ID do Documento: 113333

Atualizado em: novembro 28, 2011

Produtos Relacionados

- Cisco unificou o telefone IP 7971G-GE
- Cisco unificou o telefone IP 7941G-GE
- Telefone IP Cisco Unified 7970G
- Telefone IP Cisco Unified 7960G
- Cisco unificou o telefone IP 7941G
- Telefone IP Cisco Unified 7961G
- + mostra mais

Índice

Introdução

Este documento descreve o procedimento passo a passo para mover manualmente um telefone IP no modo seguro de um conjunto unificado Cisco do gerente de uma comunicação da fonte (CUCM) para um conjunto do destino CUCM sem manipulação do arquivo certificado da lista da confiança (CTL) instalado em tal telefone IP.

Nota: Este procedimento é independente de:

1. Protocolo de sinalização usado pelo telefone. Supõe-se que o protocolo de sinalização na fonte e os grânulos de destino permanecem o mesmo para um telefone IP específico.
2. Telefone a modelo que exclui Cisco 7940/7960 de modelo porque os telefones de 7940/7960 exigem a intervenção do utilizador final entrar um string de autenticação desde que não têm um acessório MIC.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no gerente 7.x das comunicações unificadas de Cisco.

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Certificate trust list

Todos os server no conjunto CUCM geram certificados auto-assinados. Os telefones obtêm seus próprios Certificados, que é de dois tipos.

1. Certificado instalado de fabricação dado por Cisco quando você comprar um telefone novo.
2. Localmente - certificado significativo entregue pela função do proxy da autoridade de Cisco.

O CTL é uma lista de certificados auto-assinados de todos os server no conjunto CUCM que o telefone pode confiar. O CTL é armazenado no servidor TFTP e enviado aos Telefones IP.

O dispositivo, o arquivo, e a autenticação da sinalização confiam na criação do arquivo CTL, que é criado quando você instala e configura o cliente de Cisco CTL em uma único estação de trabalho do Windows ou server que tenha um porta usb.

O arquivo CTL contém um certificado de servidor, uma chave pública, um número de série, uma assinatura, um nome de emissor, um nome do sujeito, uma função do server, um nome de DNS, e um endereço IP de Um ou Mais Servidores Cisco ICM NT para cada server. Quando você configura um Firewall no arquivo CTL, você pode fixar um Firewall de Cisco ASA como parte de um sistema seguro do gerente das comunicações unificadas de Cisco. O cliente de Cisco CTL indica o certificado do Firewall como um certificado *CCM*. A administração do gerenciador das comunicações unificadas de Cisco usa um eToken para autenticar a conexão TLS entre o cliente de Cisco CTL e o fornecedor de Cisco CTL.

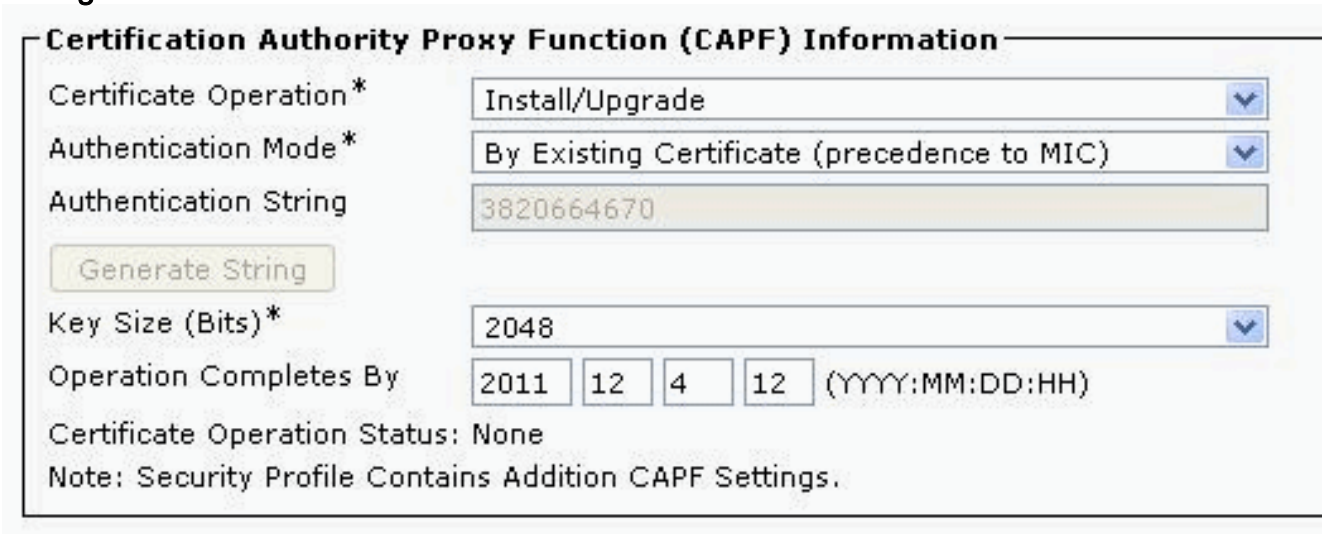
Na versão 8.X e mais recente CUCM, o pedido dos Telefones IP um arquivo CTL à revelia mesmo se isto não foi criado. Os arquivos CTL não são considerados essenciais; são apenas parte dos recursos de segurança novos que vêm com o CUCM 8.x. Refira configurar o cliente de Cisco CTL para mais informação.

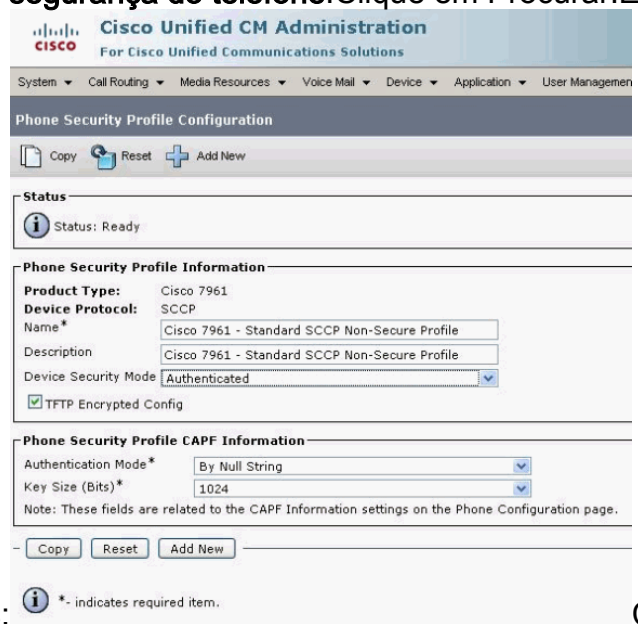
Como fixar o telefone IP

Para que o telefone aceite o arquivo CTL de todo o conjunto sem a necessidade de suprimir do existente exige que o arquivo CTL de cada conjunto tem que ser assinado pelo mesmo grupo compartilhado de eTokens. Ou seja nós precisamos de criar um arquivo CTL para cada conjunto e para assinar todos com o mesmos eToken. Adicionalmente, telefona à confiança nos servidores TFTP centralizados, você igualmente têm que adicionar os servidores TFTP centralizados em cada arquivo CTL.

Termine estas etapas a fim configurar as propriedades de segurança para um telefone IP.

1. Configurar o perfil de segurança do dispositivo. Se um perfil de segurança do dispositivo apropriado não existe na lista de drop-down da página da configuração de telefone IP, deixe-a como o padrão, **perfil NON-seguro padrão**.
2. Configurar a informação da função do proxy da autoridade de certificação (CAPF), para que o telefone IP obtenha um LSC novo, assinada pelo conjunto do destino CUCM.Isto é feito na página da configuração telefônica de CUCM. Escolha os valores do menu dropdown como mostrado e clique então a **salvaguarda**.

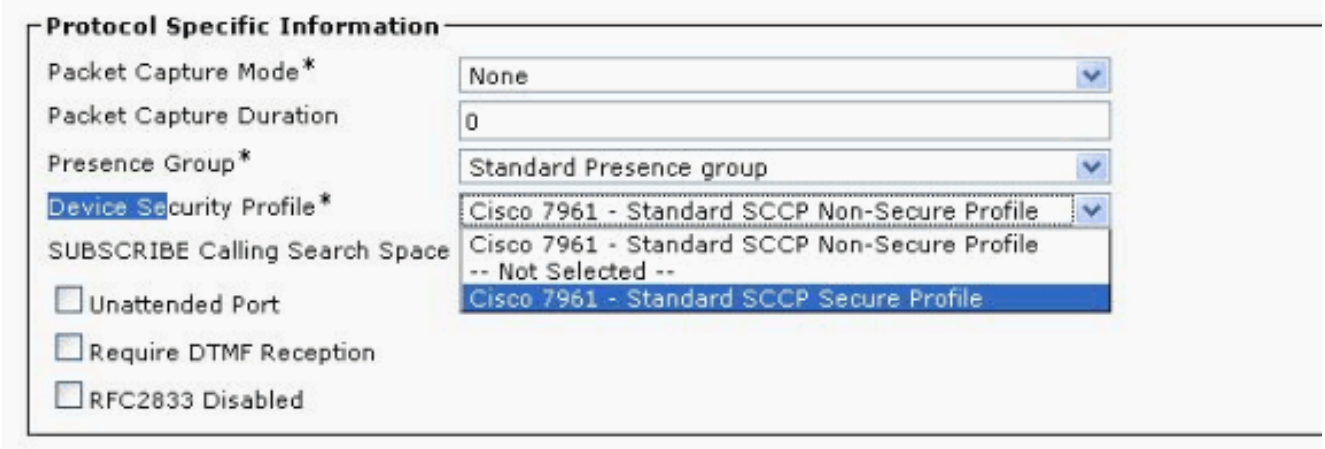


3. Configurar o perfil de segurança do dispositivo criado novo:Escolha o **perfil do > segurança do sistema > o perfil de segurança do telefone**.Clique em Procurar.Escolha o tipo de telefone e incorpore os detalhes: 

Clique a **cópia**.**Salvar**

agora a configuração como mostrado aqui:

4. Na página da configuração de telefone IP, segunda verificação que o *modo* apropriado da *segurança do dispositivo* está configurado.



5. Reinicie o telefone IP.
6. O telefone deve agora transferir um arquivo novo CTL dos grânulos de destino e deve obter um LSC assinado dos grânulos de destino.
7. O telefone é executado com o modo de segurança configurado no perfil de segurança do dispositivo.

Informações Relacionadas

- Consultivo de segurança Cisco: Excesso do montão do fornecedor do gerente CTL das comunicações unificadas de Cisco
- Segurança do telefone IP e CTL (certificate trust list)
- Suporte à Tecnologia de Voz
- Suporte ao Produto de Voz e Comunicações Unificadas
- Troubleshooting da Telefonia IP Cisco
- Suporte Técnico e Documentação - Cisco Systems

Cisco relacionado apoia discussões da comunidade

Cisco apoia a comunidade é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira convenções dos dicas técnicas da Cisco para obter informações sobre das convenções

usadas neste documento.

Atualizado em: novembro 28, 2011
ID do Documento: 113333