Trocar certificados com a ferramenta Carregador do Contact Center

Contents

Introdução

Este documento descreve a ferramenta Carregador do Contact Center que obtém e carrega certificados na solução Unified Contact Center Enterprise (UCCE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- UCCE versão 12.6(1)
- Customer Voice Portal (CVP) versão 12.6(1)
- E-mail e bate-papo corporativo (ECE) versão 12.6(1)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- UCCE 12.6(1)
- CVP 12.6(1)
- ECE 12.6(1)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Na solução UCCE/PCCE da versão 12.x, todos os dispositivos são controlados por meio do SPOG (Single Pane of Glass, painel único de controle), que é hospedado no servidor AW (Admin Workstation, estação de trabalho administrativa) principal. Devido à conformidade de gerenciamento de segurança (SRC) nas versões PCCE 12.X, toda a comunicação entre o SPOG e outros servidores na solução é feita estritamente através do protocolo HTTP seguro.

Os certificados são usados a fim de obter uma comunicação segura transparente entre o SPOG e os outros dispositivos. Em um ambiente de certificado autoassinado, a troca de certificados entre os servidores torna-se obrigatória. Essa troca de certificado também é necessária para habilitar novos recursos presentes nas versões 12.5 e 12.6, como Smart Licensing, Webex Experience Management (WXM) e Customer Virtual Assistant (CVA).

Problema

A troca de certificados pode ser uma tarefa difícil para pessoas que não estão familiarizadas com o java`keytool`especialmente quando os certificados de autoatendimento são usados.

Ações incorretas podem causar problemas com a configuração da solução e sua integridade.

Os certificados podem expirar e renová-los é outro desafio.

Solução

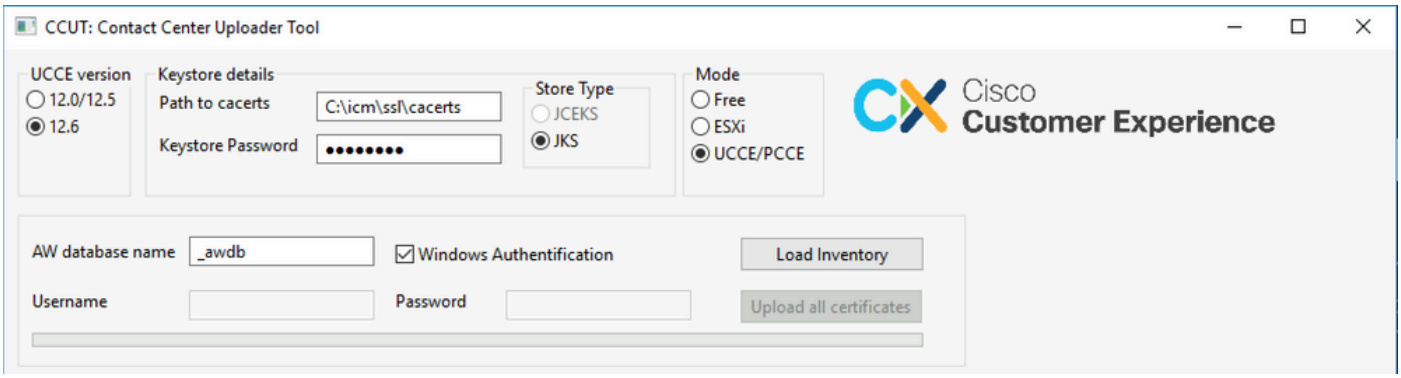
O artigo contém um link para a ferramenta Carregador do Contact Center (CCUT), escrita em Java, que ajuda você com a tarefa.

A ferramenta pode se conectar ao banco de dados UCCE ou ao host ESXi, obtém os dados sobre todos os hosts de lá, obtém um certificado de cada host e o carrega no armazenamento de confiança cacerts de java.

Observação: a ferramenta é criada pelos engenheiros do Cisco TAC e não há suporte oficial. Você pode usar ccut@cisco.com para comentários, perguntas e problemas.

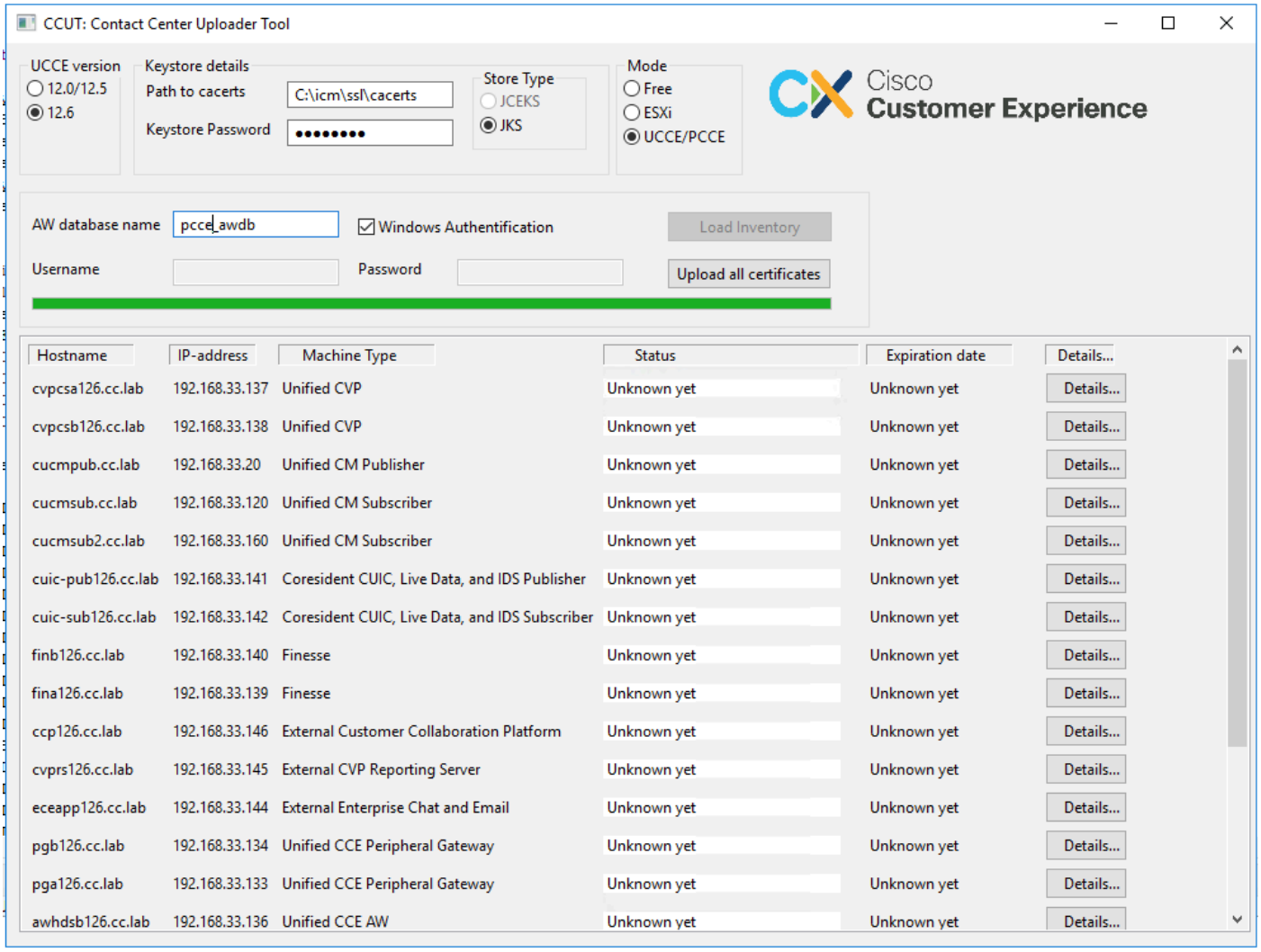
Modo UCCE/PCCE

A janela principal do aplicativo da ferramenta no modo UCCE/PCCE está na figura:



- **AW database name:** forneça o nome do banco de dados AW, Logger ou pcceinventory. Deve haver dados nas tabelas t_Machine....
  Se a ferramenta for executada no host UCCE em que o componente de banco de dados não está instalado, o nome do servidor SQL (Structured Query Language) remoto poderá ser adicionado como um prefixo ao nome do banco de dados.
  Por exemplo AWHDS-A\pcce_awdb
  Isso se aplica a computadores Gateway Periférico (PG) ou ROTEADOR.
- **Username** e **Password** para o usuário SQL com direito de acesso para ler os dados do banco de dados. Marque a caixa **Windows Authentification** para usar a autenticação integrada do Windows em vez do SQL.
- **UCCE version:** o patch do arquivo cacerts depende da versão instalada do UCCE.
- **Path to cacerts:** Local do arquivo cacerts. No UCCE 12.6.X, o sistema usa C:\icm\ssl\cacerts, o UCCE 12.5 usa o armazenamento confiável Java padrão (%CCE_JAVA_HOME%\lib\security\cacert).
- **Keystore Password:** a senha padrão para o armazenamento cacerts é changeit.
- **Store Type:** O UCCE usa o tipo JKS da loja, enquanto o CVP usa JCEKS.
- **Load Inventory** botão: A ferramenta se conecta ao banco de dados mencionado e mostra os dados do inventário.
- **Upload all certificates** botão: O botão fica disponível depois que a ferramenta obtém os dados do banco de dados.

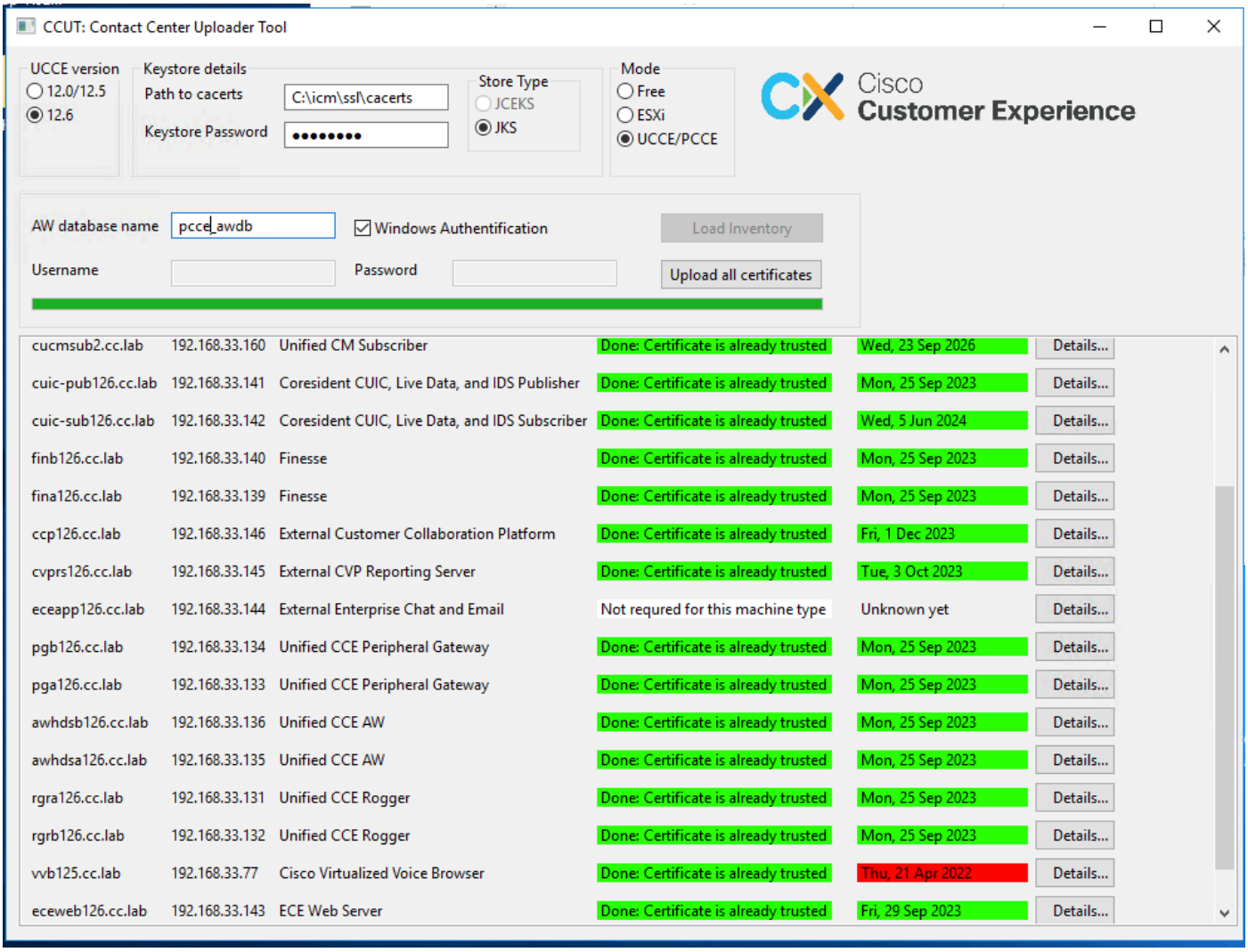
Exemplo dos dados carregados na imagem:



Os dados de inventário consistem em 6 colunas:

- Hostname
- Endereço IP
- Tipo de máquina
- Status dos dados do certificado ou detalhes do erro
- Data de vencimento do certificado
- Detalhes

Os resultados do botão Upload all Certificates:



Cada linha marcada como verde é um sucesso.

A linha vermelha ou amarela requer atenção.

Modo ESXi

O modo ESXi pode ser usado para a instalação do PCCE/UCCE quando o Inventário ainda não estiver configurado e as tabelas t_Machine... não contiverem dados.

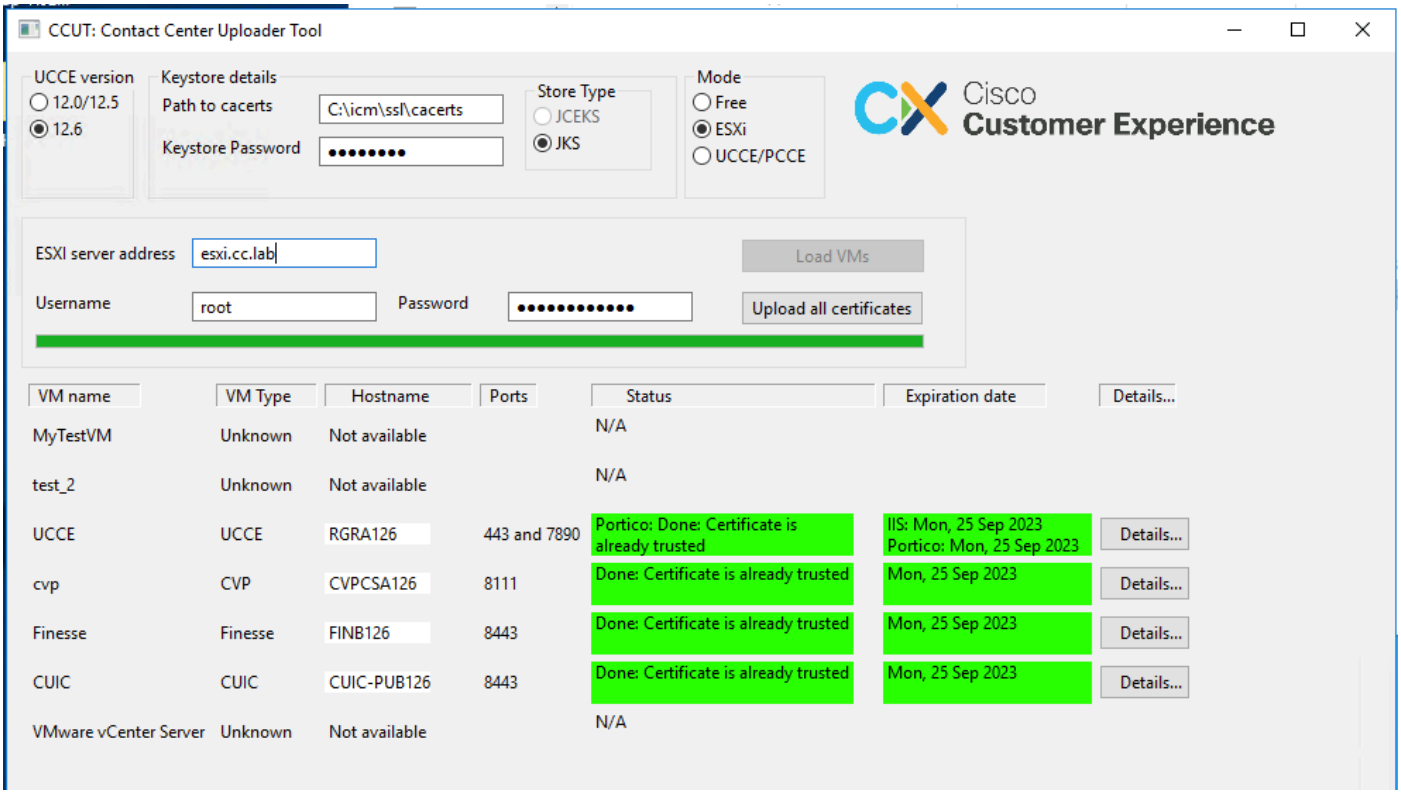
A ferramenta se conecta ao host ESXi e obtém os dados sobre todas as máquinas virtuais a partir daí.

Ele solicita o nome da máquina virtual (VM), as anotações da VM e o nome do host do sistema operacional convidado.

As anotações da VM são usadas para identificar o tipo de máquina.

As ferramentas VmWare devem ser executadas em VMs; caso contrário, o nome do host não será preenchido.

A ferramenta no modo ESXi está na figura:



Observação: VCenter não é suportado para conexões.

Modo livre

Outro modo da ferramenta é o modo Livre.

Não há nenhum requisito para ter o banco de dados UCCE disponível e a ferramenta pode ser usada para carregar qualquer certificado para CVP ou ECE.

Exemplos de casos de uso:

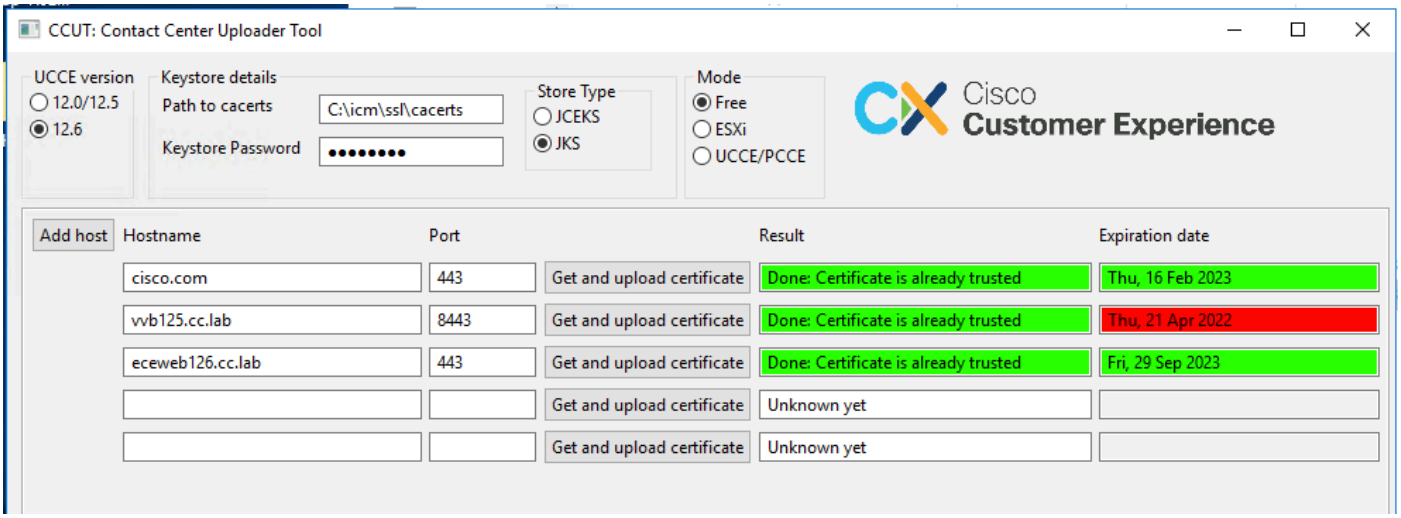
- Obtenha e carregue o certificado de serviço da Web de terceiros no CVP.

- Obter e carregar certificados de servidores de email para o servidor de serviços ECE.

- Obter e carregar certificados do Sistema de Detecção de Intrusão (IDS) para o servidor de aplicativos ECE.

Observação: a ferramenta não pode carregar certificados para o arquivo CVP .keystore devido a algumas restrições.

Um exemplo da ferramenta no modo Free está na figura:



Executar a ferramenta

Baixe a ferramenta Carregador do Contact Center.

Extraia o arquivo morto baixado.

O arquivo Launcher contém caminhos para o jar e Java.

Atualize o caminho para Java e para o arquivo jar, se necessário.

Abra o prompt de comando (cmd) com permissões de Administrador.

Vá para a pasta extraída pelo comando cd e execute o LauncherX86.bat para iniciar a ferramenta.

⚠ Cuidado: sempre fazer um backup do arquivo de repositório de confiança.

Detalhes técnicos

- A ferramenta se conecta ao host e verifica se o certificado é confiável ou não. Se não for confiável, o certificado será carregado.
- O certificado é carregado com o alias util-[nome do host]-[porta], por exemplo util-vvb125.cc.lab-8443.
- Um host pode enviar mais de um certificado. Nesse caso, a ferramenta carrega todos esses certificados como prefixos raiz e/ou intermediários.
- A ferramenta é compilada com java 1.8.
- A ferramenta se conecta ao banco de dados por localhost:1433 por padrão.
- A resolução mínima de tela é 1024x768. Não há suporte para o modo dimensionado.

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.