Gerenciar certificado de componentes PCCE para SPOG

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Nova interface de usuário - SPOG](#)
[Exportação de certificado SSL](#)
[Estação de trabalho de administração (AW)](#)
[Finesse](#)
[Cisco ECE](#)
[CUIC](#)
[IDs da Cisco](#)
[LiveData](#)
[VVB](#)
[Importação de certificado SSL para armazenamento de chaves](#)
[Servidor de Chamadas CVP e Servidor de Relatórios](#)
[Estação de Trabalho Administrativa](#)
[Finesse, CUIC, Cisco idS e VVB](#)
[Troca de certificado entre Finesse e CUIC/LiveData](#)

Introduction

Este documento descreve como trocar os certificados SSL autoassinados pela Estação de Trabalho Administrativa (AW) para o Portal de Voz do Cliente (CVP), Finesse, Cisco Enterprise Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (idS) e Virtualized Voice Browser (VVB) para Painel de Vidro Único do Package Contact Center Enterprise (PCCE) (SPOG).

Contribuído por Nagarajan Paramasivam e Robert Rogier, engenheiros do Cisco TAC.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Pacotes/Unified Contact Center Enterprises (PCCE/UCCE)
- Plataforma VOS
- Gerenciamento de Certificados

- Armazenamento de chaves de certificado

Componentes Utilizados

As informações neste documento são baseadas nestes componentes:

- Estação de trabalho administrativa (CCEADMIN/SPOG)
- CVP
- Finesse
- CUIC, IDS
- VVB
- Cisco ECE

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

Recomenda-se que você tenha lido e compreendido o Guia de Administração e Configuração do PCCE, especificamente o apêndice de Referência no final, que abrange a configuração e a configuração do certificado. Guia de administração e configuração do PCCE

Nova interface de usuário - SPOG

O Packaged CCE 12.0 tem uma nova interface de usuário que está de acordo com outras aplicações da central de contatos. A interface de usuário permite que você configure a solução por meio de um aplicativo. Entre no novo Unified CCE Administration em https://<IP Address>/cceadmin. <Endereço IP> é o endereço do AW do Side A ou B do Unified CCE ou do HDS externo opcional.

Nesta versão, a interface do Unified CCE Administration permite configurar:

- Campanhas
- Cortesia de retorno
- Grupos de servidores SIP
- Transferências de arquivo: A transferência de arquivos é possível somente através do AW principal (AW do lado A em 2000 implantação de agente e AW configurado em 4000 implantações de agente e 12000 implantações de agente).
- Padrões de roteamento: O padrão do número discado no Unified CVP Operations Console agora é chamado de Padrão de roteamento no Unified CCE Administration.
- Locais: No Unified CCE Administration, o código de roteamento agora é o prefixo do local em vez da ID do site.
- Configuração do dispositivo: O Unified CCE Administration permite configurar os seguintes dispositivos: CVP Server, CVP Reporting Server, VVB, Finesse, Identity Service (Configuração de login único).
- Recursos da equipe: O Unified CCE Administration permite definir e associar os seguintes recursos para equipes de agentes: Layout das variáveis de chamada, layout da área de trabalho, agendas telefônicas, fluxos de trabalho, motivos (Não pronto, encerrar sessão, finalizar).

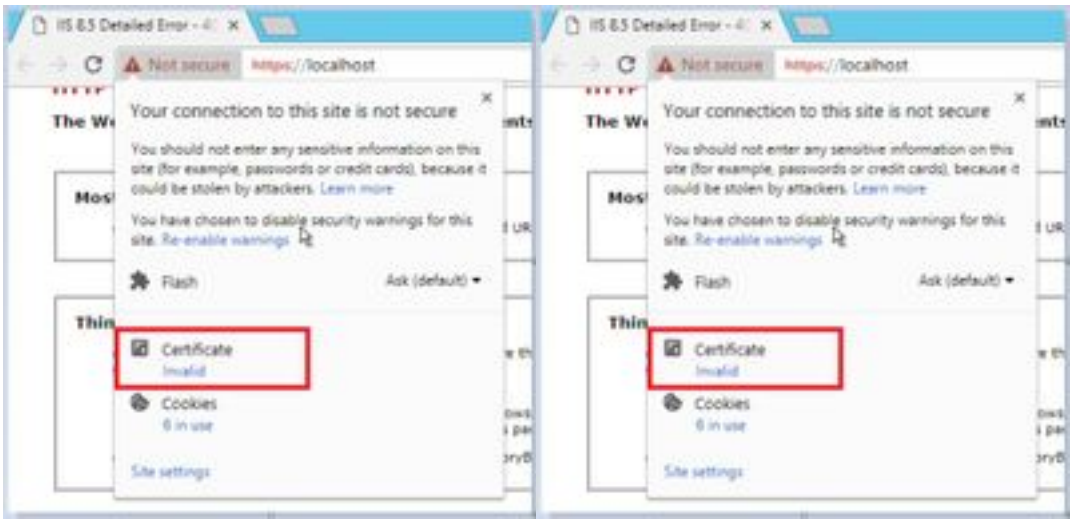
- E-mail e bate-papo

Antes de tentar gerenciar o sistema por meio do SPOG, é necessário trocar os certificados SSL entre o Customer Voice Portal (CVP), Finesse, Cisco Enterprice Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (idS) e Virtual Voice Browser (VVB) e Admin Workstation (AW) para estabelecer uma comunicação de confiança.

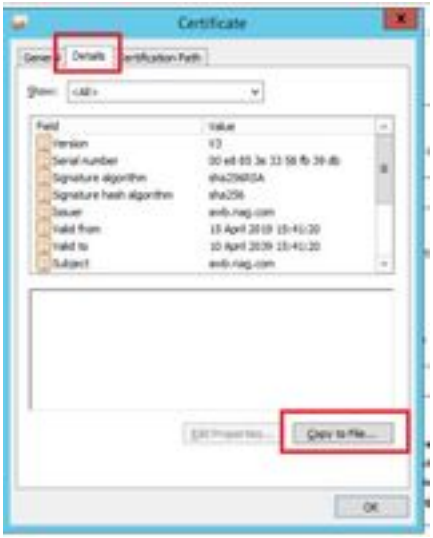
Exportação de certificado SSL

Estação de trabalho de administração (AW)

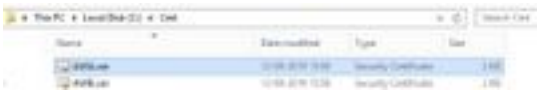
Etapa 1. Acesse o URL https://localhost no servidor AW e faça o download dos certificados SSL do servidor.



Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.

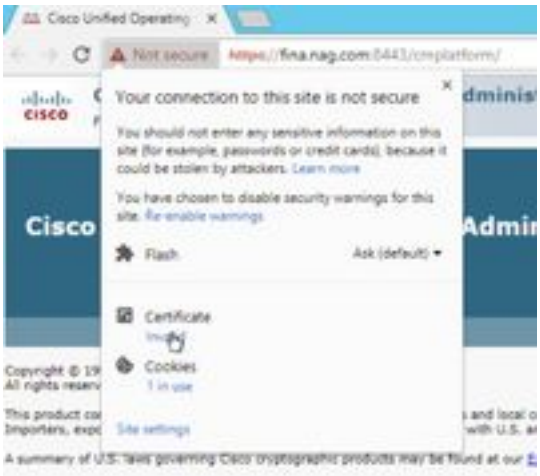


Etapa 3.Selecione X.509 (CER) codificado na base 64 e armazene o certificado no armazenamento local.



Finesse

Etapa 1. Acesse o https://Finesseserver:8443/cmplatform e baixe o certificado tomcat.

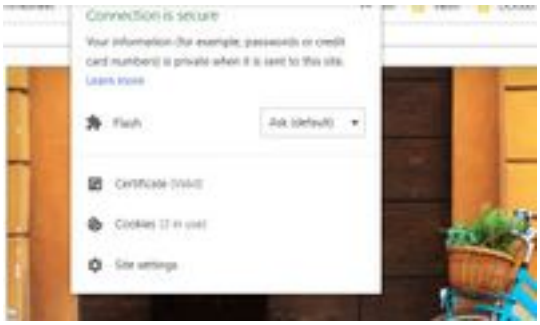


Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.

Etapa 3. Selecione X.509 (CER) codificado em Base 64 e armazene o certificado no armazenamento local.

Cisco ECE

Etapa 1. Acesse o https://ECEWebServer e baixe o certificado SSL do servidor.

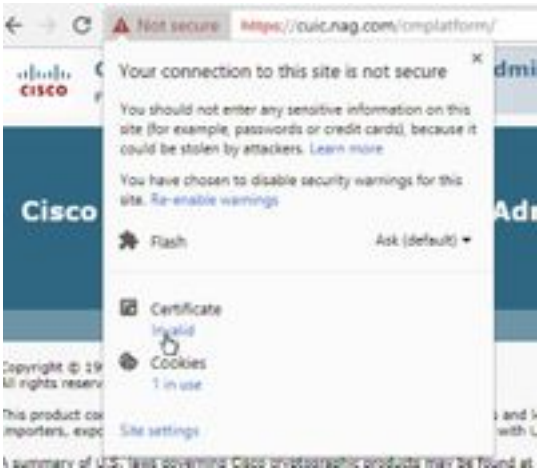


Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.

Etapa 3. Selecione X.509 (CER) codificado em Base 64 e armazene o certificado no armazenamento local.

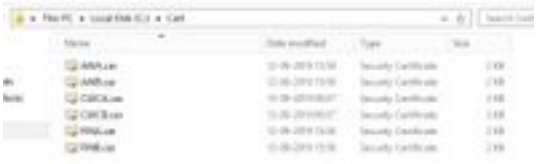
CUIC

Etapa 1. Acesse o https://CUICServer:8443/cmplatform e baixe o certificado tomcat.



Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.

Etapa 3. Selecione X.509 (CER) codificado em Base 64 e armazene o certificado no armazenamento local.

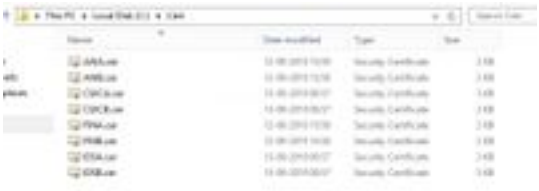


IDs da Cisco

Etapa 1. Acesse o https://IDSServer:8553/idsadmin/ e baixe o certificado tomcat.

Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.

Etapa 3. Selecione X.509 (CER) codificado em Base 64 e armazene o certificado no armazenamento local.

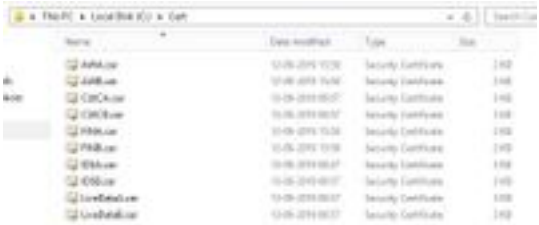


LiveData

Etapa 1. Acesse o https://LiveDataServer:8444/cuic/gadget/LiveData/ e baixe o certificado tomcat.

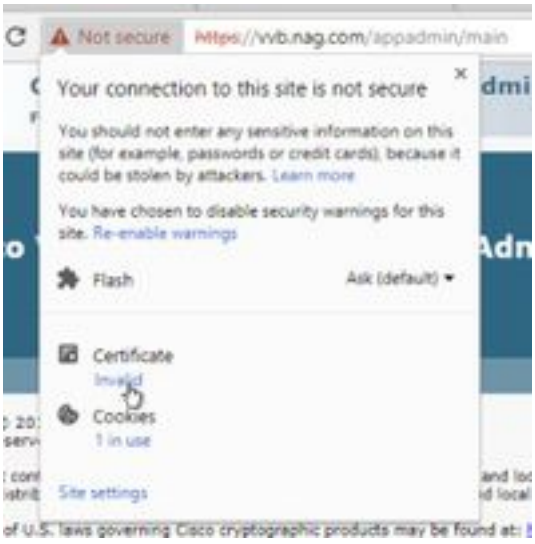
Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.

Etapa 3. Selecione X.509 (CER) codificado em Base 64 e armazene o certificado no armazenamento local.



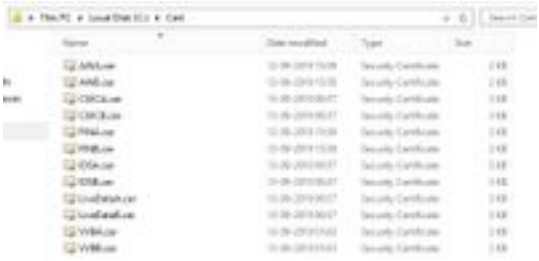
VVB

Etapa 1. Acesse o https://VVBServer/appadmin/main e baixe o certificado tomcat.



Etapa 2. Na janela de certificado, navegue até a guia Detalhes e clique no botão Copiar para arquivo.

Etapa 3. Selecione X.509 (CER) codificado em Base 64 e armazene o certificado no armazenamento local.



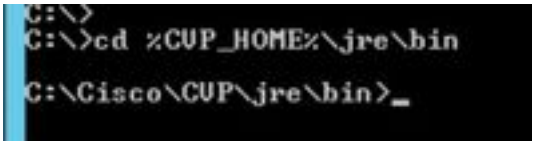
Importação de certificado SSL para armazenamento de chaves

Servidor de Chamadas CVP e Servidor de Relatórios

Etapa 1. Faça login no servidor CVP e copie os certificados AW CCE Admin para o **diretório C:\cisco\cvp\conf\security**.

Etapa 2. Navegue até **%CVP_HOME%\conf** e abra security.properties para copiar a senha do Keystore.

Etapa 3. Abra o prompt de comando como administrador e execute o comando **cd %CVP_HOME%\jre\bin**.



Etapa 4. Use este comando para importar os certificados AW para o servidor CVP.

keytool -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias awa.nag.com -file C:\Cisco\CVP\conf\security\AWA.cer

Etapa 5. No prompt de senha, cole a senha copiada de security.properties.

Etapa 6. Digite **yes** para confiar no certificado e garantir que o resultado **Certificado foi adicionado ao keystore.**

Passo 7. Há um aviso avisado junto com a importação bem-sucedida. Isso é devido ao formato proprietário Keystore, você pode ignorá-lo.

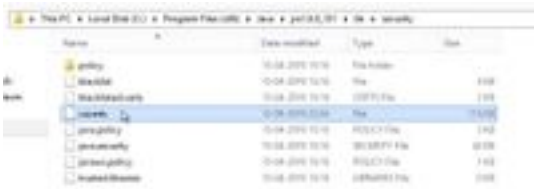
aviso:

O armazenamento de chaves JCEKS usa um formato proprietário. É recomendável migrar para PKCS12, que é um formato padrão do setor usando "keytool -import-srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore -deststoretype pkcs12".

Estação de Trabalho Administrativa

Etapa 1. Faça login no servidor AW e abra o prompt de comando como administrador.

Etapa 2. Navegue até C:\Program Files(x86)\Java\jre1.8.0_181\lib\security and ensure the cacerts file exist.



Etapa 3. Digite o comando **cd %JAVA_HOME%** e digite.

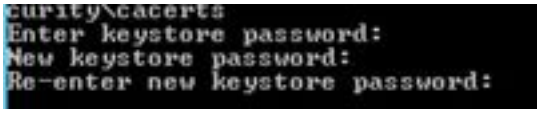
Etapa 4. Use este comando para importar os certificados Finesse para o servidor AW.

keytool -import -file C:\Users\Administrator.NAG\Downloads\Cert\FINA.cer -alias fina.nag.com-

keystore .\lib\security\cacerts

Etapa 5. Na primeira vez que utilizar esta ferramenta de chave, utilize a **alteração de** senha para alterar a senha de um arquivo de certificados.

Etapa 6. Insira uma nova senha para o Keystore e insira novamente para confirmar a senha.



Passo 7. Digite **yes** para confiar no certificado e garantir que você obtenha o resultado **Certificado adicionado ao keystore.**

Note: As etapas 1 a 7 devem ser repetidas com todos os outros nós Finesse e todos os nós CUIC também

Etapa 8. Se a senha do keystore tiver sido inserida incorretamente ou executado sem redefinir, é esperado que ela obtenha essa exceção.

Confiar neste certificado? [não]: sim

O certificado foi adicionado ao keystore

erro de ferramenta de chave: java.io.FileNotFoundException: .\lib\security\cacerts (O sistema não consegue encontrar o caminho especificado)

Digite a senha do armazenamento de chaves:
erro de ferramenta de chave: java.io.IOExceção: Keystore foi violado ou a senha estava incorreta

Etapa 9. Para alterar a senha do armazenamento de chaves, use esse comando e reinicie o procedimento novamente da Etapa 4 com a nova senha.

keytool -storepasswd -keystore .\lib\security\cacerts

Etapa 10. Após a importação bem-sucedida, use este comando para exibir o certificado do keystore.

keytool -list -keystore .\lib\security\cacerts -alias fina.nag.com

keytool -list -keystore .\lib\security\cacerts -alias cuic.nag.com

Finesse, CUIC, Cisco idS e VVB

Etapa 1. Faça login na página de administração do SO do servidor Finesse e carregue os certificados SSL AW na confiança tomcat.

Etapa 2. Navegue até **OS Administration > Security > Certificate Management.**

Etapa 3. Clique em Carregar certificado\cadeia de certificados e selecione o tomcat-trust no menu suspenso.

Etapa 4. Navegue pelo armazenamento de certificados no armazenamento local e clique no botão Carregar.

Etapa 5. Repita as etapas para carregar todo o certificado do servidor AW para o cluster Finesse.

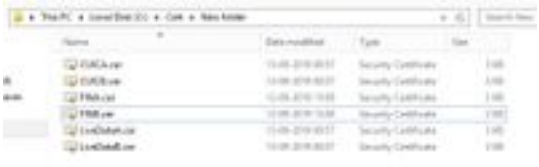
Note: Não é necessário carregar o certificado tomcat-trust para o nó secundário, isso é replicado automaticamente.

Etapa 6. Reinicie o serviço tomcat para que as alterações de certificado entrem em vigor.

Passo 7. No CUIC, IDS e VVB, siga as etapas de 2 a 4 e carregue o certificado AW.

Troca de certificado entre Finesse e CUIC/LiveData

Etapa 1. Mantenha os certificados Finesse, CUIC e LiveData em uma pasta separada.



Etapa 2. Faça login na página Finesse, CUIC e LiveData OS Administration.

Etapa 3. Navegue até **OS Administration > Security > Certificate Management.**

Etapa 4. Clique em Carregar certificado\cadeia de certificados e selecione o tomcat-trust no menu

suspenso.

Etapa 5. Navegue pelo armazenamento de certificados no armazenamento local e selecione Certificado de servidor como abaixo e clique no botão Carregar.

No servidor Finesse - CUIC e LiveData como confiabilidade Tomcat

No servidor CUIC - Finesse e LiveData como confiança tomcat

No LiveData Server - CUIC e Finesse como confiabilidade Tomcat

> Note: Não é necessário carregar o certificado tomcat-trust para o nó secundário, isso é replicado automaticamente.

Etapa 6. Reinicie o serviço tomcat em cada nó para que as alterações de certificado entrem em vigor.