Criar novos certificados de CA assinada

Contents

Introdução

Este documento descreve como gerar novamente os certificados assinados por uma CA (Certificate Authority, autoridade de certificação) no Cisco Unified Communications Manager (CUCM).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Ferramenta de monitoramento em tempo real (RTMT)
- Certificados CUCM

Componentes Utilizados

- CUCM versão 10.x, 11.x e 12.x.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de pré-verificação

Observação: para a regeneração de certificados com assinatura automática, consulte o Guia de Regeneração de Certificados. Para a regeneração de certificados Multi-SAN com assinatura de CA, consulte o Guia de Regeneração de Certificados Multi-SAN

Para entender o impacto de cada certificado e sua regeneração, consulte o Guia de Regeneração Autoassinada.

Cada tipo de CSR (Certificate Signing Request, Solicitação de assinatura de certificado) tem diferentes usos de chave, que são exigidos no certificado assinado. O Guia de Segurança inclui uma tabela com os usos de chave necessários para cada tipo de certificado.

Para alterar as configurações do assunto (localidade, estado, unidade organizacional etc.), execute este comando:

- **set web-security** orgunit orgname locality state [country] [alternatehostname]

O certificado Tomcat é gerado novamente automaticamente depois que você executa o`set web-security`comando. O novo certificado com assinatura automática não é aplicado, a menos que o serviço Tomcat seja reiniciado. Consulte esses guias para obter mais informações sobre esse comando:

- Guia de referência de linha de comando
- Link para as etapas da comunidade Cisco
- Vídeo

Configurar e regenerar certificados

As etapas para gerar novamente certificados de nó único em um cluster CUCM assinado por uma CA são listadas para cada tipo de certificado. Não é necessário gerar novamente todos os certificados no cluster se eles não tiverem expirado.

Certificado Tomcat

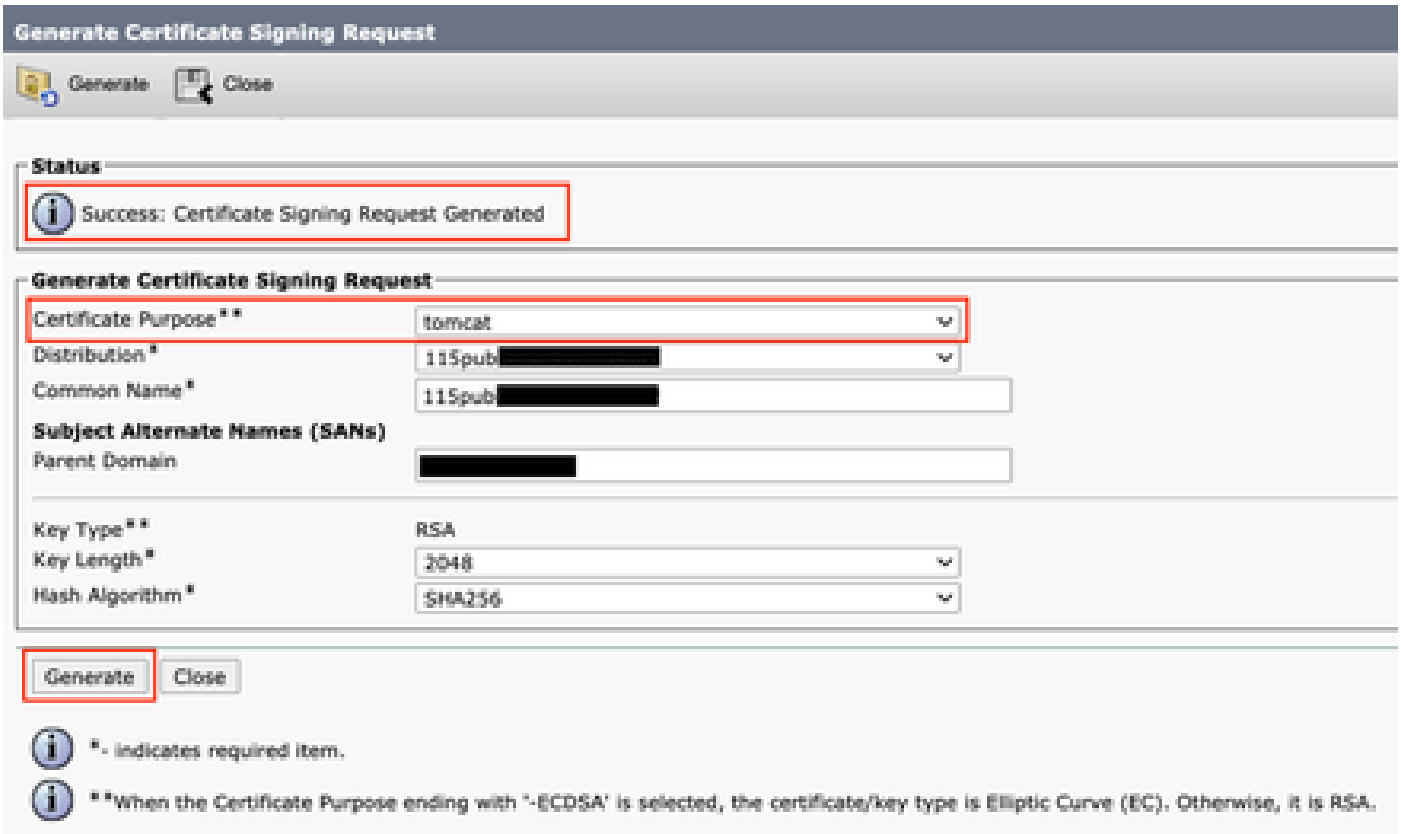
Cuidado: verifique se o SSO está desabilitado no cluster (**CM Administration** > **System** > **SAML Single Sign-On**). Se o SSO estiver habilitado, ele deverá ser desabilitado e habilitado depois que o processo de regeneração do certificado Tomcat estiver concluído.

Em todos os nós (CallManager e IM&P) do cluster:

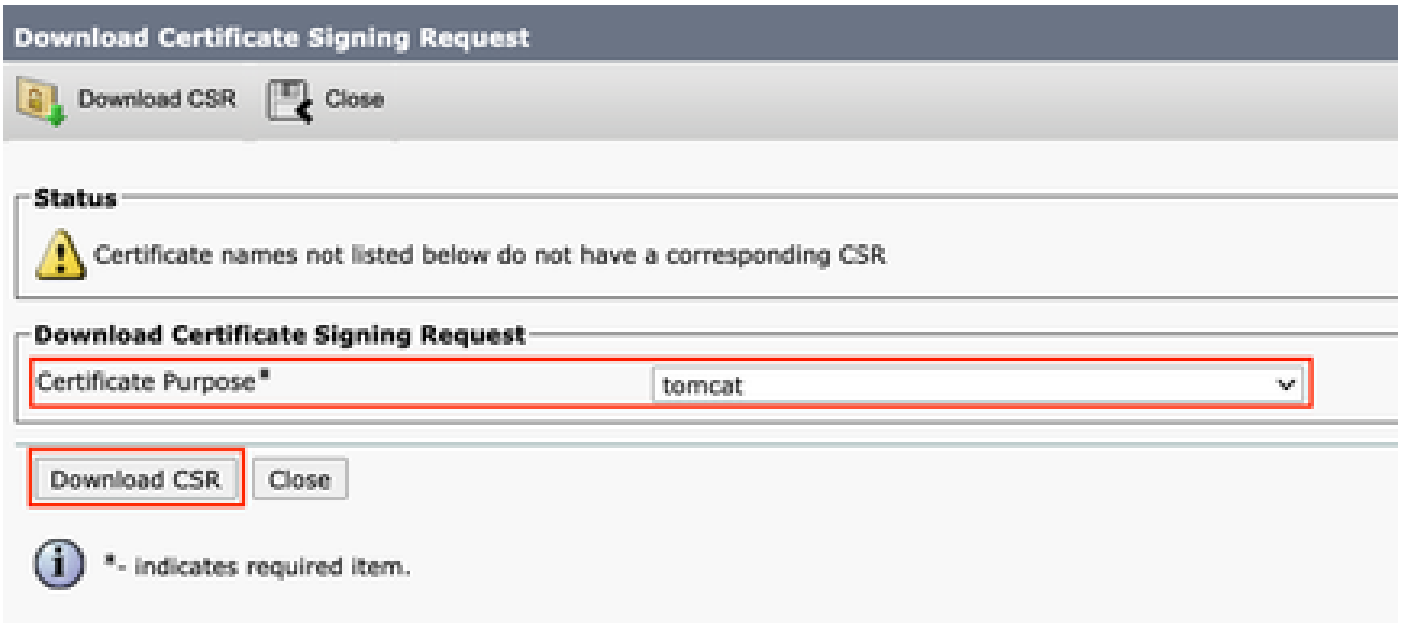
Etapa 1. Navegue até **Cisco Unified OS Administration** > **Security** > **Certificate Management** > **Find** e verifique a data

de expiração do certificado Tomcat.

Etapa 2. Clique emGenerate CSR > Certificate Purpose: tomcat. Selecione as configurações desejadas para o certificado e clique emGenerate. Aguarde até que a mensagem de êxito seja exibida e clique emClose.



Etapa 3. Faça o download do CSR. Clique emDownload CSR, selecione **Certificate Purpose: tomcat**, e clique emDownload.



Etapa 4. Envie o CSR para a autoridade de certificação.

Etapa 5. A Autoridade de Certificação retorna dois ou mais arquivos para a cadeia de certificados

assinados. Carregar os certificados nesta ordem:

- Certificado CA raiz como tomcat-trust. Navegue para **Certificate Management** > **Upload certificate** > **Certificate Purpose: tomcat-trust**. Definir a descrição do certificado e procure o arquivo de certificado Raiz.
- Certificado intermediário como tomcat-trust (Opcional). Navegue até **Certificate Management** > **Upload certificate** > **Certificate Purpose: tomcat-trust**. Defina a descrição do certificado e procure o arquivo de certificado intermediário.

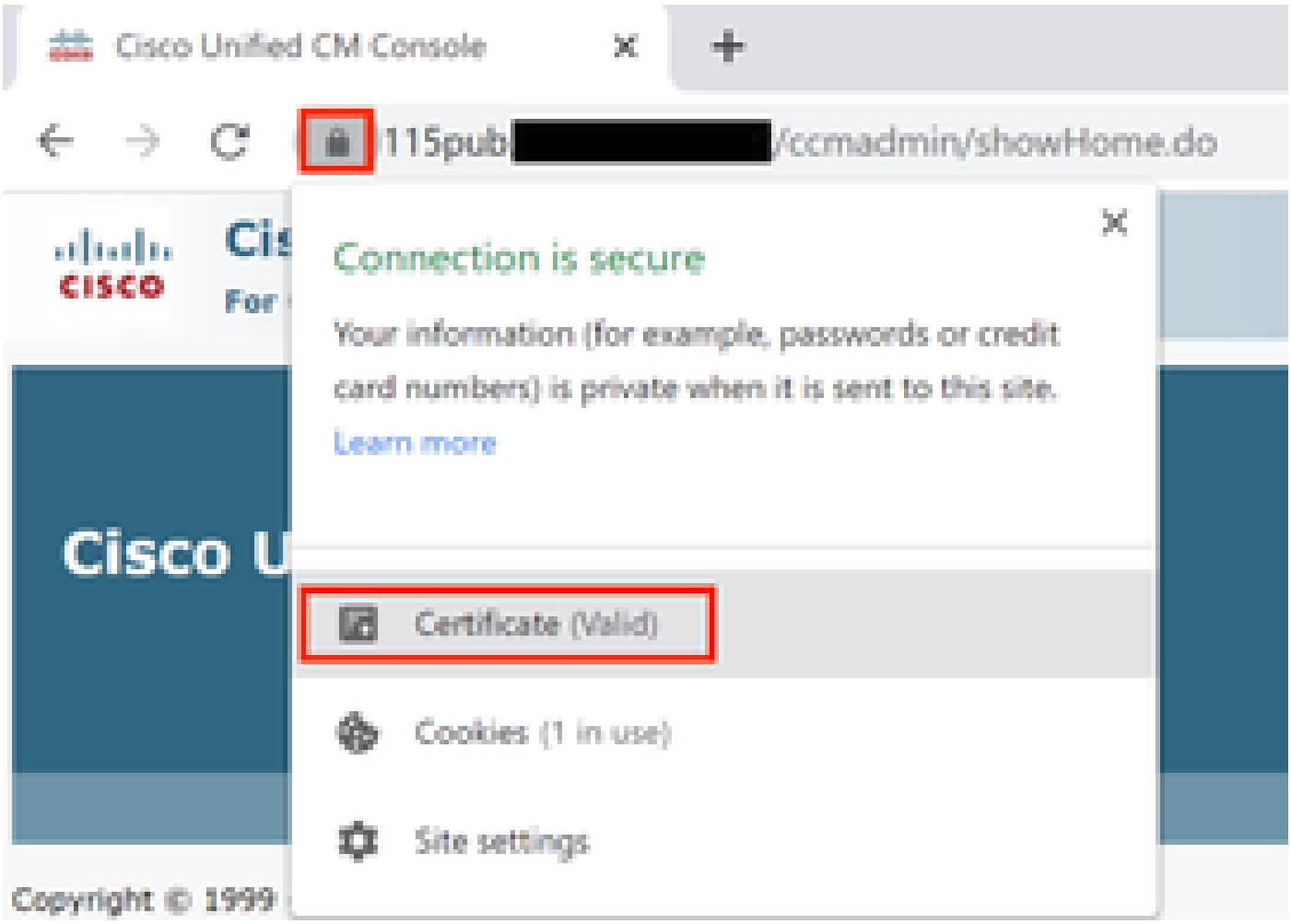
Observação: algumas CAs não fornecem um certificado intermediário. Se apenas o certificado Raiz tiver sido fornecido, essa etapa poderá ser omitida.

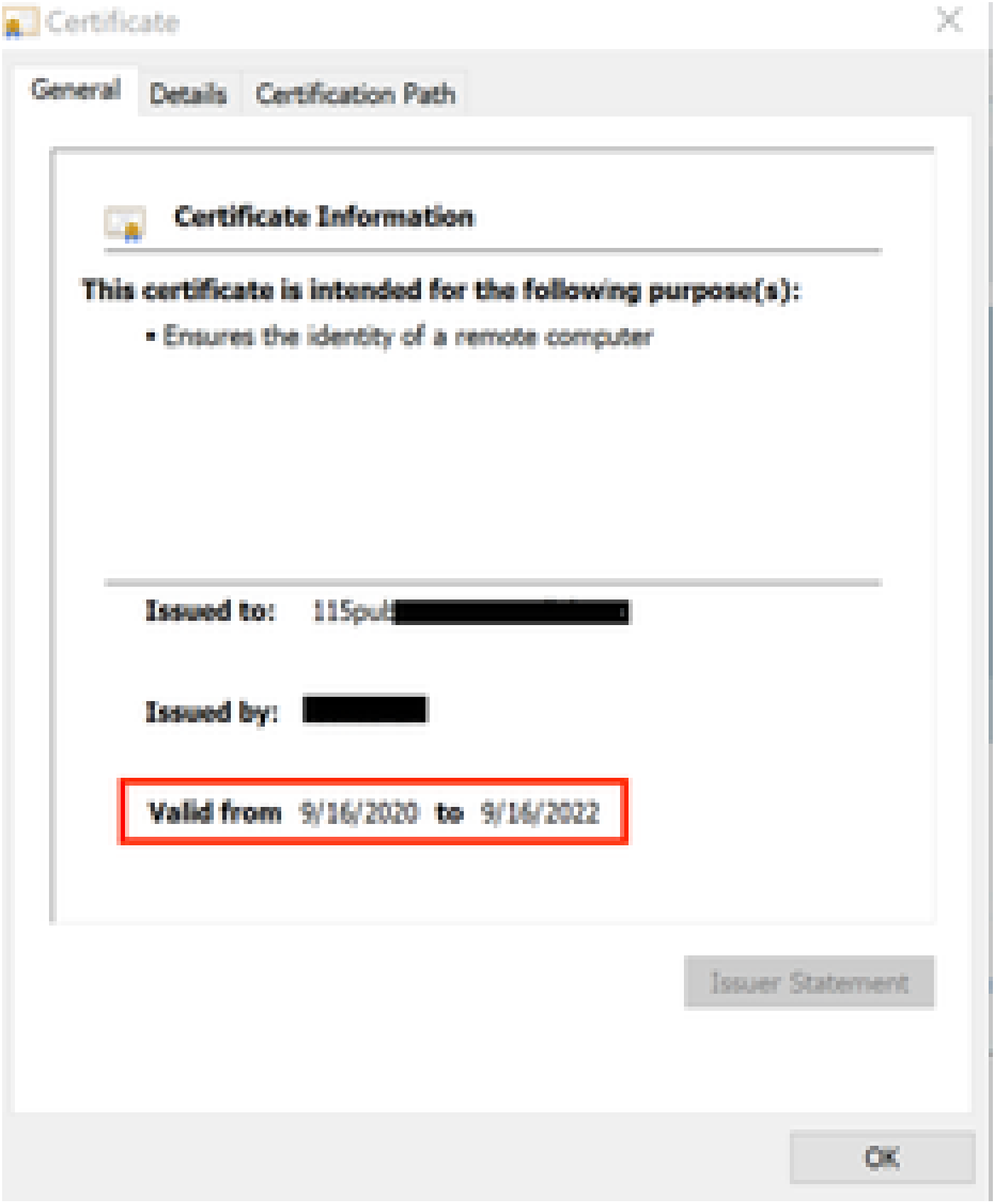
- Certificado assinado pela CA como tomcat. Navegue atéCertificate Management > Upload certificate > Certificate Purpose: tomcat. Defina a descrição do certificado e procure o arquivo de certificado assinado pela CA para o nó CUCM atual.

Observação: neste ponto, o CUCM compara o CSR e o certificado assinado por CA carregado. Se as informações coincidirem, o CSR desaparecerá e o novo certificado assinado pela CA será carregado. Se você receber uma mensagem de erro depois que o certificado for carregado, consulte a seção a seguir Upload Certificate Common Error Messages .

Etapa 6. Para que o novo certificado seja aplicado ao servidor, o serviço Cisco Tomcat precisa ser reiniciado via CLI (comece com o Publisher e, em seguida, os assinantes, um de cada vez), use o comando utils service restart Cisco Tomcat.

Para validar se o certificado Tomcat agora é usado pelo CUCM, navegue para a página da Web do nó e selecione Site Information(Ícone de bloqueio) no navegador. Clique na opção certificatee verifique a data do novo certificado.


Cisco Unified CM Console
115pub[redacted]/ccmadmin/showHome.do
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site.
Learn more
Certificate (Valid)
Cookies (1 in use)
Site settings
Copyright © 1999



Certificado do CallManager

⚠ Cuidado: não gere novamente os certificados CallManager e TVS ao mesmo tempo. Isso causa uma incompatibilidade irrecuperável com o ITL instalado nos pontos de extremidade, o que requer a remoção do ITL de TODOS os pontos de extremidade no cluster. Conclua

todo o processo para o CallManager e, uma vez que os telefones estejam registrados novamente, inicie o processo para a TVS.

Observação: para determinar se o cluster está no Modo Misto, navegue até Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non-Secure; 1 == Mixed Mode).

Para todos os nós do CallManager do cluster:

Etapa 1. Navegue Cisco Unified OS Administration > Security > Certificate Management > Find e verifique a data de expiração do certificado do CallManager.

Etapa 2. Clique emGenerate CSR > Certificate Purpose: CallManager. Selecione as configurações desejadas para o certificado e clique emGenerate. Aguarde até que a mensagem de êxito seja exibida e clique emClose.

Etapa 3. Faça o download do CSR. Clique em **Download CSR**. Select **Certificate Purpose: CallManager** and click **Download**.

Etapa 4. Envie o CSR para o Certificate Authority .

Etapa 5. A Autoridade de Certificação retorna dois ou mais arquivos para a cadeia de certificados assinados. Carregar os certificados nesta ordem:

- Certificado CA raiz como CallManager-trust. Navegue atéCertificate Management > Upload certificate > Certificate Purpose: CallManager-trust. Defina a descrição do certificado e procure o arquivo de certificado Raiz.
- Certificado intermediário como CallManager-trust (Opcional). Navegue atéCertificate Management > Upload certificate > Certificate Purpose: CallManager-trust. Defina a descrição do certificado e procure o arquivo de certificado intermediário.

Observação: algumas CAs não fornecem um certificado intermediário. Se apenas o certificado Raiz tiver sido fornecido, essa etapa poderá ser omitida.

- Certificado assinado pela CA como CallManager. Navegue atéCertificate Management > Upload certificate > Certificate Purpose: CallManager. Defina a descrição do certificado e procure o arquivo de certificado assinado pela CA para o nó CUCM atual.

Observação: neste ponto, o CUCM compara o CSR e o certificado assinado por CA carregado. Se as informações coincidirem, o CSR desaparecerá e o novo certificado assinado pela CA será carregado. Se você receber uma mensagem de erro depois que o certificado for carregado, consulte a seção Carregar Mensagens de Erro Comuns de Certificado.

Etapa 6. Se o cluster estiver no modo misto, atualize a lista de certificados confiáveis antes de

reiniciar os serviços: Token ou Sem tokens. Se o cluster estiver no Modo Não Seguro, ignore esta etapa e continue com a reinicialização dos serviços.

Passo 7. Para que o novo certificado seja aplicado ao servidor, os serviços necessários devem ser reiniciados (somente se o serviço for executado e estiver ativo). Navegue até:

- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CallManager
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CTIManager

Etapa 8. Reinicie todos os telefones:

- Navegue atéCisco Unified CM Administration > System > Enterprise Parameters > Reset. Uma janela pop-up é exibida com a instrução You are about to reset all devices in the system (Você está prestes a redefinir todos os dispositivos no sistema). Esta ação não pode ser desfeita. Continuar? selecione OK e clique em Reset .

Observação: monitore o registro do dispositivo via RTMT. Depois que todos os telefones forem registrados novamente, você poderá prosseguir com o próximo tipo de certificado.

Certificado IPSec

Cuidado: uma tarefa de backup ou restauração não deve estar ativa quando o certificado IPSec for gerado novamente.

Para todos os nós (CallManager e IM&P) do cluster:

Etapa 1. Navegue atéCisco Unified OS Administration > Security > Certificate Management > Finde verifique a data de expiração do certificado ipsec.

Etapa 2. Clique em Generate CSR > Certificate Purpose: ipsec. Selecione as configurações desejadas para o certificado e clique em Gerar. Aguarde até que a mensagem de êxito seja exibida e clique em Fechar.

Etapa 3. Faça o download do CSR. Clique em Download CSR. Selecione IPSec de propósito do certificado e clique em Download.

Etapa 4. Envie o CSR para a autoridade de certificação.

Etapa 5. A Autoridade de Certificação retorna dois ou mais arquivos para a cadeia de certificados assinados. Carregar os certificados nesta ordem:

- Certificado CA raiz como ipsec-trust. Navegue até Gerenciamento de certificados > Carregar certificado > Finalidade do certificado: ipsec-trust. Defina a descrição do certificado e procure o arquivo de certificado Raiz.
- Certificado intermediário como ipsec-trust (Opcional). Navegue até Gerenciamento de

certificados > Carregar certificado > Finalidade do certificado: tomcat-trust. Defina a descrição do certificado e procure o arquivo de certificado intermediário.

Observação: algumas CAs não fornecem um certificado intermediário. Se apenas o certificado Raiz tiver sido fornecido, essa etapa poderá ser omitida.

- Certificado assinado pela CA como IPSec. Navegue até Gerenciamento de certificados > Carregar certificado > Objetivo do certificado: ipsec. Defina a descrição do certificado e procure o arquivo de certificado assinado pela CA para o nó CUCM atual.

Observação: neste ponto, o CUCM compara o CSR e o certificado assinado por CA carregado. Se as informações coincidirem, o CSR desaparecerá e o novo certificado assinado pela CA será carregado. Se você receber uma mensagem de erro depois que o certificado for carregado, consulte a seção Carregar mensagens de erro comuns de certificados< /strong>.

Etapa 6. Para que o novo certificado seja aplicado ao servidor, os serviços necessários devem ser reiniciados (somente se o serviço for executado e estiver ativo). Navegue até:

- Cisco Unified Serviceability > Ferramentas > Centro de controle - Serviços de rede > Cisco DRF Master(Editor)
- Cisco Unified Serviceability > Ferramentas > Centro de Controle - Serviços de Rede > Cisco DRF Local (Editor e Assinantes)

Certificado CAPF

Observação: para determinar se o cluster está no Modo Misto, navegue até Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non-Secure; 1 == Mixed Mode).

Observação: o serviço CAPF é executado apenas no Publicador e esse é o único certificado usado. Não é necessário obter nós de assinante assinados por uma autoridade de certificação porque eles não são usados. Se o certificado tiver expirado nos Assinantes e você quiser evitar os alertas de certificados expirados, poderá gerar novamente os certificados CAPF do assinante como Autoassinado. Para obter mais informações, consulte Certificado CAPF como Autoassinado.

No Editor:

Etapa 1. Navegue para Cisco Unified OS Administration > Security > Certificate Management > Find e verifique a data de expiração do certificado CAPF.

Etapa 2. Clique em Generate CSR > Certificate Purpose: CAPF. Selecione as configurações

desejadas para o certificado e clique em Gerar. Aguarde até que a mensagem de êxito seja exibida e clique em Fechar.

Etapa 3. Faça o download do CSR. Clique em Download CSR. Selecione Certificate Purpose CAPF e clique em Download.

Etapa 4. Envie o CSR para a autoridade de certificação.

Etapa 5. A Autoridade de Certificação retorna dois ou mais arquivos para a cadeia de certificados assinados. Carregar os certificados nesta ordem:

- Certificado CA raiz como CAPF-trust. Navegue até Gerenciamento de certificados > Carregar certificado > Finalidade do certificado: CAPF-trust. Defina a descrição do certificado e procure o arquivo de certificado Raiz.
- Certificado intermediário como CAPF-trust (Opcional). Navegue até Gerenciamento de certificados > Carregar certificado > Finalidade do certificado: CAPF-trust. Defina a descrição do certificado e procure o arquivo de certificado intermediário.

Observação: algumas CAs não fornecem um certificado intermediário. Se apenas o certificado Raiz tiver sido fornecido, essa etapa poderá ser omitida.

- Certificado assinado pela CA como CAPF. Navegue para Gerenciamento de Certificado > Carregar certificado > Finalidade do Certificado: CAPF. Defina a descrição do certificado e procure o arquivo de certificado assinado pela CA para o nó CUCM atual.

Observação: neste ponto, o CUCM compara o CSR e o certificado assinado por CA carregado. Se as informações coincidirem, o CSR desaparecerá e o novo certificado assinado pela CA será carregado. Se você receber uma mensagem de erro após o upload do certificado, consulte a seção Upload Certificate Common Error Messages.

Etapa 6. Se o cluster estiver no modo misto, atualize a lista de certificados confiáveis antes de reiniciar os serviços: Token ou Sem tokens. Se o cluster estiver no Modo Não Seguro, ignore esta etapa e continue com a reinicialização do serviço.

Passo 7. Para obter o novo certificado aplicado ao servidor, os serviços necessários devem ser reiniciados (somente se o serviço for executado e estiver ativo). Navegue até:

- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service (Todos os nós em que o serviço é executado).
- Cisco Unified Serviceability > Ferramentas > Centro de controle - Serviços de recursos > Cisco TFTP (todos os nós em que o serviço é executado).
- Cisco Unified Serviceability > Ferramentas > Centro de Controle - Serviços de Recursos > Cisco Certificate Authority Proxy Function (Editor)

Etapa 8. Reinicie todos os telefones:

- Navegue até Cisco Unified CM Administration > System > Enterprise Parameters > Reset.

Uma janela pop-up é exibida com a instrução You are about to reset all devices in the system (Você está prestes a redefinir todos os dispositivos no sistema). Esta ação não pode ser desfeita. Continuar? selecione OK e clique em Redefinir.

Observação: monitore o registro do dispositivo via RTMT. Depois que todos os telefones forem registrados novamente, você poderá prosseguir com o próximo tipo de certificado.

Certificado TVS

Cuidado: não gere novamente os certificados CallManager e TVS ao mesmo tempo. Isso causa uma incompatibilidade irrecuperável com o ITL instalado nos pontos de extremidade, o que requer a remoção do ITL de TODOS os pontos de extremidade no cluster. Conclua todo o processo para o CallManager e, uma vez que os telefones estejam registrados novamente, inicie o processo para a TVS.

Para todos os nós TVS do cluster:

Etapa 1. Navegue para Cisco Unified OS Administration > Security > Certificate Management > Find e verifique a data de expiração do certificado TVS.

Etapa 2. Clique em Generate CSR > Certificate Purpose: TVS. Selecione as configurações desejadas para o certificado e clique em Gerar. Aguarde até que a mensagem de êxito seja exibida e clique em Fechar.

Etapa 3. Faça o download do CSR. Clique em Download CSR. Selecione Certificate Purpose TVS e clique em Download.

Etapa 4. Envie o CSR para a autoridade de certificação.

Etapa 5. A Autoridade de Certificação retorna dois ou mais arquivos para a cadeia de certificados assinados. Carregar os certificados nesta ordem:

- Certificado CA raiz como TVS-trust. Navegue até Gerenciamento de certificados > Carregar certificado > Finalidade do certificado: TVS-trust. Defina a descrição do certificado e procure o arquivo de certificado Raiz.
- Certificado intermediário como TVS-trust (Opcional). Navegue até Gerenciamento de certificados > Carregar certificado > Finalidade do certificado: TVS-trust. Defina a descrição do certificado e procure o arquivo de certificado intermediário.

Observação: algumas CAs não fornecem um certificado intermediário. Se apenas o certificado Raiz tiver sido fornecido, essa etapa poderá ser omitida.

- Certificado assinado pela CA como TVS. Navegue até Gerenciamento de certificados > Carregar certificado > Objetivo do certificado: TVS. Defina a descrição do certificado e procure o arquivo de certificado assinado pela CA para o nó CUCM atual.

Observação: neste ponto, o CUCM compara o CSR e o certificado assinado por CA carregado. Se as informações coincidirem, o CSR desaparecerá e o novo certificado assinado pela CA será carregado. Se você receber uma mensagem de erro depois que o certificado for carregado, consulte a seção Carregar Mensagens de Erro Comuns de Certificado.

Etapa 6. Para que o novo certificado seja aplicado ao servidor, os serviços necessários devem ser reiniciados (somente se o serviço for executado e estiver ativo). Navegue até:

- Cisco Unified Serviceability > Ferramentas > Centro de controle - Serviços de recursos > Cisco TFTP (Todos os nós em que o serviço é executado.)
- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service (Todos os nós em que o serviço é executado).

Passo 7. Reinicie todos os telefones:

- Navegue até Cisco Unified CM Administration > System > Enterprise Parameters > Reset. Uma janela pop-up é exibida com a instrução You are about to reset all devices in the system (Você está prestes a redefinir todos os dispositivos no sistema). Esta ação não pode ser desfeita. Continuar? selecione OK e clique em Redefinir.

Observação: monitore o registro do dispositivo via RTMT. Quando todos os telefones forem registrados novamente, você poderá prosseguir com o próximo tipo de certificado.

Solucionar problemas comuns de mensagens de erro de certificado carregado

Nesta seção, são listadas algumas das mensagens de erro mais comuns quando um certificado assinado por CA é carregado.

O Certificado de Autoridade de Certificação não está disponível no Repositório Confiável

Esse erro significa que o certificado raiz ou intermediário não foi carregado no CUCM. Verifique se esses dois certificados foram carregados como um armazenamento confiável antes do upload do certificado de serviço.

O arquivo /usr/local/platform/.security/tomcat/keys/tomcat.csr não existe

Este erro aparece quando um CSR não existe para o certificado (tomcat, callmanager, ipsec, capf, tvs). Verifique se o CSR foi criado antes e se o certificado foi criado com base nesse CSR. Pontos importantes a serem lembrados:

- Só pode existir 1 CSR por servidor e tipo de certificado. Isso significa que, se um novo CSR for criado, o antigo será substituído.

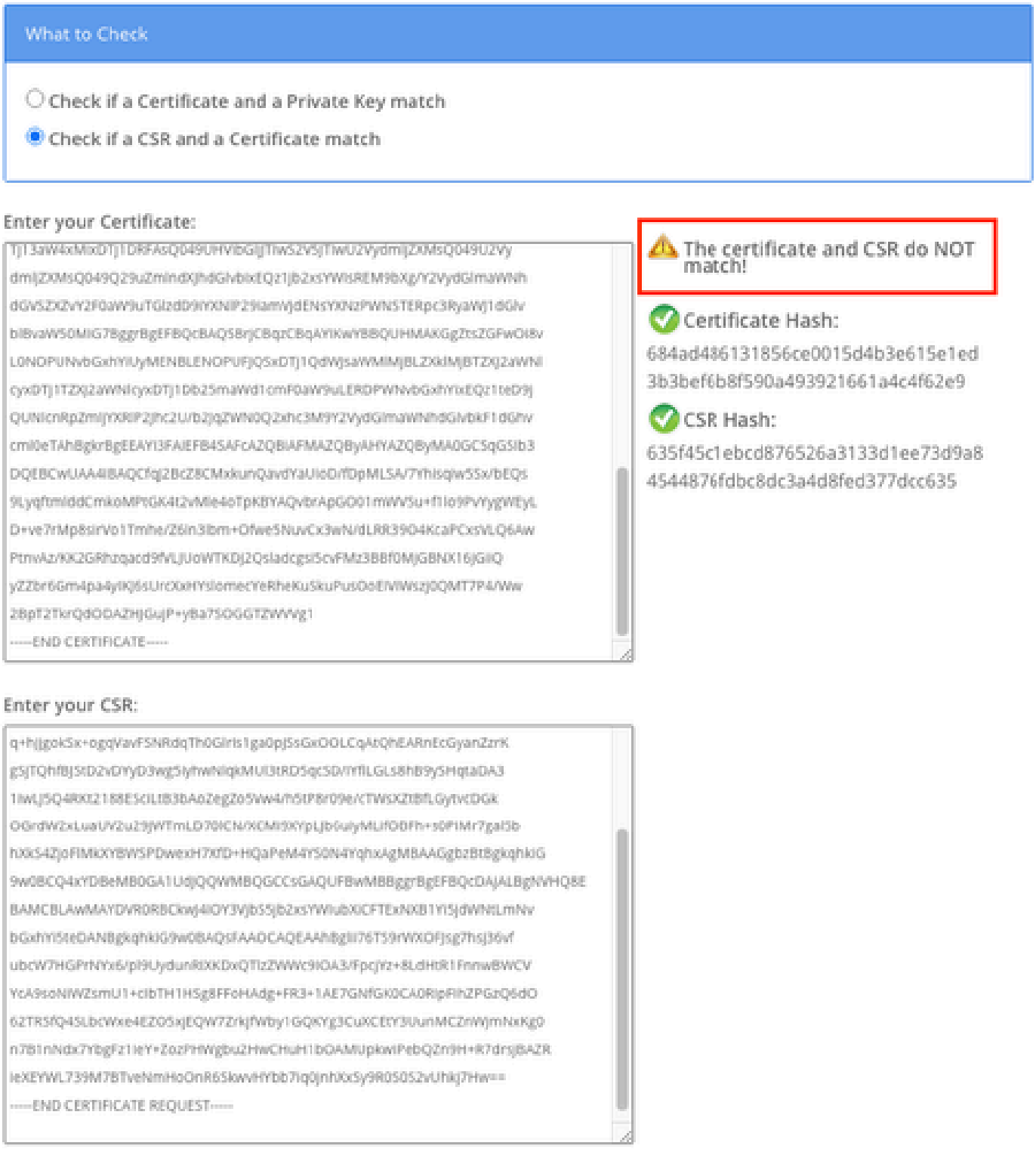
- O CUCM não oferece suporte a certificados curinga.
- Não é possível substituir um certificado de serviço que esteja em vigor sem um novo CSR.
- Outro erro possível para o mesmo problema é "Não foi possível carregar o arquivo /usr/local/platform/upload/certs//tomcat.der." Isso depende da versão do CUCM.

A chave pública CSR e a chave pública de certificado não coincidem

Este erro aparece quando o certificado fornecido pela CA tem uma chave pública diferente da enviada no arquivo CSR. As possíveis razões são:

- O certificado incorreto (talvez de outro nó) foi carregado.
- O certificado CA foi gerado com um CSR diferente.
- O CSR foi gerado novamente e substituiu o CSR antigo usado para obter o certificado assinado.

Para verificar se o CSR e a chave pública de certificado correspondem, há várias ferramentas on-line, como SSL.



Outro erro possível para o mesmo problema é "Não foi possível carregar o arquivo /usr/local/platform/upload/certs//tomcat.der." Isso depende da versão do CUCM.

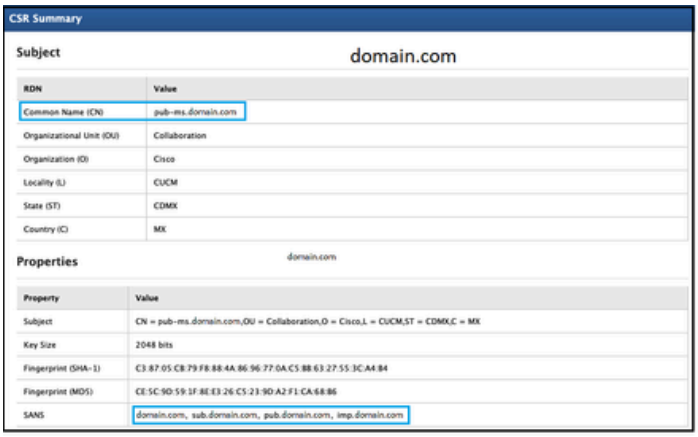
A SAN de Certificado e o Nome Alternativo de Requerente (SAN) do CSR não correspondem

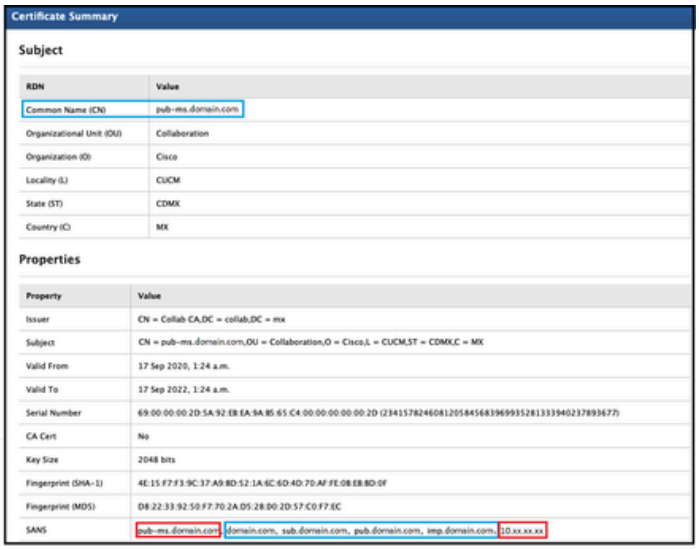
As SANs entre o CSR e o certificado devem ser as mesmas. Isso impede a certificação para Domínios que não são permitidos. Para verificar a incompatibilidade da SAN, siga estas etapas:

1. Decodifique o CSR e o certificado (base 64). Há diferentes decodificadores disponíveis online, como o Decoder.

2. Compare as entradas SAN e verifique se todas elas correspondem. A ordem não é importante, mas todas as entradas no CSR devem ser as mesmas no certificado.

Por exemplo, o certificado assinado pela CA tem duas entradas SAN adicionais adicionadas, o Nome comum do certificado e um endereço IP extra.



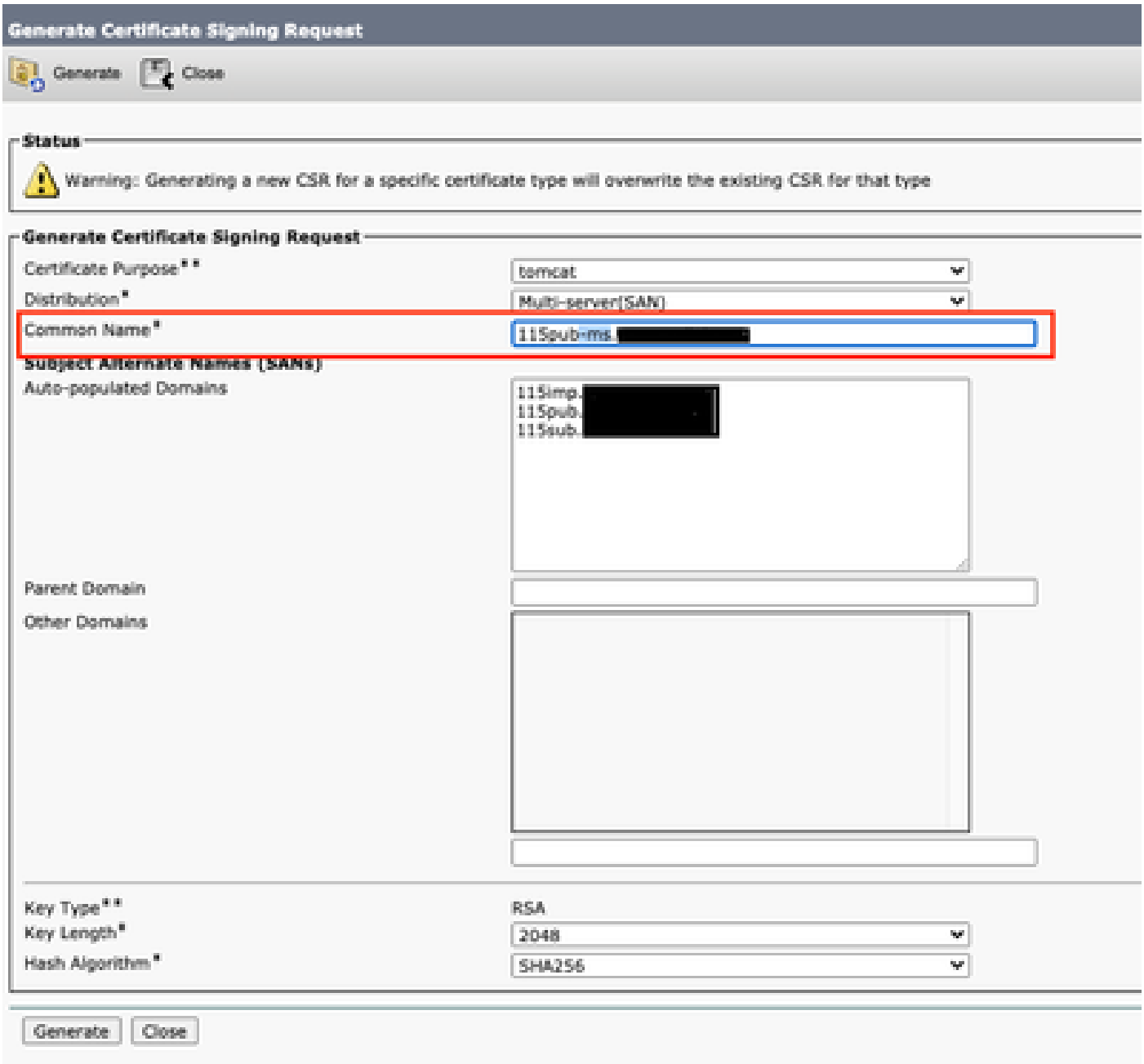


3. Depois de identificar que a SAN não corresponde, há duas opções para corrigir isso:

1. Solicite ao administrador de CA que emita um certificado com as mesmas entradas SAN enviadas no CSR.
2. Crie um CSR no CUCM que corresponda aos requisitos da CA.

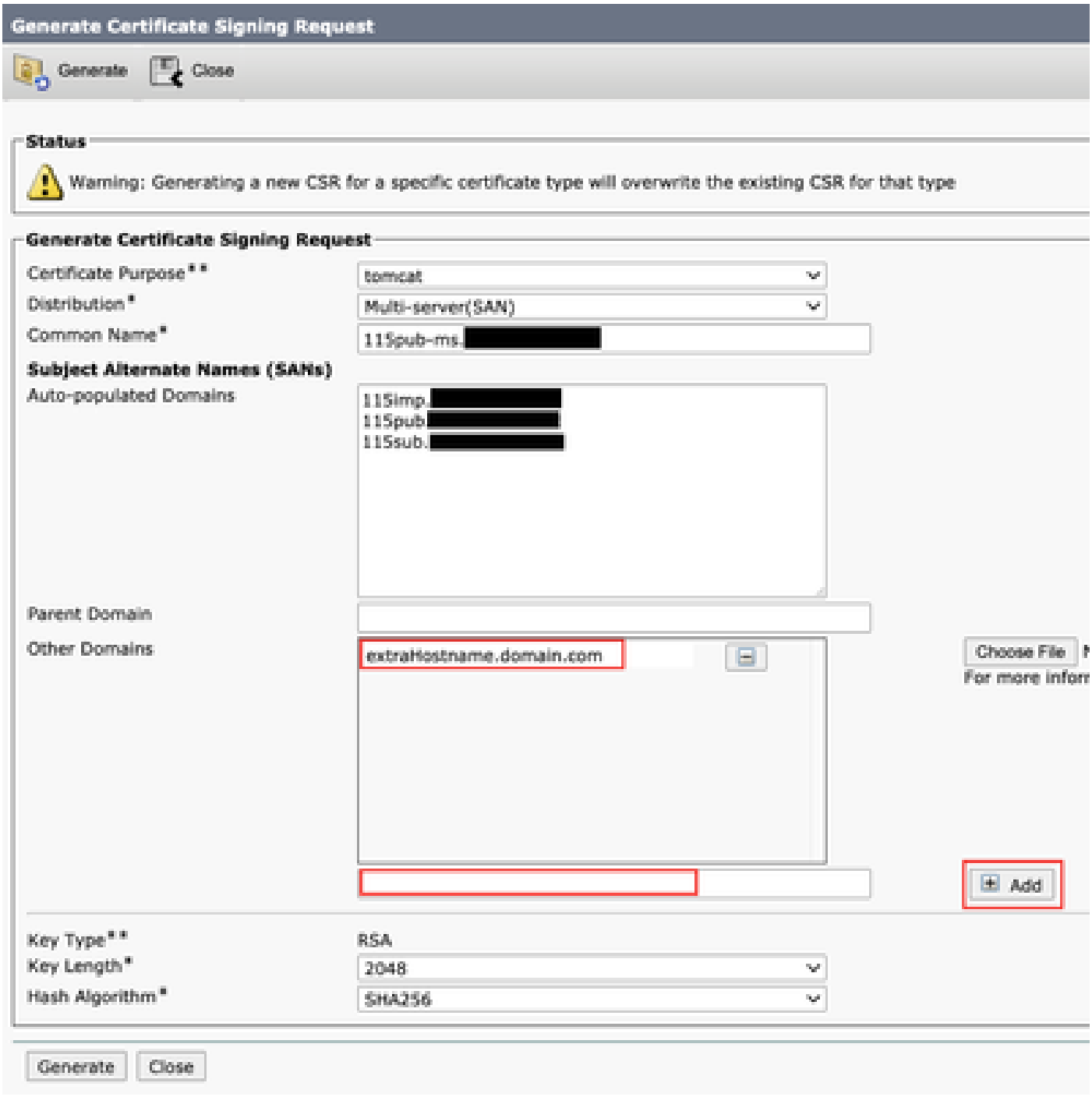
Para modificar o CSR criado pelo CUCM:

1. Se a CA remover o domínio, um CSR no CUCM pode ser criado sem o domínio. Durante a criação do CSR, remova o domínio preenchido por padrão.
2. Se um certificado Multi-SAN for criado, há algumas CAs que não aceitam o -ms no Nome comum. O -ms pode ser removido do CSR quando ele é criado.



3. Para adicionar um nome alternativo além daqueles preenchidos automaticamente pelo CUCM:

    1. Se o certificado Multi-SAN for usado, mais FQDN poderá ser adicionado. (Os endereços IP não são aceitos.)



b. Se o certificado for Single Node, use o comando`set web-security`. Esse comando se aplica até mesmo a certificados Multi-SAN. (Qualquer tipo de domínio pode ser adicionado, e os endereços IP também são permitidos.)

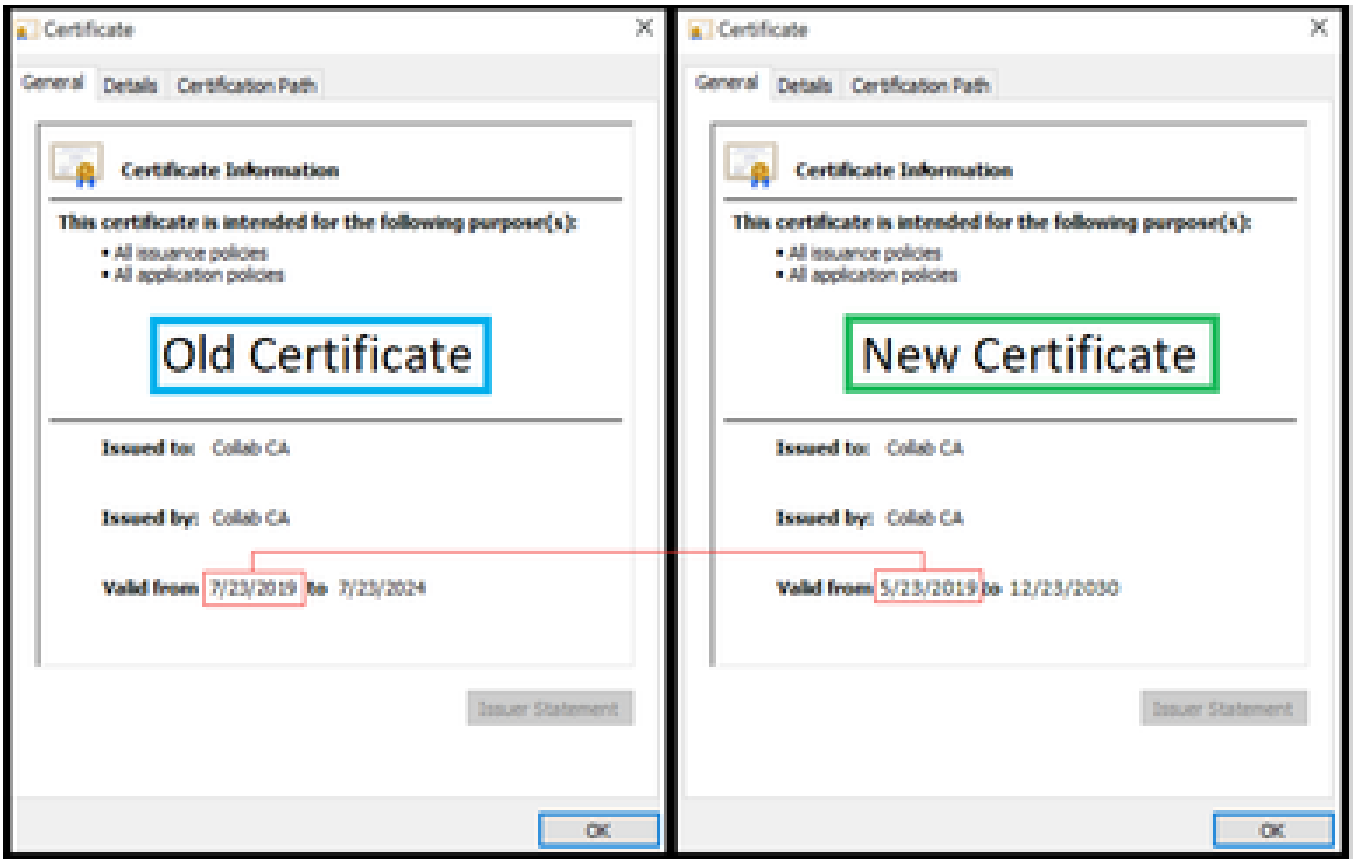
Para obter mais informações, consulte o Guia de Referência de Linha de Comando.

Certificados confiáveis com o mesmo CN não são substituídos

O CUCM foi projetado para armazenar apenas um certificado com o mesmo Nome comum e o mesmo tipo de certificado. Isso significa que se um certificado que é tomcat-trust já existe no banco de dados e precisa ser substituído por um recente com o mesmo CN, o CUCM remove o certificado antigo e o substitui pelo novo.

Há alguns casos em que o CUCM não substitui o certificado antigo:

1. O certificado carregado expirou: o CUCM não permite que você carregue um certificado expirado.
2. O certificado antigo tem uma data FROM mais recente do que o novo certificado. O CUCM mantém o certificado mais recente, e a data DE DA mais antiga é catalogada como mais antiga. Para esse cenário, é necessário excluir o certificado indesejado e carregar o novo.



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.