

HP Universal CMDB

Para los sistemas operativos Windows y Red Hat Enterprise

Versión de software: 10.00

HP Universal CMDB y Configuration Manager - Guía del sistema de protección

Fecha de publicación del documento: Junio de 2012

Fecha de lanzamiento del software: Junio de 2012



Avisos legales

Garantía

Las únicas garantías de los productos y servicios HP se exponen en el certificado de garantía que acompaña a dichos productos y servicios. El presente documento no debe interpretarse como una garantía adicional. HP no es responsable de omisiones, errores técnicos o de edición contenidos en el presente documento.

La información contenida en esta página está sujeta a cambios sin previo aviso.

Leyenda de derechos limitados

Software informático confidencial. Es necesario disponer de una licencia válida de HP para su posesión, uso o copia. De conformidad con FAR 12.211 y 12.212, el Gobierno estadounidense dispone de licencia de software informático de uso comercial, documentación del software informático e información técnica para elementos de uso comercial con arreglo a la licencia estándar para uso comercial del proveedor.

Aviso de copyright

© Copyright 2002 - 2012 Hewlett-Packard Development Company, L.P.

Avisos de marcas comerciales

Adobe™ es una marca comercial de Adobe Systems Incorporated.

Microsoft® y Windows® son marcas comerciales registradas estadounidenses de Microsoft Corporation.

UNIX® es una marca comercial registrada de The Open Group.

Actualizaciones de la documentación

La página de título de este documento contiene la siguiente información de identificación:

- Número de versión del software, que indica la versión del software.
- Fecha de publicación del documento, que cambia cada vez que se actualiza el documento.
- Fecha de lanzamiento del software, que indica la fecha desde la que está disponible esta versión del software.

Para buscar actualizaciones recientes o verificar que está utilizando la edición más reciente de un documento, visite:

<http://h20230.www2.hp.com/selfsolve/manuals>

Este sitio requiere que esté registrado como usuario de HP Passport. Para registrarse y obtener un ID de HP Passport, visite:

<http://h20229.www2.hp.com/passport-registration.html>

O haga clic en el enlace **New user registration** (Registro de nuevos usuarios) de la página de registro de HP Passport.

Asimismo, recibirá ediciones actualizadas o nuevas si se suscribe al servicio de soporte del producto correspondiente. Póngase en contacto con su representante de ventas de HP para obtener más información.

Soporte

Visite el sitio web HP Software Support Online en:

<http://www.hp.com/go/hpsoftwaresupport>

Este sitio web proporciona información de contacto y detalles sobre los productos, servicios y soporte que ofrece HP Software.

HP Software Support Online brinda a los clientes la posibilidad de auto-resolución de problemas. Ofrece una forma rápida y eficaz de acceder a las herramientas de soporte técnico interactivo necesarias para gestionar su negocio. Como cliente preferente de soporte, puede beneficiarse de utilizar el sitio web de soporte para:

- Buscar los documentos de la Base de conocimiento que le interesen
- Enviar y realizar un seguimiento de los casos de soporte y las solicitudes de mejora
- Descargar revisiones de software
- Gestionar contratos de soporte
- Buscar contactos de soporte de HP
- Consultar la información sobre los servicios disponibles
- Participar en debates con otros clientes de software
- Investigar sobre formación de software y registrarse para recibirla

Para acceder a la mayor parte de las áreas de soporte es necesario que se registre como usuario de HP Passport. En muchos casos también será necesario disponer de un contrato de soporte. Para registrarse y obtener un ID de HP Passport, visite:

<http://h20229.www2.hp.com/passport-registration.html>

Para obtener más información sobre los niveles de acceso, visite:

http://h20230.www2.hp.com/new_access_levels.jsp

Contenido

HP Universal CMDB y Configuration Manager - Guía del sistema de protección	1
Contenido	5
Introducción al sistema de protección	9
Información general del sistema de protección	9
Preparativos del sistema de protección	10
Implementar UCMDDB en una arquitectura segura	10
Acceso al sistema	11
Sistema de protección de acceso a Java JMX	11
Cambio del nombre de usuario o la contraseña del sistema en la consola JMX	13
Cambio del usuario del servicio del servidor de HP Universal CMDB	14
Cifrar la contraseña de la base de datos para Configuration Manager	15
Parámetros para el cifrado de la contraseña de la base de datos de Configuration Manager	16
Habilitar la comunicación de Capa de sockets seguros (SSL)	18
Habilitar SSL en el equipo servidor con un certificado autofirmado - UCMDDB	18
Habilitar SSL en el equipo servidor con un certificado autofirmado - Configuration Manager	20
Habilitar SSL en el equipo servidor con un certificado de una entidad de certificación - UCMDDB	21
Habilitar SSL en el equipo servidor con un certificado de una entidad de certificación - Configuration Manager	23
Habilitar SSL en los equipos cliente - UCMDDB	24
Habilitar SSL con un certificado de cliente - Configuration Manager	25
Habilitar SSL en el SDK del cliente	25
Habilitar la autenticación de certificados manual en el SDK	26
Cambiar la contraseñas del almacén de claves del servidor	27
Habilitar o deshabilitar puertos HTTP/HTTPS	28
Asignar los componentes web de UCMDDB a los puertos	29
Configurar Configuration Manager para que funcione con UCMDDB mediante SSL	31

Habilitar el adaptador KPI de UCMDDB para su uso con SSL	31
Configuración de la compatibilidad con SSL para el navegador de UCMDDB	32
Utilización de un proxy inverso	34
Información general del proxy inverso	34
Aspectos de seguridad de la utilización de un servidor proxy inverso	35
Configuración de un proxy inverso	36
Conexión de la sonda de Data Flow por proxy inverso o equilibrador de carga mediante autenticación mutua	39
administrar credenciales de Data Flow	43
Información general de la administración de credenciales de Data Flow	44
Suposiciones básicas de seguridad	45
Ejecución de la sonda de Data Flow en modo independiente	45
Mantener la caché de credenciales actualizada	46
Sincronización de todas las sondas con cambios de configuración	46
Almacenamiento protegido en la sonda	47
Visualización de información de credenciales	47
Actualización de credenciales	47
Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager	48
Configuración de LW-SSO	48
Configuración del cifrado de la comunicación de Confidential Manager	48
Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager manualmente en la sonda	50
Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas	50
Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager en la sonda	51
Configurar el cifrado de la comunicación de Confidential Manager en la sonda	51
Configurar la caché del cliente de Confidential Manager	52
Configurar el modo de caché del cliente de Confidential Manager en la sonda	53
Establecer la configuración de cifrado de caché del cliente de Confidential Manager en la sonda	53
Exportar e importar la información de credenciales e intervalos en formato cifrado	54
Cambiar el nivel de mensajes del archivo de registro del cliente de Confidential Manager	56
Archivo de registro del cliente de Confidential Manager	56

Archivo de registro de LW-SSO	56
Generar o actualizar la clave de cifrado	57
Generar una nueva clave de cifrado	58
Actualizar una clave de cifrado en un servidor de UCMDB	59
Actualizar una clave de cifrado en una sonda	60
Cambiar manualmente la clave de cifrado cuando Administrador de sonda y Puerta de enlace de sonda están instalados en equipos independientes	60
Definir varios proveedores JCE	61
Configuración de cifrado de Confidential Manager	61
Solución de problemas y limitaciones	62
Sistema de protección de la sonda de Data Flow	63
Modificar la contraseña cifrada de la base de datos MySQL	63
Secuencia de comandos clearProbeData.bat: Uso	65
Configurar la contraseña cifrada de la consola JMX	65
Configurar la contraseña de UpLoadScanFile	66
Acceso remoto a MySQL Server	67
Habilitar SSL entre el servidor UCMDB y la sonda de Data Flow con autenticación mutua	68
Información general	68
Almacenes de claves y almacenes de confianza	68
Habilitar SSL con la autenticación de servidor (unidireccional)	69
Habilitar autenticación mutua de certificados (bidireccional)	71
Controlar la ubicación del archivo domainScopeDocument	76
Crear un almacén de claves para la sonda de Data Flow	77
Cifrar las contraseñas del almacén de claves y el almacén de confianza de la sonda	77
Almacén de claves y almacén de confianza predeterminados de servidor y sonda de Data Flow	78
Servidor UCMDB	78
La sonda de Data Flow	78
Autenticación de Lightweight Single Sign-On (LW-SSO): referencia general	80
Información general de la autenticación LW-SSO	80
Requisitos del sistema de LW-SSO	81
Advertencias de seguridad de LW-SSO	81

Solución de problemas y limitaciones	83
Autenticación de inicio de sesión de HP Universal CMDB	86
Configuración de un método de autenticación	86
Habilitación del inicio de sesión en HP Universal CMDB con LW-SSO	87
Configuración de una conexión segura con el protocolo SSL (Capa de sockets seguros) ..	87
Uso de la consola JMX para probar las conexiones LDAP	88
Configuración de LDAP mediante la consola JMX	89
Habilitación y definición del método de autenticación LDAP	90
Recuperación de la configuración de LW-SSO actual en un entorno distribuido	91
Confidential Manager	92
Información general de Confidential Manager	92
Consideraciones de seguridad	92
Configurar el servidor de HP Universal CMDB	93
Definiciones	94
Propiedades de cifrado	94

Capítulo 1

Introducción al sistema de protección

Este capítulo incluye:

Información general del sistema de protección	9
Preparativos del sistema de protección	10
Implementar UCMDDB en una arquitectura segura	10
Acceso al sistema	11
Sistema de protección de acceso a Java JMX	11
Cambio del nombre de usuario o la contraseña del sistema en la consola JMX	13
Cambio del usuario del servicio del servidor de HP Universal CMDB	14
Cifrar la contraseña de la base de datos para Configuration Manager	15
Parámetros para el cifrado de la contraseña de la base de datos de Configuration Manager	16

Información general del sistema de protección

Esta sección presenta el concepto de aplicación HP Universal CMDB segura y explica la planificación y arquitectura necesarias para implementar la seguridad. Se recomienda encarecidamente leer esta sección antes de pasar a las secciones siguientes.

HP Universal CMDB se ha diseñado para poder formar parte de una arquitectura segura y, por consiguiente, puede afrontar el reto de enfrentarse a las amenazas de seguridad a las que pueda estar expuesto.

Las directrices del sistema de protección tienen que ver con la configuración necesaria para implementar un HP Universal CMDB más seguro (reforzado).

La información que se proporciona sobre el sistema de protección va dirigida principalmente a los administradores de HP Universal CMDB, quienes deben familiarizarse con la configuración y las recomendaciones del sistema de protección antes de iniciar los procedimientos de dicho sistema.

Es muy recomendable usar un proxy inverso con HP Universal CMDB para obtener una arquitectura segura. Para obtener más información sobre la configuración de un proxy inverso para utilizarlo con HP Universal CMDB, consulte "[Utilización de un proxy inverso](#)" en la página 34.

Si debe usar con HP Universal CMDB un tipo de arquitectura segura distinto del que se describe en este documento, póngase en contacto con el soporte técnico de HP para determinar cuál es la arquitectura más adecuada para usar.

Para obtener más información sobre el sistema de protección de la sonda de Data Flow, consulte "[Sistema de protección de la sonda de Data Flow](#)" en la página 63.

Nota:

- Los procedimientos del sistema de protección se basan en la suposición de que el usuario sólo va a implementar las instrucciones que se proporcionan en estos capítulos y que no va a llevar a cabo otros pasos del sistema de protección documentados en otros lugares.
- Aunque los procedimientos del sistema de protección se centran en una arquitectura distribuida concreta, ello no implica que ésta sea la arquitectura que mejor cubra las necesidades de su organización.
- Se supone que los procedimientos que se incluyen en los siguientes capítulos se van a llevar a cabo en equipos dedicados a HP Universal CMDB. El uso de los equipos para otros fines, además de para HP Universal CMDB, pueden generar resultados problemáticos.
- La información sobre el sistema de protección que se proporciona en esta sección no pretende ser una guía para la realización de evaluaciones de los riesgos de seguridad en sistemas informatizados.

Preparativos del sistema de protección

- Evalúe el riesgo de seguridad/estado de la seguridad de la red general y use las conclusiones que obtenga a la hora de decidir cuál es la mejor forma de integrar HP Universal CMDB en la red.
- Debe conocer a la perfección tanto el marco técnico como las capacidades de seguridad de HP Universal CMDB.
- Revise todas las directivas del sistema de protección
- Verifique que HP Universal CMDB funciona a la perfección antes de iniciar los procedimientos del sistema de protección.
- En todos los capítulos, siga los pasos del procedimiento del sistema de protección de forma cronológica. Por ejemplo, si decide configurar el servidor de HP Universal CMDB para que admita SSL, lea "[Habilitar la comunicación de Capa de sockets seguros \(SSL\)](#)" en la [página 18](#) y, a continuación, siga todas las instrucciones cronológicamente.
- HP Universal CMDB no admite la autenticación básica con contraseñas en blanco. No utilice una contraseña en blanco cuando configure los parámetros de conexión de autenticación básica.

Tip: Imprima los procedimientos del sistema de protección y vaya marcándolos a medida que los implemente.

Implementar UCMDB en una arquitectura segura

Se recomienda tomar varias medidas para desplegar los servidores de HP Universal CMDB de forma segura:

- **Arquitectura DMZ con un servidor de seguridad**

La arquitectura segura a la que se hace referencia en este documento es una arquitectura DMZ típica que utiliza un dispositivo como servidor de seguridad. El concepto básico de dicha arquitectura es crear una separación completa y evitar el acceso directo entre los clientes de HP Universal CMDB y el servidor de HP Universal CMDB.

- **Explorador seguro**

Internet Explorer y Firefox en un entorno Windows deben configurarse para controlar de forma segura las cookies, los applets y las secuencias de comandos Java.

- **Protocolo de comunicación SSL**

El protocolo Capa de sockets seguros (SSL) protege la conexión entre el cliente y el servidor. Las direcciones URL que requieren una conexión SSL utilizan una versión segura (HTTPS) del protocolo de transferencia de hipertexto. Para obtener más información, consulte "[Habilitar la comunicación de Capa de sockets seguros \(SSL\)](#)" en la página 18.

- **Arquitectura de proxy inverso**

Una de las soluciones más seguras y recomendadas sugiere desplegar HP Universal CMDB utilizando un proxy inverso. HP Universal CMDB es totalmente compatible con la arquitectura segura de proxy inverso. Para obtener más información, consulte "[Utilización de un proxy inverso](#)" en la página 34.

Acceso al sistema

Sistema de protección de acceso a Java JMX

Nota: El procedimiento que se describe aquí también se puede utilizar para JMX de la sonda de Data Flow.

Para garantizar que el puerto RMI de JMX es accesible solo cuando se proporcionan las credenciales de usuario, siga este procedimiento:

1. En el archivo **wrapper.conf** del servidor, que se encuentra en **C:\hp\UCMDB\UCMDBServer\bin**, ajuste lo siguiente:

wrapper.java.additional.16=-Dcom.sun.management.jmxremote.authenticate=true

Esta configuración requiere que JMX solicite la autenticación.

- **Para JMX de la sonda de Data Flow**, realice lo siguiente:

En los archivos **WrapperGateway.conf** y **WrapperManager.conf**, que se encuentran en **C:\hp\UCMDB\DataFlowProbe\bin**, ajuste lo siguiente:

wrapper.java.additional.17=-Dcom.sun.management.jmxremote.authenticate=true

2. Cambie el nombre del archivo **jmxremote.password.template** (que se encuentra en: **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) a **jmxremote.password**.

Nota: Para JMX de la sonda de Data Flow, este archivo se encuentra en:
C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management\.

3. En **jmxremote.password**, agregue contraseñas para las funciones **monitorRole** y **controlRole**.

Por ejemplo:

monitorRole QED

controlRole R&D

asignaría la contraseña **QED** a **monitorRole** y la contraseña **R&D** a **controlRole**.

Nota: Asegúrese de que solamente el propietario tenga permisos de lectura y escritura en **jmxremote.password**, ya que contiene las contraseñas en texto sin cifrar. El propietario del archivo debe ser el mismo usuario con el que se ejecuta el servidor de UCMDB.

4. En el archivo **jmxremote.access** (que se encuentra en **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**), asigne acceso a **monitorRole** y **controlRole**.

Por ejemplo:

monitorRole readonly

controlRole readwrite

asignaría acceso de solo lectura a **monitorRole** y acceso de lectura o escritura a **controlRole**.

Nota: Para JMX de la sonda de Data Flow, este archivo se encuentra en:
C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management\.

5. Proteja los archivos de la siguiente manera:

- **En Windows solamente:** Ejecute los siguientes comandos desde la línea de comandos para proteger los archivos:

cacls jmxremote.password /P <nombre de usuario>:F

cacls jmxremote.access /P <nombre de usuario>:R

donde **<nombre de usuario>** es el propietario del archivo visible en las propiedades de ambos archivos. Abra las propiedades de esos archivos y asegúrese de que sean correctas y solo tengan un propietario.

- **En sistemas operativos Solaris y Linux:** Ajuste los permisos de archivo para el archivo de contraseña ejecutando:

chmod 600 jmxremote.password

6. **Para actualizaciones de Service Pack, migraciones de servidor y recuperación ante desastres:** Cambie la propiedad del archivo **jmxremote.access** (que se encuentra en **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) al sistema operativo que ejecuta la instalación de actualización o migración.

Nota: Para JMX de la sonda de Data Flow, este archivo se encuentra en:
C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management\.

Cambio del nombre de usuario o la contraseña del sistema en la consola JMX

La consola JMX utiliza usuarios del sistema, es decir, usuarios de varios clientes en un entorno multiempresa. Puede iniciar sesión en la consola JMX con cualquier nombre de usuario del sistema. El nombre y la contraseña predeterminados son **sysadmin/sysadmin**.

Puede cambiar la contraseña a través de la consola JMX o de la herramienta Administración de servidor.

Para cambiar el nombre de usuario o la contraseña predeterminados del sistema a través de la consola JMX:

1. Inicie un explorador web y escriba la siguiente dirección: **http://localhost.<nombre de dominio>:8080/jmx-console**.
2. Introduzca las credenciales de autenticación de la consola JMX, que de forma predeterminada son:
 - Nombre de inicio de sesión = **sysadmin**
 - Contraseña = **sysadmin**
3. Localice **UCMDB:service=Authorization Services** y haga clic en el vínculo para abrir la página de operaciones.
4. Localice la operación **resetPassword**.
 - En el campo **userName**, escriba **sysadmin**.
 - En el campo **password**, escriba una contraseña nueva.
5. Haga clic en **Invoke** para guardar el cambio.

Para cambiar el nombre de usuario o la contraseña predeterminados del sistema a través de la herramienta Administración de servidor:

1. **En Windows:** ejecute el siguiente archivo: **C:\hp\UCMDB\UCMDBServer\tools\server_management.bat**.
En Linux: Ejecute **server_management.sh**, que se encuentra en la siguiente carpeta: **/opt/hp/UCMDB/UCMDBServer/tools/**.
2. Inicie sesión en la herramienta con las credenciales de autenticación: **sysadmin/sysadmin**.
3. Haga clic en el vínculo Usuarios.
4. Seleccione el usuario del sistema y haga clic en **Cambiar contraseña de usuario con sesión iniciada**.
5. Escriba la contraseña antigua y la contraseña nueva y haga clic en **Aceptar**.

Cambio del usuario del servicio del servidor de HP Universal CMDB

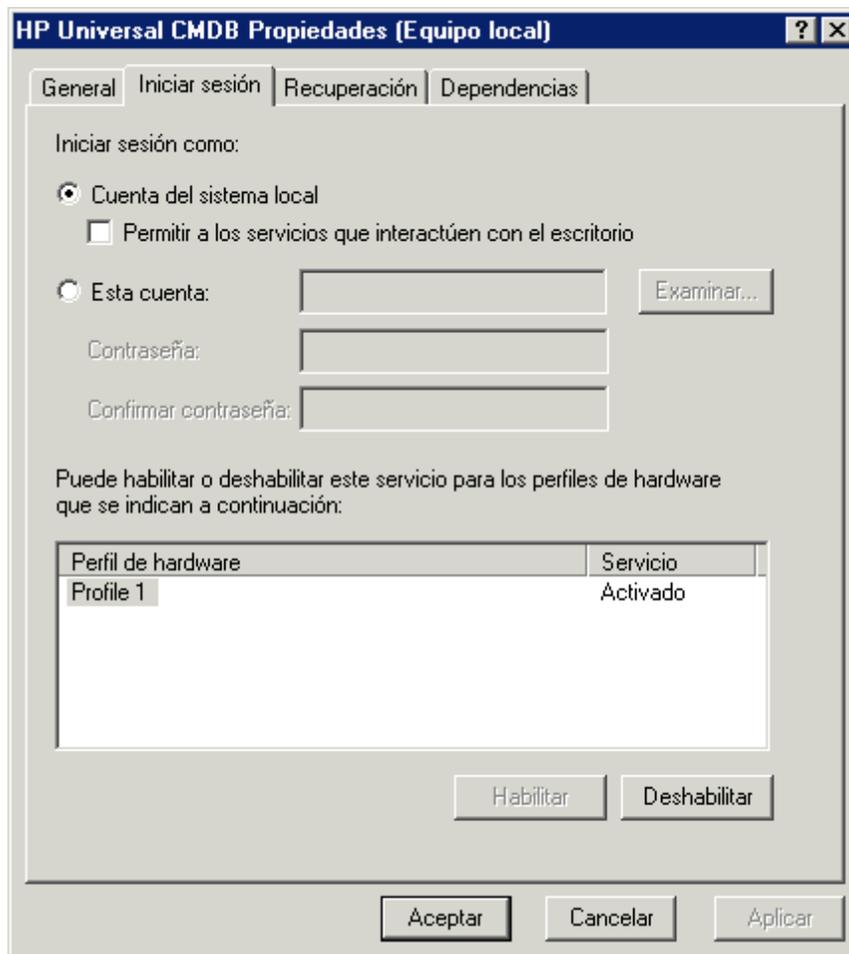
En una plataforma Windows, el servicio de HP Universal CMDB, que ejecuta todos los procesos y servicios de HP Universal CMDB, se instala cuando se ejecuta la utilidad de Configuración de servidores y bases de datos. De forma predeterminada, este servicio se ejecuta con el usuario del sistema local. Sin embargo, es posible que sea necesario asignar otro usuario para ejecutar el servicio (por ejemplo, si utiliza la autenticación NTLM).

El usuario asignado para ejecutar el servicio debe tener los siguientes permisos:

- permisos de base de datos suficientes (definidos por el administrador de bases de datos)
- permisos de red suficientes
- permisos de administrador en el servidor local

Para cambiar el usuario del servicio:

1. Deshabilite HP Universal CMDB a través del menú Inicio (**Inicio > Todos los programas > HP UCMDB > Detener HP Universal CMDB Server**) o deteniendo el servicio del servidor de HP Universal CMDB. Para obtener más información, consulte "[Start and Stop the HP Universal CMDB Server Service](#)" (on page 1).
2. En la ventana **Servicios** de Windows, haga doble clic en **UCMDB_Server**. Se abre el cuadro de diálogo **UCMDB_Server Propiedades (Equipo local)**.
3. Haga clic en la ficha Iniciar sesión.



4. Seleccione **Esta cuenta** y elija otro usuario en la lista de usuarios válidos en el equipo.
5. Introduzca la contraseña de Windows del usuario seleccionado y confírmela.
6. Haga clic en **Aplicar** para guardar la configuración y en **Aceptar** para cerrar el cuadro de diálogo.
7. Habilite HP Universal CMDB a través del menú Inicio (**Inicio > Todos los programas > HP UCMDB > Iniciar HP Universal CMDB Server**) o iniciando el servicio del servidor de HP Universal CMDB. Para obtener más información, consulte "Start and Stop the HP Universal CMDB Server Service" (on page 1).

Cifrar la contraseña de la base de datos para Configuration Manager

La contraseña de la base de datos de CM se almacena en <**Configuration Manager**, archivo **directorio de instalación**>\conf\database.properties. Si desea cifrar la contraseña, nuestro algoritmo de cifrado predeterminado cumple los estándares de FIPS 140-2.

El cifrado se logra por medio de una clave, ya que la contraseña se cifra a través de ella. Posteriormente, la propia clave se cifra mediante otra clave, que se conoce como clave maestra. Ambas claves se cifran con el mismo algoritmo. Para obtener más información sobre los

parámetros que se usan en el proceso de cifrado, consulte "Parámetros para el cifrado de la contraseña de la base de datos de Configuration Manager" abajo

Precaución: si cambia el algoritmo de cifrado, no se podrán volver a utilizar las contraseñas cifradas anteriormente.

Para cambiar el cifrado de la contraseña de la base de datos:

1. Abra el archivo <Configuration Manager directorio de instalación>\conf\encryption.properties y edite los siguientes campos:
 - **engineName.** Escriba el nombre del algoritmo de cifrado.
 - **keySize.** Especifique el tamaño de la clave maestra del algoritmo seleccionada.
2. Ejecute la secuencia de comandos **generate-keys.bat**, que crea el siguiente archivo: <Directorio de instalación de Configuration Manager>\security\encrypt_repository y genere la clave de cifrado.
3. Ejecute la utilidad **bin\encrypt-password.bat** para cifrar la contraseña. Configure el indicador **-h** para ver las opciones disponibles.
4. Copie el resultado de la utilidad de cifrado de contraseñas y pegue el cifrado resultante en el archivo **conf\database.properties**.

Parámetros para el cifrado de la contraseña de la base de datos de Configuration Manager

La siguiente tabla enumera los parámetros que se incluyen en el archivo **encryption.properties**, que se usa para el cifrado de la contraseña de la base de datos de CM. Para obtener más información sobre el cifrado de la contraseña de la base de datos, consulte "Cifrar la contraseña de la base de datos para Configuration Manager" en la página precedente.

Parámetro	Descripción
cryptoSource	Indica la infraestructura que implanta el algoritmo de cifrado. Las opciones disponibles son: <ul style="list-style-type: none"> • lw. Usa la implementación ligera de Bouncy Castle (opción predeterminada) • jce. Java Cryptography Enhancement (infraestructura de criptografía Java estándar)
storageType	Indica el tipo de almacenamiento de claves. Actualmente, sólo se admite archivo binario .
binaryFileStorageName	Indica el lugar del archivo en el que se almacena la clave maestra.
cipherType	El tipo de cifrado. Actualmente, sólo se admite symmetricBlockCipher .
engineName	El nombre del algoritmo de cifrado.

Parámetro	Descripción
	<p>Las siguientes opciones están disponibles:</p> <ul style="list-style-type: none"> • AES. American Encryption Standard. Este cifrado es compatible con FIPS 140-2. (opción predeterminada) • Blowfish • DES • 3DES. (compatible con FIPS 140-2) • Nulo. Sin cifrado
keySize	<p>El tamaño de la clave maestra. Dicho tamaño lo determina el algoritmo:</p> <ul style="list-style-type: none"> • AES. 128, 192 ó 256 (la opción predeterminada es 256) • Blowfish. 0-400 • DES. 56 • 3DES. 156
encodingMode	<p>La codificación ASCII de los resultados del cifrado binario.</p> <p>Las siguientes opciones están disponibles:</p> <ul style="list-style-type: none"> • Base64 (opción predeterminada) • Base64Url • Hex
algorithmModeName	<p>El modo del algoritmo. Actualmente, sólo se admite CBC.</p>
algorithmPaddingName	<p>El algoritmo de relleno que se usa.</p> <p>Las siguientes opciones están disponibles:</p> <ul style="list-style-type: none"> • PKCS7Padding (opción predeterminada) • PKCS5Padding
jceProviderName	<p>El nombre del algoritmo de cifrado JCE.</p> <p>Nota: Sólo es relevante cuando cryptSource es jce. Para lw, se usa engineName</p>

Capítulo 2

Habilitar la comunicación de Capa de sockets seguros (SSL)

Este capítulo incluye:

Habilitar SSL en el equipo servidor con un certificado autofirmado - UCMDB	18
Habilitar SSL en el equipo servidor con un certificado autofirmado - Configuration Manager ...	20
Habilitar SSL en el equipo servidor con un certificado de una entidad de certificación - UCMDB	21
Habilitar SSL en el equipo servidor con un certificado de una entidad de certificación - Configuration Manager	23
Habilitar SSL en los equipos cliente - UCMDB	24
Habilitar SSL con un certificado de cliente - Configuration Manager	25
Habilitar SSL en el SDK del cliente	25
Habilitar la autenticación de certificados manual en el SDK	26
Cambiar la contraseñas del almacén de claves del servidor	27
Habilitar o deshabilitar puertos HTTP/HTTPS	28
Asignar los componentes web de UCMDB a los puertos	29
Configurar Configuration Manager para que funcione con UCMDB mediante SSL	31
Habilitar el adaptador KPI de UCMDB para su uso con SSL	31
Configuración de la compatibilidad con SSL para el navegador de UCMDB	32

Habilitar SSL en el equipo servidor con un certificado autofirmado - UCMDB

En estas secciones se explica cómo configurar HP Universal CMDB para que admita la comunicación mediante el canal Capa de sockets seguros (SSL).

HP Universal CMDB utiliza Jetty 6.1 como servidor web predeterminado.

1. Requisitos previos

- a. Antes de iniciar el siguiente procedimiento, elimine el **server.keystore** antiguo que está ubicado en **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

- b. Coloque el almacén de claves de HP Universal CMDB (tipo JKS) en la carpeta **C:\hp\UCMDB\UCMDBServer\confsecurity**.

2. Generar un almacén de claves del servidor

- a. Cree un almacén de claves (tipo JKS) con un certificado autofirmado y una clave privada coincidente:

- o Desde **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**, ejecute el siguiente comando:

```
keytool -genkey -alias hpcert -keystore  
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
```

Se abre el cuadro de diálogo de la consola.

- o Escriba la contraseña del almacén de claves. Si la contraseña ha cambiado, ejecute la operación **changeKeystorePassword** de JMX, en **UCMDB:service=Security Services**. Si la contraseña no ha cambiado, utilice la contraseña **hppass** predeterminada.
- o Responda a la pregunta, **¿Cuáles son su nombre y sus apellidos?** Escriba el nombre del servidor web de HP Universal CMDB. Introduzca los restantes parámetros en función de las necesidades de su organización.
- o Escriba una contraseña de la clave. Dicha contraseña DEBE coincidir con la contraseña del almacén de claves.

Se crea un almacén de claves JKS llamado **server.keystore** con un certificado de servidor llamado **hpcert**.

- b. Exporte el certificado autofirmado a un archivo:

Desde **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**, ejecute el siguiente comando:

```
keytool -export -alias hpcert -keystore  
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass  
<su contraseña> -file hpcert
```

3. Colocar el certificado en el almacén de confianza del cliente

Después de generar **server.keystore** y exportar el certificado de servidor para todos los clientes que necesiten comunicarse con HP Universal CMDB a través de SSL utilizando este certificado autofirmado, coloque este certificado en los almacenes de confianza del cliente.

Nota: en **server.keystore**, no puede haber más de un certificado de servidor.

4. Deshabilitar el puerto HTTP 8080

Para obtener más información, consulte "[Habilitar o deshabilitar puertos HTTP/HTTPS](#)" en la [página 28](#).

Nota: Antes de cerrar el puerto HTTP, compruebe que la comunicación HTTPS funciona.

5. Reiniciar el servidor

6. Mostrar HP Universal CMDB

Para comprobar que el servidor UCMDDB es seguro, escriba la siguiente dirección URL en el explorador web: **https://<nombre o dirección IP de servidor UCMDDB>:8443/ucmdb-ui**.

Habilitar SSL en el equipo servidor con un certificado autofirmado - Configuration Manager

En estas secciones se explica cómo configurar Configuration Manager para que admita la autenticación y el cifrado utilizando el canal Capa de sockets seguros (SSL).

Configuration Manager usa Tomcat 7.0.19 como servidor de aplicaciones.

Nota: las ubicaciones de todos los directorios y archivos dependen de su plataforma concreta, del sistema operativo y de las preferencias que se elijan durante la instalación.

1. Requisitos previos

Antes de iniciar el siguiente procedimiento, suprima el antiguo archivo **tomcat.keystore** que se encuentra en la carpeta **<Directorio de instalación de Configuration Manager>\java\windows\x86_64\lib\security** o la carpeta **<Directorio de instalación de Configuration Manager>\javainux\x86_64\lib\security** (la que sea relevante), si existe.

2. Generar un almacén de claves del servidor

Cree un almacén de claves (tipo JKS) con un certificado autofirmado y una clave privada coincidente:

- Desde el directorio bin de la instalación de Java en el directorio de instalación de Configuration Manager, ejecute el siguiente comando:

```
keytool -genkey -alias tomcat -keyalg RSA -keystore ..\lib\security\tomcat.keystore
```

Se abre el cuadro de diálogo de la consola.

- Escriba la contraseña del almacén de claves. Si la contraseña ha cambiado, cámbiela manualmente en el archivo.
- Responda a la pregunta, **¿Cuáles son su nombre y sus apellidos?** Escriba el nombre del servidor web de Configuration Manager. Introduzca los restantes parámetros en función de las necesidades de su organización.
- Escriba una contraseña de la clave. Dicha contraseña DEBE coincidir con la contraseña del almacén de claves.

Se crea un almacén de claves JKS llamado **tomcat.keystore** con un certificado de servidor llamado **hpcert**.

3. Colocar el certificado en el almacén de confianza del cliente

Añada el certificado a los almacenes de confianza del cliente de Internet Explorer en el equipo (**Herramientas > Opciones de Internet > Contenido > Certificados**). Si no lo hace, se le solicitará que lo haga la primera vez que intente usar Configuration Manager.

Limitación: en `tomcat.keystore`, no puede haber más de un certificado de servidor.

4. Modificar el archivo `server.xml`

Abra el archivo `server.xml`, que se encuentra en **<Directorio de instalación de Configuration Manager>\servers\server-0\conf**. Localice la sección que empieza por

```
Connector port="8143"
```

que aparece en los comentarios. Active la secuencia de comandos quitando el carácter de comentario y agregue los siguientes atributos al conector de HTTPS:

```
keystoreFile="<ubicación del archivo tomcat.keystore>" (consulte el paso 2)
```

```
keystorePass="<contraseña>"
```

Convierta la siguiente línea en comentario:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLSEngine="on" />
```

Nota: No debe bloquear el puerto de la conexión HTTP. Si desea bloquear la comunicación HTTP, puede usar un firewall para ello.

5. Reiniciar el servidor

Reinicie el servidor de Configuration Manager.

6. Verificar la seguridad del servidor

Para verificar que el servidor de Configuration Manager es seguro, escriba la siguiente URL en el explorador web: **https://<Nombre del servidor o dirección IP de Configuration Manager>:8143/cnc**.

Tip: si no logra establecer una conexión, pruebe a usar otro explorador o actualice el explorador a una versión más reciente.

Habilitar SSL en el equipo servidor con un certificado de una entidad de certificación - UCMDB

Para usar un certificado generado por una entidad de certificación (CA), el almacén de claves debe estar en formato Java. El siguiente ejemplo explica cómo dar formato al almacén de claves en un equipo Windows.

1. Requisitos previos

Antes de iniciar el siguiente procedimiento, elimine el `server.keystore` antiguo, que está ubicado en **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

2. Generar un almacén de claves del servidor

- a. Genere un certificado firmado por CA e instálelo en Windows.
- b. Exporte el certificado a un archivo *.**pfx** (incluyendo las claves privadas) a través de Microsoft Management Console (**mmc.exe**).

Escriba cualquier cadena como contraseña del archivo **pfx**. (Esta contraseña se solicita al convertir el tipo de almacén de claves a un almacén JAVA.) El archivo **.pfx** ahora contiene un certificado público y una clave privada, y está protegido mediante contraseña.

- c. Copie el archivo **.pfx** que ha creado a la siguiente carpeta:
C:\hp\UCMDB\UCMDBServer\conf\security.

- d. Abra el símbolo del sistema y cambie el directorio a
C:\hp\UCMDB\UCMDBServer\bin\jre\bin.

Cambie el tipo de almacén de claves de **PKCS12** a un almacén de claves **JAVA**, para lo que debe ejecutar el siguiente comando:

```
keytool -importkeystore -srckeystore  
c:\hp\UCMDB\UCMDBServer\conf\security\<<nombre de archivo pfx> -  
srcstoretype PKCS12 -destkeystore server.keystore
```

Se le solicitará la contraseña del almacén de claves de origen (**.pfx**). Esta es la contraseña que introdujo al crear el archivo **pfx** en el paso b.)

- e. Escriba la contraseña del almacén de claves de destino. Debe ser la misma contraseña que la que se definió previamente en el método **changeKeystorePassword** de JMX, en Security Services. Si la contraseña no ha cambiado, utilice la contraseña **hppass** predeterminada.
- f. Después de generar el certificado, deshabilite el puerto HTTP 8080. Para obtener más información, consulte "[Habilitar o deshabilitar puertos HTTP/HTTPS](#)" en la página 28.
- g. Si ha utilizado una contraseña distinta de **hppass** o la contraseña usada en el archivo **.pfx** ejecute el método **changeKeystorePassword** de JMX y asegúrese de que la clave tiene la misma contraseña.

Nota: Antes de cerrar el puerto HTTP, compruebe que la comunicación HTTPS funciona.

3. Reiniciar el servidor

4. Verificar la seguridad del servidor

Para verificar que el servidor UCMDB es seguro, escriba la siguiente dirección URL en el explorador web: **https://<nombre o dirección IP de servidor UCMDB>:8443/ucmdb-ui**.

Precaución: en **server.keystore**, no puede haber más de un certificado de servidor.

Habilitar SSL en el equipo servidor con un certificado de una entidad de certificación - Configuration Manager

En Configuration Manager, para usar un certificado generado por una entidad de certificación (CA), el almacén de claves debe estar en formato Java. El siguiente ejemplo explica cómo dar formato al almacén de claves en un equipo Windows.

1. Requisitos previos

Antes de iniciar el siguiente procedimiento, suprima el antiguo archivo **tomcat.keystore** que se encuentra en la carpeta **<Directorio de instalación de Configuration Manager>\java\windows\x86_64\lib\security** o la carpeta **<Directorio de instalación de Configuration Manager>\java\linux\x86_64\lib\security** (la que sea relevante), si existe.

2. Generar un almacén de claves del servidor

- Genere un certificado firmado por CA e instálelo en Windows.
- Exporte el certificado a un archivo ***.pfx** (incluyendo las claves privadas) a través de Microsoft Management Console (**mmc.exe**).

Escriba cualquier cadena como contraseña del archivo **pfx**. (Esta contraseña se solicita al convertir el tipo de almacén de claves a un almacén JAVA.)

El archivo **.pfx** ahora contiene un certificado público y una clave privada, y está protegido mediante contraseña.

Copie el archivo **.pfx** que ha creado a la siguiente carpeta: **<Directorio de instalación de Configuration Manager>\java\lib\security**.

- Abra el símbolo del sistema y cambie el directorio a **<Directorio de instalación de Configuration Manager>\java\bin**.

Cambie el tipo de almacén de claves de **PKCS12** a un almacén de claves **JAVA**, para lo que debe ejecutar el siguiente comando:

```
keytool -importkeystore -srckeystore <Directorio de instalación de Configuration Manager>\conf\security\<<nombre de archivo pfx> -srcstoretype PKCS12 -destkeystore tomcat.keystore
```

Se le solicitará la contraseña del almacén de claves de origen (**.pfx**). Esta es la contraseña que introdujo al crear el archivo pfx en el paso b.

3. Modificar el archivo server.xml

Abra el archivo **server.xml**, que se encuentra en **<Directorio de instalación de Configuration Manager>\servers\server-0\conf**. Localice la sección que empieza por

```
Connector port="8143"
```

que aparece en los comentarios. Active el script quitando el carácter de comentario y agregue las dos líneas siguientes:

```
keystoreFile="../../java/lib/security/tomcat.keystore"  
keystorePass="password" />
```

Convierta la siguiente línea en comentario:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"  
SSLEngine="on" />
```

Nota: No debe bloquear el puerto de la conexión HTTP. Si desea bloquear la comunicación HTTP, puede usar un firewall para ello.

4. Reiniciar el servidor

Reinicie el servidor de Configuration Manager.

5. Verificar la seguridad del servidor

Para verificar que el servidor de Configuration Manager es seguro, escriba la siguiente URL en el explorador web: **https://<Configuration Manager Nombre del servidor o dirección IP>:8143/cnc.**

Limitación: en **tomcat.keystore**, no puede haber más de un certificado de servidor.

Nota: las ubicaciones de todos los directorios y archivos dependen de su plataforma concreta, del sistema operativo y de las preferencias que se elijan durante la instalación.

Por ejemplo: `java/{os name}/lib.`

Habilitar SSL en los equipos cliente - UCMDB

Si el certificado que usa el servidor web de HP Universal CMDB lo genera una entidad de certificación (CA) conocida, es muy probable que el explorador web pueda validar el certificado sin tener que realizar más acciones.

Si el explorador web no confía en la entidad de certificación, debe importar la ruta completa de confianza del certificado o importar el certificado que utiliza HP Universal CMDB de forma explícita en el almacén de confianza del explorador.

El siguiente ejemplo muestra cómo importar el certificado autofirmado **hpcert** en el almacén de confianza de Windows para Internet Explorer.

Para importar un certificado en el almacén de confianza de Windows:

1. Localice el certificado **hpcert** y cámbiele el nombre a **hpcert.cer**.
En el Explorador de Windows, el icono muestra que el archivo es un certificado de seguridad.
2. Haga doble clic en **hpcert.cer** para abrir el cuadro de diálogo Certificado de Internet Explorer.
3. Siga las instrucciones para habilitar la confianza instalando el certificado con el Asistente para importación de certificados.

Nota: Otro método para importar en el explorador web el certificado que emite el servidor UCMDB consiste en iniciar sesión en UCMDB e instalar el certificado cuando se muestra la advertencia que indica que el certificado no es de confianza.

Habilitar SSL con un certificado de cliente - Configuration Manager

Si el certificado que usa el servidor web de Configuration Manager lo genera una entidad de certificación (CA) conocida, es muy probable que el explorador web pueda validar el certificado sin tener que realizar más acciones.

Si el almacén de confianza del servidor no confía en el CA, importe el certificado de CA en el almacén de confianza del servidor.

El siguiente ejemplo muestra cómo importar el certificado **hpcert** autofirmado en el almacén de confianza del servidor (cacerts).

Para importar un certificado en el almacén de confianza del servidor:

1. En el equipo cliente, localice el certificado **hpcert** y cámbielo de nombre por **hpcert.cer**.
2. Copie **hpcert.cer** al equipo servidor de la carpeta **<Directorio de instalación de Configuration Manager>\javalbin**.
3. En el equipo del servidor, importe el certificado de CA en el almacén de confianza (cacerts) empleando la utilidad **keytool** con el siguiente comando:

```
<Directorio de instalación de Configuration  
Manager>\java\bin\keytool.exe -import  
-alias hp -file hpcert.cer -keystore ..\lib\security\cacerts
```

4. Modifique el archivo **server.xml** (se encuentra en la carpeta **<Directorio de instalación de Configuration Manager>\servers\server-0\conf**) de la siguiente manera:
 - a. Realice los cambios que se describen en ["Modificar el archivo server.xml"](#) en la página 23.
 - b. Inmediatamente después, añada los siguientes atributos al conector de HTTPS:

```
truststoreFile="../../java/lib/security/cacerts"  
truststorePass="changeit" />
```
 - c. Establezca `clientAuth="true"`.
5. Compruebe la seguridad del servidor tal y como se describe en ["Verificar la seguridad del servidor"](#) en la página precedente.

Habilitar SSL en el SDK del cliente

Puede utilizar el transporte HTTPS entre el SDK del cliente y el SDK del servidor:

1. En el equipo cliente, en el producto que incrusta el SDK del cliente, localice la configuración de transporte y asegúrese de que está establecida en HTTPS y no en HTTP.
2. Descargue el certificado de CA o el certificado público autofirmado en el equipo cliente, e impórtelo en el almacén de confianza **cacerts** del JRE que va a conectarse al servidor.

Use el siguiente comando:

```
Keytool -import -alias <nombre de CA> -trustcacerts -file <ruta de
certificado público del servidor> -keystore <ruta al almacén
cacerts de confianza del jre cliente (p. ej., x:\archivos de
programa\java\jre\lib\security\cacerts)>
```

Habilitar la autenticación de certificados manual en el SDK

Este modo utiliza SSL y permite tanto la autenticación del servidor por parte de UCMDB como la autenticación de cliente por parte del cliente UCMDB-API. Tanto el servidor como el cliente UCMDB-API envían sus certificados a la otra entidad para su autenticación.

Nota: El siguiente método, que consiste en habilitar SSL en el SDK con autenticación mutua, es el más seguro de los métodos y, por lo tanto, es el modo de comunicación recomendado.

1. Proteja el conector del cliente UCMDB-API en UCMDB:
 - a. Acceda a la consola JMX de UCMDB: Inicie un explorador web y escriba la siguiente dirección: **http://<nombre de equipo o dirección IP de UCMDB>:8080/jmx-console**. Es posible que deba iniciar sesión con un nombre de usuario y una contraseña (los valores predeterminados son sysadmin/sysadmin).
 - b. Localice **UCMDB:service=Ports Management Services** y haga clic en el vínculo para abrir la página de operaciones.
 - c. Localice la operación **PortsDetails** y haga clic en **Invoke**. Anote el número de puerto de HTTPS con autenticación de cliente. El valor predeterminado es 8444 y debería estar habilitado.
 - d. Vuelva a la página de operaciones.
 - e. Para asignar el conector ucmdb-api al modo de autenticación mutua, llame al método **mapComponentToConnectors** con los siguientes parámetros:
 - o **componentName:** ucmdb-api
 - o **isHTTPSWithClientAuth:** true
 - o Todos los demás indicadores: falseSe muestra el siguiente mensaje:

```
Operation succeeded. Component ucmdb-api is now mapped to:
HTTPS_CLIENT_AUTH ports.
```
 - f. Vuelva a la página de operaciones.
2. Asegúrese de que el JRE que ejecuta el cliente UCMDB-API tiene un almacén de claves que contiene un certificado de cliente.
3. Exporte el certificado de cliente UCMDB-API de su almacén de claves.
4. Importe el certificado de cliente UCMDB-API exportado al almacén de confianza del servidor UCMDB.

- a. En el equipo donde está instalado UCMDB, copie el archivo del certificado de cliente UCMDB-API creado en el siguiente directorio en UCMDB:
C:\HP\UCMDB\UCMDBServer\conf\security
 - b. Ejecute el siguiente comando:
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file <certificado de cliente UCMDB-api exportado> -alias ucmdb-api
 - c. Introduzca la contraseña del almacén de confianza del servidor UCMDB (el valor predeterminado es **hppass**).
 - d. Cuando se le pregunte **Trust this certificate?**, pulse **y**, a continuación **Intro**.
 - e. Asegúrese de que aparece el mensaje **Certificate was added to keystore**.
5. Exporte el certificado de servidor UCMDB de su almacén de claves.
- a. En el equipo donde está instalado UCMDB, ejecute el siguiente comando:
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore C:\HP\UCMDB\UCMDBServer\conf\security\server.keystore -file C:\HP\UCMDB\conf\security\server.cert
 - b. Introduzca la contraseña del almacén de confianza del servidor UCMDB (el valor predeterminado es **hppass**).
 - c. Compruebe que el certificado se crea en el siguiente directorio:
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
6. Importe el certificado de UCMDB exportado en el JRE del almacén de confianza del cliente UCMDB-API.
7. Reinicie el servidor UCMDB y el cliente UCMDB-API.
8. Para conectar del cliente UCMDB-API al servidor UCMDB-API, use el siguiente código:
- ```
UcmdbServiceProvider provider =
UcmdbServiceFactory.getServiceProvider("https", <SOME_HOST_NAME>,
<HTTPS_WITH_CLIENT_AUTH_PORT_NUMBER (default:8444)>);
UcmdbService ucmdbService = provider.connect
(provider.createCertificateCredentials(<TheClientKeystore. e.g:
"c:\\client.keystore">, <KeystorePassword>),
provider.createClientContext(<ClientIdentification>));
```

## Cambiar la contraseñas del almacén de claves del servidor

Después de instalar el servidor, se abre el puerto HTTPS y el almacén está protegido con una contraseña no segura (la contraseña predeterminada **hppass**). Si tiene previsto trabajar solamente con SSL, debe cambiar la contraseña.

A continuación se explica el procedimiento para cambiar únicamente la contraseña de **server.keystore**. Sin embargo, debe realizar el mismo procedimiento para cambiar la contraseña de **server.truststore**.

**Nota:** Debe realizar todos los pasos de este procedimiento.

1. Inicie el servidor UCMDB.
2. Ejecute el cambio de contraseña en la consola JMX.
  - a. Inicie el explorador web y especifique la dirección del servidor, del siguiente modo:  
**http://<Nombre de host del servidor UCMDB>:8080/jmx-console.**  
  
Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.
  - b. En UCMDB, haga clic en **UCMDB:service=Security Services** para abrir la página Operaciones.
  - c. Localice y ejecute la operación **changeKeystorePassword**.  
  
Este campo no debe estar vacío y debe tener al menos seis caracteres. La contraseña sólo se cambia en la base de datos.
3. Inicie el servidor UCMDB.
4. Ejecute los comandos.

Desde **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**, ejecute los siguientes comandos:

- a. Cambie la contraseña del almacén:  
  
**keytool -storepasswd -new <Nueva\_contraseña\_almacén\_de\_datos> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <contraseña\_actual\_almacén\_de\_datos>**
  - b. El siguiente comando muestra la clave interna del almacén de claves. El primer parámetro es el alias. Guarde este parámetro para el siguiente comando:  
  
**keytool -list -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**
  - c. Cambie la contraseña de clave (si el almacén no está vacío):  
  
**keytool -keypasswd -alias <alias> -keypass <contraseñaActual> -new <nuevaContraseña> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**
  - d. Escriba la contraseña nueva.
5. Inicie el servidor UCMDB.
  6. Repita el procedimiento para el almacén de confianza del servidor.

## Habilitar o deshabilitar puertos HTTP/HTTPS

Puede habilitar o deshabilitar los puertos HTTP y HTTPS desde la interfaz de usuario o desde la consola JMX.

**Para habilitar o deshabilitar los puertos HTTP/HTTPS desde la interfaz de usuario:**

1. Conéctese a HP Universal CMDB.
2. Seleccione **Administración > Configuración de infraestructura**.
3. Introduzca **http** o **https** en el cuadro **Filtro** (por Nombre) para mostrar la configuración de HTTP.
  - **Habilitar conexiones HTTP(S)**. **True**: el puerto está habilitado. **False**: el puerto está deshabilitado.
4. Reinicie el servidor para aplicar el cambio.

**Precaución:** el puerto HTTPS se abre de forma predeterminada; si se cierra este puerto se impide el funcionamiento de **Server\_Management.bat**.

#### Para habilitar o deshabilitar los puertos HTTP/HTTPS desde la consola JMX:

1. Inicie un explorador web y escriba la siguiente dirección: `http://localhost.<domain_name>:8080/jmx-console`.
2. Introduzca las credenciales de autenticación de la consola JMX, que de forma predeterminada son:
  - Nombre de inicio de sesión = **sysadmin**
  - Contraseña = **sysadmin**
3. Localice **UCMDB:service=Ports Management Services** y haga clic en el vínculo para abrir la página de operaciones.
4. Para habilitar o deshabilitar el puerto HTTP, localice la operación **HTTPSetEnable** y configure el valor.
  - **True**: el puerto está habilitado.
  - **False**: el puerto está deshabilitado.
5. Para habilitar o deshabilitar el puerto HTTPS, localice la operación **HTTPSSetEnable** y configure el valor.
  - **True**: el puerto está habilitado.
  - **False**: el puerto está deshabilitado.
6. Para habilitar o deshabilitar el puerto HTTPS con autenticación de cliente, localice la operación **HTTPSCClientAuthSetEnable** y configure el valor.
  - **True**: el puerto está habilitado.
  - **False**: el puerto está deshabilitado.

## Asignar los componentes web de UCMDB a los puertos

Puede configurar la asignación de cada componente de UCMDB a los puertos disponibles desde la consola JMX.

**Para ver las configuraciones de los componentes actuales:**

1. Inicie un explorador web y escriba la siguiente dirección: **http://localhost.<nombre de dominio>:8080/jmx-console**.
2. Introduzca las credenciales de autenticación de la consola JMX, que de forma predeterminada son:  
Nombre de inicio de sesión = **sysadmin**  
Contraseña = **sysadmin**
3. Localice **UCMDB:service=Ports Management Services** y haga clic en el vínculo para abrir la página de operaciones.
4. Localice el método **ComponentsConfigurations** y haga clic en **Invoke**.
5. En cada componente, se muestran los puertos válidos y los puertos asignados actualmente.

#### Para asignar los componentes:

1. Localice **UCMDB:service=Ports Management Services** y haga clic en el vínculo para abrir la página de operaciones.
2. Localice el método **mapComponentToConnectors**.
3. Introduzca un nombre de componente en el cuadro Value. Seleccione **True** o **False** en cada uno de los puertos según su selección. Haga clic en **Invoke**. El componente seleccionado se asigna a los puertos seleccionados. Para buscar los nombres de componentes, llame al método **serverComponentsNames**.
4. Repita el proceso en cada componente relevante.

#### Nota:

- Cada componente debe asignarse al menos a un puerto. Si no asigna un componente a ningún puerto, se asigna de forma predeterminada al puerto HTTP.
- Si asigna un componente al puerto HTTPS y al puerto HTTPS con autenticación de cliente, sólo se asigna la opción de autenticación de cliente (la otra opción es redundante en este caso).

También puede cambiar el valor asignado a cada uno de los puertos.

#### Para configurar los valores de los puertos:

1. Localice **UCMDB:service=Ports Management Services** y haga clic en el vínculo para abrir la página de operaciones.
2. Para configurar un valor en el puerto HTTP, localice el método **HTTPSetPort** e introduzca un valor en el cuadro **Value**. Haga clic en **Invoke**.
3. Para configurar un valor en el puerto HTTPS, localice el método **HTTPSSetPort** e introduzca un valor en el cuadro **Value**. Haga clic en **Invoke**.
4. Para configurar un valor en el puerto HTTPS con autenticación de cliente, localice el método **HTTPSCClientAuthSetPort** e introduzca un valor en el cuadro **Value**. Haga clic en **Invoke**.

## Configurar Configuration Manager para que funcione con UCMDB mediante SSL

Configuration Manager se puede configurar para que funcione con UCMDB utilizando Capa de sockets seguros (SSL). En UCMDB, el conector SSL del puerto 8443 está habilitado de forma predeterminada.

1. Diríjase a **<Directorio de instalación de UCMDB>\bin\jre\bin** y ejecute el siguiente comando:

```
keytool -export -alias hpcert -keystore <Dir. del servidor de UCMDB>
\conf\security\server.keystore -storepass hppass -file
<archivocertificado>
```

2. Copie el archivo de certificado en una ubicación temporal en el equipo de Configuration Manager local.
3. Realice una nueva instalación o vuelva a configurar una instalación existente de Configuration Manager. Para obtener instrucciones, consulte las secciones relevantes en la *HP Universal CMDB – Guía de implementación* interactiva.

En la pantalla de configuración de UCMDB, establezca el protocolo en HTTPS y elija el archivo de certificado que ha copiado en el paso 2.

Para configurar Configuration Manager para que funcione con otros productos (como equilibradores de carga) que usan SSL, importe el certificado de seguridad del producto en el almacén de confianza de Configuration Manager (almacén de confianza jre predeterminado), para lo que debe ejecutar el siguiente comando:

```
<CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias <alias>
-keystore <CM_JAVA_HOME>\lib\security\cacerts -storepass changeit
-file <archivocertificado>
```

## Habilitar el adaptador KPI de UCMDB para su uso con SSL

Puede configurar la información del adaptador KPI de UCMDB para que se envíe mediante Secure Sockets Layer (SSL).

1. Exporte el certificado de Configuration Manager:

```
<CM_JAVA_HOME>\bin\keytool -export -alias tomcat -keystore
<CM_JAVA_HOME>\lib\security\tomcat.keystore -storepass
<clave del almacén de datos> -file <nombre del archivo de
certificado>
```

2. Importe el certificado que ha exportado de Configuration Manager al almacén de confianza de UCMDB de la siguiente manera:

```
<Dir. del servidor de UCMDB>\bin\jre\bin keytool -import -
trustcacerts
-alias tomcat -keystore <Dir. del servidor de UCMDB>\bin\jre\lib
\security\cacerts -storepass changeit -file <archivocertificado>
```

3. Importe el certificado que ha exportado de Configuration Manager al almacén de confianza de la sonda de la siguiente manera:

- a. Abra el símbolo del sistema y ejecute el comando:

```
<DataFlowProbe dir>\bin\jre\bin\keytool.exe -import -v -keystore
<Dir. de DataFlowProbe>\conf\security\MAMTrustStoreExp.jks -file
<archivocertificado> -alias tomcat
```

- b. Escriba la contraseña del almacén de claves: logomania
- c. Cuando se le pregunte **Trust this certificate?**, pulse **y**, a continuación **Intro**.

Se muestra el siguiente mensaje:

**El certificado se agregó al almacén de claves.**

Para obtener más información sobre el sistema de protección de la sonda de Data Flow, consulte "Sistema de protección de la sonda de Data Flow" en la página 63

4. Reinicie UCMDB, la sonda de Data Flow y Configuration Manager.

## Configuración de la compatibilidad con SSL para el navegador de UCMDB

**Nota:** Las instrucciones que se proporcionan aquí son relevantes para el navegador de UCMDB, versión 1.7. Si está utilizando una versión posterior del navegador UCMDB que se haya actualizado por separado del resto del conjunto de productos UCMDB, consulte la sección acerca de la configuración de la compatibilidad con SSL en la publicación *UCMDB Browser Installation and Configuration Guide* para esa versión.

Para instalar y configurar la compatibilidad con SSL en Tomcat:

1. Cree un archivo de almacenamiento de claves para almacenar la clave privada del servidor y el certificado autofirmado ejecutando uno de los siguientes comandos:

- En Windows: **%JAVA\_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA**
- En Unix: **\$JAVA\_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA**

Para ambos comandos, use el valor de contraseña **changeit** (para todos los otros campos del cuadro de diálogo de la consola que se abre, puede usar cualquier valor).

2. Elimine los comentarios de la entrada **SSL HTTP/1.1 Connector** de **\$CATALINA\_BASE/conf/server.xml**, donde **\$CATALINA\_BASE** es el directorio en el que ha instalado Tomcat.

**Nota:** Para obtener una descripción completa de cómo configurar **server.xml** para utilizar SSL, consulte el sitio oficial de Apache Tomcat: <http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html>

3. Reinicie el servidor Tomcat.

Para utilizar el protocolo HTTPS para la conexión con el servidor UCMDB:

1. En **ucmdb\_browser\_config.xml**, asigne el valor **https** a la etiqueta **<protocol>** y asigne el valor de puerto HTTPS del servidor UCMDB (8443 de forma predeterminada) a la etiqueta **<port>**.
2. Descargue el certificado público del Servidor UCMDB en el equipo del navegador de UCMDB (si utiliza SSL en el Servidor UCMDB, el administrador de UCMDB puede proporcionarle este certificado) e impórtelo en el almacén de confianza **cacerts** del JRE que se va a conectar al servidor ejecutando el siguiente comando:

```
"%JAVA_HOME%\bin\keytool" -import -alias ucmdb -trustcacerts -file <UCMDB-Server-certificate-file> -keystore "%JAVA_HOME%\jre\lib\security\cacerts"
```

donde **<UCMDB-Server-certificate-file>** es la ruta de acceso completa al archivo de certificado público del Servidor UCMDB.

3. Reinicie el servidor Tomcat.

# Capítulo 3

---

## Utilización de un proxy inverso

Esta sección describe las ramificaciones de seguridad de un proxy inverso y contiene instrucciones para utilizar un proxy inverso con HP Universal CMDB y Configuration Manager. Se tratan los aspectos de seguridad de un proxy inverso, pero no otros aspectos como el almacenamiento en caché y el equilibrio de carga.

Este capítulo incluye:

|                                                                                                                |    |
|----------------------------------------------------------------------------------------------------------------|----|
| Información general del proxy inverso .....                                                                    | 34 |
| Aspectos de seguridad de la utilización de un servidor proxy inverso .....                                     | 35 |
| Configuración de un proxy inverso .....                                                                        | 36 |
| Conexión de la sonda de Data Flow por proxy inverso o equilibrador de carga mediante autenticación mutua ..... | 39 |

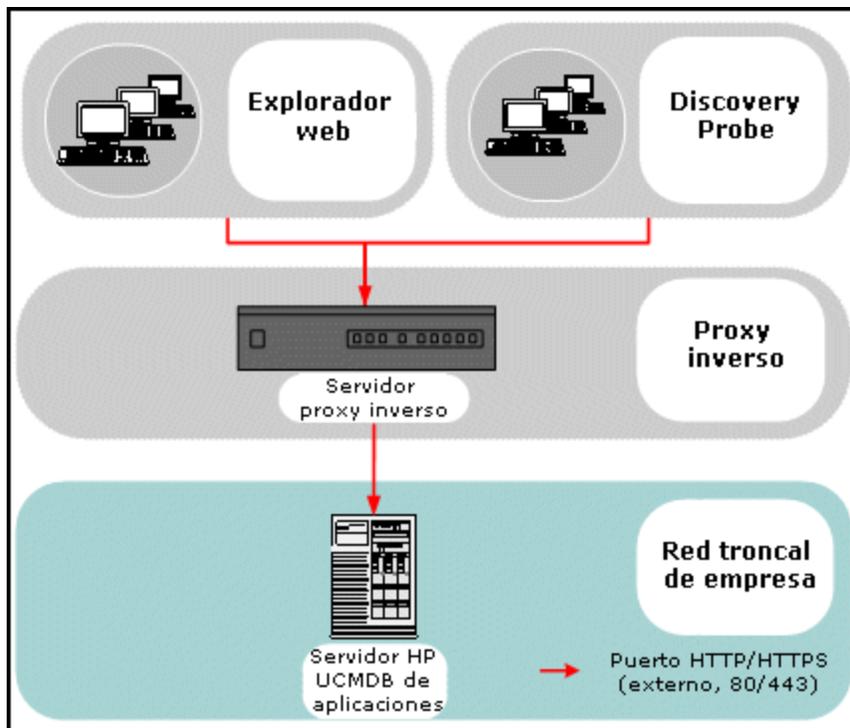
## Información general del proxy inverso

Un proxy inverso es un servidor intermedio que se encuentra entre el equipo cliente y los servidores web. En el equipo cliente, el proxy inverso aparece como un servidor web estándar que atiende las solicitudes de protocolo HTTP del equipo cliente.

El equipo cliente envía solicitudes normales de contenido web utilizando el nombre del proxy inverso en lugar del nombre de un servidor web. El proxy inverso envía la solicitud a uno de los servidores web. Aunque el proxy inverso es el que envía la respuesta al equipo cliente, éste percibe que ha sido enviada por el servidor web.

Se pueden tener varios proxies inversos, con diferentes direcciones URL, representando la misma instancia de UCMDB/CM. Como alternativa, se puede usar un solo servidor de proxy inverso para tener acceso a varios servidores de UCMDB/CM, estableciendo diferentes contextos de raíz para cada servidor de UCMDB/CM.

HP Universal CMDB y Configuration Manager admiten un proxy inverso en una arquitectura de DMZ. El proxy inverso es un mediador HTTP entre la sonda de Data Flow, el cliente web y el servidor de HP Universal CMDB/CM.



**Nota:**

- Los distintos tipos de proxy inverso requieren sintaxis de configuración diferentes. Para ver un ejemplo de una configuración de proxy inverso Apache 2.0.x, consulte " [Ejemplo: Configuración de Apache 2.0.x](#) " en la página 37.
- Solamente es necesario establecer la configuración de la dirección URL front-end cuando se crea un vínculo directo a un informe mediante el Planificador.

## Aspectos de seguridad de la utilización de un servidor proxy inverso

Un servidor proxy inverso funciona como un host defensivo. El proxy está configurado para ser el único equipo al que se dirigen directamente los clientes externos y, por lo tanto, oculta el resto de la red interna. El uso de un proxy inverso permite colocar el servidor de la aplicación en un equipo independiente en la red interna.

Esta sección trata sobre el uso de una red perimetral (DMZ) y un proxy inverso en un entorno de topología opuesta.

A continuación se exponen las principales ventajas de seguridad que supone el uso de un proxy inverso en dicho entorno:

- No se produce ninguna conversión de protocolos de DMZ. El protocolo de entrada y el protocolo de salida son idénticos (sólo se produce un cambio de encabezado).
- Sólo se permite el acceso HTTP al proxy inverso, lo que significa que los servidores de seguridad de inspección de paquetes con estado pueden proteger mejor la comunicación.

- Se puede definir en el proxy inverso un conjunto restringido y estático de solicitudes de redirección.
- La mayoría de las características de seguridad del servidor web están disponibles en el proxy inverso (métodos de autenticación, cifrado, etc.).
- El proxy inverso filtra las direcciones IP de los servidores reales, además de la arquitectura de la red interna.
- El único cliente accesible del servidor web es el proxy inverso.
- Esta configuración admite servidores de seguridad NAT (al contrario que otras soluciones).
- El proxy inverso requiere un número mínimo de puertos abiertos en el servidor de seguridad.
- El proxy inverso proporciona un buen rendimiento en comparación con otras soluciones defensivas.

## Configuración de un proxy inverso

Esta sección describe cómo configurar un proxy inverso.

### Configurar un proxy inverso mediante la configuración de infraestructura

A continuación se explica el procedimiento para acceder a la configuración de infraestructura para configurar un proxy inverso. Esta configuración solo es necesaria cuando se crea un vínculo directo con un informe mediante el Planificador.

#### Para configurar un proxy inverso:

1. Seleccione **Administración > Configuración de infraestructura > Configuración general**.
2. Cambie la configuración de URL del frontend. Introduzca la dirección; por ejemplo, **https://mi\_servidor\_proxy:443/**.

**Nota:** Tras realizar este cambio, no podrá acceder al servidor de HP Universal CMDB directamente a través de un cliente. Para cambiar la configuración del proxy inverso, utilice la consola JMX en el equipo servidor. Para obtener más información, consulte "[Configurar un proxy inverso mediante la consola JMX](#)" a continuación.

### Configurar un proxy inverso mediante la consola JMX

Puede realizar cambios en la configuración de proxy inverso mediante la consola JMX en el equipo servidor de HP Universal CMDB. Esta configuración solo es necesaria cuando se crea un vínculo directo con un informe mediante el Planificador.

#### Para cambiar la configuración de un proxy inverso:

1. En el equipo servidor de HP Universal CMDB, inicie el explorador web e introduzca la siguiente dirección:

**http://<nombre de equipo o dirección IP>.<nombre de dominio>:8080/jmx-console**

donde **<nombre de equipo o dirección IP>** es el equipo en el que está instalado HP Universal CMDB. Es posible que tenga que iniciar sesión con el nombre de usuario y la contraseña.

2. Haga clic en el vínculo **UCMDB-UI > UCMDB-UI:name=UI Server frontend settings**.

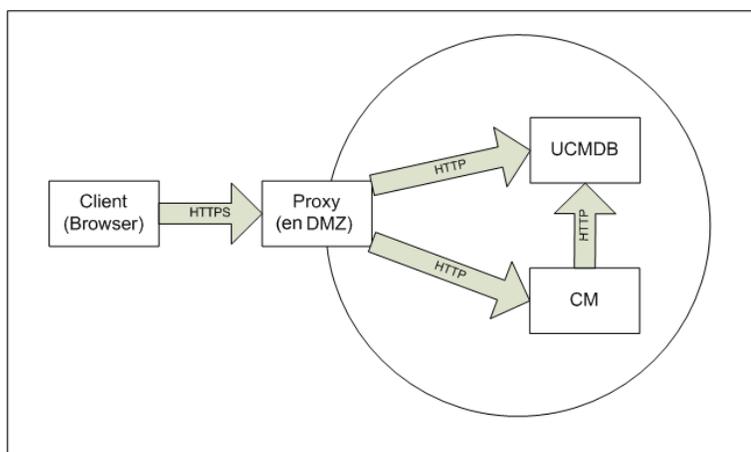
En el campo **setUseFrontendURLBySettings**, introduzca la dirección URL del servidor proxy; por ejemplo, `https://mi_servidor_proxy:443/`.

3. Haga clic en **Invoke**.
4. Para ver el valor de esta configuración, utilice el método **showFrontendURLInSettings**.

### Ejemplo: Configuración de Apache 2.0.x

Esta sección describe un ejemplo de archivo de configuración que admite el uso de un proxy inverso Apache 2.0.x cuando las sondas Data Flow y los usuarios de la aplicación se conectan a HP Universal CMDB.

El siguiente diagrama muestra el proceso de configuración de un proxy inverso para Configuration Manager y UCMDB.



#### Nota:

- En este ejemplo, el nombre DNS del equipo de HP Universal CMDB y el puerto es UCMDB\_server.
- En este ejemplo, el nombre DNS y el puerto de HP Configuration Manger es UCMDB\_CM\_server.
- Sólo deben realizar este cambio aquellos usuarios que tengan conocimientos de administración de Apache.

1. Abra el archivo `<directorio raíz del equipo Apache>\Webserver\conf\httpd.conf`.
2. Habilite los siguientes módulos:
  - **LoadModule proxy\_module modules/mod\_proxy.so**
  - **LoadModule proxy\_http\_module modules/mod\_proxy\_http.so**
  - **LoadModule headers\_module modules/mod\_headers.so**
3. Agregue las siguientes líneas al archivo `httpd.conf`:

```
ProxyRequests off

<Proxy *>
```

```
Order deny,allow

Deny from all

Allow from all

</Proxy>

ProxyPass /mam http://UCMDB_server/mam
ProxyPassReverse /mam http://UCMDB_server/mam

ProxyPass /mam_images http://UCMDB_server/mam_images
ProxyPassReverse /mam_images http://UCMDB_server/mam_images

ProxyPass /mam-collectors http://UCMDB_server/mam-collectors
ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors

ProxyPass /ucmdb http://UCMDB_server/ucmdb
ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb

ProxyPass /site http://UCMDB_server/site
ProxyPassReverse /site http://UCMDB_server/site

ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui

ProxyPass /status http://UCMDB_server/status
ProxyPassReverse /status http://UCMDB_server/status

ProxyPass /jmx-console http://UCMDB_server/jmx-console
ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console

ProxyPass /axis2 http://UCMDB_server/axis2
ProxyPassReverse /axis2 http://UCMDB_server/axis2

ProxyPass /icons http://UCMDB_server/icons
ProxyPassReverse /icons http://UCMDB_server/icons

ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api

ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs

ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0

ProxyPass /cm http://UCMDB_Server/cm
ProxyPassReverse /cm http://UCMDB_Server /cm

ProxyPass /cnc http://UCMDB_CM_server/cnc
```

```
ProxyPassReverse /cnc http://UCMDB_CM_server/cnc
ProxyPass /docs http://UCMDB_CM_server/docs
ProxyPassReverse /docs http://UCMDB_CM_server/docs
ProxyPass /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
ProxyPassReverse /ucmdb-browser http://UCMDB_CM_server/ucmdb-
browser
ProxyPreserveHost On
RequestHeader set X-Reverse-Proxy "https://<Host SRP>:<Puerto SRP>"
```

**Nota:** La línea `ProxyPreserveHost On` solo se necesita si hay un host virtual.

**Precaución:** Es esencial añadir la línea `RequestHeader set X-Reverse-Proxy "https://<Host SRP>:<Puerto SRP>"`. La configuración no funcionará sin ella.

4. Guarde los cambios.

## Conexión de la sonda de Data Flow por proxy inverso o equilibrador de carga mediante autenticación mutua

Siga este procedimiento para conectar la sonda de Data Flow mediante proxy inverso o equilibrador de carga usando autenticación mutua. Este procedimiento se aplica a la siguiente configuración:

- Autenticación SSL mutua entre la sonda y un proxy inverso o un equilibrador de carga basado en un certificado de cliente proporcionado por la sonda y requerido por el proxy inverso o el equilibrador de carga.
- Una conexión SSL regular entre el proxy inverso o el equilibrador de carga y el servidor de UCMDDB.

**Nota:** Las siguientes instrucciones utilizan el almacén de claves **cKeyStoreFile** como almacén de claves de la sonda. Es un almacén de claves del cliente predefinido que forma parte de la instalación de la sonda de Data Flow y contiene certificados autofirmados. Para obtener más información, consulte ["Almacén de claves y almacén de confianza predeterminados de servidor y sonda de Data Flow"](#) en la página 78.

Se recomienda crear un nuevo almacén de claves único que contenga una clave privada recién generada. Para obtener más información, consulte ["Crear un almacén de claves para la sonda de Data Flow"](#) en la página 77.

### Obtener un certificado de una entidad de certificación

Obtener el certificado raíz de la entidad de certificación e importarlo en las siguientes ubicaciones:

- almacén de confianza de la sonda de Data Flow
  - certificados de la entidad de certificación de JVM de la sonda de Data Flow
  - almacén de confianza del servidor de UCMDB
  - almacén de confianza del proxy inverso
1. Importe el certificado raíz de la entidad de certificación en el almacén de confianza de la sonda de Data Flow.

- a. Coloque el certificado raíz de la entidad de certificación en el siguiente directorio:  
<Directorio de instalación de la sonda de Data Flow>\conf\security\- b. Importe el certificado raíz de la entidad de certificación en el almacén de confianza de Data Flow ejecutando la siguiente secuencia de comandos:

```
<Directorio de instalación de la sonda de Data
Flow>\bin\jre\bin\keytool.exe -import -trustcacerts -alias
<SuAlias> -file C:\hp\UCMDB\DataFlowProbe\conf\security\del archivo de certificado> -keystore <Directorio de instalación
de la sonda de Data Flow>\conf\security\MAMTrustStoreExp.jks
```

La contraseña predeterminada es: **logomania**.

2. Importe el certificado raíz de la entidad de certificación en las entidades de certificación de JVM de la sonda de Data Flow ejecutando la siguiente secuencia de comandos:

```
<Directorio de instalación de la sonda de Data
Flow>\bin\jre\bin\keytool.exe -import -trustcacerts -alias
<SuAlias> -file <Directorio de instalación de la sonda de Data
Flow>\conf\security\<Directorio de instalación de la sonda de Data
Flow>\bin\jre\lib\security\cacerts
```

La contraseña predeterminada es: **changeit**.

3. Importe el certificado raíz de la entidad de certificación en el almacén de confianza de UCMDB.

- a. Coloque el certificado raíz de la entidad de certificación en el siguiente directorio:  
<Directorio de instalación de UCMDB>\conf\security\- b. Importe el certificado raíz de la entidad de certificación en el almacén de confianza de UCMDB ejecutando la siguiente secuencia de comandos:

```
<Directorio de instalación de UCMDB>\bin\jre\bin\keytool.exe -
import -trustcacerts -alias <YourAlias> -file <Directorio de
instalación de UCMDB>\conf\security\certificado> -keystore <Directorio de instalación de
UCMDB>\conf\security\sever.truststore
```

La contraseña predeterminada es: **hppass**.

4. Importe el certificado raíz de la entidad de certificación en el almacén de confianza de de proxy inverso. Este paso depende del servidor.

## Convertir el certificado en un almacén de claves Java

Obtenga el certificado del cliente (y la clave privada) para la sonda de Data Flow de la autoridad de certificación en el formato PFX/PKCS12 y conviértalo en un almacén de claves de Java ejecutando la siguiente secuencia de comandos:

```
<Directorio de instalación de la sonda de Data
Flow>\bin\jre\bin\keytool.exe -importkeystore -srckeystore <PFX
keystore full path> -destkeystore <ruta completa del nuevo almacén de
claves de destino> -srcstoretype PKCS12
```

Se le pedirá el origen de las contraseñas del almacén de claves de origen y destino.

Para la contraseña del almacén de datos de origen utilice la misma contraseña que se usó para exportar el almacén de datos de PFX.

La contraseña del almacén de claves de destino predeterminado para el almacén de datos de la sonda de Data Flow es: **logomania**.

**Nota:** Si ha especificado una contraseña del almacén de claves de destino diferente de la contraseña del almacén de claves de la sonda de Data Flow (logomania), deberá proporcionar la nueva clave en formato cifrado en el archivo **<Directorio de instalación de la sonda de Data Flow>\conf\ssl.properties** (javax.net.ssl.keyStorePassword). Para obtener más información, consulte "[Cifrar las contraseñas del almacén de claves y el almacén de confianza de la sonda](#)" en la página 77.

Coloque el nuevo almacén de claves en el siguiente directorio: **<Directorio de instalación de la sonda de Data Flow>\conf\security**.

**Precaución:** No sobrescriba el archivo **MAMKeyStoreExp.jks**.

## Cambiar el archivo de propiedades de SSL para usar el almacén de claves recién creado

Establezca el almacén de claves que contiene el certificado de cliente en el archivo **<Directorio de instalación de la sonda de Data Flow>\conf\ssl.properties** en **javax.net.ssl.keyStore**.

Si la contraseña de su almacén de claves no es la contraseña predeterminada del almacén de claves de la sonda de Data Flow (logomania), actualice **javax.net.ssl.keyStorePassword** tras cifrarlo. Para obtener más información sobre el cifrado de la contraseña, consulte "[Cifrar las contraseñas del almacén de claves y el almacén de confianza de la sonda](#)" en la página 77.

## Revisar la configuración de la sonda de Data Flow

Edite el archivo **<Directorio de instalación de la sonda de Data Flow>\conf\DataFlowProbe.properties** de la siguiente manera:

```
appilog.agent.probe.protocol = HTTPS
serverName = <dirección del servidor proxy inverso>
serverPortHttps = <el puerto HTTPS que el proxy inverso escucha para
redirigir solicitudes a UCMDB>
```

## **Configurar UCMDB para trabajar usando SSL**

Para obtener más información, consulte "[Habilitar la comunicación de Capa de sockets seguros \(SSL\)](#)" en la página 18.

Si se crea el certificado del servidor de UCMDB mediante la misma entidad de certificación que creó el resto de certificados de este procedimiento, el proxy inverso o el equilibrador de carga confía en el certificado de UCMDB.

# Capítulo 4

---

## administrar credenciales de Data Flow

Este capítulo incluye:

|                                                                                                                                                                      |    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Información general de la administración de credenciales de Data Flow .....                                                                                          | 44 |
| Suposiciones básicas de seguridad .....                                                                                                                              | 45 |
| Ejecución de la sonda de Data Flow en modo independiente .....                                                                                                       | 45 |
| Mantener la caché de credenciales actualizada .....                                                                                                                  | 46 |
| Sincronización de todas las sondas con cambios de configuración .....                                                                                                | 46 |
| Almacenamiento protegido en la sonda .....                                                                                                                           | 47 |
| Visualización de información de credenciales .....                                                                                                                   | 47 |
| Actualización de credenciales .....                                                                                                                                  | 47 |
| Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager ....                                                                      | 48 |
| Configuración de LW-SSO .....                                                                                                                                        | 48 |
| Configuración del cifrado de la comunicación de Confidential Manager .....                                                                                           | 48 |
| Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager<br>manualmente en la sonda .....                                          | 50 |
| Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del<br>cliente de Confidential Manager entre el servidor y las sondas ..... | 50 |
| Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager<br>en la sonda .....                                                      | 51 |
| Configurar el cifrado de la comunicación de Confidential Manager en la sonda .....                                                                                   | 51 |
| Configurar la caché del cliente de Confidential Manager .....                                                                                                        | 52 |
| Configurar el modo de caché del cliente de Confidential Manager en la sonda .....                                                                                    | 53 |
| Establecer la configuración de cifrado de caché del cliente de Confidential Manager en la<br>sonda .....                                                             | 53 |
| Exportar e importar la información de credenciales e intervalos en formato cifrado .....                                                                             | 54 |
| Cambiar el nivel de mensajes del archivo de registro del cliente de Confidential Manager .....                                                                       | 56 |
| Archivo de registro del cliente de Confidential Manager .....                                                                                                        | 56 |
| Archivo de registro de LW-SSO .....                                                                                                                                  | 56 |
| Generar o actualizar la clave de cifrado .....                                                                                                                       | 57 |
| Generar una nueva clave de cifrado .....                                                                                                                             | 58 |

|                                                                                                                                                    |    |
|----------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Actualizar una clave de cifrado en un servidor de UCMDB .....                                                                                      | 59 |
| Actualizar una clave de cifrado en una sonda .....                                                                                                 | 60 |
| Cambiar manualmente la clave de cifrado cuando Administrador de sonda y Puerta de enlace de sonda están instalados en equipos independientes ..... | 60 |
| Definir varios proveedores JCE .....                                                                                                               | 61 |
| Configuración de cifrado de Confidential Manager .....                                                                                             | 61 |
| Solución de problemas y limitaciones .....                                                                                                         | 62 |

## Información general de la administración de credenciales de Data Flow

Para realizar la detección o ejecutar la integración, debe configurar las credenciales de acceso al sistema remoto. Las credenciales se configuran en la ventana Configuración de la sonda de Data Flow y se guardan en el servidor de UCMDB. Para obtener más información, consulte la sección que describe la instalación de la sonda de Data Flow en la *HP Universal CMDB – Guía de Administración de Data Flow*.

El almacenamiento de credenciales se administra en el componente Confidential Manager. Para obtener más información, consulte "[Confidential Manager](#)" en la [página 92](#).

La sonda de Data Flow puede acceder a las credenciales mediante el cliente de Confidential Manager. El cliente de Confidential Manager reside en la sonda de Data Flow y se comunica con el servidor de Confidential Manager, que reside en el servidor de UCMDB. La comunicación entre el cliente de Confidential Manager y el servidor de Confidential Manager está cifrada y el cliente de Confidential Manager necesita autenticación cuando se conecta al servidor de Confidential Manager.

La autenticación del cliente de Confidential Manager en el servidor de Confidential Manager se basa en un componente de LW-SSO. Antes de conectarse al servidor de Confidential Manager, el cliente de Confidential Manager envía primero una cookie LW-SSO. El servidor de Confidential Manager comprueba la cookie y, si la comprobación es satisfactoria, se inicia la comunicación con el cliente de Confidential Manager. Para obtener más información sobre LW-SSO, consulte "[Configuración de LW-SSO](#)" en la [página 48](#).

La comunicación entre el cliente de Confidential Manager y el servidor de Confidential Manager está cifrada. Para obtener más información sobre la actualización de la configuración de cifrado, consulte "[Configuración del cifrado de la comunicación de Confidential Manager](#)" en la [página 48](#).

**Precaución:** La autenticación de Confidential Manager utiliza la hora universal definida en el equipo (UTC). Para que la autenticación sea correcta, asegúrese de que la hora universal de la sonda de Data Flow y el servidor de UCMDB sean la misma. El servidor y la sonda se pueden ubicar en zonas horarias diferentes, ya que UTC es independiente de la zona horaria o de la configuración del horario de verano.

El cliente de Confidential Manager mantiene una memoria caché local de las credenciales. El cliente de Confidential Manager está configurado para descargar todas las credenciales del

servidor de Confidential Manager y almacenarlas en una caché. Los cambios de credenciales se sincronizan automáticamente desde el servidor de Confidential Manager de forma continua. La caché puede ser un sistema de archivos o una caché en memoria, en función de la configuración predefinida. Además, la caché está cifrada y no es posible tener acceso a ella de forma externa. Para obtener más información sobre la actualización de la configuración de caché, consulte ["Configurar el modo de caché del cliente de Confidential Manager en la sonda"](#) en la página 53. Para obtener más información sobre el cifrado de caché, consulte ["Establecer la configuración de cifrado de caché del cliente de Confidential Manager en la sonda"](#) en la página 53.

Para obtener más información sobre la solución de problemas, consulte ["Cambiar el nivel de mensajes del archivo de registro del cliente de Confidential Manager"](#) en la página 56.

Puede copiar la información de credenciales de un servidor UCMDDB a otro. Para obtener más información, consulte ["Exportar e importar la información de credenciales e intervalos en formato cifrado"](#) en la página 54.

**Nota:** El archivo **DomainScopeDocument** (DSD) que se usaba para almacenar las credenciales en la sonda (en UCMDDB versión 9.01 o anterior) ya no contiene ninguna información confidencial sobre credenciales. Ahora el archivo contiene una lista de sondas e información del intervalo de red. También contiene una lista de entradas de credenciales para cada dominio, donde cada entrada incluye únicamente el Id. de credencial y el intervalo de red (definido para esta entrada de credencial).

Esta sección incluye los siguientes temas:

- ["Suposiciones básicas de seguridad"](#) abajo
- ["Ejecución de la sonda de Data Flow en modo independiente"](#) abajo
- ["Mantener la caché de credenciales actualizada"](#) en la página siguiente
- ["Sincronización de todas las sondas con cambios de configuración"](#) en la página siguiente
- ["Almacenamiento protegido en la sonda"](#) en la página 47

## Suposiciones básicas de seguridad

Tenga en cuenta la siguiente suposición de seguridad:

Ha protegido el servidor UCMDDB y la consola JMX de la sonda para permitir el acceso sólo a los administradores del sistema UCMDDB únicamente.

## Ejecución de la sonda de Data Flow en modo independiente

Cuando Puerta de enlace de sonda y Administrador de sonda se ejecutan como procesos independientes, el componente Confidential Manager cliente pasa a formar parte del proceso Administrador. La información de credenciales está almacenada en la caché y sólo la usa el Administrador de sonda. Para acceder al servidor de Confidential Manager en el sistema UCMDDB, la solicitud del cliente de Confidential Manager la gestiona el proceso de la Puerta de enlace y desde ahí se reenvía al sistema UCMDDB.

Esta configuración es automática cuando se configura la sonda en modo independiente.

## Mantener la caché de credenciales actualizada

La primera vez que se conecta correctamente al servidor de Confidential Manager, el cliente de Confidential Manager descarga todas las credenciales relevantes (todas las credenciales configuradas en el dominio de la sonda). Una vez que se ha establecido la primera comunicación satisfactoria, el cliente de Confidential Manager mantiene una sincronización continua con el servidor de Confidential Manager. La sincronización diferencial tiene lugar en intervalos de un minuto y sólo se sincronizan las diferencias entre el servidor de Confidential Manager y el cliente de Confidential Manager. Si se cambian las credenciales en el lado del servidor de UCMDB (por ejemplo, porque se agregan nuevas credenciales o se actualizan o eliminan las credenciales existentes), el cliente de Confidential Manager recibe una notificación inmediata del servidor de UCMDB y realiza una sincronización adicional.

## Sincronización de todas las sondas con cambios de configuración

Para que la comunicación se realice correctamente, el cliente de Confidential Manager debe tener actualizada la configuración de autenticación del servidor de Confidential Manager (cadena init de LW-SSO) y la configuración de cifrado (cifrado de comunicación de Confidential Manager). Por ejemplo, si se cambia la cadena init en el servidor, la sonda debe conocer la nueva cadena init para poder realizar la autenticación.

El servidor de UCMDB monitoriza constantemente los cambios en la configuración de cifrado de comunicación de Confidential Manager y en la configuración de autenticación de Confidential Manager. Esta monitorización se realiza cada 15 segundos; si se ha producido algún cambio, se envía la configuración actualizada a las sondas. La configuración se pasa a las sondas de forma cifrada y se almacena en la sonda en un almacenamiento protegido. El cifrado de la configuración que se envía se realiza mediante una clave de cifrado simétrico. De forma predeterminada, el servidor de UCMDB y la sonda de Data Flow se instalan con la misma clave de cifrado simétrico predeterminada. Para una seguridad óptima, es muy recomendable cambiar esta clave antes de agregar credenciales al sistema. Para obtener más información, consulte "[Generar o actualizar la clave de cifrado](#)" en la página 57.

**Nota:** Debido al intervalo de monitorización de 15 segundos, es posible que el cliente de Confidential Manager en la sonda no esté actualizado con la configuración más reciente durante 15 segundos.

Si elige deshabilitar la sincronización automática de la configuración de comunicación y autenticación de Confidential Manager entre el servidor de UCMDB y la sonda de Data Flow, cada vez que actualice la configuración de comunicación y autenticación de Confidential Manager en el servidor de UCMDB, también debería actualizar todas las sondas con la nueva configuración. Para obtener más información, consulte "[Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas](#)" en la página 50.

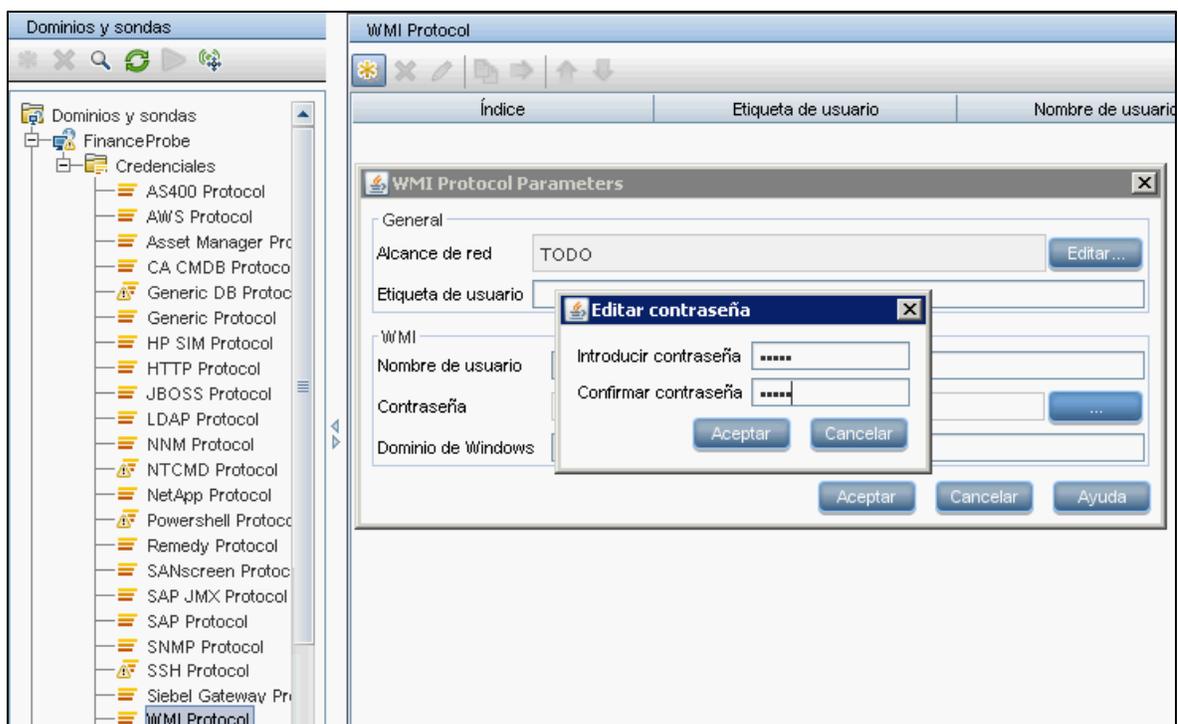
## Almacenamiento protegido en la sonda

Toda la información confidencial (por ejemplo, la configuración de comunicación y autenticación de Confidential Manager y la clave de cifrado) se almacena en la sonda en el archivo **secured\_storage.bin** de almacenamiento protegido, que está ubicado en **C:\hpl\UCMDB\DataFlowProbe\conf\security**. Este almacenamiento protegido se cifra mediante DPAPI, que se basa en la contraseña de usuario de Windows en el proceso de cifrado. DPAPI es un método estándar que se usa para proteger datos confidenciales, como certificados y claves privadas, en sistemas Windows. La sonda debería ejecutarse siempre con el mismo usuario de Windows para que, en caso de que cambie la contraseña, la sonda pueda seguir leyendo la información almacenada en almacenamiento protegido.

## Visualización de información de credenciales

**Nota:** En esta sección se explica la visualización de información de credenciales cuando la dirección de datos es desde CMDB hasta HP Universal CMDB

Las contraseñas no se envían desde CMDB hasta la aplicación. Es decir, HP Universal CMDB muestra asteriscos (\*) en el campo de contraseña, independientemente del contenido:



## Actualización de credenciales

**Nota:** En esta sección se explica la actualización de credenciales cuando la dirección de los datos es desde HP Universal CMDB hasta CMDB.

- La comunicación que se realiza en este sentido no está cifrada, de manera que debería conectarse al servidor de UCMDDB mediante https\SSL, o asegurarse de que la conexión se realice a través de una red de confianza.

Aunque no se cifre la comunicación, las contraseñas no se envían como texto legible en la red. Se cifran mediante una clave predeterminada, por lo que es muy recomendable utilizar SSL para garantizar la confidencialidad durante la comunicación.

- Es posible utilizar caracteres especiales y caracteres que no sean del idioma inglés en las contraseñas.

## Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager

Esta tarea describe la configuración de los parámetros de cifrado y la autenticación de cliente de Confidential Manager en el Servidor de UCMDDB e incluye los siguientes pasos:

- "Configuración de LW-SSO" abajo
- "Configuración del cifrado de la comunicación de Confidential Manager" abajo

### Configuración de LW-SSO

Este procedimiento describe cómo cambiar la cadena init de LW-SSO en el servidor de UCMDDB. Este cambio se envía automáticamente a las sondas (como una cadena cifrada), a menos que la configuración del servidor UCMDDB establezca que no se realice esta acción de forma automática. Para obtener más información, consulte "[Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas](#)" en la página 50.

1. En el servidor UCMDDB inicie el explorador web e introduzca la siguiente dirección:  
**http://localhost:8080/jmx-console.**
2. Haga clic en **UCMDDB-UI:name=LW-SSO Configuration** para abrir la página JMX MBEAN View.
3. Localice el método **setInitString**.
4. Introduzca una nueva cadena init de LW-SSO.
5. Haga clic en Invoke.

### Configuración del cifrado de la comunicación de Confidential Manager

Este procedimiento describe cómo cambiar la configuración de cifrado de Confidential Manager en el Servidor de UCMDDB. Esta configuración especifica el cifrado de la comunicación entre el cliente de Confidential Manager y el servidor de Confidential Manager. Este cambio se envía automáticamente a las sondas (como una cadena cifrada), a menos que la configuración del servidor UCMDDB establezca que no se realice esta acción de forma automática. Para obtener más información, consulte "[Deshabilitar la sincronización automática de la configuración de](#)

autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas" en la página 50.

1. En el servidor UCMDDB inicie el explorador web e introduzca la siguiente dirección:  
**http://localhost:8080/jmx-console.**
2. Haga clic en **UCMDDB:service=Security Services** para abrir la página JMX MBean View.
3. Haga clic en el método **CMGetConfiguration**.
4. Haga clic en **Invoke**.

Se muestra el archivo XML de la configuración de Confidential Manager actual.

5. Copie el contenido del archivo XML visualizado.
6. Regrese a la página JMX MBean View de **Security Services**.
7. Haga clic en el método **CMSetConfiguration**.
8. Pegue el XML copiado en el campo **Value**.
9. Actualice la configuración relevante relacionada con el transporte.

Para obtener más información sobre los valores que pueden actualizarse, consulte "[Configuración de cifrado de Confidential Manager](#)" en la página 61.

**Ejemplo:**

```
<transport>
 <encryptTransportMode>true</encryptTransportMode>
 <CMEncryptionDecryption>
 <encryptDecryptInitString>radiohead</encryptDecryptInitString>
 <cryptoSource>lw</cryptoSource>
 <lwJCEPBCompatibilityMode>true</lwJCEPBCompatibilityMode>
 <cipherType>symmetricBlockCipher</cipherType>
 <engineName>AES</engineName>
 <algorithmModeName>CBC</algorithmModeName>
 <algorithmPaddingName>PKCS7Padding</algorithmPaddingName>
 <keySize>256</keySize>
 <pbeCount>20</pbeCount>
 <pbeDigestAlgorithm>SHA1</pbeDigestAlgorithm>
 <encodingMode>Base64Url</encodingMode>
 <useMacWithCrypto>false</useMacWithCrypto>
 <macType>hmac</macType>
 <macKeySize>256</macKeySize>
 <macHashName>SHA256</macHashName>
 </CMEncryptionDecryption>
</transport>
```

```
</CMEncryptionDecryption>
```

```
</transport>
```

10. Haga clic en **Invoke**.

## Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager manualmente en la sonda

Esta tarea incluye los siguientes pasos:

- "Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas" abajo
- "Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager en la sonda" en la página siguiente
- "Configurar el cifrado de la comunicación de Confidential Manager en la sonda" en la página siguiente

## Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas

De forma predeterminada, el servidor UCMDDB está configurado para enviar automáticamente la configuración de Confidential Manager/LW-SSO a todas las sondas. Esta información se envía como una cadena cifrada a las sondas, que descifran la información en cuanto la reciben. Puede configurar el servidor UCMDDB para que no envíe automáticamente los archivos de configuración de Confidential Manager/LW-SSO a todas las sondas. En tal caso, es responsabilidad del usuario actualizar manualmente todas las sondas con la nueva configuración de CM/LW-SSO.

Para deshabilitar la sincronización automática de la configuración de Confidential Manager/LW-SSO:

1. En UCMDDB, haga clic en **Administración > Administrador de configuración de infraestructura > Configuración general**.
2. Seleccione **Habilitar sincronización automática de la configuración de CM/LW-SSO y cadena init con sonda**.
3. Haga clic en el campo **Valor** y cambie **Verdadero** por **Falso**.
4. Haga clic en el botón **Save**.
5. Reinicie el servidor de UCMDDB.

## Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager en la sonda

Este procedimiento es importante si la configuración del servidor de UCMDDB establece que no se envíe automáticamente a las sondas la configuración de LW-SSO/Confidential Manager. Para obtener más información, consulte "Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas" en la página precedente.

1. En el equipo donde está instalada la sonda, inicie el explorador web e introduzca la siguiente dirección: **http://localhost:1977**.

**Nota:** Si Administrador de sonda y Puerta de enlace de sonda se están ejecutando como procesos independientes, debe introducirse la dirección en el equipo que ejecuta el Administrador de sonda, del siguiente modo: **http://localhost:1978**.

2. Haga clic en **type=CMClient** para abrir la página JMX MBEAN View.
3. Localice el método **setLWSSOInitString** y proporcione la misma cadena init que se proporcionó en la configuración de LW-SSO de UCMDDB.
4. Haga clic en el botón **setLWSSOInitString**.

## Configurar el cifrado de la comunicación de Confidential Manager en la sonda

Este procedimiento es importante si la configuración del servidor UCMDDB establece que no se envíe automáticamente a las sondas la configuración de LW-SSO/Confidential Manager. Para obtener más información, consulte "Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas" en la página precedente.

1. En el equipo donde está instalada la sonda, inicie el explorador web e introduzca la siguiente dirección: **http://localhost:1977**.

**Nota:** Si Administrador de sonda y Puerta de enlace de sonda se están ejecutando como procesos independientes, debe introducirse la dirección en el equipo que ejecuta el Administrador de sonda, del siguiente modo: **http://localhost:1978**.

2. Haga clic en **type=CMClient** para abrir la página JMX MBEAN View.
3. Actualice la siguiente configuración relacionada con el transporte:

**Nota:** Debe actualizar la misma configuración que actualizó en el servidor UCMDDB. Para ello, es posible que algunos de los métodos que actualice en la sonda requieran más de un

parámetro. Para ver la configuración de sonda actual, haga clic en **displayTransportConfiguration** en la página JMX MBEAN View. Para obtener más información, consulte "Configuración del cifrado de la comunicación de Confidential Manager" en la página 48. Para obtener más información sobre los valores que pueden actualizarse, consulte "Configuración de cifrado de Confidential Manager" en la página 61.

- a. **setTransportInitString** cambia la configuración de **encryptDecryptInitString**.
  - b. **setTransportEncryptionAlgorithm** cambia la configuración de Confidential Manager en la sonda según el siguiente mapa:
    - o **Engine name** hace referencia a la entrada <engineName>
    - o **Key size** hace referencia a la entrada <keySize>
    - o **Algorithm padding name** hace referencia a la entrada <algorithmPaddingName>
    - o **PBE count** hace referencia a la entrada <pbeCount>
    - o **PBE digest algorithm** hace referencia a la entrada <pbeDigestAlgorithm>
  - c. **setTransportEncryptionLibrary** cambia la configuración de Confidential Manager en la sonda según el siguiente mapa:
    - o **Encryption Library name** hace referencia a la entrada <cryptoSource>
    - o **Support previous lightweight cryptography versions** hace referencia a la entrada <lwJCEPBCECompatibilityMode>
  - d. **setTransportMacDetails** cambia la configuración de Confidential Manager en la sonda según el siguiente mapa:
    - o **Use MAC with cryptography** hace referencia a la entrada <useMacWithCrypto>
    - o **MAC key size** hace referencia a la entrada <macKeySize>
4. Haga clic en el botón **reloadTransportConfiguration** para que los cambios surtan efecto en la sonda.

Para obtener más información sobre las distintas opciones de configuración y sus posibles valores, consulte "Configuración de cifrado de Confidential Manager" en la página 61.

## Configurar la caché del cliente de Confidential Manager

Esta tarea incluye los siguientes pasos:

- "Configurar el modo de caché del cliente de Confidential Manager en la sonda" en la página siguiente
- "Establecer la configuración de cifrado de caché del cliente de Confidential Manager en la sonda" en la página siguiente

## Configurar el modo de caché del cliente de Confidential Manager en la sonda

El cliente de Confidential Manager almacena la información de credenciales en la caché y la actualiza cuando la información cambia en el servidor. La caché puede almacenarse en el sistema de archivos o en la memoria:

- **Cuando se almacena en el sistema de archivos**, incluso si se reinicia la sonda y no puede conectarse al servidor, la información de credenciales sigue estando disponible.
- **Cuando se almacena en la memoria**, si se reinicia la sonda, se borra la caché y toda la información se recupera nuevamente del servidor. Si el servidor no está disponible, la sonda no incluye ninguna credencial, por lo que no se puede ejecutar ninguna detección o integración.

Para cambiar esta configuración:

1. Abra el archivo **DataFlowProbe.properties** en un editor de texto. El archivo está ubicado en la carpeta **c:\hp\UCMDB\DataFlowProbe\conf**.
2. Localice el siguiente atributo:  
**com.hp.ucmdb.discovery.common.security.storeCMDData=true**
  - Para almacenar la información en el sistema de archivos, deje el valor predeterminado (**true**).
  - Para almacenar la información en la memoria, introduzca **false**.
3. Guarde el archivo **DataFlowProbe.properties**.
4. Reinicie la sonda.

## Establecer la configuración de cifrado de caché del cliente de Confidential Manager en la sonda

Este procedimiento describe cómo cambiar la configuración de cifrado del archivo de caché del sistema de archivos del cliente de Confidential Manager. Tenga en cuenta que, al cambiar la configuración de cifrado de la caché del sistema de archivos del cliente de Confidential Manager, se vuelve a crear el archivo de caché del sistema de archivos. Este proceso de recreación requiere que se reinicie la sonda y se sincronice completamente con el servidor UCMDB.

1. En el equipo donde está instalada la sonda, inicie el explorador web e introduzca la siguiente dirección: **http://localhost:1977**.

**Nota:** Si Administrador de sonda y Puerta de enlace de sonda se están ejecutando como procesos independientes, debe introducirse la dirección en el equipo que ejecuta el Administrador de sonda, del siguiente modo: **http://localhost:1978**.

2. Haga clic en **type=CMClient** para abrir la página JMX MBEAN View.
3. Actualice la siguiente configuración relacionada con la caché:

**Nota:** Es posible que algunos de los métodos que actualice en la sonda requieran más de un parámetro. Para ver la configuración de sonda actual, haga clic en **displayCacheConfiguration** en la página JMX MBEAN View.

- a. **setCacheInitString** cambia la configuración de <encryptDecryptInitString> en la caché del sistema de archivos.
  - b. **setCacheEncryptionAlgorithm** cambia la configuración de caché del sistema de archivos según el siguiente mapa:
    - **Engine name** hace referencia a la entrada <engineName>
    - **Key size** hace referencia a la entrada <keySize>
    - **Algorithm padding name** hace referencia a la entrada <algorithmPaddingName>
    - **PBE count** hace referencia a la entrada <pbeCount>
    - **PBE digest algorithm** hace referencia a la entrada <pbeDigestAlgorithm>
  - c. **setCacheEncryptionLibrary** cambia la configuración de caché del sistema de archivos según el siguiente mapa:
    - **Encryption Library name** hace referencia a la entrada <cryptoSource>
    - **Support previous lightweight cryptography versions** hace referencia a la entrada <lwJCEPBCompatibilityMode>
  - d. **setCacheMacDetails** cambia la configuración de caché del sistema de archivos según el siguiente mapa:
    - **Use MAC with cryptography** hace referencia a la entrada <useMacWithCrypto>
    - **MAC key size** hace referencia a la entrada <macKeySize>
4. Haga clic en el botón **reloadCacheConfiguration** para que los cambios surtan efecto en la sonda. Esto provoca el reinicio de la sonda.

**Nota:** Asegúrese de que no haya ningún trabajo en ejecución en la sonda durante esta acción.

Para obtener más información sobre las distintas opciones de configuración y sus posibles valores, consulte "Configuración de cifrado de Confidential Manager" en la página 61.

## Exportar e importar la información de credenciales e intervalos en formato cifrado

Puede exportar e importar la información de credenciales e intervalos de red en formato cifrado para copiar la información de credenciales de un servidor de UCMDB a otro. Por ejemplo, podría realizar esta operación durante la recuperación tras un bloqueo del sistema o durante la actualización.

- **Al exportar la información de credenciales**, debe introducir una contraseña (de su elección). La información de esta contraseña está cifrada.

- **Al importar la información de credenciales**, debe usar la misma contraseña que se definió al exportar el archivo DSD.

**Nota:** El documento de credenciales exportado también contiene la información de intervalos definida en el sistema del que se exportó el documento. Durante la importación del documento de credenciales, también se importa la información de intervalos.

**Precaución:** Para importar la información de credenciales de un archivo domainScopeDocument de UCMDB versión 8.02, debe usar el archivo key.bin que se encuentra en el sistema de la versión 8.02.

#### Para exportar la información de credenciales del servidor de UCMDB:

1. En el servidor de UCMDB inicie el explorador web e introduzca la siguiente dirección:  
**http://localhost:8080/jmx-console**. Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.
2. Haga clic en **UCMDB:service=DiscoveryManager** para abrir la página JMX MBEAN View.
3. Localice la operación **exportCredentialsAndRangesInformation**. Realice lo siguiente:
  - Introduzca el Id. de cliente (el valor predeterminado es 1).
  - Introduzca un nombre para el archivo exportado.
  - Escriba la contraseña.
  - Establezca **isEncrypted=True** si desea cifrar el archivo exportado con la contraseña proporcionada o **isEncrypted=False** si no desea cifrar el archivo exportado (en cuyo caso no se exportan las contraseñas ni ninguna otra información confidencial).
4. Haga clic en **Invoke** para exportar.

Cuando el proceso de exportación finaliza de forma satisfactoria, el archivo se guarda en la ubicación siguiente: **c:\hp\UCMDB\UCMDBServer\conf\discovery\.**

#### Para importar la información de credenciales del servidor de UCMDB:

1. En el servidor de UCMDB inicie el explorador web e introduzca la siguiente dirección:  
**http://localhost:8080/jmx-console**.  
Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.
2. Haga clic en **UCMDB:service=DiscoveryManager** para abrir la página JMX MBEAN View.
3. Localice una de las siguientes operaciones:
  - Localice la operación **importCredentialsAndRangesInformation** si el archivo que está importando se exportó de un servidor de UCMDB de una versión posterior a la 8.02.
  - Localice la operación **importCredentialsAndRangesWithKey** si el archivo que está importando se exportó de un servidor UCMDB de la versión 8.02.
4. Introduzca el Id. de cliente (el valor predeterminado es 1).
5. Introduzca el nombre del archivo que se va a importar. Este archivo debe estar ubicado en la carpeta **c:\hp\UCMDB\UCMDBServer\conf\discovery\.**

6. Escriba la contraseña. Debe ser la misma contraseña que la que se usó al exportar el archivo.
7. Si el archivo se exportó de un sistema UCMDB de la versión 8.02, introduzca el nombre de archivo **key.bin**. Este archivo debe estar ubicado en el directorio **c:\hp\UCMDB\UCMDBServer\confdiscovery\<customer\_dir>**, junto con el archivo que se va a importar.
8. Haga clic en **Invoke** para importar las credenciales.

## Cambiar el nivel de mensajes del archivo de registro del cliente de Confidential Manager

La sonda proporciona dos archivos de registro que contienen información relativa a la comunicación relacionada con Confidential Manager entre el servidor de Confidential Manager y el cliente de Confidential Manager. Estos archivos son:

- "Archivo de registro del cliente de Confidential Manager" abajo
- "Archivo de registro de LW-SSO" abajo

## Archivo de registro del cliente de Confidential Manager

El archivo **security.cm.log** está ubicado en la carpeta **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

El registro contiene mensajes de información que intercambian el servidor de Confidential Manager y el cliente de Confidential Manager. De forma predeterminada, el nivel de registro de estos mensajes está establecido en INFO.

### Para cambiar el nivel de registro de los mensajes al nivel DEBUG:

1. En el servidor del administrador de la sonda de Data Flow, vaya a **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Abra el archivo **security.properties** en un editor de texto.
3. Cambie la línea:

```
loglevel.cm=INFO
```

por:

```
loglevel.cm=DEBUG
```

4. Guarde el archivo.

## Archivo de registro de LW-SSO

El archivo **security.lwssso.log** está ubicado en la carpeta **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

El registro contiene mensajes de información relacionados con LW-SSO. De forma predeterminada, el nivel de registro de estos mensajes está establecido en INFO.

**Para cambiar el nivel de registro de los mensajes al nivel DEBUG:**

1. En el servidor del administrador de la sonda de Data Flow, vaya a **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Abra el archivo `security.properties` en un editor de texto.
3. Cambie la línea:

```
loglevel.lwssso=INFO
```

por:

```
loglevel.lwssso=DEBUG
```

4. Guarde el archivo.

## Generar o actualizar la clave de cifrado

Puede generar o actualizar una clave de cifrado que se usará para cifrar o descifrar las configuraciones de comunicación y autenticación de Confidential Manager que intercambian el servidor de UCMDDB y la sonda de Data Flow. Tanto en la generación como en la actualización, el servidor UCMDDB crea una nueva clave de cifrado a partir de los parámetros suministrados (por ejemplo, longitud de clave, ciclos PBE adicionales, proveedor JCE) y la distribuye a las sondas.

La ejecución del método **generateEncryptionKey** da como resultado la generación de una nueva clave de cifrado. Esta clave sólo se almacena en almacenamiento protegido y se desconocen tanto su nombre como sus detalles. Si vuelve a instalar una sonda Data Flow existente o conecta una nueva sonda al servidor de UCMDDB, la nueva sonda no reconoce esta nueva clave generada. En tales casos, es preferible utilizar el método **changeEncryptionKey** para cambiar las claves de cifrado. De este modo, si se vuelve a instalar una sonda o se instala una nueva, se puede importar la clave existente (cuyo nombre y ubicación son conocidos) ejecutando el método **importEncryptionKey** en la consola JMX de la sonda.

**Nota:**

- La diferencia entre los métodos que se usan para crear una clave (**generateEncryptionKey**) y actualizar una clave (**changeEncryptionKey**) es que **generateEncryptionKey** crea una clave de cifrado nueva y aleatoria, mientras que **changeEncryptionKey** importa una clave de cifrado cuyo nombre proporciona el usuario.
- Sólo puede haber una clave de cifrado en un sistema, independientemente del número de sondas instaladas.

Esta tarea incluye los siguientes pasos:

- ["Generar una nueva clave de cifrado"](#) en la página siguiente
- ["Actualizar una clave de cifrado en un servidor de UCMDDB"](#) en la página 59
- ["Actualizar una clave de cifrado en una sonda"](#) en la página 60
- ["Cambiar manualmente la clave de cifrado cuando Administrador de sonda y Puerta de enlace de sonda están instalados en equipos independientes"](#) en la página 60
- ["Definir varios proveedores JCE"](#) en la página 61

## Generar una nueva clave de cifrado

Puede generar una nueva clave que el servidor UCMDDB y la sonda de Data Flow usarán para cifrar o descifrar. El servidor UCMDDB reemplaza la clave antigua por la nueva clave generada y la distribuye entre las sondas.

### Para generar una nueva clave de cifrado mediante la consola JMX:

1. En el servidor UCMDDB inicie el explorador web e introduzca la siguiente dirección:  
**http://localhost:8080/jmx-console.**  
  
Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.
2. Haga clic en **UCMDDB:service=DiscoveryManager** para abrir la página JMX MBEAN View.
3. Localice la operación generateEncryptionKey.
  - a. En el cuadro del parámetro **customerIid**, escriba 1 (el valor predeterminado).
  - b. En **keySize**, especifique la longitud de la clave de cifrado. Los valores válidos son 128, 192 ó 256.
  - c. En **usePBE**, especifique **True** o **False**:
    - **True**: usar ciclos hash PBE adicionales.
    - **False**: no usar ciclos hash PBE adicionales.
  - d. En **jceVendor**, puede optar por utilizar un proveedor JCE no predeterminado. Si el cuadro está vacío, se utiliza el proveedor predeterminado.
  - e. En **autoUpdateProbe**, especifique **True** o **False**:
    - **True**: el servidor distribuye la nueva clave a las sondas automáticamente.
    - **False**: la nueva clave debe colocarse en las sondas manualmente.
  - f. En **exportEncryptionKey**, especifique **True** o **False**.
    - **True**: además de crear la nueva contraseña y almacenarla en almacenamiento seguro, el servidor exporta la contraseña nueva al sistema de archivos (c:\hp\UCMDDB\UCMDDBServer\conf\discovery\key.bin). Esta opción le permite actualizar manualmente las sondas con la nueva contraseña.
    - **False**: la nueva contraseña no se exporta al sistema de archivos. Para actualizar las sondas manualmente, establezca **autoUpdateProbe** en False y **exportEncryptionKey** en True.

**Nota:** Asegúrese de que la sonda está funcionando y conectada al servidor. Si la sonda deja de funcionar, la clave no puede llegar a la sonda. Si cambia la clave antes de que la sonda deje de funcionar, cuando vuelva a estar en funcionamiento, la clave se enviará de nuevo a la sonda. Sin embargo, si cambia la clave más de una vez antes de que la sonda deje de funcionar, debe cambiar la

clave manualmente a través de la consola JMX. (Seleccione **False** en **exportEncryptionKey**).

4. Haga clic en **Invoke** para generar la clave de cifrado.

## Actualizar una clave de cifrado en un servidor de UCMDB

El método **changeEncryptionKey** se utiliza para importar la propia clave de cifrado en el servidor de UCMDB y distribuirla entre todas las sondas.

**Para actualizar una clave de cifrado a través de la consola JMX:**

1. En el servidor de UCMDB inicie el explorador web e introduzca la siguiente dirección:  
**http://localhost:8080/jmx-console.**

Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

2. Haga clic en **UCMDB:service=DiscoveryManager** para abrir la página JMX MBEAN View.
3. Localice la operación **changeEncryptionKey**.
  - a. En el cuadro del parámetro **customerId**, escriba **1** (el valor predeterminado).
  - b. En **newKeyFileName**, escriba el nombre de la nueva clave.
  - c. En **keySizeInBits**, especifique la longitud de la clave de cifrado. Los valores válidos son 128, 192 ó 256.
  - d. En **usePBE**, especifique **True** o **False**:
    - **True**: usar ciclos hash PBE adicionales.
    - **False**: no usar ciclos hash PBE adicionales.
  - e. En **jceVendor**, puede optar por utilizar un proveedor JCE no predeterminado. Si el cuadro está vacío, se utiliza el proveedor predeterminado.
  - f. En **autoUpdateProbe**, especifique **True** o **False**:
    - **True**: el servidor distribuye la nueva clave a las sondas automáticamente.
    - **False**: la nueva clave debe distribuirse manualmente mediante la consola JMX de la sonda.

**Nota:** Asegúrese de que la sonda está funcionando y conectada al servidor. Si la sonda deja de funcionar, la clave no puede llegar a la sonda. Si cambia la clave antes de que la sonda deje de funcionar, cuando vuelva a estar en funcionamiento, la clave se enviará de nuevo a la sonda. Sin embargo, si cambia la clave más de una vez antes de que la sonda deje de funcionar, debe cambiar la

clave manualmente a través de la consola JMX. (Seleccione **False** en **autoUpdateProbe**).

4. Haga clic en **Invoke** para generar y actualizar la clave de cifrado.

## Actualizar una clave de cifrado en una sonda

Si opta por no distribuir una clave de cifrado del servidor de UCMDDB a todas las sondas automáticamente porque le preocupa la seguridad, debe descargar la nueva clave de cifrado en todas las sondas y ejecutar el método **importEncryptionKey** en la sonda:

1. Coloque el archivo de clave de cifrado en el directorio **C:\hp\UCMDB\DataFlowProbelconfsecurity\**.
2. En el equipo donde está instalada la sonda, inicie el explorador web e introduzca la siguiente dirección: **http://localhost:1977**.

Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

**Nota:** Si Administrador de sonda y Puerta de enlace de sonda se están ejecutando como procesos independientes, debe introducirse la dirección en el equipo que ejecuta el Administrador de sonda, del siguiente modo: **http://localhost:1978**.

3. En el dominio Sonda, haga clic en **type=SecurityManagerService**.
4. Localice el método **importEncryptionKey**.
5. Escriba el nombre del archivo de clave de cifrado ubicado en **C:\hp\UCMDB\DataFlowProbelconfsecurity\**. Este archivo contiene la clave que se va a importar.
6. Haga clic en el botón **importEncryptionKey**.
7. Realice un reinicio de la sonda.

## Cambiar manualmente la clave de cifrado cuando Administrador de sonda y Puerta de enlace de sonda están instalados en equipos independientes

1. En el equipo donde está instalado Administrador de sonda, inicie el servicio Administrador de sonda (**Inicio > Programas > HP UCMDDB > Administrador de sonda**).
2. Importe la clave del servidor mediante la consola JMX de Administrador de sonda. Para obtener más información, consulte "Generar una nueva clave de cifrado" en la página 58.
3. Tras importar la clave de cifrado correctamente, reinicie los servicios Administrador de sonda y Puerta de enlace de sonda.

## Definir varios proveedores JCE

Cuando se genera una clave de cifrado mediante la consola JMX, se pueden definir varios proveedores JCE mediante los métodos **changeEncryptionKey** y **generateEncryptionKey**.

**Para cambiar el proveedor JCE predeterminado:**

1. Registre los archivos jar del proveedor JCE en **\$JRE\_HOME/lib/ext**.
2. Copie los archivos jar en la carpeta **\$JRE\_HOME**:
  - En el servidor de UCMDB: **\$JRE\_HOME** reside en: **c:\hp\UCMDB\UCMDBServer\bin\jre**
  - En la sonda de Data Flow: **\$JRE\_HOME** reside en: **c:\hp\UCMDB\DataFlowProbe\bin\jre**
3. Agregue la clase de proveedor al final de la lista de proveedores en el archivo **\$JRE\_HOME\lib\security\java.security**.
4. Actualice los archivos **local\_policy.jar** y **US\_export\_policy.jar** para incluir directivas JCE ilimitadas. Puede descargar estos archivos jar del sitio web de Sun.
5. Reinicie el servidor de UCMDB y la sonda de Data Flow.
6. Localice el campo de proveedor JCE en el método **changeEncryptionKey** o **generateEncryptionKey** y agregue el nombre del proveedor JCE.

## Configuración de cifrado de Confidential Manager

Esta tabla contiene una lista de la configuración de cifrado que puede cambiarse mediante diversos métodos de JMX. Esta configuración de cifrado es importante para cifrar las comunicaciones entre el cliente de Confidential Manager y el servidor de Confidential Manager y para cifrar la caché del cliente de Confidential Manager.

Nombre de config. de Confidential Manager	Nombre de config. de Confidential Manager de la sonda	Descripción de la configuración	Valores posibles	Valor predet.
cryptoSource	Encryption Library name	Esta configuración define la biblioteca de cifrado que se va a usar.	lw, jce, windowsDPAPI, lwJCECompatible	lw
lwJCEPBE Compatibilidad Modo	Support previous lightweight cryptography versions	Esta configuración define si se admite la criptografía ligera anterior o no.	true, false	true

Nombre de config. de Confidential Manager	Nombre de config. de Confidential Manager de la sonda	Descripción de la configuración	Valores posibles	Valor predet.
engineName	Engine name	Nombre del mecanismo de cifrado	AES, DES, 3DES, Blowfish	AES
keySize	Key size	Longitud de la clave de cifrado en bits	En AES: 128, 192 ó 256; En DES - 64; En 3DES - 192; En Blowfish: cualquier número entre 32 y 448	256
algoritmo Relleno Nombre	Algorithm padding name	Estándares de relleno	PKCS7Padding, PKCS5Padding	PKCS7Padding
pbeCount	PBE count	Número de veces que hay que ejecutar el hash para crear la clave a partir de la contraseña (cadena init)	Cualquier número positivo	20
pbeDigest Algoritmo	PBE digest algorithm	Tipo de hash	SHA1, SHA256, MD5	SHA1
useMacWith Crypto	Use MAC with cryptography	Indicación sobre el uso de MAC con la criptografía	true, false	false
macKeySize	MAC key size	Depende del algoritmo MAC	256	256

## Solución de problemas y limitaciones

Si cambia el nombre de dominio predeterminado en el servidor UCMDDB, en primer lugar debe verificar que la sonda de Data Flow no está en ejecución. Tras aplicar el nombre de dominio predeterminado, debe ejecutar la secuencia de comandos

**DataFlowProbe\tools\clearProbeData.bat** en la sonda de Data Flow.

**Nota:** La ejecución de la secuencia de comandos clearProbeData.bat causará un ciclo de detección en la sonda una vez que esta esté activa.

## Capítulo 5

---

# Sistema de protección de la sonda de Data Flow

Este capítulo incluye:

Modificar la contraseña cifrada de la base de datos MySQL .....	63
Secuencia de comandos clearProbeData.bat: Uso .....	65
Configurar la contraseña cifrada de la consola JMX .....	65
Configurar la contraseña de UpLoadScanFile .....	66
Acceso remoto a MySQL Server .....	67
Habilitar SSL entre el servidor UCMDB y la sonda de Data Flow con autenticación mutua ....	68
Información general .....	68
Almacenes de claves y almacenes de confianza .....	68
Habilitar SSL con la autenticación de servidor (unidireccional) .....	69
Habilitar autenticación mutua de certificados (bidireccional) .....	71
Controlar la ubicación del archivo domainScopeDocument .....	76
Crear un almacén de claves para la sonda de Data Flow .....	77
Cifrar las contraseñas del almacén de claves y el almacén de confianza de la sonda .....	77
Almacén de claves y almacén de confianza predeterminados de servidor y sonda de Data Flow .....	78
Servidor UCMDB .....	78
La sonda de Data Flow .....	78

## Modificar la contraseña cifrada de la base de datos MySQL

Esta sección explica cómo modificar la contraseña cifrada para el usuario de la base de datos MySQL.

1. Crear el formato cifrado de una contraseña (AES, clave de 192 bits)
  - a. Acceda a la consola JMX de la sonda de Data Flow. Inicie un explorador web y escriba la siguiente dirección: **http://<nombre de equipo o dirección IP de la sonda de Data Flow>:1977**. Si ejecuta la sonda de Data Flow de forma local, introduzca

<http://localhost:1977>.

Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

**Nota:** Si no ha creado un usuario, utilice el nombre de usuario predeterminado `sysadmin` y la contraseña `sysadmin` para iniciar sesión.

- b. Localice el servicio **Type=MainProbe** y haga clic en el vínculo para abrir la página de operaciones.
- c. Localice la operación **getEncryptedDBPassword**.
- d. En el campo **DB Password**, introduzca la contraseña que hay que cifrar.
- e. Llame a la operación haciendo clic en el botón **getEncryptedDBPassword**.

El resultado de la llamada es una cadena de contraseña cifrada como, por ejemplo:

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
```

## 2. Detener la sonda de Data Flow

Inicio > Todos los programas > HP UCMDB > Detener la sonda de Data Flow

## 3. Ejecutar la secuencia de comandos `set_dbuser_password.cmd`

Esta secuencia de comandos está ubicada en la carpeta siguiente:

**C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\set\_dbuser\_password.cmd**

Ejecute la secuencia de comandos **set\_dbuser\_password.cmd** con la nueva contraseña como primer argumento y la contraseña de la cuenta raíz de MySQL como segundo argumento (o vacío si la cuenta raíz de MySQL no está protegida con una contraseña).

Por ejemplo:

**set\_dbuser\_password <mi\_contraseña><contraseña\_raíz>**.

La contraseña debe introducirse sin cifrar (como texto sin formato).

## 4. Actualizar la contraseña en los archivos de configuración de la sonda de Data Flow

- a. La contraseña debe estar cifrada en los archivos de configuración. Para recuperar el formato cifrado de la contraseña, utilice el método **getEncryptedDBPassword** de JMX, como se explica en el paso 1.
- b. Agregue la contraseña cifrada a las siguientes propiedades del archivo **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

- o **appilog.agent.probe.jdbc.pwd**

Por ejemplo:

```
appilog.agent.probe.jdbc.user = mamprobe
appilog.agent.probe.jdbc.pwd =
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
```

- `appilog.agent.local.jdbc.pwd`
- `appilog.agent.normalization.jdbc.pwd`

5. Iniciar la sonda de Data Flow

**Inicio > Todos los programas > HP UCMDB > Iniciar la sonda de Data Flow.**

## Secuencia de comandos `clearProbeData.bat`: Uso

La secuencia de comandos `clearProbeData.bat` recrea el usuario de la base de datos sin alterar su contraseña actual.

La secuencia de comandos espera recibir la contraseña de la cuenta raíz de MySQL como primer argumento. Si no se transfieren parámetros, presupone que la contraseña de la cuenta raíz de MySQL está vacía.

**Después de ejecutar la secuencia de comandos:**

- Revise el siguiente archivo para ver si hay errores:  
`C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log`
- Elimine el siguiente archivo, ya que contiene la contraseña de la base de datos:  
`C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log`

## Configurar la contraseña cifrada de la consola JMX

Esta sección explica cómo cifrar la contraseña para el usuario de JMX. La contraseña cifrada se almacena en el archivo `DataFlowProbe.properties`. Los usuarios deben iniciar sesión para acceder a la consola JMX.

### 1. Crear el formato cifrado de una contraseña (AES, clave de 192 bits)

- Acceda a la consola JMX de la sonda de Data Flow. Inicie un explorador web y escriba la siguiente dirección: **`http://<nombre de equipo o dirección IP de la sonda de Data Flow>:1977`**. Si ejecuta la sonda de Data Flow de forma local, introduzca **`http://localhost:1977`**.

Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

**Nota:** Si no ha creado un usuario, utilice el nombre de usuario predeterminado `sysadmin` y la contraseña `sysadmin` para iniciar sesión.

- Localice el servicio **Type=MainProbe** y haga clic en el vínculo para abrir la página de operaciones.
- Localice la operación **getEncryptedKeyPassword**.
- En el campo **Key Password**, introduzca la contraseña que hay que cifrar.
- Llame a la operación haciendo clic en el botón **getEncryptedKeyPassword**.

El resultado de la llamada es una cadena de contraseña cifrada como, por ejemplo:

```
85, -9, -61, 11, 105, -93, -81, 118
```

## 2. Detener la sonda de Data Flow

Inicio > Todos los programas > HP UCMDB > Detener la sonda de Data Flow

## 3. Agregar la contraseña cifrada

Agregue la contraseña cifrada a la siguiente propiedad del archivo

**C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties.**

**appilog.agent.Probe.JMX.BasicAuth.Pwd**

Por ejemplo:

```
appilog.agent.Probe.JMX.BasicAuth.User=sysadmin
appilog.agent.Probe.JMX.BasicAuth.Pwd=12, -35, -37, 82, -2, 20, 57, -40,
38, 80, -111, -99, -64, -5, 35, -122
```

**Nota:** Para deshabilitar la autenticación, deje estos campos en blanco. De esta forma, los usuarios podrán abrir la página principal de la consola JMX de la sonda sin necesidad de autenticación.

## 4. Iniciar la sonda de Data Flow

Inicio > Todos los programas > HP UCMDB > Iniciar la sonda de Data Flow

Pruebe el resultado en un explorador web.

# Configurar la contraseña de UploadScanFile

Esta sección explica cómo configurar la contraseña para **UploadScanFile**, utilizada para guardar la exploración de forma remota. La contraseña cifrada se almacena en el archivo

**DataFlowProbe.properties**. Los usuarios deben iniciar sesión para acceder a la consola JMX.

### 1. Crear el formato cifrado de una contraseña (AES, clave de 192 bits)

- Acceda a la consola JMX de la sonda de Data Flow. Inicie un explorador web y escriba la siguiente dirección: **http://<nombre de equipo o dirección IP de la sonda de Data Flow>:1977**. Si ejecuta la sonda de Data Flow de forma local, introduzca **http://localhost:1977**.

Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

**Nota:** Si no ha creado un usuario, utilice el nombre de usuario predeterminado **sysadmin** y la contraseña **sysadmin** para iniciar sesión.

- Localice el servicio **Type=MainProbe** y haga clic en el vínculo para abrir la página de operaciones.
- Localice la operación **getEncryptedKeyPassword**.
- En el campo **Key Password**, introduzca la contraseña que hay que cifrar.

- e. Llame a la operación haciendo clic en el botón **getEncryptedKeyPassword**.

El resultado de la llamada es una cadena de contraseña cifrada como, por ejemplo:

```
85,-9,-61,11,105,-93,-81,118
```

## 2. Detener la sonda de Data Flow

**Inicio > Todos los programas > HP UCMDB > Detener la sonda de Data Flow**

## 3. Agregar la contraseña cifrada

Agregue la contraseña cifrada a la siguiente propiedad del archivo

**C:\hp\UCMDB\DataFlowProbelconf\DataFlowProbe.properties.**

**appilog.agent.Probe.JMX.BasicAuth.Pwd**

Por ejemplo:

```
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.User=UploadScanFile
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd=116,116,21,34,-59,
77,-108,14,127,4,-89,101,-33,-31,116,53
```

## 4. Iniciar la sonda de Data Flow

**Inicio > Todos los programas > HP UCMDB > Iniciar la sonda de Data Flow**

Pruebe el resultado en un explorador web.

# Acceso remoto a MySQL Server

Esta sección explica cómo permitir/restringir el acceso a la cuenta de la sonda de Data Flow de MySQL desde equipos remotos.

### Nota:

- De forma predeterminada, el acceso está restringido.
- No puede acceder a la cuenta raíz de MySQL desde equipos remotos.

### Para permitir el acceso a MySQL:

1. Ejecute la siguiente secuencia de comandos en una ventana del símbolo del sistema:  
**C:\hp\UCMDB\DataFlowProbeltools\dbscripts\enable\_remote\_user\_access.cmd**
2. Cuando se le solicite, especifique la contraseña de la cuenta raíz de MySQL como primer argumento. (Esta contraseña es la misma que la contraseña introducida durante la instalación de la sonda).

### Para restringir el acceso a MySQL:

1. Ejecute la siguiente secuencia de comandos en una ventana del símbolo del sistema:  
**C:\hp\UCMDB\DataFlowProbeltools\dbscripts\remove\_remote\_user\_access.cmd**
2. Cuando se le solicite, especifique la contraseña de la cuenta raíz de MySQL como primer argumento. (Esta contraseña es la misma que la contraseña introducida durante la instalación de la sonda).

# Habilitar SSL entre el servidor UCMDB y la sonda de Data Flow con autenticación mutua

Puede configurar la autenticación en la sonda de Data Flow y el servidor UCMDB con certificados. El certificado de cada componente se envía y se autentica antes de establecer la conexión.

**Nota:** El siguiente método, que consiste en habilitar SSL en la sonda de Data Flow con autenticación mutua, es el más seguro de los métodos y, por lo tanto, es el modo de comunicación recomendado. Este método reemplaza el procedimiento de autenticación básica.

Esta sección incluye los siguientes temas:

- "Información general" abajo
- "Almacenes de claves y almacenes de confianza" abajo
- "Habilitar SSL con la autenticación de servidor (unidireccional)" en la página siguiente
- "Habilitar autenticación mutua de certificados (bidireccional)" en la página 71

## Información general

UCMDB admite los siguientes modos de comunicación entre el servidor UCMDB y la sonda de Data Flow:

- **Autenticación del servidor.** Este modo utiliza SSL y la sonda autentica el certificado del servidor UCMDB. Para obtener más información, consulte "[Habilitar SSL con la autenticación de servidor \(unidireccional\)](#)" en la página siguiente.
- **Autenticación mutua.** Este modo utiliza SSL y permite tanto la autenticación del servidor por parte de la sonda como la autenticación de cliente por parte del servidor. Para obtener más información, consulte "[Habilitar autenticación mutua de certificados \(bidireccional\)](#)" en la página 71.
- **HTTP estándar.** Sin comunicación SSL. Es el modo predeterminado y el componente de la sonda de Data Flow de UCMDB no requiere ningún certificado. La sonda de Data Flow se comunica con el servidor a través del protocolo HTTP estándar.

**Nota:** La detección no puede utilizar cadenas de certificados cuando trabaja con SSL. Por lo tanto, si está utilizando cadenas de certificados, debe generar un certificado autofirmado para que la sonda de Data Flow pueda comunicarse con el Servidor de UCMDB.

## Almacenes de claves y almacenes de confianza

El servidor UCMDB y la sonda de Data Flow utilizan almacenes de claves y almacenes de confianza:

- **Almacén de claves.** Un archivo que contiene entradas de claves (un certificado y su correspondiente clave privada).
- **Almacén de confianza.** Un archivo que contiene certificados que se utilizan para comprobar un host remoto (por ejemplo, cuando se usa la autenticación de servidor, el almacén de confianza de la sonda de Data Flow debería incluir el certificado del servidor UCMDDB).

#### Limitación de la autenticación mutua

El almacén de claves de la sonda de Data Flow (como se define en **C:\HP\UCMDDB\DataFlowProbe\confsecurity\ssl.properties**) debe contener 1 (una) sola entrada de clave.

## Habilitar SSL con la autenticación de servidor (unidireccional)

Se utiliza SSL y la sonda autentica el certificado del servidor.

Esta tarea incluye:

- "Requisitos previos" abajo
- "Configuración del servidor UCMDDB" abajo
- "Configuración de la sonda de Data Flow" en la página 71
- "Reiniciar los equipos" en la página 71

### Requisitos previos

1. Compruebe que UCMDDB y la sonda de Data Flow se estén ejecutando.

**Nota:** Si la sonda está instalada en modo independiente, estas instrucciones hacen referencia a Puerta de enlace de sonda.

2. Si UCMDDB o la sonda de Data Flow no están instalados en las carpetas predeterminadas, tenga en cuenta la ubicación correcta y cambie los comandos como corresponda.

### Configuración del servidor UCMDDB

1. **Exportar el certificado de UCMDDB**

- a. Abra el símbolo del sistema y ejecute el comando:

```
C:\HP\UCMDDB\UCMDDBServer\bin\jre\bin\keytool.exe -export -alias
<alias de almacén de claves> -keystore <ruta de acceso de
archivo de almacén de claves> -file
C:\HP\UCMDDB\UCMDDBServer\conf\security\server.cert
```

donde:

- **alias de almacén de claves** es el nombre dado al almacén de claves.
- **Ruta de acceso de archivo de almacén de claves** es la ruta de acceso completa de la ubicación del archivo de almacén de claves.

Por ejemplo, para el archivo `server.keystore` listo para su uso, utilice el comando siguiente:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
```

- b. Escriba la contraseña del almacén de claves. Por ejemplo, la contraseña del almacén de claves listo para su uso es **hppass**.
- c. Compruebe que el certificado se creó en el siguiente directorio:  
**C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

## 2. Proteja el conector de la sonda de Data Flow en UCMDB

- a. Acceda a la consola JMX de UCMDB: En el navegador web, introduzca la siguiente dirección URL: **http://<nombre de equipo o dirección IP de UCMDB>:8080/jmx-console**. Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.
- b. Seleccione el servicio: **Servicios de administración de puertos**.
- c. Invoque el método **PortsDetails** y anote el número de puerto para HTTPS. (Valor predeterminado: 8443) Asegúrese de que el valor de la columna **Is Enabled** es **True**.
- d. Vuelva a **Servicios de administración de puertos**.
- e. Para asignar el conector de la sonda de Data Flow al modo de autenticación de servidor, invoque el método **mapComponentToConnectors** con los siguientes parámetros:
  - o **componentName**: mam-collectors
  - o **isHTTPS**: true
  - o **Todos los demás indicadores**: false

Se muestra el siguiente mensaje:

```
Operation succeeded. Component mam-collectors is now mapped to: Puertos HTTPS.
```

- f. Vuelva a **Servicios de administración de puertos**.
- g. Para asignar el conector de Confidential Manager al modo de autenticación de servidor, invoque el método **mapComponentToConnectors** con los siguientes parámetros:
  - o **componentName**: cm
  - o **isHTTPS**: true
  - o **Todos los demás indicadores**: false

Se muestra el siguiente mensaje:

```
Operation succeeded. Component cm is now mapped to: HTTPS ports.
```

### 3. Copie el certificado de UCMDB a cada equipo de sonda

Copie el archivo de certificado, **C:\HP\UCMDB\UCMDBServer\confsecurity\server.cert**, en el equipo de UCMDB Server a la carpeta siguiente en cada uno de los equipos de sonda de Data Flow **C:\HP\UCMDB\DataFlowProbe\confsecurity\**

## Configuración de la sonda de Data Flow

**Nota:** Debe configurar cada equipo de sonda de Data Flow.

### 1. Importe el archivo **server.cert**, creado en "Exportar el certificado de UCMDB " en la página 69, al almacén de confianza de la sonda.

- a. Abra el símbolo del sistema y ejecute el comando:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -
keystore
C:\HP\UCMDB\DataFlowProbe\conf\security\MAMTrustStoreExp.jks -
file C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -alias
ucmdbcert
```

- b. Escriba la contraseña del almacén de claves: **logomania**
- c. Cuando se le pregunte **Trust this certificate?**, pulse **y**, a continuación **Intro**.

Se muestra el siguiente mensaje:

**El certificado se agregó al almacén de claves.**

### 2. Abra el archivo **DiscoveryProbe.properties** que se encuentra en: **C:\HP\UCMDB\DataFlowProbe\conf\**

- a. Actualice la propiedad **appilog.agent.probe.protocol** a **HTTPS**.
- b. Actualice la propiedad **serverPortHttps** al número de puerto relevante. (Utilice el número de puerto del paso 2c de "Configuración del servidor UCMDB" en la página 69.)

## Reiniciar los equipos

Reinicie el servidor UCMDB y los equipos de sonda.

# Habilitar autenticación mutua de certificados (bidireccional)

Este modo utiliza SSL y permite tanto la autenticación del servidor por parte de la sonda como la autenticación de cliente por parte del servidor. Tanto el servidor como la sonda envían sus certificados a la otra entidad para su autenticación.

Esta tarea incluye:

- "Requisitos previos" en la página siguiente
- "Configuración del servidor UCMDB inicial" en la página siguiente

- "Configuración de la sonda de Data Flow" en la página siguiente
- "Configuración adicional del servidor UCMDB" en la página 75
- "Reiniciar los equipos" en la página 76

### Requisitos previos

1. Compruebe que UCMDB y la sonda de Data Flow se estén ejecutando.

**Nota:** Si la sonda está instalada en modo independiente, estas instrucciones hacen referencia a Puerta de enlace de sonda.

2. Si UCMDB o la sonda de Data Flow no están instalados en las carpetas predeterminadas, tenga en cuenta la ubicación correcta y cambie los comandos como corresponda.

### Configuración del servidor UCMDB inicial

#### 1. Exportar el certificado de UCMDB

- a. Abra el símbolo del sistema y ejecute el comando:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias
<alias de almacén de claves> -keystore <ruta de acceso de
archivo de almacén de claves> -file
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
```

donde:

- **alias de almacén de claves** es el nombre dado al almacén de claves.
- **Ruta de acceso de archivo de almacén de claves** es la ruta de acceso completa de la ubicación del archivo de almacén de claves.

Por ejemplo, para el archivo server.keystore listo para su uso, utilice el comando siguiente:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -
alias hpcert -keystore
C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
```

- b. Escriba la contraseña del almacén de claves. Por ejemplo, la contraseña del almacén de claves listo para su uso es **hpass**.
- c. Compruebe que el certificado se creó en el siguiente directorio:  
**C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

#### 2. Proteja el conector de la sonda de Data Flow en UCMDB

- a. Acceda a la consola JMX de UCMDB: En el navegador web, introduzca la siguiente dirección URL: **http://<nombre de equipo o dirección IP de UCMDB>:8080/jmx-console**. Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.
- b. Seleccione el servicio: **Servicios de administración de puertos**.

- c. Invoque el método **PortsDetails** y anote el número de puerto para HTTPS con la autenticación del cliente. (Valor predeterminado: 8444) Asegúrese de que el valor de la columna **Is Enabled** es **True**.
- d. Vuelva a **Servicios de administración de puertos**.
- e. Para asignar el conector de la sonda de Data Flow al modo de autenticación mutua, invoque el método **mapComponentToConnectors** con los siguientes parámetros:
  - o **componentName**: mam-collectors
  - o **isHTTPSWithClientAuth**: true
  - o **Todos los demás indicadores**: false

Se muestra el siguiente mensaje:

```
Operation succeeded. Component mam-collectors is now mapped to: HTTPS_CLIENT_AUTH ports.
```

- f. Vuelva a **Servicios de administración de puertos**.
- g. Para asignar el conector de Confidential Manager al modo de autenticación mutua, invoque el método **mapComponentToConnectors** con los siguientes parámetros:
  - o **componentName**: cm
  - o **isHTTPSWithClientAuth**: true
  - o **Todos los demás indicadores**: false

Se muestra el siguiente mensaje:

```
Operation succeeded. Component cm is now mapped to: HTTPS_CLIENT_AUTH ports.
```

### 3. Copie el certificado de UC MDB a cada equipo de sonda

Copie el archivo de certificado, **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**, en el equipo de UC MDB Server a la carpeta siguiente en cada uno de los equipos de sonda de Data Flow: **C:\HP\UCMDB\DataFlowProbe\conf\security\**

## Configuración de la sonda de Data Flow

**Nota:** Debe configurar cada equipo de sonda de Data Flow.

1. **Importe el archivo server.cert, creado en "Exportar el certificado de UC MDB " en la página precedente, al almacén de confianza de la sonda.**
  - a. Abra el símbolo del sistema y ejecute el comando:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore
C:\HP\UCMDB\DataFlowProbe\conf\security\MAMTrustStoreExp.jks -file C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -alias ucmbcert
```

- b. Escriba la contraseña del almacén de claves: logomania
- c. Cuando se le pregunte **Trust this certificate?**, pulse **y**, a continuación **Intro**.

Se muestra el siguiente mensaje:

**El certificado se agregó al almacén de claves.**

## 2. Crear un nuevo archivo `client.keystore`

- a. Abra el símbolo del sistema y ejecute el comando:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool -genkey -alias
<NombreSonda> -keyalg RSA -keystore
C:\HP\UCMDB\DataFlowProbe\conf\security\client.keystore
```

donde **NombreSonda** es el alias único de la sonda de Data Flow.

**Nota:** Para asegurarse de que este alias es único, utilice el identificador del nombre de sonda que se dio a la sonda al definirla.

- b. Introduzca la contraseña del almacén de claves, de 6 caracteres como mínimo, y tome nota de la misma.
- c. Vuelva a introducir la contraseña para confirmarla.
- d. Pulse **Intro** para responder a cada una de las preguntas siguientes:

**¿Cuáles son su nombre y sus apellidos? [Desconocido]:**

**¿Cuál es el nombre de su unidad organizativa? [Desconocido]:**

**¿Cuál es el nombre de su organización? [Desconocido]:**

**¿Cuál es el nombre de su ciudad o localidad? [Desconocido]:**

**¿Cuál es el nombre de su estado o provincia? [Desconocido]:**

**¿Cuál es el código de dos letras de esta unidad? [Desconocido]:**

- e. Escriba **yes** cuando se le solicite **¿Es CN=Desconocido, OU=Desconocido, O=Desconocido, L=Desconocido, ST=Desconocido, C=Desconocido correcto?**
- f. Pulse **Intro** para responder a la pregunta siguiente:

**Introduzca la contraseña de clave de <probekey> (RETORNO si es la misma que la contraseña del almacén de claves):**

- g. Compruebe que el archivo se creó en la carpeta siguiente y asegúrese de que su tamaño es mayor que 0: **C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore**

## 3. Exportar el nuevo certificado de cliente

- a. Abra el símbolo del sistema y ejecute el comando:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -export -alias
<NombreSonda> -keystore
C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore -file
C:\hp\UCMDB\DataFlowProbe\conf\security\<NombreSonda>.cert
```

- b. Cuando se le solicite, escriba la contraseña del almacén de claves. (La contraseña del [paso 2b](#) anterior.)

Se muestra el siguiente mensaje:

```
Certificado almacenado en el archivo
<C:\hp\UCMDB\DataFlowProbe\confsecurity\<>NombreSonda>.cert
```

4. **Abra el archivo DiscoveryProbe.properties que se encuentra en:**  
**C:\HP\UCMDB\DataFlowProbe\conf**
  - a. Actualice la propiedad **appilog.agent.probe.protocol** a **HTTPS**.
  - b. Actualice la propiedad **serverPortHttps** al número de puerto relevante. (Utilice el número de puerto del paso 2c de "Configuración del servidor UCMDB inicial" en la página 72.)
5. **Abra el archivo ssl.properties ubicado en:**  
**C:\HP\UCMDB\DataFlowProbe\confsecurity\**
  - a. Actualice la propiedad **javax.net.ssl.keyStore** a **client.keystore**.
  - b. Cifre la contraseña del [paso 2b](#) anterior:
    - i. Inicie la sonda de Data Flow (o asegúrese de que se está ejecutando).
    - ii. Acceda a la sonda JMX. Vaya a: **http://<nombre\_host\_sonda>:1977**  
Por ejemplo, si ejecuta la sonda localmente, vaya a: **http://localhost:1977**.
    - iii. Pulse el vínculo **type=MainProbe**.
    - iv. Desplácese hasta la operación **getEncryptedKeyPassword**.
    - v. Introduzca la contraseña en el campo **Key Password**.
    - vi. Pulse el botón **getEncryptedKeyPassword**.
  - c. Copie y pegue la contraseña cifrada para actualizar la propiedad **javax.net.ssl.keyStorePassword**.

**Nota:** Los números se separan con comas. Por ejemplo: -20,50,34,-40,-50.)

#### 6. Copiar el certificado de sonda al equipo de UCMDB

Copie el archivo **C:\HP\UCMDB\DataFlowProbe\confsecurity\client.cert** desde el equipo de la sonda de Data Flow al equipo de UCMDB en **C:\HP\UCMDB\UCMDBServer\confsecurity\<>NombreSonda>.cert**.

### Configuración adicional del servidor UCMDB

1. **Agregue cada certificado de sonda al almacén de confianza de UCMDB**

**Nota:** Debe completar los pasos siguientes para cada certificado de sonda.

- a. Abra el símbolo del sistema y ejecute el comando:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -
keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.truststore
-file C:\hp\UCMDB\UCMDBServer\conf\security\<<NombreSonda>.cert -
alias <NombreSonda>
```

- b. Escriba la contraseña del almacén de claves. Por ejemplo, la contraseña del almacén de claves listo para su uso es **hppass**.
- c. Cuando se le pregunte **Trust this certificate?**, pulse **y** y, a continuación **Intro**.

Se muestra el siguiente mensaje:

**El certificado se agregó al almacén de claves**

## Reiniciar los equipos

Reinicie el servidor UCMDB y los equipos de sonda.

# Controlar la ubicación del archivo domainScopeDocument

El sistema de archivos de la sonda contiene (de manera predeterminada) tanto la clave de cifrado como el archivo **domainScopeDocument**. Cada vez que se inicia la sonda, recupera el archivo **domainScopeDocument** del servidor y lo almacena en su sistema de archivos. Para evitar que usuarios no autorizados obtengan esas credenciales, puede configurar la sonda para que el archivo **domainScopeDocument** se almacene en la memoria de la sonda y no en su sistema de archivos.

### Para controlar la ubicación del archivo domainScopeDocument:

1. Abra **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** y cambie:

```
appilog.collectors.storeDomainScopeDocument=true
```

por:

```
appilog.collectors.storeDomainScopeDocument=false
```

Las carpetas **serverData** de Puerta de enlace de sonda y Administrador de sonda ya no contienen el archivo **domainScopeDocument**.

Para obtener más información sobre el uso del archivo **domainScopeDocument** para proteger DFM, consulte "[administrar credenciales de Data Flow](#)" en la página 43.

2. Reinicie la sonda.

## Crear un almacén de claves para la sonda de Data Flow

1. En el equipo donde está instalada la sonda, ejecute el siguiente comando:  

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool -genkey -alias probekey -keyalg RSA -keystore C:\HP\UCMDB\DataFlowProbe\conf\security\client.keystore
```
2. Escriba una contraseña para el nuevo almacén de claves.
3. Introduzca la información cuando se le pida.
4. Cuando se le pregunte **Is CN=... C=... Correct?**, introduzca **yes** y, a continuación, pulse **Intro**.
5. Pulse **Intro** de nuevo para aceptar la contraseña del almacén de claves como la contraseña de clave.
6. Compruebe que **client.keystore** se crea en el siguiente directorio:  
**C:\HP\UCMDB\DataFlowProbe\conf\security\**

## Cifrar las contraseñas del almacén de claves y el almacén de confianza de la sonda

Las contraseñas del almacén de claves y el almacén de confianza de la sonda se almacenan cifradas en **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**. Este procedimiento explica cómo cifrar la contraseña.

1. Inicie la sonda de Data Flow (o compruebe que se está ejecutando).
2. Acceda a la consola JMX de la sonda de Data Flow: Inicie un explorador web y escriba la siguiente dirección: `http://<Dirección IP o nombre del equipo de la sonda de Data Flow>:1977`. Si está ejecutando la sonda de Data Flow localmente, escriba `http://localhost:1977`.

**Nota:** Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña. Si no ha creado un usuario, utilice el nombre de usuario predeterminado `sysadmin` y la contraseña `sysadmin` para iniciar sesión.

3. Localice el servicio **Type=MainProbe** y haga clic en el vínculo para abrir la página de operaciones.
4. Localice la operación **getEncryptedKeyPassword**.
5. Introduzca la contraseña del almacén de claves o el almacén de confianza en el campo **Key Password** y llame a la operación haciendo clic en **getEncryptedKeyPassword**.
6. El resultado de la llamada es una cadena de contraseña cifrada como, por ejemplo:

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,
112,65,61,61
```

- Copie y pegue la contraseña cifrada en la línea correspondiente al almacén de claves o almacén de confianza en el siguiente archivo:  
**C:\HP\UCMDB\DataFlowProbe\confsecurity\ssl.properties.**

## Almacén de claves y almacén de confianza predeterminados de servidor y sonda de Data Flow

Esta sección incluye los siguientes temas:

- "Servidor UCMDB" abajo
- "La sonda de Data Flow" abajo

### Servidor UCMDB

Los archivos están ubicados en el siguiente directorio:

**C:\HP\UCMDB\UCMDBServer\confsecurity.**

Entidad	Nombre de archivo/Término	Contraseña/Término	Alias
Almacén de claves del servidor	server.keystore (sKeyStoreFile)	hppass (sKeyStorePass)	hpcert
Almacén de confianza del servidor	server.truststore (sTrustStoreFile)	hppass (sTrustStorePass)	clientcert (entrada de confianza predeterminada)
Almacén de claves del cliente	client.keystore (cKeyStoreFile)	clientpass (cKeyStorePass)	clientcert

### La sonda de Data Flow

Los archivos están ubicados en el siguiente directorio:

**C:\HP\UCMDB\DataFlowProbe\confsecurity.**

Entidad	Nombre de archivo/Término	Contraseña/Término	Alias
Almacén de claves de la sonda	MAMKeyStoreExp.jks (pKeyStoreFile)	logomania (pKeyStorePass)	mam
La sonda de Data Flow utiliza el almacén de claves <b>cKeyStoreFile</b> como almacén de claves predeterminado durante el procedimiento de autenticación. Se trata de un almacén de claves de cliente que forma parte de la instalación de UCMDB.			
Almacén de confianza de la	MAMTrustStoreExp.jks (pTrustStoreFile)	logomania (pTrustStorePass)	mam (entrada de confianza)

Entidad	Nombre de archivo/Término	Contraseña/Término	Alias
sonda			predeterminada)
La contraseña <b>cKeyStorePass</b> es la contraseña predeterminada de <b>cKeyStoreFile</b> .			

## Capítulo 6

---

# Autenticación de Lightweight Single Sign-On (LW-SSO): referencia general

Este capítulo incluye:

Información general de la autenticación LW-SSO .....	80
Requisitos del sistema de LW-SSO .....	81
Advertencias de seguridad de LW-SSO .....	81
Solución de problemas y limitaciones .....	83

## Información general de la autenticación LW-SSO

LW-SSO es un método de control de acceso que permite a los usuarios iniciar sesión una vez y obtener acceso a los recursos de diversos sistemas de software sin tener que volver a iniciar sesión. Las aplicaciones de un grupo configurado de sistemas de software confían en la autenticación, por lo que no se requiere ninguna autenticación adicional al moverse de una aplicación a otra.

La información de esta sección se aplica a las versiones 2.2 y 2.3 de LW-SSO.

- **Caducidad del token LW-SSO**

El valor de caducidad del token LW-SSO determina la validez de la sesión de la aplicación. Por lo tanto, su valor de caducidad debe ser, como mínimo, el mismo que el valor de caducidad de la sesión de la aplicación.

- **Configuración recomendada de la caducidad del token LW-SSO**

Todas las aplicaciones que usen LW-SSO deben configurar la caducidad de tokens. El valor recomendado es 60 minutos. En el caso de las aplicaciones que no requieren un alto nivel de seguridad, se puede configurar un valor de 300 minutos.

- **Hora GMT**

Todas las aplicaciones que participan en una integración LW-SSO deben utilizar la misma hora GMT con una diferencia máxima de 15 minutos.

- **Funcionalidad multidominio**

La funcionalidad multidominio requiere que todas las aplicaciones que participan en la integración de LW-SSO configuren las opciones de `trustedHosts` (o las de **protectedDomains**) si son necesarias para realizar la integración con aplicaciones de diferentes dominios DNS. Además, también deben añadir el dominio correcto al elemento **lwssso** de la configuración.

- **Obtener la funcionalidad SecurityToken para URL**

Para obtener información enviada como una **SecurityToken para URL** desde otras aplicaciones, la aplicación host debe configurar el dominio correcto en el elemento **lwssso** de la configuración.

## Requisitos del sistema de LW-SSO

Aplicación	Versión	Comentarios
Java	1.5 y posterior	
HTTP Servlets API	2.1 y posterior	
Internet Explorer	6.0 y posterior	El explorador debe tener habilitada las cookies en la sesión HTTP y la funcionalidad de redirección 302 de HTTP.
Firefox	2.0 y posterior	El explorador debe tener habilitada las cookies en la sesión HTTP y la funcionalidad de redirección 302 de HTTP.
Autenticaciones de JBoss	JBoss 4.0.3 JBoss 4.3.0	
Autenticaciones de Tomcat	Tomcat 5.0.28 independiente Tomcat 5.5.20 independiente	
Autenticaciones de Acegi	Acegi 0.9.0 Acegi 1.0.4	
Motores de servicios web	Axis 1 - 1,4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

## Advertencias de seguridad de LW-SSO

En esta sección se describen advertencias de seguridad que son relevantes para la configuración de LW-SSO:

- **Parámetro InitString confidencial en LW-SSO.** LW-SSO utiliza una clave de cifrado simétrica para validar y crear un token LW-SSO. El parámetro **initString** de la configuración se utiliza para la inicialización de la clave secreta. Una aplicación crea un token y todas las aplicaciones que tengan el mismo parámetro **initString** validan el token.

**Precaución:**

- No es posible utilizar LW-SSO sin definir el parámetro **initString**.
- El parámetro **initString** es información confidencial y debe tratarse como tal en términos de publicación, transporte y persistencia.
- El parámetro **initString** sólo debe compartirse entre aplicaciones que se integren entre sí empleando LW-SSO.
- La longitud mínima del parámetro **initString** debe ser 12 caracteres.

- **Habilitar LW-SSO sólo si es estrictamente necesario.** LW-SSO debe estar deshabilitado, a menos que se requiera específicamente.
- **Nivel de seguridad de la autenticación.** La aplicación que usa el marco de autenticación más débil y genera un token LW-SSO en el que confían otras aplicaciones integradas determina el nivel de seguridad de la autenticación de todas las aplicaciones.

Se recomienda que sólo puedan generar tokens LW-SSO aquellas aplicaciones que usen marcos de autenticación sólidos y seguros.

- **Implicaciones del cifrado simétrico.** LW-SSO usa criptografía simétrica para generar y validar los tokens LW-SSO. Por consiguiente, todas las aplicaciones que usen LW-SSO pueden generar un token en el que confíen las demás aplicaciones que usen el mismo parámetro **initString**. El riesgo potencial es relevante cuando una aplicación que comparte un **initString** se encuentra en una ubicación que no es de confianza o cuando se puede acceder a ella desde dicha ubicación.
- **Asignación de usuarios (sincronización).** El marco LW-SSO no garantiza la asignación de usuarios entre las aplicaciones integradas. Por lo tanto, la aplicación integrada debe supervisar la asignación de usuarios. Se recomienda compartir el mismo registro de usuarios (como LDAP/AD) entre todas las aplicaciones integradas.

Si no se asignan usuarios, pueden aparecer infracciones de seguridad y el comportamiento de la aplicación se puede resentir. Por ejemplo, el mismo nombre de usuario se puede asignar a los diferentes usuarios reales de las distintas aplicaciones.

Además, en los casos en que un usuario inicie sesión en una aplicación (AppA) y seguidamente acceda a una segunda aplicación (AppB) que use la autenticación de contenedores o aplicaciones, si no se asigna el usuario, obligará al usuario a iniciar sesión manualmente en AppB y especificar un nombre de usuario. Si el usuario especifica un nombre de usuario distinto del que se usó para iniciar sesión en AppA, puede producirse el siguiente comportamiento: si el usuario accede posteriormente a una tercera aplicación (AppC) desde AppA o AppB, accederá a ella usando los mismos nombres de usuario que se emplearon para iniciar sesión en AppA o AppB, respectivamente.

- **Gestor de identidades.** Se usa para la autenticación, todos los recursos sin proteger del Gestor de identidades se deben configurar con la opción **nonsecureURLs** en el archivo de seguridad de LW-SSO.
- **Modo de demostración de LW-SSO.**
  - El modo de demostración debe usarse exclusivamente con fines de demostración.
  - El modo de demostración debe usarse exclusivamente en redes no protegidas.

- El modo de demostración no debe usarse en un entorno de producción. No debe usarse ninguna combinación del modo de demostración y el modo de producción.

## Solución de problemas y limitaciones

En esta sección se describen los problemas y las limitaciones conocidas cuando se trabaja con la autenticación de LW-SSO.

### Problemas conocidos

En esta sección se describen los problemas conocidos de la autenticación de LW-SSO.

- **Contexto de seguridad.** El contexto de seguridad de LW-SSO sólo admite un valor de atributo por nombre de atributo.

Por lo tanto, si el token SAML2 envía más de un valor para el mismo nombre de atributo, el marco de LW-SSO sólo aceptará uno de ellos.

De igual forma, si el token IdM está configurado para enviar más de un valor para el mismo nombre de atributo, el marco de LW-SSO sólo aceptará uno de ellos.

- **Funcionalidad de desconexión multidominio al utilizar Internet Explorer 7.** La funcionalidad de desconexión multidominio puede fallar en las siguientes condiciones:

- El explorador usado es Internet Explorer 7 y la aplicación está invocando a más tres verbos de redireccionamiento HTTP 302 consecutivos en el procedimiento de desconexión.

En ese caso, Internet Explorer 7 puede gestionar de forma incorrecta la respuesta de redirección HTTP 302 y mostrar una página de error **Internet Explorer no puede mostrar la página web** en su lugar.

Como solución temporal, se recomienda reducir, en la medida de lo posible, el número de comandos de redirección de aplicaciones en la secuencia de desconexión.

### Limitaciones

Tenga en cuenta las siguientes limitaciones al trabajar con la autenticación LW-SSO:

- **Acceso de los clientes a la aplicación.**

**Si se define un dominio en la configuración de LW-SSO:**

- Los clientes de la aplicación deben acceder a la aplicación con un nombre de dominio completo en la dirección URL de conexión, por ejemplo, `http://myserver.companydomain.com/WebApp`.
- LW-SSO no admite direcciones URL con una dirección IP, por ejemplo, `http://192.168.12.13/WebApp`.
- LW-SSO no admite direcciones URL sin un dominio, por ejemplo, `http://myserver/WebApp`.

**Si se define un dominio en la configuración de LW-SSO:** el cliente puede acceder a la aplicación sin un nombre de dominio completo en la dirección URL de conexión. En ese caso, se crea una cookie de la sesión de LW-SSO específicamente para un equipo individual sin información de dominio. Por consiguiente, el explorador no delega la cookie a otro, por lo que no pasa a otros equipos ubicados en el mismo dominio DNS, lo que significa que LW-SSO no funciona en el mismo dominio.

- **Integración del marco LW-SSO.** Las aplicaciones sólo pueden usar y aprovechar las capacidades de LW-SSO si están integradas previamente en el marco de LW-SSO.
- **Compatibilidad con múltiples dominios.**
  - La funcionalidad multidominio se basa en el sitio de referencia HTTP. Por consiguiente, LW-SSO admite enlaces de una aplicación a otra y no permite escribir una URL en una ventana del explorador, salvo cuando ambas aplicaciones están en el mismo dominio.
  - No se admite el primer vínculo entre dominios que usen **HTTP POST**.

La funcionalidad multidominio no admite la primera solicitud **HTTP POST** en una segunda aplicación (sólo se admite la solicitud **HTTP GET**). Por ejemplo, si la aplicación tiene un vínculo HTTP a una segunda aplicación, se admite una solicitud **HTTP GET**, pero no se admite una solicitud **HTTP FORM**. Todas las solicitudes a partir de la primera pueden ser **HTTP POST** o **HTTP GET**.

- **Tamaño del token LW-SSO:**

El tamaño de la información que LW-SSO puede transferir de una aplicación de un dominio a otra aplicación de otro dominio está limitada a 15 grupos/funciones/atributos (tenga en cuenta que cada elemento puede tener una longitud media de 15 caracteres).

- **Vinculación de un sitio protegido (HTTPS) a otro no protegido (HTTP) en un escenario multidominio:**

La funcionalidad multidominio no funciona al vincular una página protegida (HTTPS) a otra no protegida (HTTP). Ésta es una limitación del explorador en la que el encabezado del remitente no se envía al vincular un recurso protegido a otro no protegido. Por ejemplo, consulte:

<http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP>

- **Comportamiento de cookies de terceros en Internet Explorer:**

Microsoft Internet Explorer 6 contiene un módulo que admite la especificación P3P (Plataforma para preferencias de privacidad), lo que significa que las cookies procedentes de un dominio de terceros se bloquean, de forma predeterminada, en la zona de seguridad Internet. Las cookies de la sesión también se consideran cookies de terceros en Internet Explorer, por lo que se bloquean y provocan que LW-SSO deje de funcionar. Para obtener más información, consulte: <http://support.microsoft.com/kb/323752/en-us>.

Para solucionar este problema, agregue la aplicación iniciada (o un subconjunto de dominio DNS como \*.midominio.com) a la zona Intranet/Sitios de confianza del equipo (en Microsoft Internet Explorer, seleccione **Menú > Herramientas > Opciones de Internet > Seguridad > Intranet local > Sitios > Opciones avanzadas**) y se aceptarán las cookies.

**Precaución:** La cookie de la sesión LW-SSO sólo es una de las cookies utilizadas por la aplicación de terceros bloqueada.

- **Token SAML2**

- La funcionalidad de desconexión no se admite cuando se usa el token SAML2.

Por lo tanto, si el token SAML2 se usa para acceder a una segunda aplicación, los usuarios que se desconecten de la primera aplicación no se desconectarán de la segunda.

- **La caducidad del token SAML2 no aparece reflejada en la gestión de sesiones de la aplicación.**

Por consiguiente, si el token SAML2 se usa para acceder a una segunda aplicación, la gestión de sesiones de cada aplicación se trata de forma independiente.

- **Dominio JAAS.** El dominio JAAS de Tomcat no es compatible.
- **Uso de espacios en directorios de Tomcat.** No se admite el uso de espacios en directorios de Tomcat.

LW-SSO no se puede utilizar cuando una ruta de instalación de Tomcat (carpetas) incluye espacios (por ejemplo, Archivos de programa) y el archivo de configuración de LW-SSO se encuentra en la carpeta **common\classes** de Tomcat.

- **Configuración del equilibrador de carga.** Debe configurarse un equilibrador de carga implantado en LW-SSO para utilizar sesiones adheridas.
- **Modo de demostración.** En el modo de demostración, LW-SSO admite vínculos de una aplicación a otra pero no permite escribir una dirección URL en la ventana del explorador, porque no hay ningún encabezado de origen de referencia de HTTP en este caso.

## Capítulo 7

---

# Autenticación de inicio de sesión de HP Universal CMDB

Este capítulo incluye:

Configuración de un método de autenticación .....	86
Habilitación del inicio de sesión en HP Universal CMDB con LW-SSO .....	87
Configuración de una conexión segura con el protocolo SSL (Capa de sockets seguros) .....	87
Uso de la consola JMX para probar las conexiones LDAP .....	88
Configuración de LDAP mediante la consola JMX .....	89
Habilitación y definición del método de autenticación LDAP .....	90
Recuperación de la configuración de LW-SSO actual en un entorno distribuido .....	91

## Configuración de un método de autenticación

Se puede realizar la autenticación:

- **En el servicio de HP Universal CMDB interno.**
- **Mediante el Protocolo ligero de acceso a directorios (LDAP).** Puede utilizar un servidor LDAP externo y dedicado para almacenar la información de autenticación en lugar de utilizar el servicio de HP Universal CMDB interno. El servidor LDAP debe residir en la misma subred que todos los servidores de HP Universal CMDB.

Para obtener más información sobre LDAP, consulte la sección acerca de la asignación LDAP en la *HP Universal CMDB – Guía de administración*.

El método de autenticación predeterminado utiliza el servicio de HP Universal CMDB interno. Si utiliza el método predeterminado, no es necesario realizar ningún cambio en el sistema.

Estas opciones se aplican a los inicios de sesión que se realizan a través de los servicios web y a través de la interfaz de usuario.

- **Mediante LW-SSO.** HP Universal CMDB está configurado con LW-SSO. LW-SSO permite iniciar sesión en HP Universal CMDB y tener acceso automático a otras aplicaciones configuradas que se ejecutan en el mismo dominio, sin que sea necesario iniciar sesión en esas aplicaciones.

Cuando se habilita el soporte de autenticación LW-SSO (está deshabilitado de forma predeterminada), hay que asegurarse de que las demás aplicaciones del entorno Single Sign-On tengan LW-SSO habilitado y funcionen con el mismo parámetro `initString`.

## Habilitación del inicio de sesión en HP Universal CMDB con LW-SSO

Para habilitar LW-SSO en HP Universal CMDB, siga este procedimiento:

1. Para acceder a la consola JMX, introduzca la siguiente dirección en el explorador web: **http://<nombre\_servidor>:8080/jmx-console**, donde **<nombre\_servidor>** equivale al nombre del equipo donde se ha instalado HP Universal CMDB.
2. En **UCMDB-UI**, haga clic en **name=LW-SSO Configuration** para abrir la página de operaciones.
3. Configure la cadena init mediante el método **setInitString**.
4. Configure el nombre de dominio del equipo en el que está instalado UCMDB mediante el método **setDomain**.
5. Llame al método **setEnabledForUI** con el parámetro establecido en **True**.
6. **Opcional**. Si desea trabajar usando la funcionalidad multidominio, seleccione el método **addTrustedDomains**, introduzca los valores del dominio y haga clic en **Invoke**.
7. **Opcional**. Si desea trabajar usando un proxy inverso, seleccione el método **updateReverseProxy**, ajuste el parámetro **Está habilitado el proxy inverso** en **True**, especifique una dirección URL para el parámetro **Dirección URL del servidor completo del proxy inverso** y haga clic en **Invoke**. Si desea acceder a UCMDB directamente y usando un proxy inverso, establezca la siguiente configuración adicional: seleccione el método **setReverseProxyIPs**, especifique la dirección IP para el parámetro ip/s de proxy inverso y haga clic en **Invoke**.
8. **Opcional**. Si desea acceder a UCMDB usando un punto de autenticación externo, seleccione el método **setValidationPointHandlerEnable**, establezca el parámetro **El gestor de punto de validación está habilitado** en **True**, especifique la dirección URL para el punto de autenticación en el parámetro **Servidor de punto de autenticación** y haga clic en **Invoke**.
9. Para ver la configuración de LW-SSO cuando se guarda en el mecanismo de configuración, llame al método **retrieveConfigurationFromSettings**.
10. Para ver la configuración real de LW-SSO cargada, llame al método **retrieveConfiguration**.

**Nota:** No puede habilitar LW-SSO mediante la interfaz de usuario.

## Configuración de una conexión segura con el protocolo SSL (Capa de sockets seguros)

Dado que en el proceso de inicio de sesión se pasa información confidencial entre HP Universal CMDB y el servidor LDAP, se puede aplicar un determinado nivel de seguridad al contenido. Para ello, es necesario habilitar la comunicación SSL en el servidor LDAP y configurar HP Universal CMDB para trabajar con SSL.

HP Universal CMDB admite SSL que utiliza un certificado emitido por una entidad de certificación (CA) de confianza.

La mayoría de servidores LDAP, incluido Active Directory, puede mostrar un puerto seguro para una conexión basada en SSL. Si utiliza Active Directory con una CA privada, debe agregar la CA a la lista de entidades de certificación de confianza en JRE.

Para obtener más información sobre la configuración de la plataforma HP Universal CMDB para permitir la comunicación mediante SSL, consulte "[Habilitar la comunicación de Capa de sockets seguros \(SSL\)](#)" en la página 18.

#### Para agregar una CA a la lista de entidades de certificación de confianza para mostrar un puerto seguro en una conexión basada en SSL:

1. Exporte un certificado de la CA e impórtelo en la JVM que utiliza HP Universal CMDB, siguiendo estos pasos:
  - a. En el equipo servidor de UCMDB, acceda a la carpeta **UCMDBServer\bin\JRE\bin**.
  - b. Ejecute el siguiente comando:

```
Keytool -import -file <su archivo de certificado> -keystore
C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
```

Por ejemplo:

```
Keytool -import -file c:\ca2ss_ie.cer -keystore
C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
```

2. Seleccione **Administración > Configuración de infraestructura > General de LDAP**.

**Nota:** También es posible establecer esta configuración mediante la consola JMX. Para obtener más información, consulte "[Configuración de LDAP mediante la consola JMX](#)" en la página siguiente.

3. Localice **URL del servidor LDAP** e introduzca un valor, con el formato:

```
ldaps://<host ldap>[:<puerto>]/[<DN de base>][??ámbito]
```

Por ejemplo:

```
ldaps://my.ldap.server:389/ou=People,o=myOrg.com??sub
```

Tenga en cuenta la **s** en **ldaps**.

4. Haga clic en **Guardar** para guardar el nuevo valor o en **Restaurar predeterm.** para reemplazar la entrada por el valor predeterminado (una dirección URL en blanco).

## Uso de la consola JMX para probar las conexiones LDAP

Esta sección describe un método para probar la configuración de autenticación LDAP mediante la consola JMX.

1. Inicie el explorador Web e introduzca la siguiente dirección: **http://<nombre\_servidor>:8080/jmx-console**, donde **<nombre\_servidor>** equivale al nombre del equipo donde se ha instalado HP Universal CMDB.

Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

2. En **UCMDB**, haga clic en **UCMDB-UI:name=LDAP Settings** para abrir la página de operaciones.
3. Localice **testLDAPConnection**.
4. En el cuadro **Value** del parámetro **customer id**, introduzca el Id. de cliente.
5. Haga clic en **Invoke**.

La página JMX MBEAN Operation Result indica si la conexión LDAP se ha establecido correctamente. Si se ha establecido correctamente, la página muestra además los grupos raíz de LDAP.

## Configuración de LDAP mediante la consola JMX

Esta sección describe cómo establecer la configuración de autenticación LDAP mediante la consola JMX.

### Para establecer la configuración de autenticación LDAP:

1. Inicie el explorador Web e introduzca la siguiente dirección: **http://<nombre\_servidor>:8080/jmx-console**, donde **<nombre\_servidor>** equivale al nombre del equipo donde se ha instalado HP Universal CMDB.  
  
Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.
2. En **UCMDB**, haga clic en **UCMDB-UI:name=LDAP Settings** para abrir la página de operaciones.
3. Para ver la configuración de autenticación LDAP actual, localice el método **getLDAPSettings**. Haga clic en **Invoke**. Se muestra una tabla con toda la configuración de LDAP y sus valores.
4. Para cambiar los valores de la configuración de autenticación LDAP, localice el método **configureLDAP**. Introduzca los valores de configuración relevantes y haga clic en **Invoke**. La página JMX MBEAN Operation Result indica si la configuración de autenticación LDAP se ha actualizado correctamente.

**Nota:** Si no introduce un valor en un parámetro de configuración, se conserva el valor actual.

5. Tras establecer la configuración LDAP, puede comprobar las credenciales de usuario LDAP. Localice el método **verifyLDAPCredentials**. Introduzca el Id. de cliente, el nombre de usuario y la contraseña, y haga clic en **Invoke**. La página JMX MBEAN Operation Result indica si el usuario pasa la autenticación LDAP.

# Habilitación y definición del método de autenticación LDAP

Puede habilitar y definir el método de autenticación LDAP en un sistema HP Universal CMDB.

## Para habilitar y definir el método de autenticación LDAP:

1. Seleccione **Administración > Configuración de infraestructura > General de LDAP**.
2. Seleccione **URL del servidor LDAP** e introduzca el valor de la dirección URL de LDAP, con el formato:

```
ldap://<host ldap>[:<puerto>]/[<DN de base>][??ámbito]
```

Por ejemplo:

```
ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub
```

3. Seleccione la categoría **Definición de grupo LDAP**, localice **DN de base de grupos** e introduzca el nombre distintivo del grupo general.
4. Localice **DN de base de grupos raíz** e introduzca el nombre distintivo del grupo raíz.
5. Seleccione la categoría **General de LDAP**, localice **Habilitar sincronización de permisos de usuario** y compruebe que el valor está establecido en **Verdadero**.
6. Seleccione la categoría **Autenticación general para LDAP**, localice **Contraseña de usuario con derecho a búsqueda** y rellene la contraseña.
7. Seleccione la categoría **Opciones LDAP para clases y atributos**, localice **Objeto de clase de grupo** y rellene el nombre de clase de objeto (**grupo** para Microsoft Active Directory y **groupOfUniqueNames** para Oracle Directory Server).
8. Localice **Atributo de miembro de grupos** y rellene el nombre de atributo (**miembro** para Microsoft Active Directory y **uniqueMember** para Oracle Directory Server).
9. Localice **Clase de objeto de usuarios** y rellene el nombre de la clase de objeto (**usuario** para Microsoft Active Directory e **inetOrgPerson** para Oracle Directory Server).
10. Localice **Atributo UUID** y rellene el atributo de identificación único para un usuario de su servidor de directorio. Asegúrese de seleccionar un atributo que sea único en el servidor de directorio. Por ejemplo, cuando se usa SunOne/Oracle Directory Server, el atributo de UID no es único. En tal caso, utilice el atributo de dirección de correo electrónico o el nombre distintivo. El uso de un atributo que no sea único como atributo de identificación único en UCMDB puede provocar un comportamiento incoherente durante el inicio de sesión.
11. Guarde los nuevos valores. Para reemplazar una entrada por el valor predeterminado, haga clic en **Restaurar predeterm.**
12. Si la configuración de infraestructura **Se aplica la distinción entre mayúsculas y minúsculas durante la autenticación con LDAP** en **General de LDAP**, se establece en **True**, la autenticación distingue entre mayúsculas y minúsculas.

**Precaución:** Cuando se cambia el valor de la configuración de esta infraestructura, todos los usuarios externos deben eliminar manualmente el administrador de UCMDDB.

13. Asigne grupos de usuarios LDAP a grupos de usuario de UCMDDB. Para obtener más información, consulte "[Autenticación de inicio de sesión de HP Universal CMDB](#)" en la página 86.
14. Si desea definir un conjunto predeterminado de permisos para usuarios de un grupo LDAP que no tiene una asignación de grupo, seleccione la categoría **General de LDAP**, localice **Grupo de usuarios asignado automáticamente** e introduzca el nombre del grupo.

El protocolo predeterminado que se usa para comunicarse con el servidor LDAP es TCP, pero puede cambiar el protocolo a SSL. Para obtener más información, consulte "[Configuración de una conexión segura con el protocolo SSL \(Capa de sockets seguros\)](#)" en la página 87.

**Nota:** Cada usuario de LDAP tiene un nombre, un apellido y una dirección de correo electrónico guardados en el repositorio local. Si el valor de cualquier de esos parámetros que se almacena en el servidor LDAP es diferente del valor del repositorio local, los valores del servidor LDAP sobrescribirán los valores locales de cada inicio de sesión.

## Recuperación de la configuración de LW-SSO actual en un entorno distribuido

Si UCMDDB está incrustado en un entorno distribuido, por ejemplo, en un despliegue de BSM, lleve a cabo el siguiente procedimiento para recuperar la configuración de LW-SSO actual en el equipo de procesamiento.

### Para recuperar la configuración de LW-SSO actual:

1. Inicie un explorador web y escriba la siguiente dirección: `http://localhost.<domain_name>:8080/jmx-console`.

Es posible que se le solicite un nombre de usuario y una contraseña.

2. Localice **UCMDDB:service=Security Services** y haga clic en el vínculo para abrir la página Operaciones.
3. Localice la operación **retrieveLWSSOConfiguration**.
4. Haga clic en **Invoke** para recuperar la configuración.

# Capítulo 8

---

## Confidential Manager

Este capítulo incluye:

Información general de Confidential Manager .....	92
Consideraciones de seguridad .....	92
Configurar el servidor de HP Universal CMDB .....	93
Definiciones .....	94
Propiedades de cifrado .....	94

## Información general de Confidential Manager

El marco Confidential Manager soluciona los problemas de administración y distribución de datos confidenciales en HP Universal CMDB y otros productos de HP Software.

Confidential Manager consta de dos componentes principales: el cliente y el servidor. Estos dos componentes son responsables de transferir datos de manera segura.

- El cliente de Confidential Manager es una biblioteca que las aplicaciones utilizan para acceder a datos confidenciales.
- El servidor de Confidential Manager recibe las solicitudes de los clientes de Confidential Manager, o de clientes de terceros, y realiza las tareas necesarias. El servidor de Confidential Manager es responsable de guardar los datos de forma segura.

Confidential Manager cifra las credenciales en el transporte, la caché del cliente, la persistencia y la memoria. Confidential Manager utiliza criptografía simétrica para transportar credenciales entre el cliente de Confidential Manager y el servidor de Confidential Manager mediante un secreto compartido. Confidential Manager utiliza diversos secretos para el cifrado de la caché, la persistencia y el transporte según la configuración.

Para obtener directrices detalladas sobre la administración del cifrado de credenciales en la sonda de Data Flow, consulte "[administrar credenciales de Data Flow](#)" en la [página 43](#).

## Consideraciones de seguridad

- Puede utilizar los siguientes tamaños de clave en el algoritmo de seguridad: 128, 192 y 256 bits. El algoritmo se ejecuta con mayor rapidez con la clave más pequeña, pero es la menos segura. El tamaño de 128 bits es suficientemente seguro en la mayoría de los casos.
- Para aumentar la seguridad del sistema, utilice MAC: ajuste **useMacWithCrypto** en **true**. Para obtener más información, consulte "[Propiedades de cifrado](#)" en la [página 94](#).
- Para aprovechar los proveedores de seguridad sólida de clientes, puede utilizar el modo JCE.

## Configurar el servidor de HP Universal CMDB

Al trabajar con HP Universal CMDB, debe configurar el secreto y las propiedades de cifrado mediante los siguientes métodos de JMX:

1. En el equipo servidor de HP Universal CMDB, inicie el explorador web e introduzca la dirección del servidor, del siguiente modo: **http://<Nombre de host del servidor UCMDDB o IP>:8080/jmx-console**.

Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

2. En UCMDDB, haga clic en **UCMDDB:service=Security Services** para abrir la página Operaciones.
3. Para recuperar la configuración actual, localice la operación **CMGetConfiguration**. Haga clic en **Invoke** para mostrar el archivo XML de configuración del servidor de Confidential Manager.
4. Para realizar cambios en la configuración, copie el XML al que llamó en el paso anterior en un editor de texto. Realice cambios conforme a la tabla de "Propiedades de cifrado" en la página siguiente.

Localice la operación **CMSetConfiguration**. Copie la configuración actualizada en el cuadro **Value** y haga clic en **Invoke**. La nueva configuración se escribe en el servidor UCMDDB.

5. Para agregar usuarios a Confidential Manager para la autorización y la réplica, localice la operación **CMAddUser**. Este proceso también es útil en el proceso de réplica. En la réplica, el servidor esclavo debe comunicarse con el servidor maestro mediante un usuario con privilegios.
  - **username**. El nombre de usuario.
  - **customer**. El valor predeterminado es ALL\_CUSTOMERS.
  - **resource**. El nombre del recurso. El valor predeterminado es ROOT\_FOLDER.
  - **permission**. Elija entre ALL\_PERMISSIONS, CREATE, READ, UPDATE y DELETE. El valor predeterminado es ALL\_PERMISSIONS.

Haga clic en **Invoke**.

6. Si es necesario, reinicie HP Universal CMDB.

**Nota:** En la mayoría de los casos no es necesario reiniciar el servidor. Es posible que deba reiniciar el servidor cuando cambie uno de los siguientes recursos:

- Tipo de almacenamiento
- Nombres de columnas o nombre de tabla de la base de datos
- El creador de la conexión de base de datos
- Las propiedades de conexión a la base de datos (es decir, dirección URL, usuario, contraseña, nombre de clase de controlador)
- Tipo de base de datos

**Nota:**

- Es importante que el servidor UCMDDB y sus clientes tengan las mismas propiedades de cifrado de transporte. Si se cambian estas propiedades en el servidor UCMDDB, debe cambiarlas en todos los clientes. (Esto no es relevante para la sonda de Data Flow, ya que se ejecuta en el mismo proceso con el servidor UCMDDB; es decir, no se requiere configuración de cifrado de transporte).
- La réplica de Confidential Manager no está configurada de forma predeterminada y puede configurarse en caso necesario.
- Si se habilita la réplica de Confidential Manager y cambia la propiedad **initString** de transporte o cualquier otra propiedad de cifrado del maestro, todos los esclavos deben adoptar los cambios.

## Definiciones

**Propiedades de cifrado de almacenamiento.** Configuración que define cómo el servidor contiene y cifra los datos (si en una base de datos o en un archivo, qué propiedades de cifrado deben cifrar o descifrar los datos, etc.), cómo se almacenan las credenciales de forma segura, cómo se procesa el cifrado y conforme a qué configuración.

**Propiedades de cifrado de transporte.** La configuración de transporte define cómo el servidor y los clientes cifran el transporte entre sí, qué configuración se usa, cómo se transfieren las credenciales de forma segura, cómo se procesa el cifrado y conforme a qué configuración. Debe utilizar las mismas propiedades de cifrado para cifrar y descifrar el transporte, tanto en el servidor como en el cliente.

**Réplicas y propiedades de cifrado de réplica.** Los datos que Confidential Manager contiene de forma segura se replican de manera segura entre varios servidores. Estas propiedades definen cómo se transfieren los datos entre el servidor esclavo y el servidor maestro.

**Nota:**

- La tabla de base de datos que contiene la configuración del servidor de Confidential Manager se denomina: **CM\_CONFIGURATION**.
- El archivo de configuración predeterminado del servidor de Confidential Manager está ubicado en app-infra.jar y se denomina **defaultCMServerConfig.xml**.

## Propiedades de cifrado

La siguiente tabla describe las propiedades de cifrado. Para obtener más información sobre estos parámetros, consulte "Configurar el servidor de HP Universal CMDB" en la página precedente.

Parámetro	Descripción	Valor recomendado
encryptTransportMode	Cifra los datos transportados:	true

Parámetro	Descripción	Valor recomendado
	true, false	
encryptDecrypt InitString	Contraseña de cifrado	Más de 8 caracteres
cryptoSource	Biblioteca de implementación de cifrado que se va a usar: <ul style="list-style-type: none"> <li>• lw</li> <li>• jce</li> <li>• windowsDPAPI</li> <li>• lwJCECompatible</li> </ul>	lw
lwJCEPBE CompatibilityMode	Admite versiones anteriores de criptografía ligera: <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul>	true
cipherType	El tipo de cifrado que utiliza Confidential Manager. Confidential Manager solo admite un valor: <b>symmetricBlockCipher</b>	symmetric BlockCipher
engineName	<ul style="list-style-type: none"> <li>• AES</li> <li>• Blowfish</li> <li>• DES</li> <li>• 3DES</li> <li>• Null (sin cifrado)</li> </ul>	AES
algorithmModeName	Modo de algoritmo de cifrado de bloque: <ul style="list-style-type: none"> <li>• CBC</li> </ul>	CBC
algorithmPaddingName	Estándares de relleno: <ul style="list-style-type: none"> <li>• PKCS7Padding</li> <li>• PKCS5Padding</li> </ul>	PKCS7Padding
keySize	Depende del algoritmo (lo que admita <b>engineName</b> )	256
pbeCount	Número de veces que hay que ejecutar el hash para crear la clave a partir de <b>encryptDecryptInitString</b> . Cualquier número positivo.	1000
pbeDigestAlgorithm	Tipo de hash: <ul style="list-style-type: none"> <li>• SHA1</li> </ul>	SHA256

Parámetro	Descripción	Valor recomendado
	<ul style="list-style-type: none"> <li>• SHA256</li> <li>• MD5</li> </ul>	
encodingMode	Representación ASCII del objeto cifrado: <ul style="list-style-type: none"> <li>• Base64</li> <li>• Base64Url</li> </ul>	Base64Url
useMacWithCrypto	Define si se utiliza MAC con la criptografía: <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul>	false
macType	Tipo de código de autenticación de mensajes (MAC): <ul style="list-style-type: none"> <li>• hmac</li> </ul>	hmac
macKeySize SHA256	Depende del algoritmo MAC	256
macHashName	El algoritmo MAC hash: <ul style="list-style-type: none"> <li>• SHA256</li> </ul>	SHA256

