Guia de gerenciamento de certificado da solução UCCX

Contents

Introduction

Este documento descreve como configurar o Cisco Unified Contact Center Express (UCCX) para o uso de certificados autoassinados e assinados.

Prerequisites

Requirements

Antes de prosseguir com as etapas de configuração descritas neste documento, certifique-se de que você tenha acesso à página de Administração do Sistema Operacional (SO) para estes aplicativos:

- UCCX
- SocialMiner
- MediaSense

Um administrador também deve ter acesso ao armazenamento de certificados nos computadores cliente do agente e do supervisor.

FQDN, DNS e domínios

Énecessário que todos os servidores na configuração do UCCX sejam instalados com os servidores DNS (Domain Name System) e os nomes de domínio. Também é necessário que agentes, supervisores e administradores acessem os aplicativos de configuração do UCCX por meio do FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado).

O UCCX versão 10.0+ requer que o nome de domínio e os servidores DNS sejam preenchidos na instalação. Os certificados gerados pelo instalador do UCCX Versão 10.0+ contêm o FQDN, conforme apropriado. Adicione os servidores DNS e um domínio ao cluster do UCCX antes de atualizar para o UCCX versão 10.0+.

Se o domínio for alterado ou preenchido pela primeira vez, os certificados deverão ser regenerados. Depois de adicionar o nome de domínio à configuração do servidor, gere novamente todos os certificados Tomcat antes de instalá-los em outros aplicativos, nos navegadores clientes ou na geração do CSR (Certificate Signing Request) para assinatura.

Componentes Utilizados

As informações descritas neste documento são baseadas nestes componentes de hardware e software:

- Serviços Web UCCX
- Serviço de notificação do UCCX
- Tomcat da plataforma UCCX
- Cisco Finesse Tomcat
- Tomcat do Cisco Unified Intelligence Center (CUIC)
- Tomcat do SocialMiner
- Serviços Web MediaSense

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. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

Com a introdução do co-residente Finesse e CUIC, a integração entre o UCCX e o SocialMiner para e-mail e bate-papo e o uso do MediaSense para gravar, entender e instalar certificados via Finesse, a capacidade de solucionar problemas de certificado agora é extremamente importante.

Este documento descreve o uso de certificados autoassinados e assinados no ambiente de configuração do UCCX que abrange:

- Serviços de notificação do UCCX
- Serviços Web UCCX
- Scripts UCCX
- Coresidente Finesse
- CUIC co-residente (dados dinâmicos e relatórios históricos)
- MediaSense (gravação e marcação baseada no Finesse)
- SocialMiner (bate-papo)

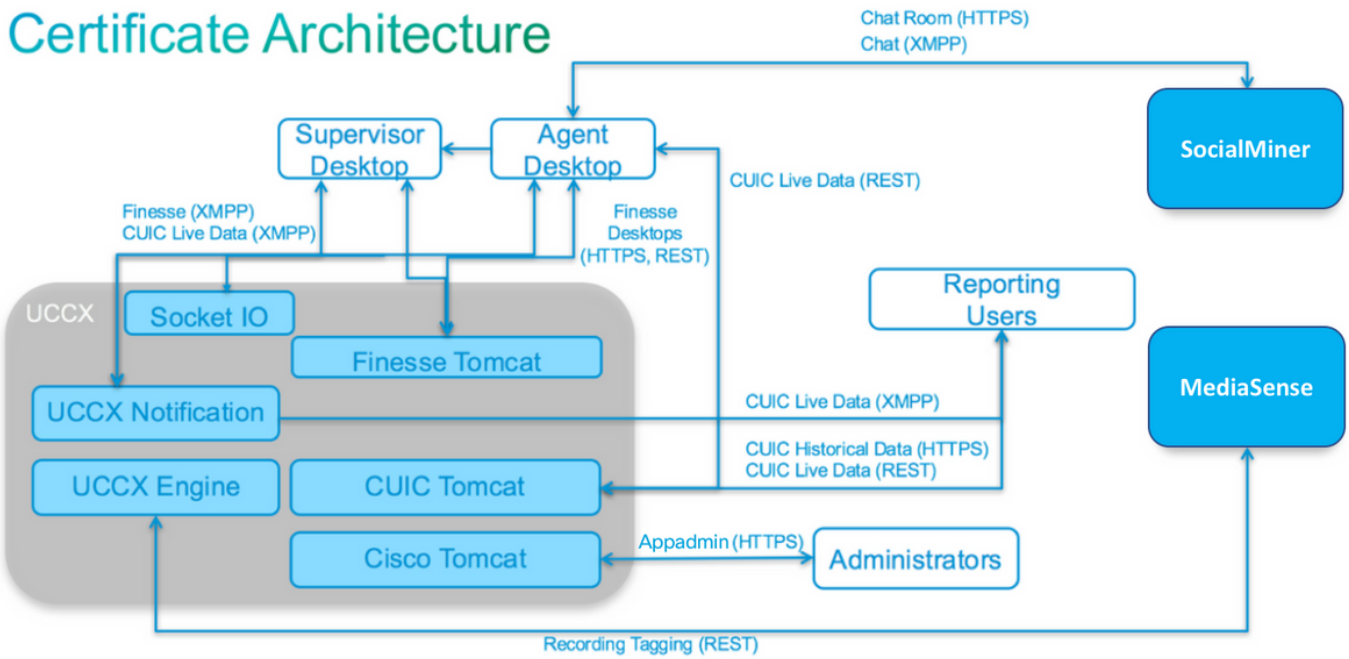
Os certificados, assinados ou autoassinados, devem ser instalados nos aplicativos (servidores) na configuração do UCCX, bem como nos desktops cliente do agente e do supervisor.

No Unified Communications Operating System (UCOS) 10.5, foram adicionados certificados de vários servidores para que um único CSR pudesse ser gerado para um cluster em vez de ter que assinar um certificado individual para cada nó no cluster. Esse tipo de certificado não tem suporte explícito para UCCX, MediaSense e SocialMiner.

Configurar

Esta seção descreve como configurar o UCCX para o uso de certificados autoassinados e assinados.

Diagrama de configuração



Arquitetura da solução UCCX válida a partir do UCCX 11.0. Diagrama de comunicação HTTPS.

Certificados assinados

O método recomendado de gerenciamento de certificados para a configuração do UCCX é aproveitar certificados assinados. Esses certificados podem ser assinados por uma CA interna ou por uma CA de terceiros bem conhecida.

Nos principais navegadores, como o Mozilla Firefox e o Internet Explorer, os certificados raiz para CAs de terceiros bem conhecidas são instalados por padrão. Os certificados para aplicativos de configuração do UCCX assinados por essas autoridades de certificação são confiáveis por padrão, pois sua cadeia de certificados termina em um certificado raiz que já está instalado no navegador.

O certificado raiz de uma CA interna também pode ser pré-instalado no navegador do cliente por meio de uma Diretiva de Grupo ou outra configuração atual.

Você pode escolher se deseja que os certificados do aplicativo de configuração do UCCX sejam assinados por uma CA de terceiros bem conhecida ou por uma CA interna com base na disponibilidade e pré-instalação do certificado raiz para as CAs no navegador do cliente.

Instalar certificados de aplicativo Tomcat assinados

Conclua estas etapas para cada nó dos aplicativos UCCX Publisher and Subscriber, SocialMiner e MediaSense Publisher and Subscriber Administration:

1. Navegue até a página **OS Administration** e escolha **Security > Certificate Management**.
2. Clique em **Gerar CSR**.
3. Na lista suspensa **Lista de certificados**, escolha **tomcat** como o nome do certificado e clique em **Gerar CSR**.
4. Navegue até **Security > Certificate Management** e escolha **Download CSR**.
5. Na janela pop-up, escolha **tomcat** na lista suspensa e clique em **Download CSR**.

Envie o novo CSR à CA de terceiros ou assine-o com uma CA interna, conforme descrito anteriormente. Este processo deve produzir os seguintes certificados assinados:

- Certificado raiz para a autoridade de certificação
- Certificado de Aplicativo de Editor do UCCX
- Certificado de aplicativo de assinante do UCCX
- Certificado de aplicativo do SocialMiner
- Certificado de aplicativo MediaSense Publisher
- Certificado de aplicativo de assinante MediaSense

Note: Deixe o campo **Distribution** no CSR como o FQDN do servidor.

Note: O certificado "Multi-servidor (SAN)" é compatível com o UCCX a partir da versão 11.6. No entanto, a SAN deve incluir somente o UCCX Node-1 e Node-2. Outros servidores, como o SocialMiner, não devem ser incluídos na SAN do UCCX.

Note: O UCCX suporta apenas tamanhos de chave de certificado de 1024 e 2048 bits.

Conclua estas etapas em cada servidor de aplicativos para carregar o certificado raiz e o certificado de aplicativo nos nós:

Note: Se você carregar certificados raiz e intermediários em um editor (UCCX ou MediaSense), eles deverão ser automaticamente replicados para o assinante. Não há necessidade de carregar certificados raiz ou intermediários em outros servidores não editores na configuração se todos os certificados de aplicativos forem assinados pela mesma cadeia de certificados.

1. Navegue até a página **OS Administration** e escolha **Security > Certificate Management**.
2. Clique em **Carregar certificado**.
3. Carregue o certificado raiz e escolha **tomcat-trust** como o tipo de certificado.
4. Clique em **Upload File**.
5. Clique em **Carregar certificado**.
6. Carregue o certificado do aplicativo e escolha **tomcat** como o tipo de certificado.
7. Clique em **Upload File**. **Note**: Se uma CA subordinada assinar o certificado, carregue o certificado raiz da CA subordinada como o certificado *tomcat-trust* em vez do certificado raiz. Se um certificado intermediário for emitido, carregue esse certificado no repositório *tomcat-trust* além do certificado do aplicativo.
8. Após a conclusão, reinicie estes aplicativos: Editor e assinante do Cisco MediaSenseCisco SocialMinerEditor e assinante do Cisco UCCX

Note: Quando você usa UCCX, MediaSense e SocialMiner 11.5 e posterior, há um novo certificado chamado tomcat-ECDSA. Quando você carregar um certificado tomcat-ECDSA assinado no servidor, carregue o certificado do aplicativo como um certificado tomcat-ECDSA — não um certificado tomcat. Para obter mais informações sobre o ECDSA, consulte a seção Informações Relacionadas para obter o link para entender e configurar os certificados ECDSA.

Certificados Autoassinados

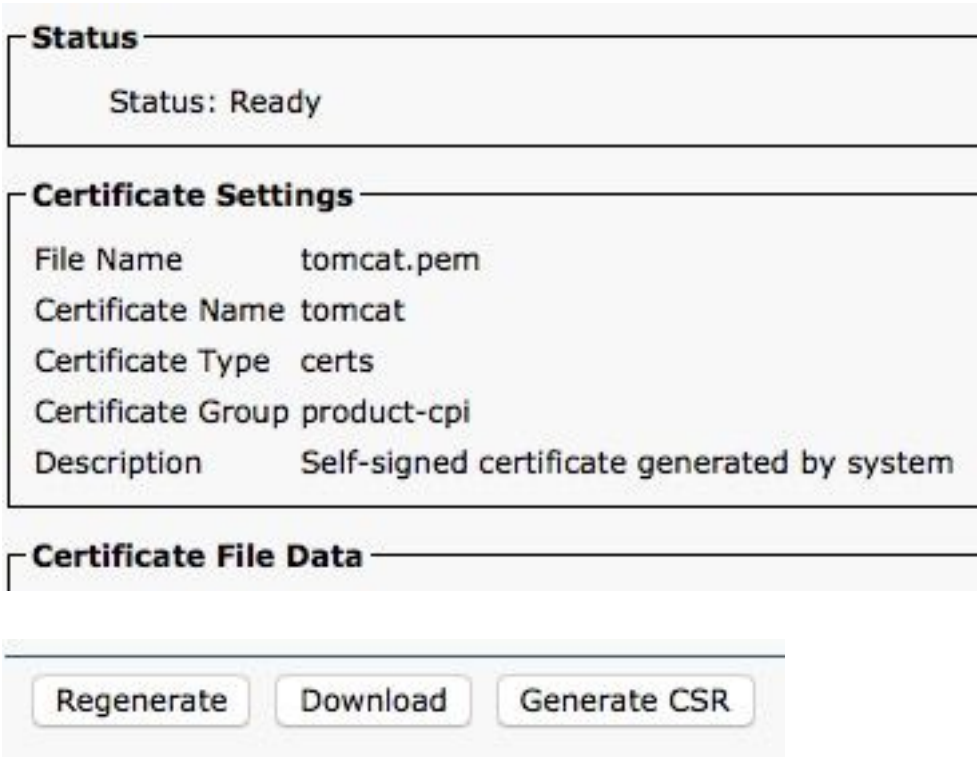
Instalação Em Servidores Periféricos

Todos os certificados usados na configuração do UCCX vêm pré-instalados nos aplicativos de configuração e são autoassinados. Esses certificados autoassinados não são implicitamente confiáveis quando apresentados a um navegador cliente ou a outro aplicativo de configuração. Embora seja recomendável assinar todos os certificados na configuração do UCCX, você pode usar os certificados autoassinados pré-instalados.

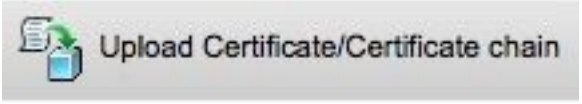
Para cada relacionamento de aplicativo, você deve baixar o certificado apropriado e carregá-lo no aplicativo. Conclua estas etapas para obter e carregar os certificados:

1. Acesse a página **Administração do SO do** aplicativo e escolha **Segurança > Gerenciamento de Certificado**.

2. Clique no arquivo de certificado **.pem** apropriado e escolha **Download**:



3. Para carregar um certificado no aplicativo apropriado, navegue até a página **OS Administration** e escolha **Security > Certificate Management**.
4. Clique em **Carregar certificado / Cadeia de certificados:**



5. Após a conclusão, reinicie estes servidores:

   Editor e assinante do Cisco MediaSenseCisco SocialMinerEditor e assinante do Cisco UCCX

Para instalar certificados autoassinados no computador cliente, use uma diretiva de grupo ou um gerenciador de pacotes, ou instale-os individualmente no navegador de cada PC do agente.

Para o Internet Explorer, instale os certificados autoassinados do lado do cliente no repositório **Autoridades de Certificação Raiz Confiáveis**.

Para o Mozilla Firefox, siga estes passos:

1. Navegue até **Ferramentas > Opções**.
2. Clique na guia Advanced.
3. Clique em **Exibir certificados**.
4. Navegue até a guia **Servers**.
5. Clique em **Adicionar exceção**.

Regenerando Certificados Autoassinados

Caso os certificados autoassinados expirem, eles precisarão ser regenerados e as etapas de configuração de **Instalação em servidores periféricos** precisarão ser executadas novamente.

1. Acessar o aplicativo **Administração do SO** e escolha **Segurança > Gerenciamento de Certificados**.
2. Clique no certificado apropriado e escolha **Regenerar**.
3. O servidor cujo certificado foi gerado novamente deve ser reiniciado.
4. Para cada relacionamento de aplicativo, você deve baixar o certificado apropriado e carregá-lo no aplicativo seguindo as etapas de configuração de **Instalação em Servidores Periféricos.**

Integração e configuração do cliente

UCCX para MediaSense

O UCCX consome a interface de programação de aplicativo (API) REST dos serviços Web MediaSense para duas finalidades:

- Para assinar as notificações de novas gravações que são invocadas no Cisco Unified Communications Manager (CUCM).
- Para marcar as gravações dos agentes do UCCX com informações do agente e da fila do Contact Service (CSQ).

O UCCX consome a API REST nos nós de administração do MediaSense. Há um máximo de dois em qualquer cluster MediaSense. O UCCX não se conecta via API REST aos nós de expansão do MediaSense. Ambos os nós do UCCX devem consumir a API REST do MediaSense; portanto, instale os dois certificados MediaSense Tomcat nos dois nós do UCCX.

Carregue a cadeia de certificados assinados ou autoassinados dos servidores MediaSense no armazenamento de chaves UCCX *tomcat-trust*.

MediaSense para Finesse

O MediaSense consome a API REST dos serviços Web Finesse para autenticar agentes para o gadget Pesquisa e reprodução do MediaSense no Finesse.

O servidor MediaSense configurado no layout Finesse XML para o gadget Pesquisar e reproduzir deve consumir a API REST Finesse, então instale os dois certificados UCCX Tomcat nesse nó

MediaSense.

Carregue a cadeia de certificados assinados ou autoassinados dos servidores UCCX no armazenamento de chaves *tomcat-trust* do MediaSense.

UCCX para SocialMiner

O UCCX consome as APIs REST e Notification do SocialMiner para gerenciar contatos e configurações de email. Os dois nós do UCCX devem consumir a API REST do SocialMiner e ser notificados pelo serviço de notificação do SocialMiner. Portanto, instale o certificado Tomcat do SocialMiner nos dois nós do UCCX.

Carregue a cadeia de certificados assinados ou autoassinados do servidor do SocialMiner no armazenamento de chaves *tomcat-trust* do UCCX.

Certificado de cliente AppAdmin do UCCX

O certificado de cliente UCCX AppAdmin é usado para administração do sistema UCCX. Para instalar o certificado UCCX AppAdmin para administradores do UCCX, no PC cliente, navegue para **https://<UCCX FQDN>/appadmin/main** para cada um dos nós do UCCX e instale o certificado por meio do navegador.

Certificado de cliente da plataforma UCCX

Os serviços Web do UCCX são usados para a entrega de contatos de bate-papo para navegadores clientes. Para instalar o certificado da plataforma UCCX para agentes e supervisores do UCCX, no PC cliente, navegue para **https://<UCCX FQDN>/appadmin/main** para cada um dos nós do UCCX e instale o certificado por meio do navegador.

Certificado do cliente do Notification Service

O serviço de notificação do CCX é usado pelo Finesse, UCCX e CUIC para enviar informações em tempo real para o desktop do cliente através do Extensible Messaging and Presence Protocol (XMPP). Isso é usado para a comunicação Finesse em tempo real, bem como o CUIC Live Data.

Para instalar o certificado de cliente do Notification Service no PC dos agentes e supervisores ou usuários de relatórios que usam Live Data, navegue até **https://<UCCX FQDN>:7443/** para cada um dos nós do UCCX e instale o certificado por meio do navegador.

Certificado do cliente Finesse

O certificado de cliente Finesse é usado pelos desktops Finesse para se conectar à instância Finesse Tomcat para fins de comunicação da API REST entre o desktop e o servidor Finesse co-residente.

Para instalar o certificado Finesse para agentes e supervisores, no PC cliente, navegue para **https://<UCCX FQDN>:8445/** para cada um dos nós UCCX e instale o certificado através dos prompts do navegador.

Para instalar o certificado Finesse para administradores Finesse, no PC cliente, navegue para

https://<UCCX FQDN>:8445/cfadmin para cada um dos nós UCCX e instale o certificado através dos prompts do navegador.

Certificado de cliente do SocialMiner

O certificado Tomcat do SocialMiner deve estar instalado no computador cliente. Quando um agente aceita uma solicitação de bate-papo, o gadget de bate-papo é redirecionado para uma URL que representa a sala de bate-papo. Esta sala de chat é hospedada pelo servidor do SocialMiner e contém o cliente ou o contato de chat.

Para instalar o certificado do SocialMiner no navegador, no PC cliente, navegue até **https://<SocialMiner FQDN>/** e instale o certificado através dos prompts do navegador.

Certificado de cliente CUIC

O certificado Tomcat CUIC deve ser instalado na máquina cliente para agentes, supervisores e usuários de relatórios que usam a interface da Web CUIC para relatórios de histórico ou relatórios de Dados dinâmicos na página da Web CUIC ou nos gadgets na área de trabalho.

Para instalar o certificado CUIC Tomcat no navegador, no PC cliente, navegue até **https://<UCCX FQDN>:8444/** e instale o certificado através dos prompts do navegador.

Certificado do CUIC Live Data (desde 11.x)

O CUIC usa o Serviço de E/S de soquete para o back-end Live data. Este certificado deve ser instalado na máquina cliente para agentes, supervisores e usuários de relatórios que usam a interface da Web do CUIC para Live Data ou que usam os gadgets Live Data no Finesse.

Para instalar o certificado de Soquete E/S no navegador, no PC cliente, navegue para **https://<UCCX FQDN>:12015/** e instale o certificado através dos prompts do navegador.

Aplicativos de terceiros acessíveis a partir de scripts

Se um script do UCCX for projetado para acessar um local seguro em um servidor de terceiros (por exemplo, a etapa *Obter Documento de URL* para um URL HTTPS ou uma *Fazer Chamada Rest* para um URL REST HTTPS), carregue a cadeia de certificados assinada ou autoassinada do serviço de terceiros no armazenamento de chaves UCCX *tomcat-trust*. Para obter esse certificado, acesse a página **Administração do SO** do UCCX e escolha **Carregar certificado**.

O Mecanismo UCCX é configurado para pesquisar o armazenamento de chaves Tomcat da plataforma para cadeias de certificados de terceiros quando apresentado a esses certificados por aplicativos de terceiros quando acessam locais seguros através de etapas de script.

Toda a cadeia de certificados deve ser carregada no armazenamento de chaves Tomcat da plataforma, acessível por meio da página **OS Administration**, já que o armazenamento de chaves Tomcat não contém certificados raiz por padrão.

Após concluir essas ações, reinicie o Cisco UCCX Engine.

Verificar

Para verificar se todos os certificados estão instalados corretamente, você pode testar os recursos descritos nesta seção. Se nenhum erro de certificado for exibido e todos os recursos funcionarem corretamente, os certificados serão instalados corretamente.

- Configure o Finesse para que ele registre automaticamente um agente por meio do fluxo de trabalho. Depois que uma chamada for tratada pelo agente, use o aplicativo MediaSense Search and Play para encontrá-la. Verifique se a chamada tem as marcas de agente, uma fila do Contact Service e uma equipe anexadas aos metadados de gravação no MediaSense.
- Configure o Web Chat do agente através do SocialMiner. Injete um contato de bate-papo pelo formulário da Web. verifique se o agente recebe o banner para aceitar o contato de chat e também verifique se, depois que o contato de chat for aceito, o formulário de chat será carregado corretamente e se o agente pode receber e enviar mensagens de chat.
- Tentativa de fazer logon em um agente via Finesse. Verifique se nenhum aviso de certificado é exibido e se a página da Web não solicita a instalação de certificados no navegador. Verifique se o agente pode alterar os estados corretamente e se uma nova chamada para o UCCX foi apresentada corretamente ao agente.
- Depois de configurar os gadgets de Dados dinâmicos no layout de área de trabalho do agente e supervisor Finesse, faça logon em um agente, um supervisor e um usuário de relatórios. Verifique se os gadgets de Dados dinâmicos são carregados corretamente, se os dados iniciais são preenchidos no gadget e se os dados são atualizados quando os dados subjacentes são alterados.
- Tente se conectar de um navegador à URL do AppAdmin nos dois nós do UCCX. Verifique se nenhum aviso de certificado aparece quando solicitado com a página de login.

Troubleshoot

Problema - ID de usuário/senha inválida

Os Agentes do UCCX Finesse não podem fazer logon com o erro "**ID de usuário/senha inválida**".

Causas

O Unified CCX lança uma exceção "SSLHandshakeException" e não estabelece uma conexão com o Unified CM.

Solução

- Verifique se o certificado Unified CM Tomcat não expirou.
- Certifique-se de que qualquer certificado carregado no Unified CM tenha qualquer uma destas extensões marcada como crítica:
  Uso da chave X509v3 (OID - 2.5.29.15)
  Restrições básicas do X509v3 (OID - 2.5.29.19)
  Se você marcar outras extensões como críticas, a comunicação falhará entre o Unified CCX e o Unified CM devido à falha na verificação do certificado do Unified CM.

Problema - SAN CSR e SAN Certificada Não Correspondem

O carregamento de um certificado assinado por uma autoridade de certificação exibe o erro "CSR SAN e SAN de certificado não corresponde".

Causas

A autoridade de certificação pode ter adicionado outro domínio pai no campo Nomes alternativos do assunto (SAN) do certificado. Por padrão, o CSR terá estas SANs:

SubjectAltName [
  example.com (dNSName)
  hostname.example.com (dNSName)
]

As autoridades de certificação podem retornar um certificado com outra SAN adicionada ao certificado: www.hostname.example.com. O certificado terá uma SAN extra nesse caso:

SubjectAltName [
  example.com (dNSName)
  hostname.example.com (dNSName)

  www.hostname.example.com (dNSName)
]

Isso causa o erro de incompatibilidade de SAN.

Solução

Na seção "Nome alternativo do assunto (SANs)" da página "Gerar solicitação de assinatura de certificado" do UCCX, gere o CSR com um campo Domínio pai vazio. Dessa forma, o CSR não é gerado com um atributo SAN, a CA pode formatar as SANs e não haverá uma incompatibilidade de atributos SAN quando você carregar o certificado no UCCX. Observe que o campo Domínio pai assume como padrão o domínio do servidor UCCX, portanto, o valor deve ser explicitamente removido enquanto as configurações para o CSR são configuradas.

Problema - NET::ERR_CERT_COMMON_NAME_INVALID

Ao acessar qualquer página da Web do UCCX, MediaSense ou SocialMiner, você recebe uma mensagem de erro.

"Sua conexão não é privada.

Os invasores podem estar tentando roubar suas informações do <Server_FQDN> (por exemplo, senhas, mensagens ou cartões de crédito). NET::ERR_CERT_COMMON_NAME_INVALID

Este servidor não pôde provar que é <Server_FQDN>; seu certificado de segurança é de [missing_subjectAltName]. Isso pode ser causado por um erro de configuração ou um invasor interceptando sua conexão."

Causas

A versão 58 do Chrome introduziu um novo recurso de segurança em que ele relata que o certificado de um site não é seguro se o seu nome comum (CN) não estiver também incluído como uma SAN.

Solução

- Você pode navegar para **Avançado >** Prosseguir para <Server_FQDN> (não seguro) para continuar até o site e aceitar o erro do certificado.
- Você pode evitar o erro completamente com os certificados assinados pela CA. Quando você gera um CSR, o FQDN do servidor é incluído como uma SAN. A CA pode assinar o CSR e, depois que você carregar o certificado assinado de volta no servidor, o certificado do servidor terá o FQDN no campo SAN para que o erro não seja apresentado.

Mais informações

Consulte a seção "Remove support for commonName matching in certificates" em Deprecations and Removals no Chrome 58.

Defeitos do certificado

- ID de bug Cisco CSCvb46250 - UCCX: Impacto do certificado Tomcat ECDSA no Finesse Live Data
- ID de bug Cisco CSCvb58580 - Não é possível fazer login no SocialMiner com tomcat e tomcat-ECDSA assinados pela RSA CA
- ID de bug Cisco CSCvd56174 - UCCX: Falha de logon do agente Finesse devido a SSLHandshakeException
- ID de bug da Cisco CSCuv89545 - Vulnerabilidade ao Logjam Finesse

Informações Relacionadas

- Entender os certificados ECDSA em uma solução UCCX
- Suporte SHA 256 para UCCX
- Exemplo de configuração de certificados assinados e autoassinados do UCCX
- Suporte Técnico e Documentação - Cisco Systems

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.