Contenido

Introducción

Muchos administradores de la red eligen implementar el Cisco Unified Communications Manager Express (CME) con la Seguridad. En vez del Certificate Authority IOS del accesorio (IOS-CA), los administradores de la red pueden elegir integrar el CME seguro con su infraestructura existente del Public Key Infrastructure (PKI). Este documento describe cómo configurar el CME seguro para actuar con asegura la señalización, y los media, vía los Certificados de las de otras compañías.

Prerrequisitos

Requisitos

Este documento asume que el Cisco Unified Communications Manager Express (CME) en su entorno se está ejecutando y completamente - funcional. Todos los teléfonos que deben ser operativos en Cisco seguro unificaron la necesidad CME de poder primero registrarse con éxito al CME. Refiera a la guía de administrador de sistema del Cisco Unified Communications Manager Express para la información sobre cómo configurar el CME.

Este documento también asume que la Voz y las funciones de seguridad están habilitadas.

Componentes Utilizados

La información en este documento se basa en el Cisco Unified Communications Manager Express (CME).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener información sobre las convenciones sobre documentos.

Configurar

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Pasos para la configuración sumarios

1. Cree el caso IOS-CA.
2. Cree el trustpoints para sostener los Certificados de CA de las de otras compañías.
3. Genere los pedidos de firma de certificado (CSR) del trustpoints.
4. Firme los CSR con el uso de la autenticación de servidor, y obtenga la certificación de CA.
5. Autentique el trustpoints con el certificado de CA, e importe los certificados de identidad respectivos.
6. Valide el trustpoints del certificado de las de otras compañías.
7. Cree el trustpoint IOS CA CME.
8. Configure Certificate Trust List (Lista de confianza del certificado) al cliente (CTL).
9. Configure el servidor de la función de proxy del Certificate Authority (CAPF).
10. Configure el servicio de telefonía.
11. Configure el teléfono de prueba.
12. Verifique.

Ejemplo de la configuración detallada

1. Cree el caso IOS-CA. El caso IOS-CA presenta el certificado autofirmado que se utiliza para firmar el teléfono localmente - el certificado significativo (LSC).
2. Cree el trustpoints que generará los CSR para la firma de las de otras compañías. Este trustpoints sostiene eventual el certificado de CA de las de otras compañías, así como los certificados de identidad, que son un resultado de los CSR.

3. Genere los CSR del trustpoints. **El pki crypto alista el** comando produce el CSR que se proporciona a las de otras compañías CA para firmar.

   Ejemplo 1:
   Ejemplo 2:
4. Utilice los dos CSR para generar los Certificados con los permisos de la autenticación de servidor.
   Notas: Es esencial que la Cadena de certificados llena está obtenida para uno de los dos Certificados de CA. La Cadena de certificados proporciona CA y el certificado de identidad de CA de firma.Asegúrese de que los Certificados estén descargados en el formato del base 64.Es muy importante que el certificado de CA está utilizado para la autenticación para cada

trustpoint y que los certificados de identidad están importados en cada trustpoint, en esa orden.

5. Autentique el trustpoints con los Certificados de CA, e importe los certificados de identidad SAST.

   Ejemplo 1:

   Ejemplo 2:

6. Una vez que CA y los certificados de identidad se cargan en el trustpoints respectivo, valide la Cadena de certificados para cada trustpoint. Este paso se asegura de que los pasos anteriores fueran completados con éxito.

7. Cree el trustpoint IOS CA CME.

   Porque el trustpoint IOS-CA no se puede utilizar para la autenticación de cliente (conexión llana de la Seguridad del transporte (TLS) con los teléfonos), usted debe crear otro trustpoint y poner el certificado IOS-CA en él.

   Este trustpoint se utiliza para autorizar solamente el pedido del teléfono del IP una conexión TLS (así que los puede registrarse correctamente).

8. Configure al cliente CTL.

   Nota: Asegúrese de que el archivo CTL fuera creado con éxito:

9. Configure el servidor del CAPF.

10. Configure el servicio de telefonía.

11. Configure el teléfono de prueba (ephone) para actualizar su certificado y utilizar el modo cifrado. Una vez que la configuración es completa, reajuste el teléfono y espérelo para registrarse.

    Nota: Antes de que se reajuste el teléfono, asegúrese de que no haya presente de la Configuración de seguridad ya. Si una Configuración de seguridad está presente, debe ser quitada o completar manualmente una restauración de la fábrica del teléfono de prueba antes del registro para asegurar el CME unificado Cisco.

    Para reajustar el teléfono, ejecute estos comandos:Una vez que el teléfono ha recibido el LSC actualizado, se quita el comando de la **cadena nula de la actualización auténtico-MODE de la CERT-operación**.

12. Verifique que el teléfono se haya registrado con la autenticación y el cifrado.

Asegure el CME unificado Cisco debe ser completamente - funcional con los Certificados de las de otras compañías.

Información Relacionada

- Guía de Administrador de Sistema de Cisco Unified Communications Manager Express
- Asegure la Voz en el TAC de Cisco Wiki
- Soporte Técnico y Documentación - Cisco Systems