Regeneração de certificados para CUCM

Contents

Introduction

Este documento descreve o procedimento para gerar novamente certificados no Cisco Unified Communications Manager (CUCM) versão 8.X e posterior.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CUCM versão 8.X e superior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve o procedimento passo a passo sobre como gerar novamente certificados no Cisco Unified Communications Manager (CUCM) versão 8.X e mais recente. No entanto, isso não reflete as alterações após 12.0 para recuperação de ITL.

Instalar RTMT

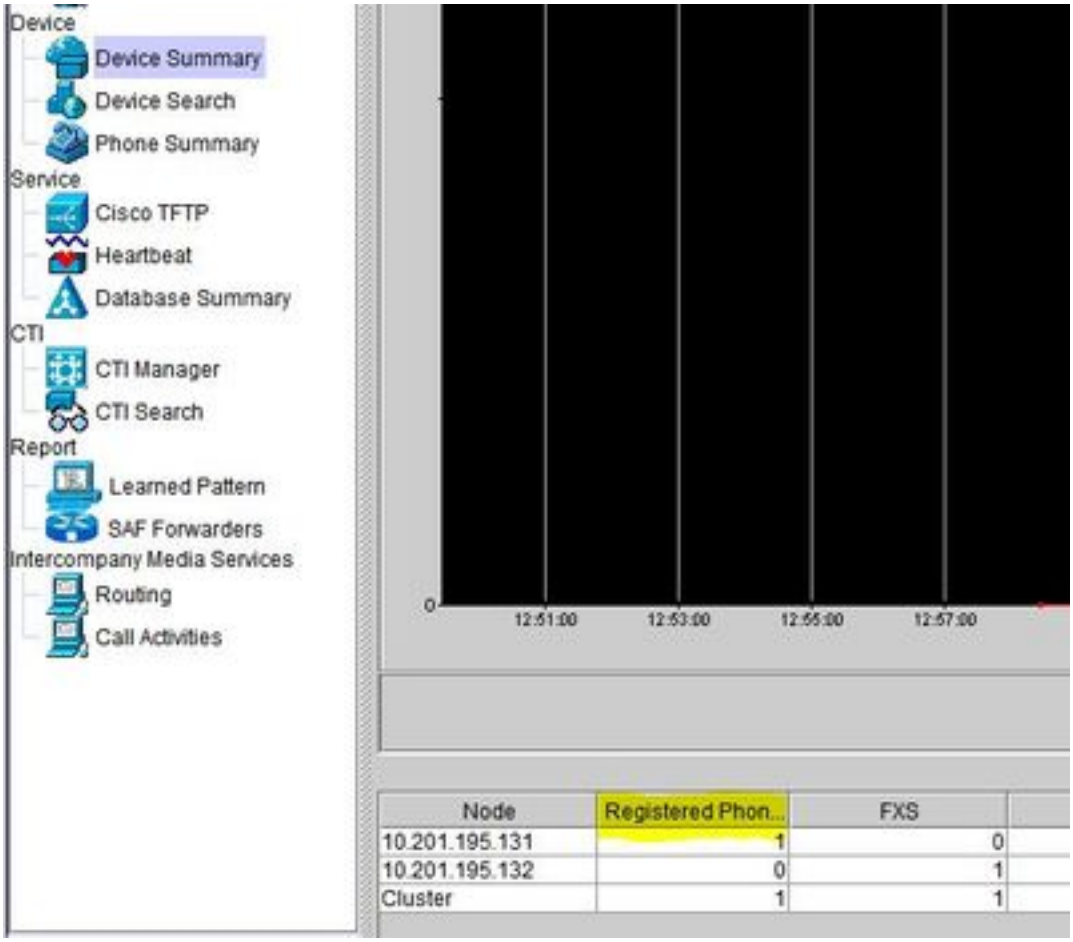
- Baixe e instale a ferramenta RTMT do Call Manager. Navegue até Call Manager (CM) Administration: **Aplicativo > Plug-ins > Localizar > Ferramenta de monitoramento em tempo real Cisco Unified - Windows > Download** Instalar e iniciar

Monitorar endpoints com RTMT

- Inicie a RTMT e insira o endereço IP ou o nome de domínio totalmente qualificado (FQDN), depois o nome de usuário e a senha para acessar a ferramenta:
- Selecione a **guia Voz/Vídeo**.Selecione **Device Summary**. Esta seção identifica o número total de terminais registrados e quantos cada nóMonitorar enquanto o ponto de extremidade é redefinido para garantir o registro antes da regeneração do próximo certificado

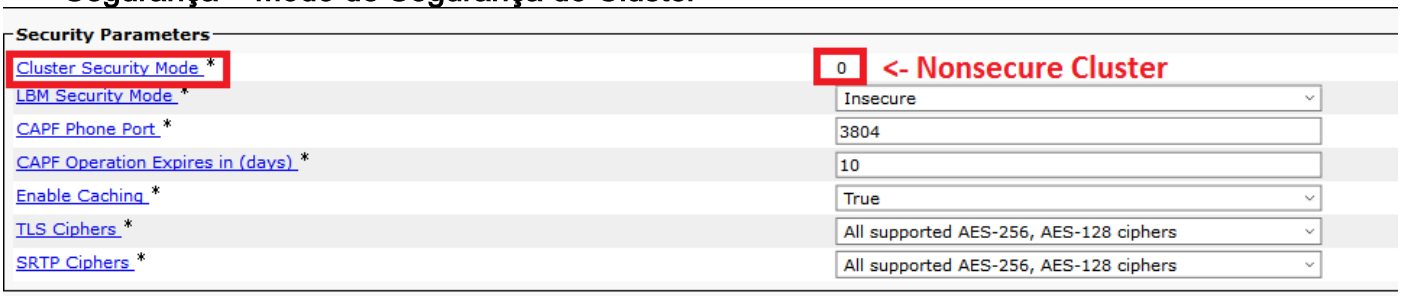
Tip: O processo de regeneração de alguns certificados pode afetar o ponto de extremidade. Considere um plano de ação após o horário comercial devido à necessidade de reiniciar os serviços e reinicializar os telefones. Verifique se o registro do telefone via RTMT é altamente recomendado.

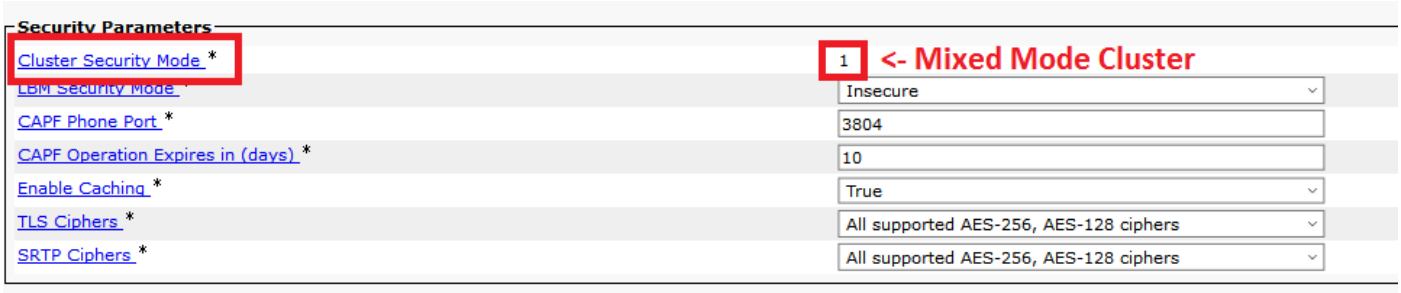
aviso: Endpoints com incompatibilidade de ITL atual podem ter problemas de registro após esse processo. A exclusão do ITL no endpoint é uma solução típica de práticas recomendadas depois que o processo de regeneração é concluído e todos os outros telefones são registrados.



Identifique se o cluster está no modo misto ou não seguro

- Navegue até Administração do CM. **Sistema > Parâmetros do Enterprise > Parâmetros de Segurança > Modo de Segurança do Cluster**





Impacto pelo armazenamento de certificados

Éessencial para a funcionalidade bem-sucedida do sistema ter todos os certificados atualizados no cluster CUCM. Se os certificados expirarem ou forem inválidos, poderão afetar significativamente a funcionalidade normal do sistema. O impacto pode variar dependendo da

configuração do sistema. Uma lista de serviços para os certificados específicos que são inválidos ou expiraram é mostrada aqui:

CallManager.pem

- Telefones criptografados/autenticados não registram
- O Trivial File Transfer Protocol (TFTP) não é confiável (os telefones não aceitam arquivos de configuração assinados e/ou arquivos ITL)
- Os serviços telefônicos podem ser afetados
- Troncos SIP (Secure Session Initiation Protocol) ou recursos de mídia (pontes de conferência, Media Termination Point (MTP), Xcoders e assim por diante) não se registram nem funcionam.
- A solicitação AXL falhará.

Tomcat.pem

- Os telefones não podem acessar serviços HTTPs hospedados no nó CUCM, como o diretório corporativo
- O CUCM pode ter vários problemas da Web, como a incapacidade de acessar páginas de serviço de outros nós no cluster
- Problemas de Mobilidade de Ramal (EM) ou Mobilidade de Ramal entre Clusters
- Logon Único (SSO)
- Se o UCCX (Unified Contact Center Express) estiver integrado, devido à alteração de segurança do CCX 12.5, será necessário carregar o certificado Tomcat do CUCM (autoassinado) ou o certificado raiz e intermediário do Tomcat (para CA assinado) no armazenamento tomcat-trust do UCCX, pois isso afeta os logons do desktop Finesse.

CAPF.pem

- Os telefones não autenticam para VPN de telefone, 802.1x ou proxy de telefone
- Não é possível emitir certificados LSC (Locally Significant Certificate) para os telefones.
- Os arquivos de configuração criptografados não funcionam

IPSec.pem

- O Sistema de recuperação de desastres (DRS)/Estrutura de recuperação de desastres (DRF) não funciona corretamente
- Túneis IPsec para gateway (GW) para outros clusters CUCM não funcionam

TVS (Trust Verification Service)

O Serviço de Verificação de Confiança (TVS) é o principal componente da Segurança por padrão. O TVS permite que os Cisco Unified IP Phones autentiquem servidores de aplicativos, como serviços EM, diretório e MIDlet, quando o HTTPS é estabelecido.

A TVS oferece estes recursos:

- Escalabilidade - Os recursos do telefone IP Cisco Unified não são afetados pelo número de certificados confiáveis.
- Flexibilidade - Adição ou remoção de certificados confiáveis são refletidas automaticamente no sistema.
- Segurança por padrão - Os recursos de segurança de sinal e não mídia fazem parte da instalação padrão e não exigem intervenção do usuário.

ITL e CTL

- O ITL contém a função de certificado para TFTP do Call Manager, todos os certificados TVS no cluster e a função de proxy da autoridade de certificação (CAPF) quando executada.
- A lista de certificados confiáveis contém entradas para os serviços System Administrator Security Token (SAST), Cisco CallManager e Cisco TFTP que são executados no mesmo servidor, CAPF, servidor(es) TFTP e firewall Adaptive Security Appliance (ASA). A TVS não é referenciada na CTL.

Processo de regeneração de certificado

> **Note**: Todos os endpoints precisam ser ativados e registrados antes da regeneração dos certificados. Caso contrário, os telefones não conectados exigem a remoção do ITL.

Certificado Tomcat

Identificar se os certificados de terceiros estão em uso:

1. Navegue até cada servidor do cluster (em guias separadas do navegador da Web) começando pelo editor, seguido por cada assinante. Navegue para **Cisco Unified OS Administration > Segurança > Gerenciamento de Certificado > Localizar**.
   Observe a coluna Descrição se o Tomcat afirmar Certificado autoassinado gerado pelo sistema. Se o Tomcat for assinado por terceiros, siga o link fornecido e execute essas etapas após a regeneração do Tomcat.Certificados assinados de terceiros, consulte CUCM Uploading CCMAdmin Web GUI Certificates.
2. Selecione **Find** para mostrar todos os certificados: Selecione o certificado **Tomcat pem**.Depois de abrir, selecione **Regenerar** e aguarde até ver o pop-up Êxito, depois feche o pop-up ou volte e selecione **Localizar/Lista**.
3. Continue com cada Assinante subsequente, siga o mesmo procedimento na etapa 2 e conclua em todos os Assinantes em seu cluster.
4. Depois que todos os nós tiverem gerado novamente o certificado Tomcat, reinicie o serviço tomcat em todos os nós. Comece com o editor e depois com os assinantes. Para reiniciar o Tomcat, você precisa abrir uma sessão CLI para cada nó e executar o comando **utils service restart Cisco Tomcat**.

```
admin:
admin:utils service restart Cisco Tomcat
 Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

5. Estas etapas são necessárias no ambiente CCX, se aplicável:

- Se o certificado autoassinado for usado, carregue os certificados Tomcat de todos os nós do cluster CUCM para o armazenamento confiável do Unified CCX Tomcat.
- Se um certificado assinado pela CA ou um certificado assinado pela CA privada for usado, carregue o certificado CA raiz do CUCM no armazenamento confiável do Unified CCX Tomcat.
- Reinicie os servidores conforme mencionado no documento de regeneração de certificado do CCX.

Referências adicionais:

- Guia de gerenciamento de certificado da solução UCCX
- Utilitário de verificação de integridade do Unified CCX

Certificado IPSEC

Note: CUCM/Instant Messaging and Presence (IM&P) anterior à versão 10.X do DRF Master O agente é executado no Editor do CUCM e no Editor do IM&P. O serviço DRF Local é executado nos assinantes, respectivamente. Versões 10.X e posteriores, DRF Master O agente é executado somente no Editor do CUCM e no serviço DRF Local em Assinantes do CUCM e Editor e Assinantes do IM&P.

Note: O Sistema de recuperação de desastres usa uma comunicação baseada em Secure Socket Layer (SSL) entre o Master Agente e Agente local para autenticação e criptografia de dados entre os nós de cluster do CUCM. O DRS usa os certificados IPSec para sua criptografia de chave pública/privada. Lembre-se de que se você excluir o arquivo de armazenamento confiável IPSEC (hostname.pem) da página Gerenciamento de certificados, o DRS não funcionará como esperado. Se você excluir o arquivo IPSEC-trust manualmente, deverá carregar o certificado IPSEC no armazenamento IPSEC-trust. Para obter mais detalhes, consulte a página de ajuda do gerenciamento de certificados nos Guias de Segurança do Cisco Unified Communications Manager.

1. Navegue até cada servidor do cluster (em guias separadas do navegador da Web) começando pelo editor, seguido por cada assinante. Navegue para **Cisco Unified OS Administration > Segurança > Gerenciamento de Certificado > Localizar**:
   Selecione o certificado **IPSEC pem**.Depois de abrir, selecione **Regenerar** e aguarde até ver o pop-up Êxito, depois feche o pop-up ou volte e selecione **Localizar/Lista**.
2. Continuar com os Assinantes subsequentes; siga o mesmo procedimento na etapa 1 e conclua em todos os assinantes do cluster.
3. Depois que todos os nós tiverem gerado novamente o certificado IPSEC, reinicie os serviços.
   Navegue até o editor **Cisco Unified Serviceability**. **Cisco Unified Serviceability > Ferramentas**

> **Centro de controle - Serviços de rede**.Selecione **Reiniciar** em **Cisco DRF Master**serviço.Quando a reinicialização do serviço for concluída, selecione **Restart** no **Cisco DRF Local Service** no editor, continue com os assinantes e selecione **Restart** no **Cisco DRF Local Service**.

O certificado IPSEC.pem no editor deve ser válido e estar presente em todos os assinantes como repositórios confiáveis IPSEC. O certificado IPSEC.pem do assinante não pode estar presente no editor como armazenamento confiável IPSEC em uma implantação padrão. Para verificar a validade, compare os números de série no certificado IPSEC.pem do PUB com IPSEC-trust nos SUBs. Eles devem coincidir.

Certificado CAPF

> **aviso:** Antes de continuar, verifique se você identificou se o cluster está no modo misto. Consulte a seção **Identificar se o cluster está no Modo Misto ou no Modo Não Seguro**.

1. Navegue até **Cisco Unified CM Administration > System > Enterprise Parameters**. Verifique a seção Parâmetros de Segurança e se o Modo de Segurança do Cluster está definido como 0 ou 1. Se o valor for 0, o cluster está no Modo Não Seguro. Se for 1, o cluster estará no modo misto e você precisará atualizar o arquivo CTL antes da reinicialização dos serviços. Consulte Links de token e sem token.
2. Navegue até cada servidor do cluster (em guias separadas do navegador da Web) começando pelo editor e, em seguida, para cada assinante. Navegue para **Cisco Unified OS Administration > Segurança > Gerenciamento de Certificado > Localizar**. Selecione o Certificado **CAPF pem**.Depois de abrir, selecione **Regenerar** e aguarde até ver o pop-up Êxito, depois feche o pop-up ou volte e selecione **Localizar/Lista**
3. Continuar com assinantes subsequentes; siga o mesmo procedimento na etapa 2 e conclua em todos os assinantes do cluster. Se o cluster estiver em Mixed-Mode ONLY e a CAPF tiver sido regenerada - Atualize a CTL antes de continuar com o Token - Sem Tokens.Se o cluster estiver no modo misto, o serviço do Call Manager também precisará ser reiniciado antes da reinicialização de outros serviços.
4. Depois que todos os nós tiverem gerado novamente o certificado CAPF, reinicie os serviços. Navegue até o editor **Cisco Unified Serviceability**. **Cisco Unified Serviceability > Ferramentas > Centro de controle - Serviços de recursos**.Comece com o editor e selecione **Restart** no **Cisco Certificate Authority Proxy Function Service** somente onde ativo.
5. Navegue até **Cisco Unified Serviceability > Tools > Control Center - Network Services**. Comece com o editor e continue com os assinantes, selecione **Restart** no **Cisco Trust Verification** Service**.** Navegue para **Cisco Unified Serviceability > Ferramentas > Centro de controle - Serviços de recurso**.Comece com o editor e continue com os assinantes; reinicie o **Cisco TFTP Service** somente onde estiver ativo.
6. Reinicializar todos os telefones: **Administração do Cisco Unified CM > Sistema > Parâmetros corporativos**Selecione **Reset** e você verá um pop-up com a instrução **You are about to reset all devices in the system. Esta ação não pode ser desfeita. Continuar?,**selecione **OK** e selecione **Redefinir**.

Os telefones agora são redefinidos. Monitore suas ações por meio da ferramenta RTMT para garantir que a redefinição tenha sido bem-sucedida e que os dispositivos sejam registrados novamente no CUCM. Aguarde a conclusão do registro do telefone antes de prosseguir para o próximo certificado. Esse processo de registro de telefones pode levar algum tempo. Observe que os dispositivos que tinham ITLs inválidos antes do processo de regeneração não se registram

novamente no cluster até que ele seja removido.

Certificado do CallManager

> **aviso:** Antes de continuar, verifique se você identificou se o cluster está no modo misto. Consulte a seção **Identificar se o cluster está no Modo Misto ou no Modo Não Seguro**.

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

1. Navegue até **Cisco Unified CM Administration > System > Enterprise Parameters**: Verifique a seção Parâmetros de Segurança e se o Modo de Segurança do Cluster está definido como 0 ou 1. Se o valor for 0, o cluster está no Modo Não Seguro. Se for 1, o cluster estará no modo misto e você precisará atualizar o arquivo CTL antes da reinicialização dos serviços. Consulte Links de token e sem token.
2. Navegue até cada servidor do cluster (em guias separadas do navegador da Web) começando pelo editor e, em seguida, para cada assinante. Navegue para **Cisco Unified OS Administration > Segurança > Gerenciamento de Certificado > Localizar**.
   Selecione o certificado PEM do CallManager.Depois de abrir, selecione **Regenerar** e aguarde até ver o pop-up Êxito, depois feche o pop-up ou volte e selecione **Localizar/Lista**.
3. Continuar com assinantes subsequentes; siga o mesmo procedimento na etapa 2 e conclua em todos os assinantes do cluster. Se o cluster estiver em Mixed-Mode ONLY e o certificado do CallManager tiver sido regenerado - Atualize a lista de certificados confiáveis antes de continuar com o Token - Sem tokens
4. Faça login no Publisher Cisco Unified Serviceability: Navegue até **Cisco Unified Serviceability > Tools > Control Center - Feature Services**.Comece com o editor e continue com os assinantes; reinicie o **Cisco CallManager Service** onde estiver ativo.
5. Navegue até **Cisco Unified Serviceability > Ferramentas > Centro de controle - Serviços de recurso**
   Comece com o Editor e continue com os assinantes. Reinicie o **Cisco CTIManager Service** somente onde estiver ativo.
6. Navegue até **Cisco Unified Serviceability > Tools > Control Center - Network Services**. Comece com o Publicador e continue com os assinantes. Reinicie o **Cisco Trust Verification Service**.
7. Navegue até **Cisco Unified Serviceability > Tools > Control Center - Feature Services**. Comece com o Publicador e continue com os assinantes. Reinicie o **Cisco TFTP Service** somente onde estiver ativo.
8. Reinicializar todos os telefones: **Administração do Cisco Unified CM > Sistema > Parâmetros corporativos**Selecione **Reset** e você verá um pop-up com a instrução **You are about to reset all devices in the system. Esta ação não pode ser desfeita. Continuar?,**selecione **OK e, em seguida, selecione Redefinir**

Os telefones agora são redefinidos. Monitore suas ações por meio da ferramenta RTMT para garantir que a redefinição tenha sido bem-sucedida e que os dispositivos sejam registrados novamente no CUCM. Aguarde a conclusão do registro do telefone antes de prosseguir para o

próximo certificado. Esse processo de registro de telefones pode levar algum tempo. Observe que os dispositivos que tinham ITLs inválidos antes do processo de regeneração não são registrados novamente no cluster até que o ITL seja removido.

Certificado TVS

> **aviso:** Não gere novamente os certificados CallManager.PEM e TVS.PEM ao mesmo tempo. Isso causa uma incompatibilidade irrecuperável com o ITL instalado nos pontos de extremidade que exigem a remoção do ITL de TODOS os pontos de extremidade no cluster.

> **Note**: O TVS autentica certificados em nome do Call Manager. Regenerar este certificado por último.

Navegue até cada servidor do cluster (em guias separadas do navegador da Web) começando pelo editor e, em seguida, para cada assinante. Navegue para **Cisco Unified OS Administration > Segurança > Gerenciamento de Certificado > Localizar**:

- Selecione o certificado **TVS pem**.
- Depois de abrir, selecione **Regenerar** e aguarde até ver o pop-up Êxito, depois feche o pop-up ou volte e selecione **Localizar/Lista**.

1. Continuar com assinantes subsequentes; siga o mesmo procedimento na etapa 1 e conclua em todos os assinantes do cluster. Depois que todos os nós tiverem gerado novamente o certificado TVS, reinicie os serviços: Faça login no Publisher **Cisco Unified Serviceability**. Navegue até **Cisco Unified Serviceability > Tools > Control Center - Network Services**.No editor, selecione **Reiniciar** no **Cisco Trust Verification Service**.Quando a reinicialização do serviço for concluída, continue com os assinantes e reinicie o **Cisco Trust Verification Service**.
2. Comece com o Publicador e continue com os assinantes. Reinicie o **Cisco TFTP Service** somente onde estiver ativo.
3. Reinicializar todos os telefones: **Cisco Unified CM Administration > Sistema > Parâmetros da empresa**.Selecione **Reset** e você verá um pop-up com a instrução **You are about to reset all devices in the system. Esta ação não pode ser desfeita. Continuar?,**selecione **OK** e selecione **Redefinir**.

Os telefones agora são redefinidos. Monitore suas ações por meio da ferramenta RTMT para garantir que a redefinição tenha sido bem-sucedida e que os dispositivos sejam registrados novamente no CUCM. Aguarde a conclusão do registro do telefone antes de prosseguir para o próximo certificado. Esse processo de registro de telefones pode levar algum tempo. Observe que os dispositivos que tinham ITLs inválidos antes do processo de regeneração não são registrados novamente no cluster até que o ITL seja removido.

Certificado ITLRecovery

> **Note**: O Certificado ITLRecovery é usado quando dispositivos perdem seu status confiável. O certificado aparece no ITL e CTL (quando o provedor CTL está ativo).
> Se os dispositivos perderem seu status de confiança, você poderá usar o comando **utils itl reset localkey** para clusters não seguros e o comando **utils ctl reset localkey** para clusters de modo misto. Leia o guia de segurança da versão do Call Manager para se familiarizar com o

uso do certificado ITLRecovery e o processo necessário para recuperar o status confiável. Se o cluster tiver sido atualizado para uma versão que suporte um comprimento de chave de 2048 e os certificados do servidor de clusters tiverem sido regenerados para 2048 e o ITLRecovery não tiver sido regenerado e tiver atualmente um comprimento de chave de 1024, o comando de recuperação de ITL falhará e o método ITLRecovery não será usado.

1. Navegue até cada servidor do cluster (em guias separadas do navegador da Web) começando pelo editor e, em seguida, para cada assinante. Navegue para **Cisco Unified OS Administration > Segurança > Gerenciamento de Certificado > Localizar**:
   Selecione o certificado **ITLRecovery pem**.Depois de abrir, selecione **Regenerar** e aguarde até ver o pop-up Êxito, depois feche o pop-up ou volte e selecione **Localizar/Lista**.
2. Continuar com os Assinantes subsequentes; siga o mesmo procedimento na etapa 2 e conclua em todos os assinantes do cluster.
3. Depois que todos os nós tiverem gerado novamente o certificado ITLRecovery, os serviços precisarão ser reiniciados na seguinte ordem: Se você estiver no Modo Misto - Atualize a lista de certificados confiáveis antes de continuar com o Token - Sem tokens.Faça login no Publisher **Cisco Unified Serviceability**. Navegue até **Cisco Unified Serviceability > Tools > Control Center - Network Services**.No editor, selecione **Reiniciar** no **Cisco Trust Verification Service**. Quando a reinicialização do serviço for concluída, continue com os assinantes e reinicie o **Cisco Trust Verification Service**.
4. Comece com o Publicador e continue com os assinantes. Reinicie o **Cisco TFTP Service** somente onde estiver ativo.
5. Reinicializar todos os telefones: **Administração do Cisco Unified CM > Sistema > Parâmetros corporativos**Selecione **Reset** e você verá um pop-up com a instrução **You are about to reset all devices in the system. Esta ação não pode ser desfeita. Continuar?,**selecione **OK** e selecione **Redefinir**.
6. Os telefones agora carregam o novo ITL/CTL enquanto reinicializam.

Excluir Certificados de Confiança Expirados

Note: Identifique os certificados confiáveis que precisam ser excluídos, não são mais necessários ou expiraram. Não exclua os cinco certificados básicos que incluem CallManager.pem, tomcat.pem, ipsec.pem, CAPF.pem e TVS.pem. Os certificados confiáveis podem ser excluídos quando apropriado. O próximo serviço a ser reiniciado foi projetado para apagar informações de certificados herdados dentro desses serviços.

1. Navegue até **Cisco Unified Serviceability > Tools > Control Center - Network Services**. No menu suspenso, selecione o Editor do CUCM.Selecione **Stop** Certificate Change Notification.Repita para cada nó do Call Manager em seu cluster.Se você tiver um servidor IMP: No menu suspenso, selecione seus servidores IMP, um de cada vez, e selecione **Stop Platform Administration Web Services e Cisco Intercluster Sync Agent**.
2. Navegue para **Cisco Unified OS Administration > Segurança > Gerenciamento de Certificado > Localizar**.
   Localize os certificados confiáveis expirados. (Para as versões 10.X e posteriores, você pode filtrar por Expiração. Para versões anteriores à 10.0, é necessário identificar os certificados específicos manualmente ou através dos alertas RTMT, se recebidos.)O mesmo certificado confiável pode aparecer em vários nós. Ele deve ser excluído individualmente de

cada nó.Selecione o certificado confiável a ser excluído (dependendo da sua versão, você obterá um pop-up ou navegará até o certificado na mesma página) Selecione **Excluir**. (Você recebe um pop-up que começa com "você está prestes a excluir permanentemente este certificado".*)*Selecione **OK**.

3. Repita o processo para cada certificado de confiança a ser excluído.
4. Após a conclusão, os serviços que estão diretamente relacionados aos certificados devem ser reiniciados e excluídos. Não é necessário reinicializar os telefones nesta seção. O Call Manager e o CAPF devem estar afetando o endpoint. Tomcat-trust: reinicie o serviço Tomcat pela linha de comando (consulte a seção Tomcat)CAPF-trust: reinicie a Cisco Certificate Authority Proxy Function (consulte a Seção CAPF) Não reinicialize os pontos de extremidade.CallManager-trust: CallManager Service/CTIManager (Consulte a seção CallManager) Não reinicialize os pontos finais. Afeta os endpoints e causa reinicializações.IPSEC-trust: DRF Master/DRF Local (Consulte a seção IPSEC).TVS (Autoassinado) não possui certificados confiáveis.
5. Reinicie os serviços anteriormente interrompidos na etapa 1.

Verificação

Os procedimentos de verificação não estão disponíveis para esta configuração.

Troubleshoot

Os procedimentos de solução de problemas não estão disponíveis para esta configuração.

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.