Compreenda Certificados ECDSA em uma solução UCCX

Índice

Introdução

Este documento descreve como configurar a solução do Cisco Unified Contact Center Express (UCCX) para o uso de Certificados elípticos do Digital Signature Algorithm da curva (ECDSA).

Pré-requisitos

Requisitos

Antes que você continue com as etapas de configuração que estão descritas neste documento, assegure-se de que você tenha o acesso à página de administração do operating system (OS) para estes aplicativos:

- UCCX
- SocialMiner
- Gerente das comunicações unificadas de Cisco (CUCM)
- Configuração do certificado da solução UCCX - http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html

Um administrador deve igualmente ter o acesso à loja do certificado no cliente PC do agente e do supervisor.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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 sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Informações de Apoio

Como parte dos critérios comuns (CC) da certificação, o gerente das comunicações unificadas de Cisco adicionou Certificados ECDSA na versão 11.0. Isto afeta todo o Produtos do sistema operacional da Voz (VOS) tal como UCCX, SocialMiner, MediaSense, etc. da versão 11.5.

Mais detalhes sobre o **Digital Signature Algorithm elíptico da curva** podem ser encontrados aqui: https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767

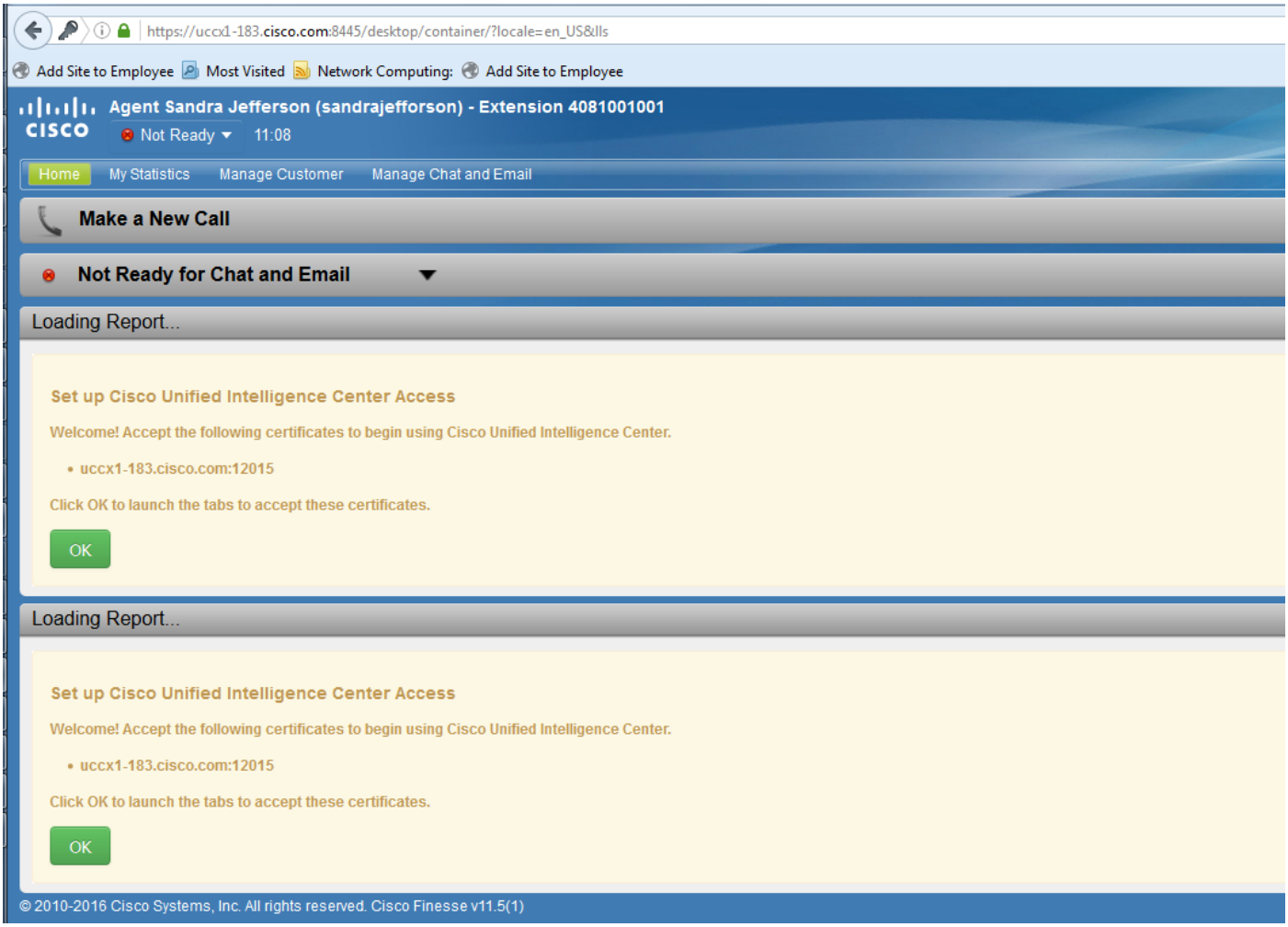
No que diz respeito à solução UCCX, quando você promove a 11.5, você é oferecido um certificado adicional que não esteja mais adiantado atual. Este é o certificado de Tomcat-ECDSA.

Isto foi documentado igualmente na comunicação da PRE-liberação: https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200651-UCCX-Version-11-5-Prerelease-Field-Commu.html?cachemode=refresh

Experiência do agente

Depois que uma elevação a 11.5, o agente pôde ser pedida para aceitar Certificados no desktop da fineza baseado sobre se o certificado auto-está assinado ou no Certificate Authority (CA) assinado.

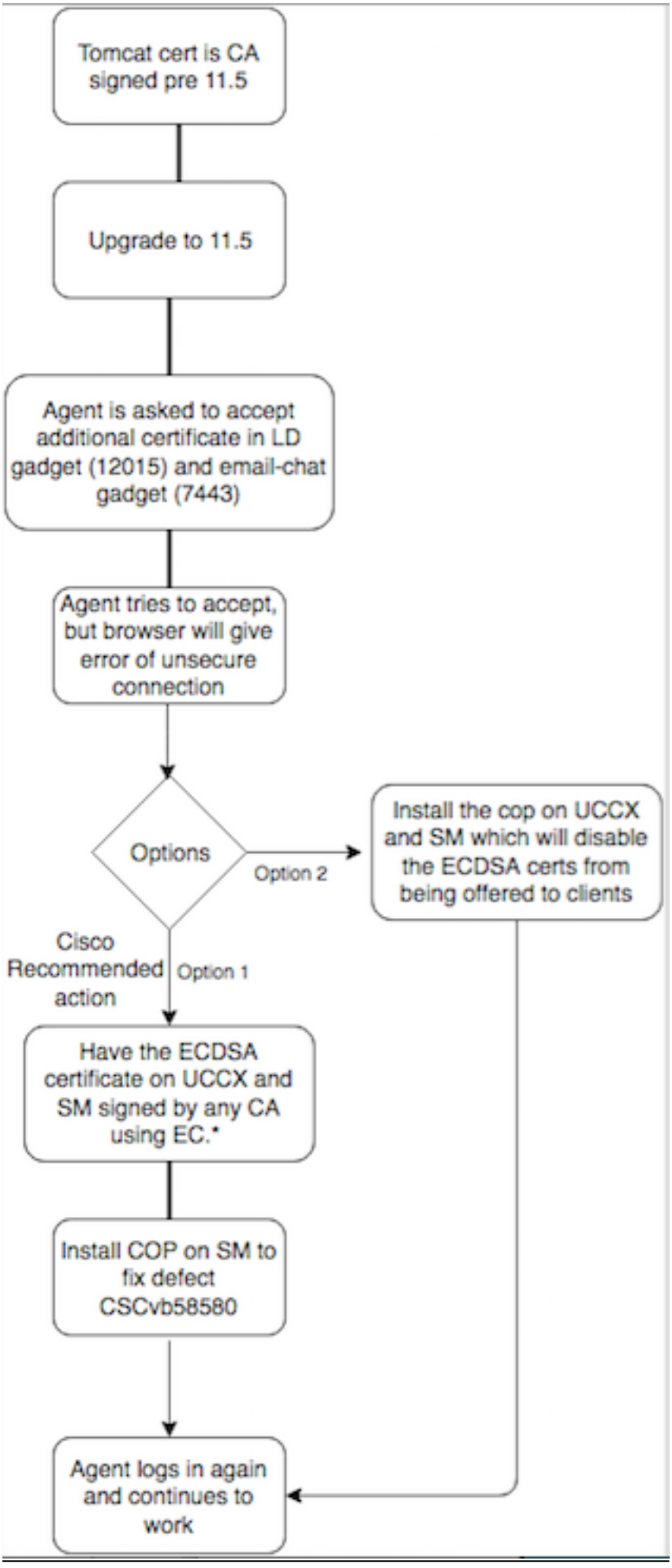
Elevação do cargo da experiência do usuário a 11.5



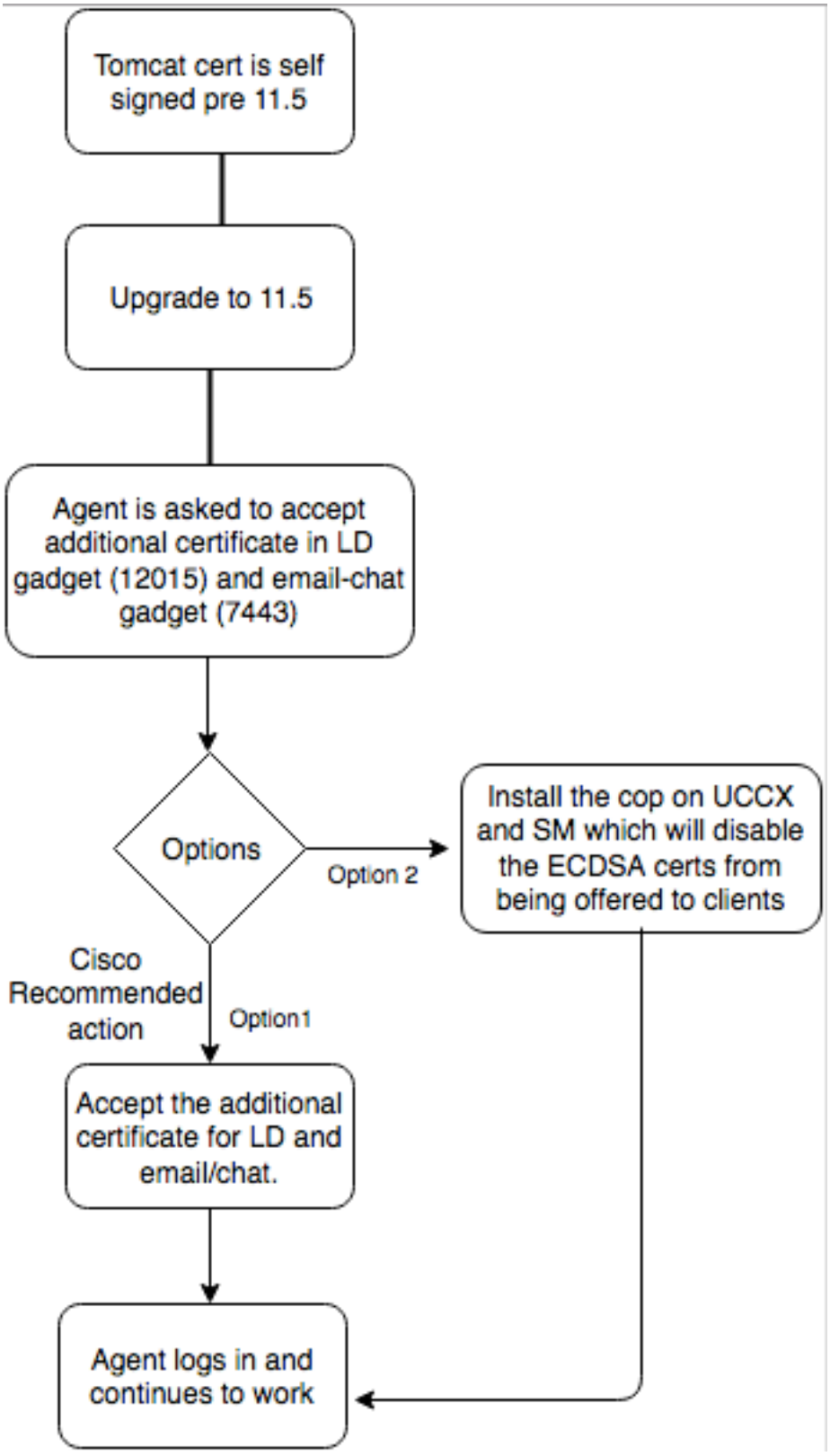
Isto é porque o desktop da fineza é oferecido agora um certificado ECDSA que não seja oferecido mais cedo.

Procedimento

PRE-elevação dos certificados assinados de CA


Tomcat cert is CA signed pre 11.5
Upgrade to 11.5
Agent is asked to accept additional certificate in LD gadget (12015) and email-chat gadget (7443)
Agent tries to accept, but browser will give error of unsecure connection
Options
Option 2
Install the cop on UCCX and SM which will disable the ECDSA certs from being offered to clients
Cisco Recommended action
Option 1
Have the ECDSA certificate on UCCX and SM signed by any CA using EC.*
Install COP on SM to fix defect CSCvb58580
Agent logs in again and continues to work

PRE-elevação dos certificados auto-assinados



Configurar

O melhor prática recomendado para este certificado

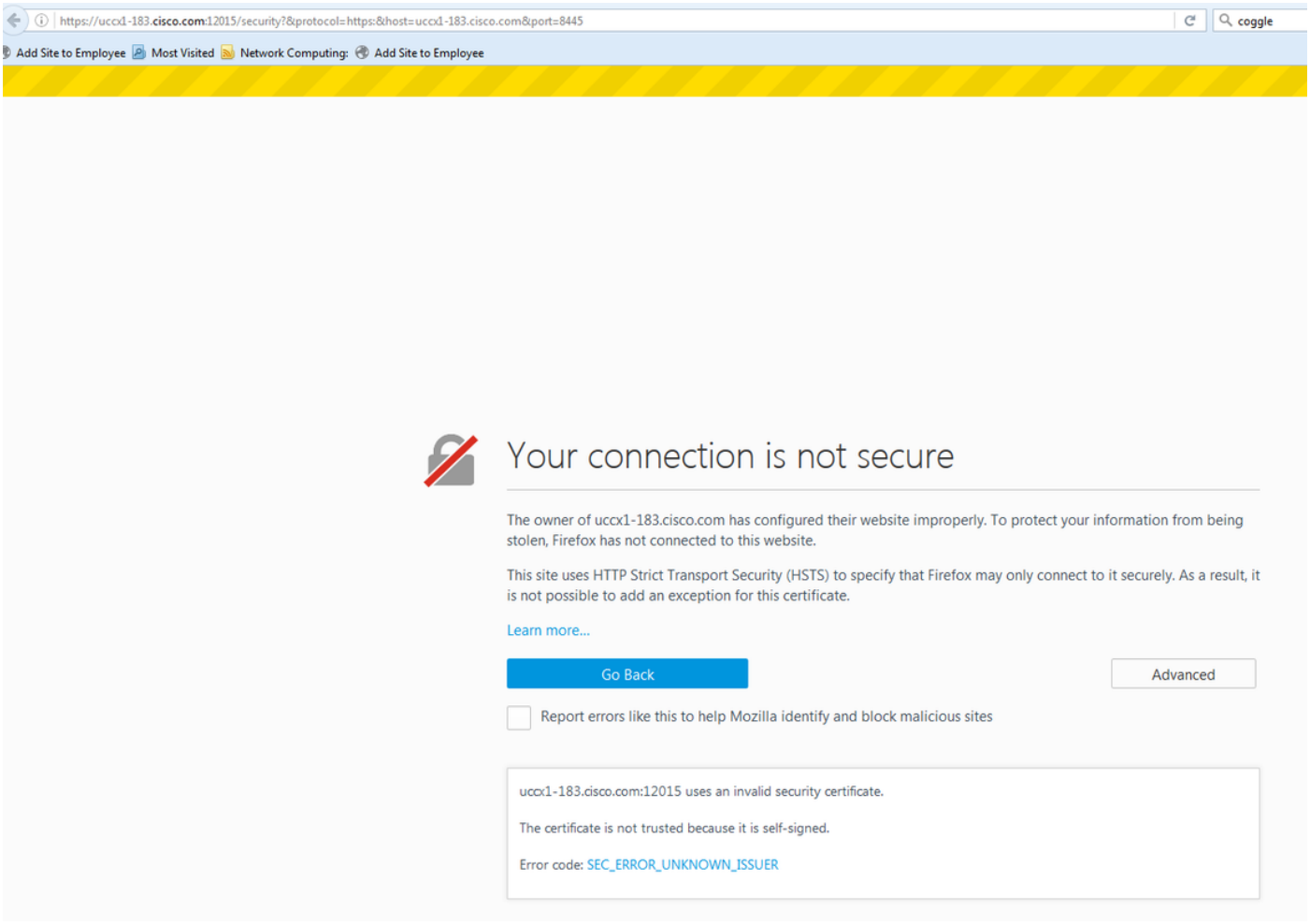
Certificados assinados para UCCX e SocialMiner

Se você usa certificados assinados de CA, este certificado ECDSA deve ser assinado por um Certificate Authority (CA) junto com outros Certificados

> **Note**: Se CA assina este certificado ECDSA com RSA, este certifictate não estaria apresentado ao cliente. Para a segurança avançada, os Certificados ECDSA oferecidos ao cliente são o melhor prática recomendado.

> **Note**: Se o certificado ECDSA em SocialMiner é assinado por CA com RSA, causa edições com email e bate-papo. Isto é documentado no defeito CSCvb58580 e um arquivo da bobina está disponível. Esta BOBINA assegura-se de que os Certificados ECDSA não estejam oferecidos aos clientes. Se você tem CA que é capaz assinar Certificados ECDSA com RSA somente, não use este certificado. Use a bobina de modo que o certificado ECDSA não seja oferecido e você tenha um ambiente RSA somente.

Se você usa certificados assinados de CA e depois que a elevação você não tem o certificado ECDSA assinado e transferido arquivos pela rede, os agentes experimentam uma mensagem para aceitar o certificado adicional. Quando clicam sobre a **APROVAÇÃO,** estão reorientados ao Web site. Contudo, esta falha devido à aplicação de Segurança do lado do navegador desde que o certificado ECDSA é auto assinado e seus outros Certificados da Web são CA assinaram. Esta comunicação é percebida como um risco securiry.



Termine estas etapas em cada nó da publisher e subscriber e do SocialMiner UCCX, após uma elevação a UCCX e a SocialMiner na versão 11.5:

1. Navegue à **página de administração do OS** e escolha o **> gerenciamento de certificado da**

Segurança.

2. O clique **gerencie o CSR**.

3. Da lista de drop-down da **lista do certificado**, escolha **Tomcat-ECDSA** como o nome do certificado e o clique **gerencie o CSR**.

4. Navegue ao **> gerenciamento de certificado da Segurança** e escolha a **transferência CSR**.

5. Da janela pop-up, escolha **Tomcat-ECDSA da** lista de drop-down e clique a **transferência CSR**.

Envie o CSR novo a CA da terceira ou assine-o com CA interno que assina Certificados EC. Isto produziria estes certificados assinados:

- Certificado de raiz para CA (se você usa mesmo CA para Certificados do aplicativo e Certificados EC, você pode saltar esta etapa)
- Certificado assinado do editor ECDSA UCCX
- Certificado assinado do subscritor ECDSA UCCX
- Certificado assinado de SocialMiner ECDSA

Note: Se você transfere arquivos pela rede os Certificados da raiz e do intermediário em um editor (UCCX), automaticamente replicated ao subscritor. Não há nenhuma necessidade de transferir arquivos pela rede os Certificados da raiz ou do intermediário nos outro, server do NON-editor na configuração se todos os Certificados do aplicativo são assinados através do mesmo certificate chain. Igualmente você pode saltar esta transferência de arquivo pela rede do certificado de raiz se mesmo CA assina o certificado EC e você tem feito já este quando você configurou os Certificados do aplicativo UCCX.

Termine estas etapas em cada server de aplicativo a fim transferir arquivos pela rede o certificado de raiz e o certificado EC aos Nós:

1. Navegue à **página de administração do OS** e escolha o **> gerenciamento de certificado da Segurança**.

2. Clique o **certificado da transferência de arquivo pela rede**.

3. Transfira arquivos pela rede o certificado de raiz e escolha a Tomcat-**confiança** como o tipo do certificado.

4. Clique o **arquivo da transferência de arquivo pela rede**.

5. Clique o **certificado da transferência de arquivo pela rede**.

6. Transfira arquivos pela rede o certificado do aplicativo e escolha **Tomcat-ECDSA** como o tipo do certificado.

7. Clique o **arquivo da transferência de arquivo pela rede**.

Note: Se CA subordinado assina o certificado, transfira arquivos pela rede o certificado de

raiz de CA subordinado como o certificado da Tomcat-*confiança* em vez do certificado de raiz. Se um certificado intermediário é emitido, transfira arquivos pela rede este certificado à loja da Tomcat-*confiança* além do que o certificado do aplicativo. Igualmente você pode saltar esta transferência de arquivo pela rede do certificado de raiz se mesmo CA assina o certificado EC e você tem feito já este quando você configurou Certificados do aplicativo UCCX.

8. Uma vez que completo, reinicie estes aplicativos:

   Cisco SocialMinerPublisher e subscriber de Cisco UCCX

Certificados auto-assinados para UCCX e SocialMiner

Se os certificados auto-assinados do uso UCCX ou de SocialMiner, os agentes precisam de ser recomendados para aceitar o aviso do certificado estão oferecidos no dispositivo do bate-papo-email e vivem dispositivos dos dados.

A fim instalar certificados auto-assinados na máquina cliente, use um gerente da política ou do pacote do grupo, ou instale-os individualmente no navegador de cada agente PC.

Para o internet explorer, instale os certificados auto-assinados do lado do cliente na loja das **Autoridades de certificação de raiz confiável**.

Para Mozilla Firefox, termine estas etapas:

1. Navegue às **ferramentas > às opções**.
2. Clique na guia Advanced.
3. Clique **Certificados da vista**.
4. Navegue à aba dos **server**.
5. O clique **adiciona a exceção**.

1. **Note**: Você pode igualmente adicionar a exceção da Segurança para instalar o certificado que é equivalente ao processo acima. Esta é uma configuração de uma vez no cliente.

Perguntas mais frequentes (FAQ)

Nós temos certificados assinados de CA, e queremo-los usar o certificado ECDSA que necessidades de ser assinado por um EC CA. Quando nós esperarmos o certificado assinado de CA para estar disponíveis, nós precisamos de ter dados vivos acima. O que eu posso fazer?

Nós não queremos assinar este certificado adicional ou mandar agentes aceitar este certificado adicional. O que eu posso fazer?

Embora a recomendação seja ter Certificados ECDSA apresentado aos navegadores, há uma

opção para desabilitá-lo. Você pode instalar um arquivo da bobina em UCCX e em SocialMiner que se assegura de que somente os Certificados RSA estejam apresentados ao cliente. O certificado ECDSA ainda permanece no keystore, mas não seria oferecido aos clientes.

Se eu uso esta bobina para desabilitar os Certificados ECDSA oferecidos aos clientes, posso eu permiti-la para trás?

Sim, há uma bobina do rollback fornecida. Uma vez que isso é aplicado, você pode obter este certificado assinado e uplaoded aos server.

Todos os Certificados seriam feitos a ECDSA?

Atualmente não, mas atualizações mais adicionais da Segurança na plataforma VOS no futuro.

Quando você instala a BOBINA UCCX?

- Quando você usar certificados auto-assinados e não quiser agentes aceitar Certificados adicionais
- Quando você não puder obter o certificado adicional assinado por CA

Quando você instala a BOBINA S?

- Quando você usar certificados auto-assinados e não quiser agentes aceitar Certificados adicionais
- Quando você não puder obter o certificado adicional assinado por CA
- Quando você tiver CA que é capaz assinar Certificados ECDSA com RSA somente

Que são os Certificados que são oferecidos por exemplos diferentes do servidor de Web à revelia?

Combinação/servidor de Web do certificado	Opte pela experiência do agente após a elevação 11.5 (sem alguma bobina)	UCCX Tomcat	UCCX Openfire (o serviço de notificação unificado Cisco CCX)	UCCX SocketIO	SocialMiner To
Tomcat assinado auto, auto assinou Tomcat-ECDSA	Os agentes seriam pedidos para aceitar o certificado no dispositivo vivo dos dados e no dispositivo do bate-papo-email	Auto-assinado	Auto-assinado	Auto-assinado	Auto-assinado
O RSA Tomcat assinado CA, RSA CA assinou Tomcat-ECDSA	Os agentes podem usar a fineza e dados vivos, mas o dispositivo do email-bate-papo não carregará e o Web page de SocialMiner não faz load.*	RSA	RSA	RSA	RSA
O RSA Tomcat assinado CA, EC CA assinou Tomcat-	Os agentes podem usar a fineza com ambos vivem dados	RSA	RSA	ECDSA	RSA

ECDSA	e chat-email*				
O RSA Tomcat assinado CA, auto assinou Tomcat-ECDSA	Os agentes seriam pedidos para aceitar o certificado adicional no dispositivo vivo dos dados e do email-bate-papo. Aceite o certificado do dispositivo vivo dos dados falha, aceitam o certificado do dispositivo do email-bate-papo seria successful.*	RSA	RSA	Auto-assinado (os agentes não podem aceitar devido à medida de Segurança reforçada navegador. Refira o tiro de tela acima. Você deve obter o certificado assinado por um EC CA ou instalar a bobina em UCCX para desabilitar os Certificados ECDSA oferecidos aos clientes.)	RSA

Informações Relacionadas

- BOBINA UCCX ECDSA - https://software.cisco.com/download/release.html?mdfid=286309734&softwareid=280840578&release=11.5(1)&flowid=80822
- BOBINA de SocialMiner ECDSA - https://software.cisco.com/download/release.html?mdfid=283613136&flowid=73189&release=11.5(1)&softwareid=283812550&sortparam=
- Informação do certificado UCCX - http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html