Segurança do Cisco IP Conference Phone

Visão geral da segurança do Telefone IP Cisco

Os recursos de segurança protegem contra várias ameaças, incluindo ameaças à identidade do telefone e aos dados. Os recursos estabelecem e mantêm fluxos de comunicação autenticados entre o telefone e o servidor Cisco Unified Communications Manager, além de garantir que o telefone use apenas arquivos assinados digitalmente.

O Cisco Unified Communications Manager versão 8.5(1) e posterior inclui a opção Segurança por padrão, que fornece os seguintes recursos de segurança para Telefones IP Cisco sem executar o cliente CTL:

- Assinatura dos arquivos de configuração do telefone
- Criptografia dos arquivos de configuração do telefone
- HTTPS com Tomcat e outros serviços Web

Observação Os recursos de mídia e sinalização segura ainda exigem que você execute o cliente CTL e use eTokens físicos.

Para obter mais informações sobre os recursos de segurança, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Um LSC (Locally Significant Certificate) é instalado nos telefones depois que você executa as tarefas necessárias associadas à função de proxy de autoridade de certificação (CAPF). Você pode usar a Administração do Cisco Unified Communications Manager para configurar um LSC. Para obter mais informações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Um LSC não pode ser usado como o certificado do usuário para EAP-TLS com autenticação WLAN.

Opcionalmente, você pode iniciar a instalação de um LSC no menu Configuração de segurança do telefone. Este menu também permite atualizar ou remover um LSC.

O Telefone IP Cisco de conferência 8832 está em conformidade com a norma FIPS (Federal Information Processing Standard). Para funcionar corretamente, o modo FIPS requer uma chave RSA de 2048 bits ou

mais. Se o certificado do servidor RSA não tiver 2048 bits ou mais, o telefone não será registrado no Cisco Unified Communications Manager e a mensagem `Falha ao registrar o telefone. O tamanho da chave do certificado não é compatível com FIPS` é exibida em mensagens de status do telefone.

Você não pode usar chaves privadas (LSC ou MIC) no modo FIPS.

Se o telefone tiver uma chave LSC existente menor do que 2048 bits, você precisa atualizar o tamanho da chave LSC para 2048 bits ou mais antes de ativar FIPS.

Tópicos relacionados

Configurar um certificado localmente significativo, na página 5
Documentação do Cisco Unified Communications Manager

Aprimoramentos de segurança para sua rede de telefonia

Você pode ativar o Cisco Unified Communications Manager 11.5(1) e 12.0(1) para operar em um ambiente de segurança avançada. Com esses aprimoramentos, sua rede de telefonia opera sob um conjunto de controles rígidos de gerenciamento de segurança e riscos para proteger você e seus usuários.

O Cisco Unified Communications Manager 12.5(1) não é compatível com um ambiente de segurança optimizada. Desative FIPS antes de atualizar para o Cisco Unified Communications Manager 12.5(1) ou seu TFTP e outros serviços não funcionará corretamente.

O ambiente de segurança optimizada inclui os seguintes recursos:

- Autenticação de pesquisa de contatos.
- O TCP como o protocolo padrão para o registro em log de auditoria remota.
- Modo FIPS.
- Uma política de credenciais aprimorada.
- Suporte à família SHA-2 de hashes para assinaturas digitais.
- Suporte para uma chave RSA de 512 e 4096 bits.

Com o Cisco Unified Communications Manager versão 14.0 e o firmware do Telefone IP Cisco versão 14.0 e posterior, os telefones suportam autenticação SIP OAuth.

O OAuth é compatível com proxy trivial File Transfer Protocol (TFTP) com Cisco Unified Communications Managerversão 14.0(1)SU1 ou posterior e Cisco IP Phone firmware versão 14.1(1). Proxy TFTP e OAuth para proxy TFTP não são compatíveis com o Mobile Remote Access (MRA).

Para obter informações adicionais sobre a segurança, consulte o seguinte:

- *Guia de configuração do sistema do Cisco Unified Communications Manager, versão 12.0(1)* ou posterior (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html).
- *Guia de segurança para o Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html)

- SIP OAuth: *Guia de configuração de recursos do Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html)

Observação O Telefone IP Cisco só pode armazenar um número limitado de arquivos Identity Trust List (ITL). Os arquivos ITL não podem exceder o limite de 64K no limite, por isso, limite o número de arquivos que o Cisco Unified Communications Manager envia para o telefone.

Recursos de segurança suportados

Os recursos de segurança protegem contra várias ameaças, incluindo ameaças à identidade do telefone e aos dados. Os recursos estabelecem e mantêm fluxos de comunicação autenticados entre o telefone e o servidor Cisco Unified Communications Manager, além de garantir que o telefone use apenas arquivos assinados digitalmente.

O Cisco Unified Communications Manager versão 8.5(1) e posterior inclui a opção Segurança por padrão, que fornece os seguintes recursos de segurança para Telefones IP Cisco sem executar o cliente CTL:

- Assinatura dos arquivos de configuração do telefone
- Criptografia dos arquivos de configuração do telefone
- HTTPS com Tomcat e outros serviços Web

Observação Os recursos de mídia e sinalização segura ainda exigem que você execute o cliente CTL e use eTokens físicos.

Implementar a segurança no sistema Cisco Unified Communications Manager impede o roubo de identidade do telefone e do servidor Cisco Unified Communications Manager, impede a violação de dados e impede a adulteração da sinalização de chamadas do fluxo de mídia.

Para minimizar essas ameaças, a rede de telefonia IP da Cisco estabelece e mantém fluxos de comunicação seguros (criptografados) entre um telefone e o servidor, assina digitalmente os arquivos antes de serem transferidos para um telefone e criptografa fluxos de mídia e a sinalização de chamadas entre Telefones IP Cisco.

Um LSC (Locally Significant Certificate) é instalado nos telefones depois que você executa as tarefas necessárias associadas à função de proxy de autoridade de certificação (CAPF). Você pode usar a Administração do Cisco Unified Communications Manager para configurar um LSC, conforme descrito no Guia de segurança do Cisco Unified Communications Manager. Opcionalmente, você pode iniciar a instalação de um LSC no menu Configuração de segurança do telefone. Este menu também permite atualizar ou remover um LSC.

Um LSC não pode ser usado como o certificado do usuário para EAP-TLS com autenticação WLAN.

Os telefones usam o perfil de segurança do telefone, que define se o dispositivo está seguro ou não. Para obter informações sobre como aplicar o perfil de segurança ao telefone, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Se você definir configurações de segurança na Administração do Cisco Unified Communications Manager, o arquivo de configuração do telefone conterá informações confidenciais. Para garantir a privacidade de um

arquivo de configuração, você deve configurá-lo para criptografia. Para obter informações detalhadas, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Implementar a segurança no sistema Cisco Unified Communications Manager impede o roubo de identidade do telefone e do servidor Cisco Unified Communications Manager, impede a violação de dados e impede a adulteração da sinalização de chamadas do fluxo de mídia.

A tabela a seguir fornece uma visão geral dos recursos de segurança que são compatíveis com o Telefone IP Cisco de conferência 8832. Para obter mais informações sobre esses recursos, o Cisco Unified Communications Manager e a segurança do Telefone IP Cisco, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Tabela 1: Visão geral dos recursos de segurança

Recurso	Descrição
Autenticação de imagem	Arquivos binários assinados (com a extensão .sbn) impedem a telefone. A falsificação com a imagem causa falha no processo
Instalação de certificado no site do cliente	Cada telefone exige um certificado exclusivo para autenticaçã fabricante), mas para segurança adicional, você pode especific certificado seja instalado usando a CAPF (Função de proxy de (Certificado localmente significativo) no menu Configuração d
Autenticação do dispositivo	Ocorre entre o servidor Cisco Unified Communications Manag Determina se uma conexão segura entre o telefone e um Cisco caminho de sinalização seguro entre as entidades usando o prot a menos que possa autenticá-los.
Autenticação de arquivo	Valida arquivos assinados digitalmente baixados pelo telefone. ocorreu depois da criação do arquivo. Os arquivos que falham rejeita tais arquivos sem outro processamento.
Autenticação de sinalização	Usa o protocolo TLS para confirmar que não houve falsificaçã
Certificado instalado pelo fabricante	Cada telefone contém um MIC (certificado instalado pelo fabri de identidade exclusiva permanente do telefone e permite que
Referência SRST segura	Depois de configurar uma referência SRST para segurança e re Communications Manager, o servidor TFTP adiciona o certific telefone seguro usa uma conexão TLS para interagir com o rot
Criptografia de mídia	Usa SRTP para garantir que os fluxos de mídia entre dispositiv receba e leia os dados. Inclui criação de um par de chaves prim protegendo a entrega das chaves enquanto são transportadas.
CAPF (Função de proxy de autoridade de certificação)	Implementa partes do procedimento de geração do certificado geração de chave e instalação do certificado. A CAPF pode ser co pelo cliente em nome do telefone ou pode ser configurada para
Perfis de segurança	Define se o telefone não é seguro e se está autenticado ou cript
Arquivos de configuração criptografados	Permite que você assegure a privacidade dos arquivos de confi

Recurso	Descrição
Desativação opcional da funcionalidade do servidor Web para um telefone	Você pode impedir o acesso à página da Web de um telefon
Proteção do telefone	Opções de segurança adicionais, que você controla na Adm • Desativar acesso a páginas da Web de um telefone **Observação** Você pode visualizar as configurações atuais d menu Configuração do telefone.
Autenticação 802.1X	O telefone pode usar autenticação 802.1X para solicitar e c
Criptografia AES 256	Quando conectados ao Cisco Unified Communications Ma para TLS e SIP para sinalização e criptografia de mídia. Iss baseadas em AES-256 em conformidade com os padrões SH Processing Standards). As novas cifras são: • Para conexões TLS: • TLS_ECDHE_RSA_WITH_AES_256_GCM_S • TLS_ECDHE_RSA_WITH_AES_128_GCM_S • Para sRTP: • AEAD_AES_256_GCM • AEAD_AES_128_GCM Para obter mais informações, consulte a documentação do
Certificados Elliptic Curve Digital Signature Algorithm (ECDSA)	Como parte da certificação Common Criteria (CC), o Cisco Isso afeta todos os produtos de Voice Operating System (V

Tópicos relacionados

Documentação do Cisco Unified Communications Manager

Configurar um certificado localmente significativo

Essa tarefa se aplica à configuração de um LSC com o método de cadeia de autenticação.

Antes de Iniciar

Verifique se configurações de segurança apropriadas do Cisco Unified Communications Manager e da CAPF (Função de proxy de autoridade de certificação) foram concluídas:

- O arquivo CTL ou ITL tem um certificado CAPF.
- Na Administração do sistema operacional do Cisco Unified Communications, verifique se o certificado CAPF está instalado.
- A CAPF está em execução e foi configurada.

Para obter mais informações sobre essas configurações, consulte a documentação da sua versão específica do Cisco Unified Communications Manager.

Procedimento

Etapa 1 Obtenha o código de autenticação da CAPF que foi definido quando a CAPF foi configurada.

Etapa 2 No telefone, escolha **Configurações**.

Etapa 3 Selecione **Configurações do administrador** > **Configurações de segurança**.

Observação Você pode controlar o acesso ao menu Configurações usando o campo Acesso às configurações na janela Configuração do telefone da Administração do Cisco Unified Communications Manager.

Etapa 4 Escolha **LSC** e pressione **Selecionar** ou **Atualizar**.

O telefone solicita uma string de autenticação.

Etapa 5 Insira o código de autenticação e pressione **Enviar**.

O telefone começa a instalar, atualizar ou remover o LSC, dependendo de como a CAPF foi configurada. Durante o procedimento, uma série de mensagens aparecerá no campo Opção de LSC no menu Configuração de segurança para que você possa monitorar o andamento. Quando o procedimento estiver concluído, será exibida a mensagem Instalado ou Não instalado no telefone.

O processo de instalação, atualização ou remoção do LSC pode demorar bastante para ser concluído.

Quando o procedimento de instalação do telefone for bem-sucedido, a mensagem `Instalado` será exibida. Se o telefone exibir `Não instalado`, a string de autorização pode estar incorreta ou a atualização do telefone pode não estar ativada. Se a operação de CAPF excluir o LSC, o telefone exibirá `Não instalado` para indicar que a operação foi bem-sucedida. O servidor CAPF registra em log as mensagens de erro. Consulte a documentação do servidor CAPF para localizar os logs e entender o significado das mensagens de erro.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager

Ativar modo FIPS

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone** e localize o telefone.

Etapa 2 Navegue até a área Configuração específica do produto.

Etapa 3 Defina o campo **Modo FIPS** como Ativado.

Etapa 4 Selecione **Aplicar config.**

Etapa 5 Selecione **Salvar**.

Etapa 6 Reinicie o telefone.

Segurança da chamada telefônica

Quando a segurança é implementada para um telefone, você pode identificar chamadas telefônicas seguras por ícones na tela do telefone. Também será possível determinar se o telefone conectado está seguro e protegido se um tom de segurança for tocado no início da chamada.

Em uma chamada segura, todos os fluxos de mídia e sinalização de chamada são criptografados. Uma chamada segura oferece um alto nível de segurança, fornecendo integridade e privacidade à chamada. Quando uma chamada em andamento é criptografada, o ícone de andamento da chamada à direita do temporizador de duração da chamada na tela do telefone muda para o seguinte ícone: 

Observação Se a chamada for roteada por meio de segmentos de chamada não IP, por exemplo, o PSTN, ela poderá não ser segura, mesmo que esteja criptografada na rede IP e tenha um ícone de cadeado associado a ela.

Em uma chamada segura, um tom de segurança é tocado no início para indicar que o outro telefone conectado também está recebendo e transmitindo áudio seguro. Se a chamada se conectar a um telefone não seguro, o tom de segurança não será tocado.

Observação A chamada segura é permitida entre dois telefones. A conferência segura, o Cisco Extension Mobility e as linhas compartilhadas podem ser configurados por um recurso de conferência seguro.

Quando um telefone é configurado como seguro (criptografado e confiável) no Cisco Unified Communications Manager, ele pode receber o status de "protegido". Depois disso, se desejado, o telefone protegido pode ser configurado para tocar um tom indicativo no início de uma chamada:

- Dispositivo protegido: para alterar o status de um telefone seguro para protegido, marque a caixa de seleção Dispositivo protegido na janela Configuração do telefone na Administração do Cisco Unified Communications Manager (**Dispositivo** > **Telefone**).
- Tocar tom indicativo de seguro: para permitir que o telefone protegido toque um tom indicativo de seguro ou não seguro, defina a configuração Play Secure Indication Tone (Tocar tom indicativo de seguro) como Verdadeiro. Por padrão, a opção Tocar tom indicativo de seguro é definida como Falso. Você define essa opção na Administração do Cisco Unified Communications Manager (**Sistema** > **Parâmetros de serviço**). Selecione o servidor e, em seguida, o serviço do Unified Communications Manager. Na janela Configuração de parâmetro de serviço, selecione a opção na área Recurso - Tom de seguro. O padrão é Falso.

Identificação de chamada de conferência segura

Você pode iniciar uma chamada de conferência segura e monitorar o nível de segurança dos participantes. Uma chamada de conferência segura é estabelecida por este processo:

1. Um usuário inicia a conferência de um telefone seguro.
2. O Cisco Unified Communications Manager atribui um recurso de conferência seguro à chamada.
3. Conforme os participantes são adicionados, o Cisco Unified Communications Manager verifica o modo de segurança de cada telefone e mantém o nível seguro para a conferência.

4. O telefone exibe o nível de segurança da chamada de conferência. Uma conferência segura exibe o ícone de proteção à direita da **Conferência** na tela do telefone.

Observação A chamada segura é permitida entre dois telefones. Em telefones protegidos, alguns recursos, como a chamada de conferência, as linhas compartilhadas e o Extension Mobility, não estão disponíveis quando a chamada segura é configurada.

A tabela a seguir fornece informações sobre alterações nos níveis de segurança da conferência, de acordo com o nível de segurança do telefone do iniciador, os níveis de segurança dos participantes e a disponibilidade dos recursos de conferência seguros.

Tabela 2: Restrições de segurança com chamadas de conferência

Nível de segurança do telefone do iniciador	Recurso usado	Nível de segurança dos participantes	Resultados da ação
Não seguro	Conferência	Seguro	Recurso de conferência não seguro Conferência não segura
Seguro	Conferência	Pelo menos um membro não seguro.	Recurso de conferência seguro Conferência não segura
Seguro	Conferência	Seguro	Recurso de conferência seguro Conferência de nível criptografado seguro
Não seguro	Meet Me	Nível mínimo de segurança é criptografado.	O iniciador recebe a mensagem `Does not m Security Level, call rejected ( atende ao Nível de segurança, c rejeitada).`
Seguro	Meet Me	Nível mínimo de segurança é não seguro.	Recurso de conferência seguro A conferência aceita todas as chamadas.

Identificação de chamada telefônica segura

Uma chamada segura é estabelecida quando seu telefone, assim como o telefone na outra ponta, é configurado para chamada segura. O outro telefone pode estar na mesma rede IP Cisco ou em uma rede fora da rede IP. As chamadas seguras podem ser feitas apenas entre dois telefones. As chamadas de conferência devem dar suporte à chamada segura após a configuração do recurso de conferência protegida.

Uma chamada segura é estabelecida usando este processo:

1. Um usuário inicia a chamada de um telefone seguro (modo de segurança protegido).
2. O ícone de proteção é exibido na tela do telefone. Esse ícone indica que o telefone está configurado para chamadas seguras, mas isso não significa que o outro telefone conectado também está protegido.

3. O usuário ouve um tom de segurança se a chamada se conectar a outro telefone protegido, indicando que ambas as extremidades da conversa estão criptografadas e protegidas. Se a chamada se conectar a um telefone não seguro, o usuário não ouvirá o tom de segurança.

Observação A chamada segura é permitida entre dois telefones. Em telefones protegidos, alguns recursos, como a chamada de conferência, as linhas compartilhadas e o Extension Mobility, não estão disponíveis quando a chamada segura é configurada.

Somente os telefones protegidos tocam esses tons indicativos de telefones seguros ou não seguros. Os telefones não protegidos nunca tocam tons. Se o status geral da chamada mudar durante a chamada, o tom indicativo também mudará e o telefone protegido tocará o tom apropriado.

Um telefone protegido toca um tom ou não sob estas circunstâncias:

- Quando a opção Play Secure Indication Tone (Tocar tom indicativo de seguro) estiver ativada:
  - Quando uma mídia segura de ponta a ponta for estabelecida e o status da chamada for seguro, o telefone tocará o tom indicativo seguro (três bipes longos com pausas).
  - Quando uma mídia não segura de ponta a ponta for estabelecida e o status da chamada for não seguro, o telefone tocará o tom indicativo não seguro (seis bipes curtos com pausas rápidas).

Se a opção Play Secure Indication Tone (Tocar tom indicativo de seguro) estiver desativada, nenhum tom será tocado.

Fornecer criptografia para intercalação

O Cisco Unified Communications Manager verifica o status de segurança do telefone quando são estabelecidas conferências e muda a indicação de segurança da conferência ou bloqueia a conclusão da chamada para manter a segurança e a integridade do sistema.

Um usuário não pode entrar em uma chamada criptografada se o telefone usado para isso não está configurado para criptografia. Quando a intercalação falha nesse caso, é reproduzido um tom de reordenação (sinal de ocupado) no telefone em que a intercalação foi iniciada.

Se o telefone do iniciador estiver configurado para criptografia, o iniciador da intercalação poderá entrar em uma chamada não segura do telefone criptografado. Depois que acontece a intercalação, o Cisco Unified Communications Manager classifica a chamada como não segura.

Se o telefone do iniciador estiver configurado para criptografia, o iniciador da intercalação poderá entrar em uma chamada criptografada e o telefone indicará que a chamada está criptografada.

Segurança na WLAN

Como todos os dispositivos de WLAN que estão no intervalo podem receber todo o tráfego da WLAN, proteger a comunicação por voz é algo essencial nessas redes. Para garantir que intrusos não manipulem nem interceptem o tráfego de voz, a arquitetura do Cisco SAFE Security oferece suporte para os APs do Telefone IP Cisco e do Cisco Aironet. Para obter mais informações sobre a segurança em redes, consulte http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

A solução de telefonia IP sem fio da Cisco fornece segurança de rede sem fio que impede inícios de sessão não autorizados e comunicações comprometidas usando os seguintes métodos de autenticação aceitos pelo Telefone IP sem fio Cisco:

- Autenticação aberta: qualquer dispositivo sem fio pode solicitar autenticação em um sistema aberto. O AP que recebe a solicitação pode conceder autenticação para qualquer solicitante ou apenas para solicitantes encontrados em uma lista de usuários. A comunicação entre o dispositivo sem fio e o AP pode não estar criptografada ou os dispositivos podem usar chaves WEP para fornecer segurança. Os dispositivos que usam WEP só tentam se autenticar com um ponto de acesso que está usando WEP.
- Autenticação EAP-FAST: essa arquitetura de segurança de cliente-servidor criptografa transações EAP dentro de um túnel TLS entre o AP e o servidor RADIUS, como o Cisco Access Control Server (ACS).

  O túnel TLS usa credenciais de acesso protegido (PACs) para autenticação entre o cliente (telefone) e o servidor RADIUS. O servidor envia um ID de autoridade (AID) para o cliente (telefone), que por sua vez seleciona a PAC apropriada. O cliente (telefone) retorna uma PAC-Opaque para o servidor RADIUS. O servidor descriptografa a PAC com a chave primária. Agora s dois pontos de extremidade contêm a chave PAC, e um túnel TLS é criado. O EAP-FAST oferece suporte para provisionamento automático de PAC, mas você precisa ativá-lo no servidor RADIUS.

Observação No Cisco ACS, por padrão, a PAC expira em uma semana. Se a PAC do telefone tiver expirado, a autenticação no servidor RADIUS será mais demorada enquanto o telefone obtém uma nova PAC. Para evitar atrasos no provisionamento da PAC, defina o período de expiração para 90 dias ou mais no servidor ACS ou RADIUS.

- Autenticação Extensible Authentication Protocol-Transport Layer Security (EAP-TLS): o EAP-TLS exige um certificado de cliente para autenticação e acesso à rede. Para EAP-TLS com fio, o certificado de cliente pode ser o MIC ou LSC do telefone. O LSC é o certificado de autenticação de cliente recomendado para EAP-TLS com fio.
- Protocolo de autenticação extensível protegido (PEAP): esquema de autenticação mútua baseada em senha e proprietário da Cisco entre o cliente (telefone) e um servidor RADIUS. O Telefone IP Cisco pode usar PEAP para autenticação na rede sem fio. Somente o PEAP MSCHAPV2 é compatível. O PEAP-GTC não é compatível.

Os seguintes esquemas de autenticação usam o servidor RADIUS para gerenciar chaves de autenticação:

- WPA/WPA2: usa informações do servidor RADIUS para gerar chaves exclusivas para autenticação. Como essas chaves são geradas no servidor RADIUS centralizado, o WPA/WPA2 oferece que mais segurança do que as chaves pré-compartilhadas WPA que são armazenadas no AP e no telefone.
- Roaming rápido e seguro: usa informações do servidor RADIUS e de um servidor de domínio sem fio (WDS) para gerenciar e autenticar as chaves. O WDS cria um cache de credenciais de segurança para dispositivos cliente ativados para o CCKM, para uma nova autenticação rápida e segura. O Telefone IP Cisco série 8800 oferece suporte para 802.11r (FT). 11r (FT) e CCKM são compatíveis para permitir roaming rápido e seguro. Mas a Cisco recomenda altamente a utilização do método pelo ar 802.11r (FT).

Com o WPA/WPA2 e o CCKM, as chaves de criptografia não são inseridas no telefone, mas derivadas automaticamente entre o AP e o telefone. Porém, o nome do usuário EAP e a senha que são usados para autenticação devem ser inseridos em cada telefone.

Para garantir que o tráfego de voz esteja seguro, o Telefone IP Cisco oferece suporte para WEP, TKIP e padrões de criptografia avançada (AES) para criptografia. Quando esses mecanismos são usados para criptografia, tanto os pacotes SIP de sinalização quanto os pacotes RTP (Real-Time Transport Protocol) de voz são criptografados entre o AP e o Telefone IP Cisco.

WEP

Com o uso do WEP na rede sem fio, a autenticação acontece no AP usando a autenticação de chave aberta ou de chave compartilhada. A chave WEP configurada no telefone deve corresponder à chave WEP que está configurada no AP para que as conexões sejam bem-sucedidas. O Telefone IP Cisco oferece suporte para chaves WEP que usam criptografia de 40 bits ou uma criptografia de 128 bits e permanecem estáticas no telefone e no AP.

A autenticação EAP e do CCKM pode usar chaves WEP para criptografia. O servidor RADIUS gerencia a chave WEP e passa uma chave exclusiva para o AP depois da autenticação para criptografar todos os pacotes de voz; consequentemente, essas chaves WEP podem mudar a cada autenticação.

TKIP

WPA e CCKM usam criptografia TKIP, que tem diversas melhorias em relação ao WEP. TKIP fornece vetores de inicialização (IVs) mais longos e criptografia de chave por pacote que reforçam a criptografia. Além disso, uma verificação de integridade das mensagens (MIC) garante que os pacotes criptografados não estejam sendo alterados. O TKIP remove a capacidade de previsão do WEP que ajuda os invasores a decifrar a chave WEP.

AES

Um método de criptografia usado para autenticação WPA2. Esse padrão nacional de criptografia usa um algoritmo simétrico que tem a mesma chave para criptografia e descriptografia. O AES usa criptografia CBC de 128 bits, que suporta tamanhos de chave de pelo menos 128, 192 e 256 bits. O Telefone IP Cisco suporta um tamanho de chave de 256 bits.

Observação O Telefone IP Cisco não oferece suporte para o protocolo de integridade de chave Cisco (CKIP) com CMIC.

Esquemas de autenticação e criptografia são configuradas na LAN sem fio. As VLANs configuradas na rede e nos APs e especificam diferentes combinações de autenticação e criptografia. Um SSID é associado a uma VLAN e ao esquema de autenticação e criptografia específico. Para que os dispositivos cliente sem fio sejam autenticados corretamente, você deve configurar os mesmos SSIDs com os esquemas de autenticação e criptografia deles nos APs e no Telefone IP Cisco.

Alguns esquemas de autenticação exigem tipos específicos de criptografia. Com a autenticação aberta, você pode usar WEP estático para criptografia para aumentar a segurança. Mas se você estiver usando autenticação de chave compartilhada, deve configurar o WEP estático para criptografia e uma chave WEP no telefone.

Observação

- Quando você usa uma chave pré-compartilhada WPA ou WPA2, a chave pré-compartilhada deve ser definida de forma estática no telefone. Essas chaves devem coincidir com as chaves que estão no AP.
- O Telefone IP Cisco não oferece suporte para negociação automática de EAP; para usar o modo EAP-FAST, você deve especificá-lo.

A tabela a seguir mostra uma lista de esquemas de autenticação e criptografia configurados nos APs do Cisco Aironet que são suportados pelo Telefone IP Cisco. A tabela mostra a opção de configuração de rede para o telefone que corresponde à configuração do AP.

Tabela 3: Esquemas de autenticação e criptografia

Configuração do Telefone IP Cisco	Configuração do AP			
Modo de segurança	Segurança	Gerenciamento de tecla	Criptografia	Roaming rápido
Nenhuma	Nenhuma	Nenhuma	Nenhuma	N/A
WEP	WEP estático	Static	WEP	N/A
PSK	PSK	WPA	TKIP	Nenhuma
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

Para obter mais informações sobre como configurar esquemas de autenticação e criptografia em APs, consulte o *Cisco Aironet Configuration Guide* do seu modelo e versão no seguinte URL:

http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

Segurança da LAN sem fio

Os telefones Cisco compatíveis com Wi-Fi têm mais requisitos de segurança e exigem configuração extra. Essas etapas extras incluem instalar certificados e configurar a segurança nos telefones e no Cisco Unified Communications Manager.

Para obter mais informações, consulte o *Guia de segurança do Cisco Unified Communications Manager*.

Página de administração do Telefone IP Cisco

Os telefones Cisco que oferecem suporte de Wi-Fi possuem páginas da Web especiais diferentes das páginas de outros telefones. Você utiliza essas páginas da Web especiais para configuração de segurança do telefone quando o SCEP (Simple Certificate Enrollment Protocol) não estiver disponível. Use essas páginas para instalar manualmente certificados de segurança em um telefone, para baixar um certificado de segurança ou para configurar manualmente a data e hora do telefone.

Essas páginas da Web também mostram as mesmas informações que você vê em páginas da Web de outros telefones, incluindo informações do dispositivo, configuração de rede, registros e informações estatísticas.

Configurar a página de administração do telefone

A página da Web de administração é ativada quando o telefone é enviado pela fábrica, e a senha é definida como Cisco. Mas, se um telefone for registrado no Cisco Unified Communications Manager, será preciso ativar a página da Web de administração e configurar uma nova senha.

Ative essa página da Web e defina as credenciais de acesso antes de usar a página da Web pela primeira vez depois que o telefone for registrado.

Uma vez ativada, a página da Web de administração estará acessível na porta HTTPS 8443 (`https://x.x.x.x:8443`, onde x.x.x.x é o endereço IP do telefone).

Antes de Iniciar

Defina uma senha antes de ativar a página da Web de administração. A senha pode ser formada por qualquer combinação de letras ou números, mas deve conter entre 8 e 127 caracteres.

Seu nome de usuário é permanentemente definido como admin.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone**.

Etapa 2 Localize seu telefone.

Etapa 3 Na seção **Layout da configuração específica do produto**, defina **Administrador Web** como **Ativado**.

Etapa 4 No campo **Senha do administrador**, insira uma senha.

Etapa 5 Selecione **Salvar** e clique em **OK**.

Etapa 6 Selecione **Aplicar config.** e clique em **OK**.

Etapa 7 Reinicie o telefone.

Acessar a página da Web de administração do telefone

Quando você quiser acessar as páginas da Web de administração, terá de especificar a porta de administração.

Procedimento

Etapa 1 Obtenha o endereço IP do telefone:

- Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone** e localize o telefone. Os telefones registrados no Cisco Unified Communications Manager exibem o endereço IP na janela **Localizar e listar telefones** e na parte superior da janela **Configuração do telefone**.

Etapa 2 Abra um navegador da Web e insira o seguinte URL, onde *endereço_IP* é o endereço IP do Telefone IP Cisco:

`https://<IP_address>:8443`

Etapa 3 Digite a senha no campo Senha.

Etapa 4 Clique em **Enviar**.

Instalar um certificado de usuário na página da Web de administração do telefone

Você pode instalar manualmente um certificado de usuário no telefone se o protocolo SCEP (Simple Certificate Enrollment Protocol) não estiver disponível.

O Certificado instalado pelo fabricante (MIC) pré-instalado pode ser usado como o certificado do usuário para EAP-TLS.

Depois de instalar o certificado do usuário, você precisa adicioná-lo à lista de confiança do servidor RADIUS.

Antes de Iniciar

Para poder instalar um certificado de usuário para um telefone, você precisa ter:

- Um certificado de usuário salvo em seu PC. O certificado deve estar no formato PKCS #12.
- A senha de extração do certificado.

Procedimento

Etapa 1 Na página da Web de administração do telefone, selecione **Certificados**.
Etapa 2 Navegue até o certificado em seu PC.
Etapa 3 No campo **Extrair senha**, insira a senha de extração do certificado.
Etapa 4 Clique em **Carregar**.
Etapa 5 Reinicie o telefone depois que o upload terminar.

Instalar um certificado de autenticação de servidor usando a página da Web de administração do telefone

Você pode instalar manualmente um certificado de servidor de autenticação no telefone se o protocolo SCEP (Simple Certificate Enrollment Protocol) não estiver disponível.

O certificado raiz de CA que emitiu o certificado de servidor RADIUS deve estar instalado para o EAP-TLS.

Antes de Iniciar

Antes de instalar um certificado em um telefone, você deve ter um certificado de servidor de autenticação salvo no PC. O certificado deve ser codificado no PEM (Base 64) ou DER.

Procedimento

Etapa 1 Na página da Web de administração do telefone, selecione **Certificados**.
Etapa 2 Localize o campo **CA (página da Web de administração) do servidor de autenticação** e clique em **Instalar**.
Etapa 3 Navegue até o certificado em seu PC.
Etapa 4 Clique em **Carregar**.
Etapa 5 Reinicie o telefone depois que o upload terminar.

Se estiver instalando mais de um certificado, instale todos os certificados antes de reiniciar o telefone.

Remover manualmente um certificado de segurança da página da Web de administração do telefone

Você pode remover manualmente um certificado de segurança de um telefone se o protocolo SCEP (Simple Certificate Enrollment Protocol) não estiver disponível.

Procedimento

Etapa 1 Na página da Web de administração do telefone, selecione **Certificados**.

Etapa 2 Localize o certificado na página **Certificados**.

Etapa 3 Clique em **Excluir**.

Etapa 4 Reinicie o telefone depois que o processo de exclusão for concluído.

Definir manualmente a data e a hora do telefone

Com a autenticação baseada em certificados, o telefone deve exibir a data e a hora corretas. Um servidor de autenticação verifica a data e a hora do telefone em relação à data de expiração do certificado. Se as datas e horas do telefone e do servidor não coincidirem, o telefone deixará de funcionar.

Use este procedimento para definir manualmente a data e a hora do telefone se ele não estiver recebendo as informações corretas de sua rede.

Procedimento

Etapa 1 Na página da Web de administração do telefone, role até **Data e hora**.

Etapa 2 Realize uma das seguintes opções:

- Clique em **Definir telefone para Data e hora local** para sincronizar o telefone com um servidor local.
- Nos campos **Data e hora específica**, selecione mês, dia, ano, hora, minuto e segundo usando os menus e clique em **Definir telefone para data e hora específica**.

Configuração do SCEP

O protocolo SCEP (Simple Certificate Enrollment Protocol) é o padrão para fornecimento e renovação automática de certificados. Evite a instalação manual de certificados em seus telefones.

Definir os parâmetros de configuração específicos do produto SCEP

Você deve configurar os seguintes parâmetros do SCEP na página da Web do telefone

- Endereço IP do RA
- Impressão digital SHA-1 ou SHA-256 do certificado raiz da CA para o servidor SCEP

A Autoridade de registro (RA) do Cisco IOS atua como um proxy para o servidor SCEP. O cliente SCEP no telefone usa os parâmetros que são baixados do Cisco Unified Communication Manager. Depois que você configura os parâmetros, o telefone envia uma solicitação `SCEP getcs` para o RA, e o certificado raiz da CA é validado usando a impressão digital definida.

Procedimento

Etapa 1 Na Administração do Cisco Unified Communications Manager, selecione **Dispositivo** > **Telefone**.

Etapa 2 Localize o telefone.

Etapa 3 Role até a área **Layout da configuração específica do produto**.

Etapa 4 Marque a caixa de seleção **Servidor WLAN SCEP** para ativar o parâmetro SCEP.

Etapa 5 Marque a caixa de seleção **Impr. digital CA de raiz WLAN (SHA256 ou SHA1)** para ativar o parâmetro QED SCEP.

Suporte ao servidor SCEP (Simple Certificate Enrollment Protocol)

Se você estiver usando um servidor SCEP (Simple Certificate Enrollment Protocol), o servidor poderá manter automaticamente seus certificados de usuário e de servidor. No servidor SCEP, configure o agente de registro (RA) SCEP para:

- Agir como um ponto de confiança PKI
- Agir como um RA PKI
- Executar a autenticação de dispositivos usando um servidor RADIUS

Para obter mais informações, consulte a documentação do servidor SCEP.

Autenticação 802.1x

Os Telefones IP Cisco são compatíveis com a Autenticação 802.1X.

Os Telefones IP Cisco e os switches do Cisco Catalyst tradicionalmente usam o CDP (Cisco Discovery Protocol) para identificar um ao outro e determinar parâmetros como a alocação de VLAN e os requisitos de potência embutida.

O suporte à autenticação 802.1X exige vários componentes:

- Telefone IP Cisco: o telefone inicia a solicitação para acessar a rede. Os telefones contêm um suplicante 802.1X. Esse suplicante permite aos administradores de rede controlar a conectividade dos telefones IP para as portas de switch da LAN. A versão atual do suplicante 802.1X do telefone usa as opções EAP-FAST e EAP-TLS para autenticação de rede.
- Switch do Cisco Catalyst (ou outro switch de terceiros): o switch deve ser compatível com 802.1X para que possa atuar como o autenticador e passar as mensagens entre o telefone e o servidor de autenticação. Após a conclusão da troca, o switch concede ou nega o acesso do telefone à rede.

Você deve executar as ações a seguir para configurar a 802.1X.

- Configure os outros componentes antes de ativar a Autenticação 802.1X no telefone.

- Configure a VLAN de voz — Como o padrão 802.1X não considera as VLANs, você deve definir essa configuração com base no suporte ao switch.
  - Ativado — Se você estiver usando um switch que aceita a autenticação de vários domínios, você poderá continuar usando a VLAN de voz.
  - Desativado — Se o switch não aceitar a autenticação de vários domínios, desative a VLAN de voz e considere a atribuição da porta à VLAN nativa.

Tópicos relacionados

Documentação do Cisco Unified Communications Manager

Sobre a tradução

A Cisco pode fornecer traduções no idioma local deste conteúdo em alguns locais. Observe que essas traduções são fornecidas apenas para fins informativos e, se houver alguma inconsistência, a versão em inglês deste conteúdo prevalecerá.