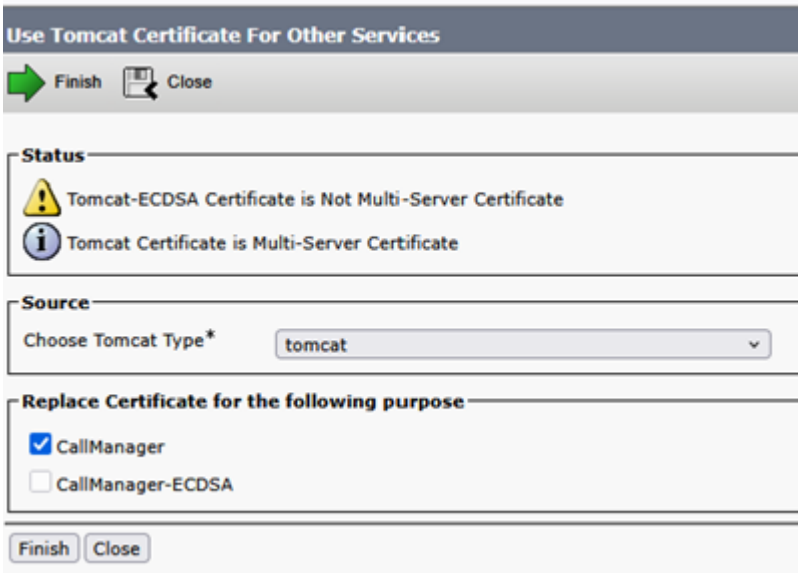
O certificado Tomcat agora está assinado pela CA.

Para reutilizar o certificado Tomcat como certificado do Callmanager agora.

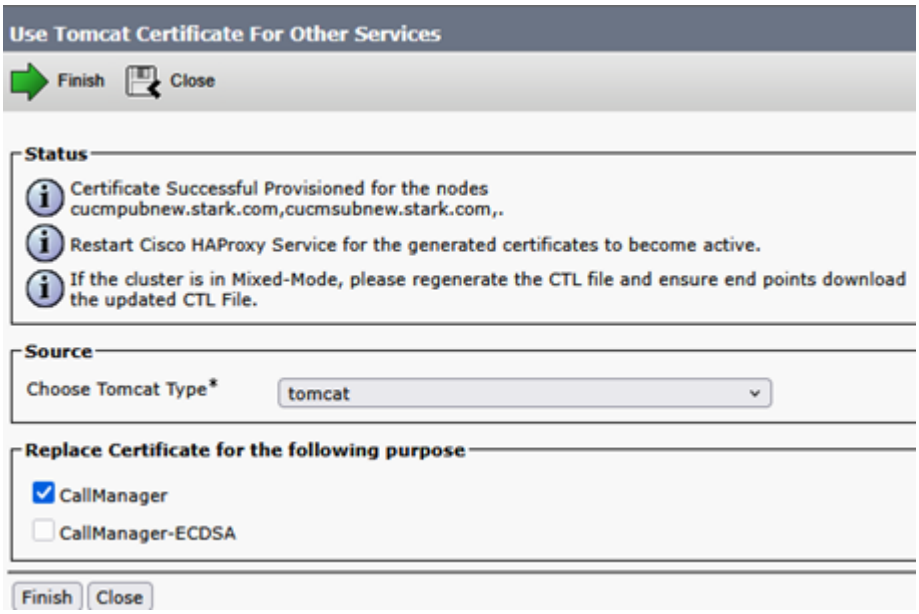
Clique em Reutilizar certificado.



Escolha Tomcat no menu suspenso e verifique o certificado do Callmanager.



Clique em Finish.



O certificado Tomcat agora é reutilizado como certificado do Callmanager. Isso pode ser validado pelo CLI.

Número de série (SN) do certificado do Callmanager: 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
```

SN de certificado do Tomcat: 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
```

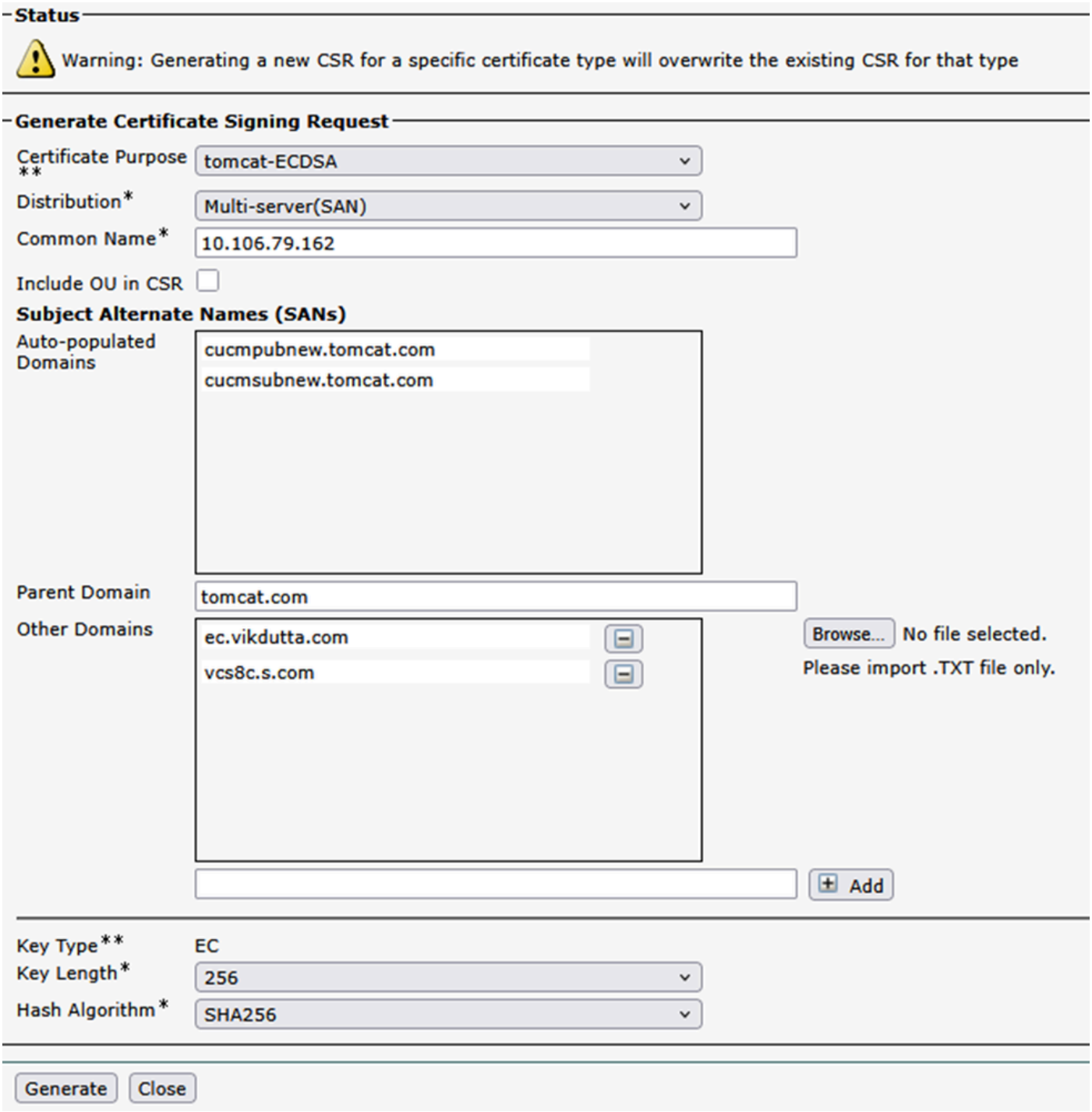
Execute as mesmas etapas no Assinante.

Vamos assinar o certificado ECDSA agora para que ele possa ser reutilizado como Callmanager-ECDSA.

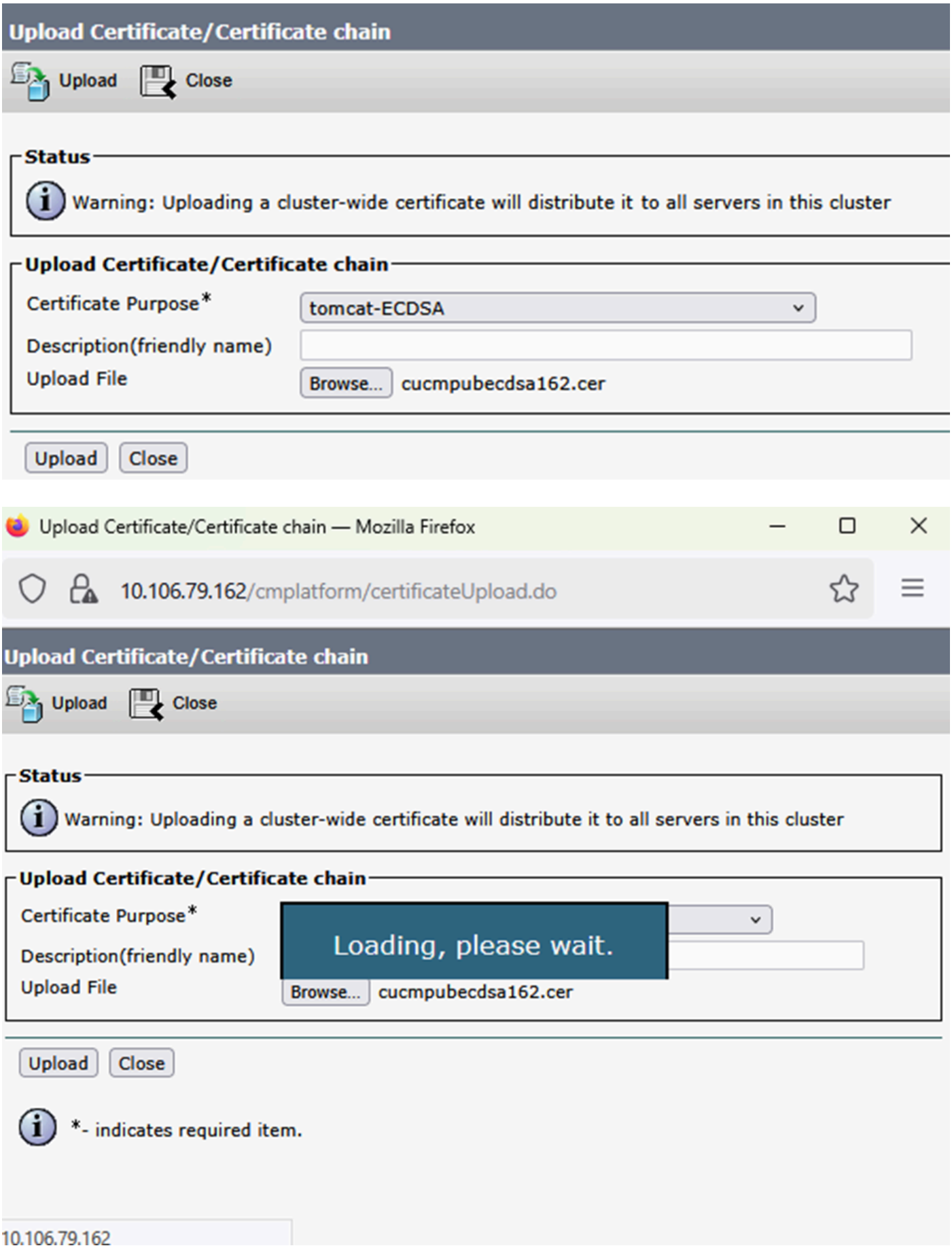
O certificado Tomcat-ECDSA atual é autoassinado.

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_4b404cd202f54cabf8abdb8c15d46	Identity	self-signed	EC	cucmpubnew.tomcat.com	cucmpubnew-EC.tomcat.com	10/23/2030	Self-signed certificate generated by system

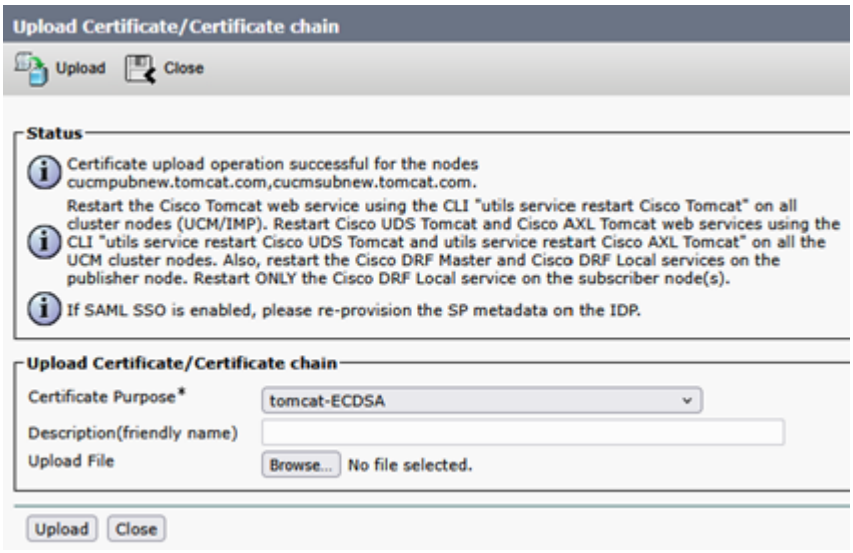
Assine CSR multisseano para o certificado Tomcat-ECDSA.



Assine o certificado usando CSR e carregue.

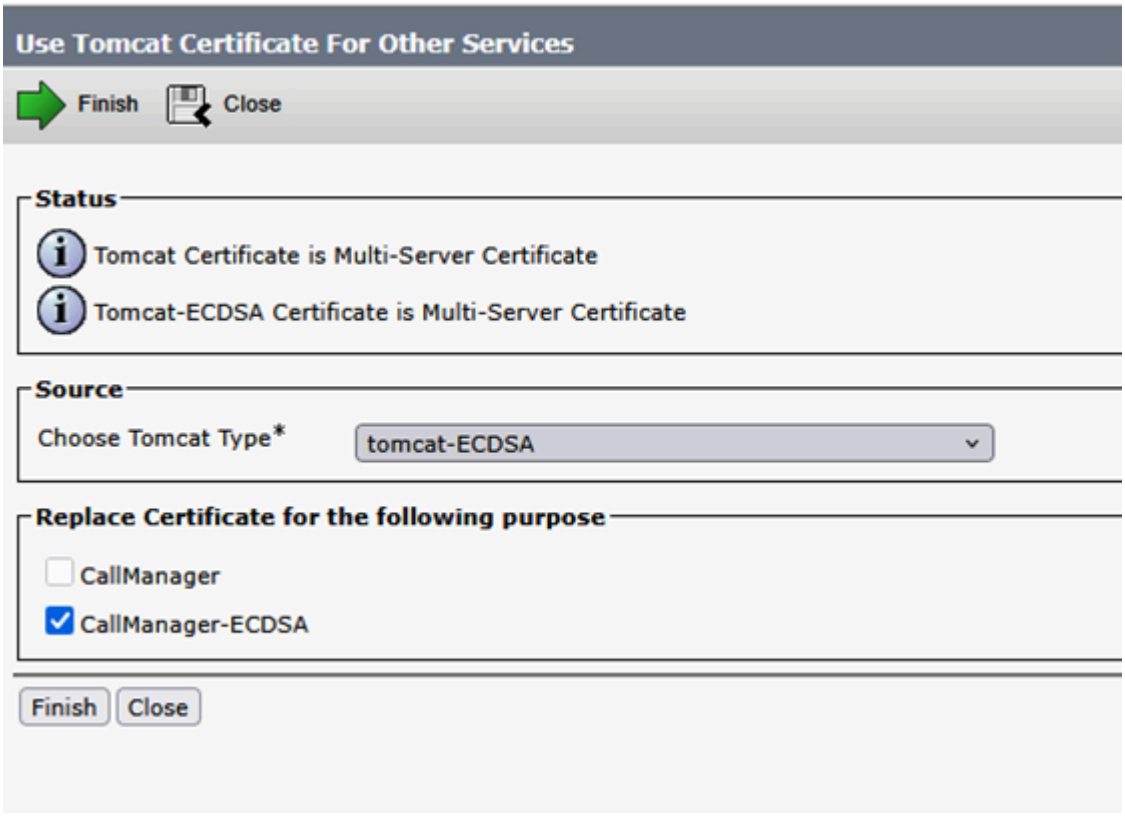


Carregamento bem-sucedido. Reinicie os serviços relevantes conforme solicitado.

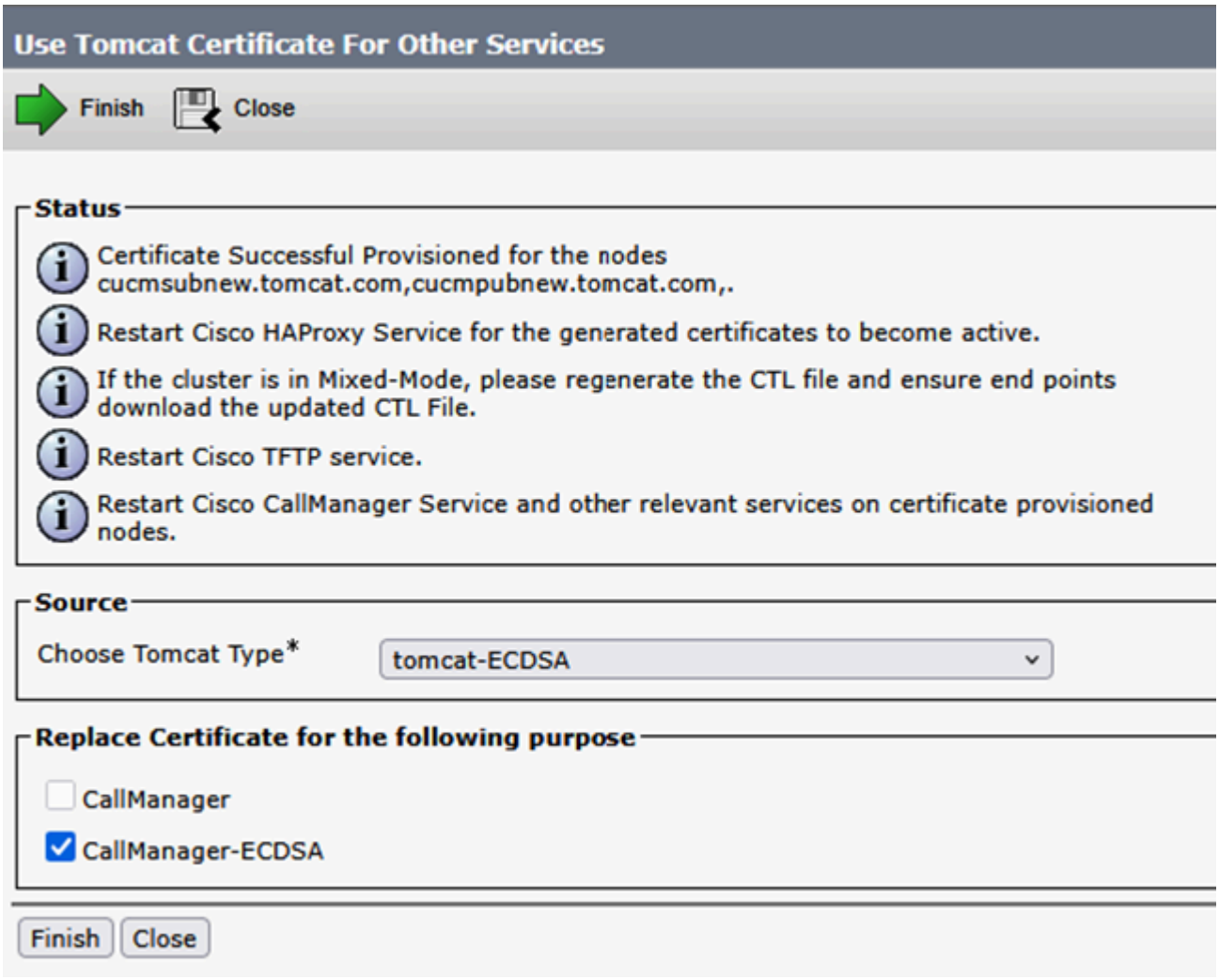


Tomcat e Tomcat-ECDSA assinados pela CA.

Agora reutilize Tomcat-ECDSA como certificado Callmanager-ECDSA.



Carregamento bem-sucedido. Reinicie os serviços relevantes conforme solicitado.



Verifique os certificados da CLI.

SN de certificado do Callmanager-ECDSA:
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
```

Certificado Tomcat-ECDSA 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)
```

Como você agora está usando um certificado para dois serviços, ou seja, o certificado Tomcat para serviços Tomcat e Callmanager, e o Tomcat-ECDSA para serviços Tomcat-ECDSA e Callmanager-ECDSA, torna-se menos incômodo carregar certificados no repositório de confiança do Expressway (se necessário, carregar).

Ter o TLS de verificação 'Ativado' ao adicionar o UCM no expressway-core para MRA ficou mais fácil do que nunca. Basta adicionar uma CA de certificado do Tomcat ou um certificado do servidor para fazer o trabalho (porque o certificado é compartilhado agora entre o Callmanager e o serviço Tomcat).

Se uma atualização para x14.2 ou posterior tiver causado uma interrupção do acesso remoto móvel, você também pode consultar este documento abrangente para Solucionar o problema.

Histórico de Versão do Apache Traffic Server

Para verificar a versão em seu servidor, faça login no root e execute ~ # /apache2/bin/httpd -v.

Expressway x8.11.4
Versão do servidor: Apache/2.4.34 (Unix)
Compilação do servidor: 12 de novembro de 2018 19:04:23

Expressway x12.6

Versão do servidor: Apache/2.4.43 (Unix)
Compilação do servidor: 26 de maio de 2020 18:27:21

Expressway x14.0.8

Versão do servidor: Apache/2.4.53 (Unix)
Compilação do servidor: 4 de maio de 2022 08:52:57

Expressway x15.3

Versão do servidor: Apache/2.4.62 (Unix)
Compilação do servidor: 16 de julho de 2025 12:10:19

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.