Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Problema - Incapaz de aplicar los certificados firmados usando el procedimiento en la guía.](#)
[Solución - El procedimiento a manejar/implementa los certificados firmados para el CVP 8.5](#)
[Información Relacionada](#)

Introducción

Este documento explica cómo manejar el certificado autofirmado con el certificado firmado en el sistema de archivos para el Cisco Unified Customer Voice Portal (CVP) 8.5(1) para manejar los contenidos del archivo .keystore.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el CVP unificado Cisco 8.5.

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 TécnicosCisco para obtener más información sobre las convenciones del documento.

Problema - Incapaz de aplicar los certificados firmados usando el procedimiento en la guía.

El procedimiento documentado de substituir el certificado autofirmado por el certificado firmado en el sistema de archivos se aplica no más:

Solución - El procedimiento a manejar/implementa los certificados firmados para el CVP 8.5

Para manejar los Certificados en el CVP 8.5(1), usted necesita manejar los contenidos del archivo .keystore.

Complete estos pasos:

1. Abra el `archivo del %CVP_HOME% \ conf \ security.properties` para extraer la contraseña .keystore. Usted necesitará navegar hasta el %CVP_HOME% `a través del` directorio de instalación de la blanco para el CVP unificado (por abandono éste es C:\Cisco\CVP).
2. El archivo de propiedades debe contener una propiedad: Security.keystorePW.
3. Para manejar el keystore, después de que usted ingrese un comando, el keytool pedirá usted ingresar la contraseña del keystore. Copie el valor de la propiedad Security.keystorePW, y pegúelo en la ventana de la línea de comandos para ingresar su contraseña del keystore.Por ejemplo, considere el archivo del %CVP_HOME% \ conf \ security.properties contiene la línea de propiedad:La contraseña a copiar sería `[3X}}E7@nhMXGy{ou.5AL!+4Ffm868.`
4. Cree un respaldo del %CVP_HOME% \ conf \ directorio de la Seguridad.
5. Abra una ventana del intérprete de comandos, y cambie al directorio de Configuración de seguridad:
6. Utilice la entrada de clave privada para el vxml_certificate, para crear el pedido de firma de certificado, recordando ingresar la contraseña del keystore cuando está indicado. Un nuevo archivo csr será creado en el sistema de archivos:
7. Dé el archivo del pedido de firma de certificado (vxml_certificate.csr) a un Certificate Authority de confianza. Firmarán, devolviendo uno o más certificados confiables.
8. Importe el archivo de certificado firmado (por ejemplo, signed_vxml.crt) de su Certificate Authority de confianza. Los Certificados se deben importar en la orden de la jerarquía encadenada (raíz, intermedio, certificado firmado).

Nota: Esto se documenta en el Id. de bug Cisco CSCts21084 (clientes registrados solamente).

Información Relacionada

- Guías de configuración del Cisco Unified Customer Voice Portal
- Soporte Técnico y Documentación - Cisco Systems