Novell® sentinel™

5.1.3

www.novell.com

Volumen V: GUÍA DE INTEGRACIÓN DE PRODUCTOS DE OTROS FABRICANTES

7 de julio de 2006

Novell®

Aviso legal

Novell, Inc. no otorga ninguna garantía respecto al contenido y el uso de esta documentación, y específicamente renuncia a cualquier garantía explícita o implícita de comercialización o adecuación para un fin determinado.Asimismo, Novell, Inc. se reserva el derecho a revisar esta publicación y a realizar cambios en su contenido en cualquier momento,sin obligación de notificar tales cambios a ninguna persona o entidad.

Además, Novell, Inc. no ofrece ninguna garantía con respecto a ningún software, y rechaza específicamente cualquier garantía explícita o implícita de comercialización o adecuación para un fin determinado Por otra parte, Novell, Inc. se reserva el derecho a realizar cambios en cualquiera de las partes o en la totalidad del software de Novell en cualquier momento, sin obligación de notificar tales cambios a ninguna persona ni entidad.

Cualquier producto o información técnica suministrado al amparo de este acuerdo puede estar sujeto a controles de exportación de EE.UU., así como a las leyes comerciales de otros países. Usted manifiesta estar de acuerdo en cumplir todas las normativas de control de exportación y obtener cualquier licencia o clasificación necesaria para exportar, reexportar o importar artículos. Asimismo, manifiesta su acuerdo en no exportar ni reexportar a entidades que se encuentran en las listas actuales de exclusión de exportación de los EE.UU. o que radiquen en países bajo embargo o terroristas, tal como se especifica en las leyes de exportación de los EE.UU. Asimismo, manifiesta estar de acuerdo en no utilizar artículos cuyo uso final esté destinado a armamento nuclear, de mísiles o químico biológico prohibido. Consulte www.novell.com/info/exports/ para obtener más información acerca de cómo exportar software de Novell. Novell no asume ninguna responsabilidad si no consigue obtener las aprobaciones necesarias para la exportación.

Copyright © de 1999 a 2006, Novell, Inc. Reservados todos los derechos. Ninguna parte de esta publicación puede ser reproducida, fotocopiada, almacenada en un sistema de recuperación o transmitida sin la expresa autorización por escrito del editor.

Novell, Inc. posee derechos de propiedad intelectual sobre la tecnología incorporada en el producto descrito en este documento. En concreto, y sin limitaciones, dichos derechos de propiedad intelectual pueden incluir una o varias patentes de los EE.UU. listadas en http://www.novell.com/company/legal/patents/ y una o varias patentes adicionales o aplicaciones pendientes de patente en los EE.UU. y en otros países.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
EE.UU.
www.novell.com

Documentación en línea: Para acceder a la documentación en línea de este y otros productos de Novell y obtener actualizaciones, consulte www.novell.com/documentation.

Marcas comerciales de Novell

Para obtener información sobre marcas comerciales de Novell, consulte la lista de marcas comerciales y de marcas de servicio de Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiales de otros fabricantes

Todas las marcas comerciales de otros fabricantes son propiedad de sus respectivos propietarios.

Avisos legales de otros fabricantes

Sentinel 5 contiene tecnologías de otros fabricantes:

- Apache Axis y Apache Tomcat, Copyright © de 1999 a 2005, Apache Software Foundation. Para obtener más información y consultar las restricciones y renuncias, visite http://www.apache.org/licenses/
- ANTLR. Para obtener más información y consultar las restricciones y renuncias, visite http://www.antlr.org/
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000-2004, the Legion of Bouncy Castle. Para obtener más información y consultar las restricciones y renuncias, visite http://www.bouncycastle.org/.
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, paquete de utilidades. Copyright © Doug Lea. Se utiliza sin las clases CopyOnWriteArrayList ni ConcurrentReaderHashMap.
- Crypto++ Compilation. Copyright © 1995-2003, Wei Dai, que incorpora los siguientes trabajos sujetos a copyright: mars.cpp de Brian Gladman y Sean Woods. Para obtener más información y consultar las restricciones y renuncias, visite http://www.eskimo.com/~weidai/License.txt.
- Crystal Reports Developer y Crystal Reports Server. Copyright © 2004 Business Objects Software Limited.
- DataDirect Technologies Corp. Copyright © 1991-2003.
- edpFTPj, con licencia Lesser GNU Public License. Para obtener más información y consultar las restricciones y renuncias, visite http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, con licencia Lesser General Public License disponible en: http://shark.objectweb.org/license.html.
- ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003-2004.
- ILOG, Inc. Copyright © 1999-2004.
- Installshield Universal. Copyright © 1996–2005, Macrovision Corporation y/o Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Para obtener más información y consultar las restricciones y renuncias, visite http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt.

La plataforma Java 2 también contiene los siguientes productos de otros fabricantes:

- CoolServlets © 1999
- DES y 3xDES © 2000 de Jef Poskanzer
- Crimson © 1999-2000 The Apache Software Foundation
- Xalan J2 © 1999-2000 The Apache Software Foundation
- NSIS 1.0j © 1999-2000 Nullsoft, Inc.
- Eastman Kodak Company © 1992
- Lucinda es una marca comercial o una marca comercial registrada de Bigelow and Holmes
- Taligent, Inc.
- IBM, algunas partes se encuentran disponibles en: http://oss.software.ibm.com/icu4j/

Para obtener más información acerca de estas tecnologías de otros fabricantes y consultar las restricciones y renuncias de responsabilidad correspondientes, visite: http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. Para obtener más información y consultar las restricciones y renuncias, visite http://www.java.sun.com/products/javabeans/glasgow/jaf.html y haga clic en download > license.
- JavaMail. Copyright © Sun Microsystems, Inc. Para obtener más información y consultar las restricciones y renuncias, visite http://www.java.sun.com/products/javamail/downloads/index.html y haga clic en download > license.
- Java Ace, de Douglas C. Schmidt y su grupo de investigación de la Universidad de Washington y Tao (con empaquetadores ACE) de Douglas C. Schmidt y su grupo de investigación en las universidades de Washington, California, Irvine y Vanderbilt. Copyright © de 1993 a 2005. Para obtener más información y consultar las restricciones y renuncias, visite http://www.cs.wustl.edu/~schmidt/ACE-copying.html y http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html
- Módulos Java de servicios de autorización y autenticación, con licencia Lesser General Public License. Para obtener más información y consultar las restricciones y renuncias, visite http://free.tagish.net/jaas/index.jsp
- Java Network Launching Protocol (JNLP). Copyright © Sun Microsystems, Inc. Para obtener más información y consultar las restricciones y renuncias, visite http://www.java.sun.com/products/javawebstart/download-jnlp.html y haga clic en download > license.
- Java Service Wrapper. Copyright de partes como se indica a continuación: Copyright © 1999, 2004 Tanuki Software y Copyright © 2001 Silver Egg Technology. Para obtener más información y consultar las restricciones y renuncias, visite http://wrapper.tanukisoftware.org/doc/english/license.html.
- JIDE. Copyright © de 2002 a 2005, JIDE Software, Inc.
- jTDS con licencia Lesser GNU Public License. Para obtener más información y consultar las restricciones y renuncias, visite http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, con licencia Lesser General Public License. Para obtener más información y consultar las restricciones y renuncias, visite http://web.ukonline.co.uk/mseries.
- Monarch Charts. Copyright © 2005, Singleton Labs.
- Net-SNMP. Partes del código están sujetas a copyright de varias entidades, las cuales se reservan todos los derechos. Copyright © 1989, 1991, 1992 de Carnegie Mellon University; Copyright © 1996, de 1998 a 2000, Junta de regentes de la Universidad de California; Copyright © de 2001 a 2003 Networks Associates Technology, Inc.; Copyright © de 2001 a 2003, Cambridge Broadband, Ltd.; Copyright © 2003 Sun Microsystems, Inc. y Copyright © de 2003 a 2004, Sparta, Inc. Para obtener más información y consultar las restricciones y renuncias, visite http://net-snmp.sourceforge.net.

- The OpenSSL Project. Copyright © 1998-2004. the Open SSL Project. Para obtener más información y consultar las restricciones y renuncias, visite http://www.openssl.org.
- Oracle Help for Java. Copyright © 1994-2006, Oracle Corporation.
- RoboHELP Office. Copyright © Adobe Systems Incorporated, antes conocido como Macromedia.
- Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Con la licencia Apache Software License. Para obtener más información y consultar las restricciones y renuncias, visite https://skinlf.dev.java.net/.
- Sonic Software Corporation. Copyright © 2003-2004. El software de SSC contiene software de seguridad bajo licencia de RSA Security, Inc.
- Tinyxml. Para obtener más información y consultar las restricciones y renuncias, visite http://grinninglizard.com/tinyxmldocs/index.html.
- SecurityNexus. Copyright © de 2003 a 2006. SecurityNexus, LLC. Reservados todos los derechos.
- Xalan y Xerces, ambos se otorgan bajo licencia de Apache Software Foundation Copyright © de 1999 a 2004. Para obtener más información y consultar las restricciones y renuncias, visite http://xml.apache.org/dist/LICENSE.txt.
- **yWorks. Copyright © de 2003 a 2006, yWorks.**

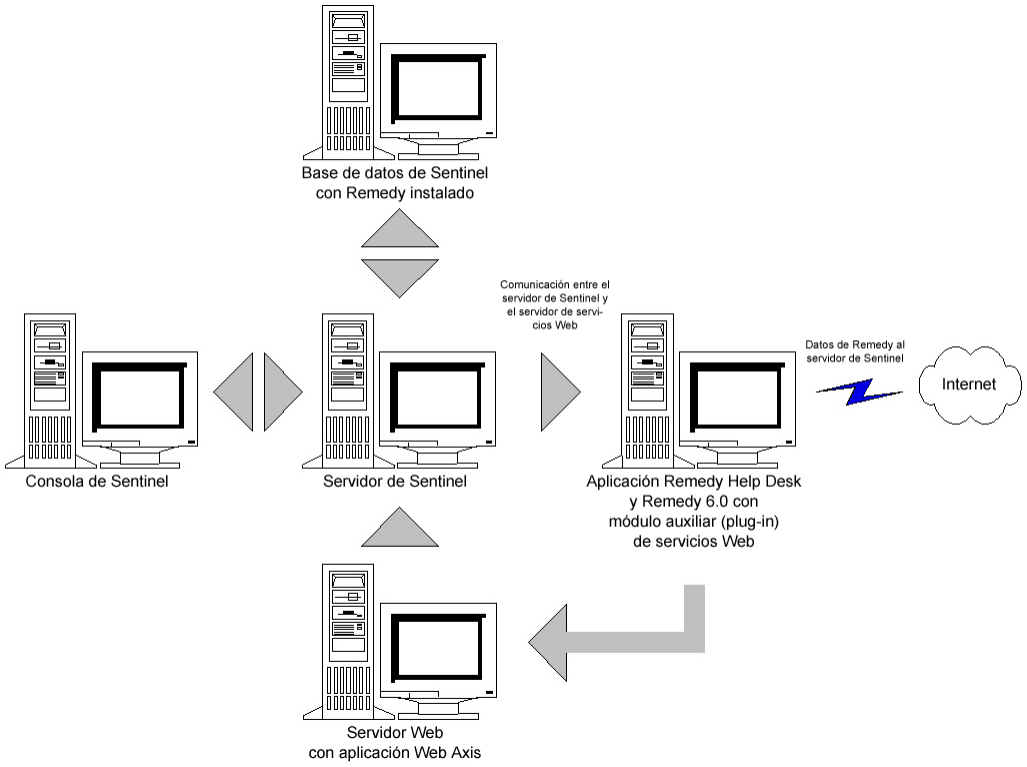
NOTA: A fecha de publicación de este documento, los enlaces indicados anteriormente están activos. En caso de que alguno de los enlaces anteriores esté roto o la página a la que enlace esté inactiva, póngase en contacto con Novell, en la dirección Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 EE.UU.

Contenido

1 Integración con Remedy

La integración de soluciones de Sentinel v4.2 o v5 puede utilizarse para crear aplicaciones de flujo de trabajo integradas tanto con el sistema Trouble Ticketing de Remedy como con el sistema Sentinel. Las características principales de la integración con Remedy son:

- Posibilidad de crear un nuevo caso en Remedy Help Desk (Ayuda técnica de Remedy) basado en una incidencia de Sentinel.
- Posibilidad de actualizar un caso relacionado en Help Desk (Ayuda técnica) cuando se actualice una incidencia de Sentinel.
- Posibilidad de actualizar una incidencia de Sentinel cuando se actualice un caso relacionado en Help Desk (Ayuda técnica).



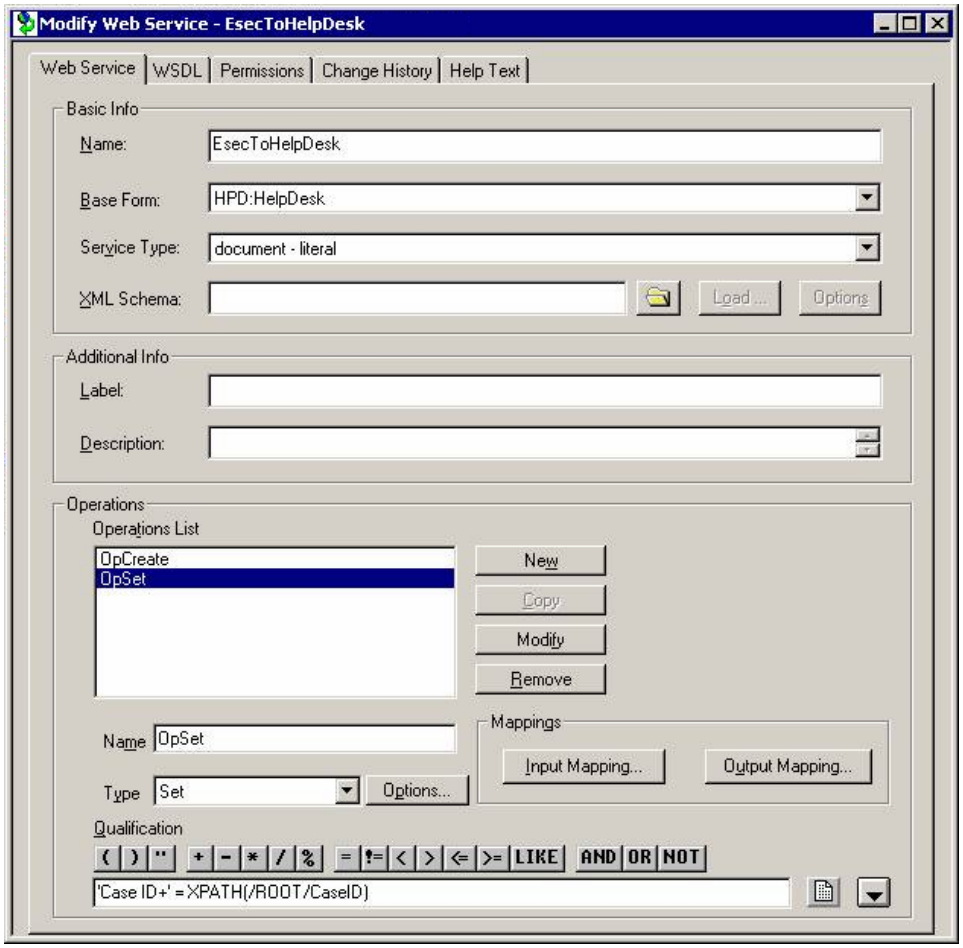
Configuración

Para cambiar el formulario de Remedy Help Desk Case (Caso de ayuda técnica de Remedy)

1. Entre a la sesión de *Remedy Administrador (Administrador de Remedy) > Forms (Formularios)*; haga doble clic en *HPD HelpDesk*.
2. Para que la integración con Sentinel sea posible, es necesario añadir un campo carácter (EsecIncidentId) y uno repositorio de adjuntos (Attachment Pool) al formulario de Help Desk Case (Caso de ayuda técnica). Estas entradas de campo servirán para añadir adjuntos de incidencias al formulario.
3. Para añadir el campo carácter EsecIncidentId:
   - Haga clic en el botón 'New Character Field' (Campo carácter nuevo) y colóquelo en cualquier lugar del formulario.
   - En la pestaña Display (Visualizar), defina una etiqueta.
   - En la pestaña Database (Base de datos), escriba el nombre para EsecIncidentID en el campo Name (Nombre).
4. Para añadir el campo de carácter Attachment Pool (Repositorio de adjuntos) con los tres campos siguientes: EsecEvents, EsecVuln y EsecAdv.
   - Haga clic en el botón '*Create Attachment Pool*' (Crear repositorio de adjuntos).
   - En la pestaña Display (Visualizar), introduzca un nombre para la etiqueta en el campo de la etiqueta (p. ej.: adjuntos esec).
   - En Adjuntar campos, en 'Enter Attachments Field Label' (Introducir etiqueta de campo de adjuntos), introduzca:
     - EsecEvent y haga clic en Añadir.
     - EsecVuln y haga clic en Añadir.
     - EsecAdv y haga clic en Añadir.
5. Haga clic en *Guardar*.

Creación del servicio Web

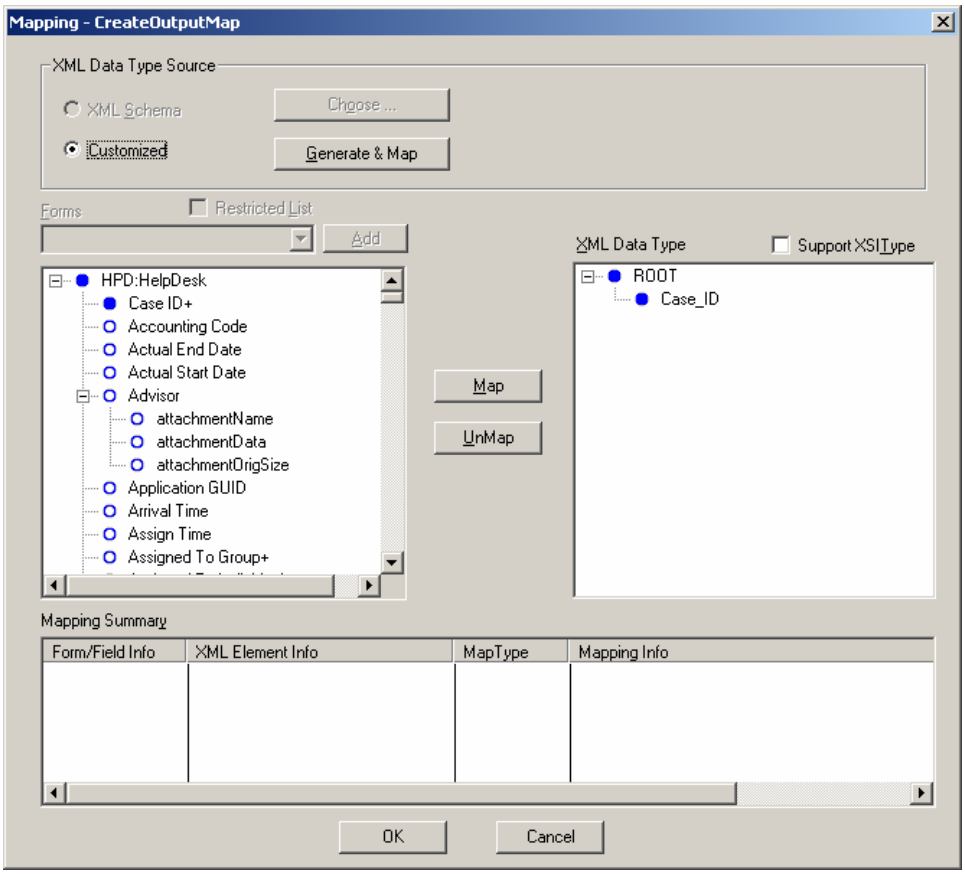
1. En el panel de navegación del Administrador de Remedy, resalte '*Servicios Web*'. Haga clic con el botón derecho del ratón en > *New Web Services* (Nuevos servicios Web) y, a continuación, haga clic en la pestaña '*Web Services*' (Servicios Web).



2. Con Help Desk Case (Caso de ayuda técnica) como formulario básico, cree un servicio Web denominado '*EsecToHelpDesk*' y seleccione 'HPD HelpDesk' como formulario básico.
3. Realice dos operaciones para este servicio Web denominadas:
   - opCreate
   - opSet

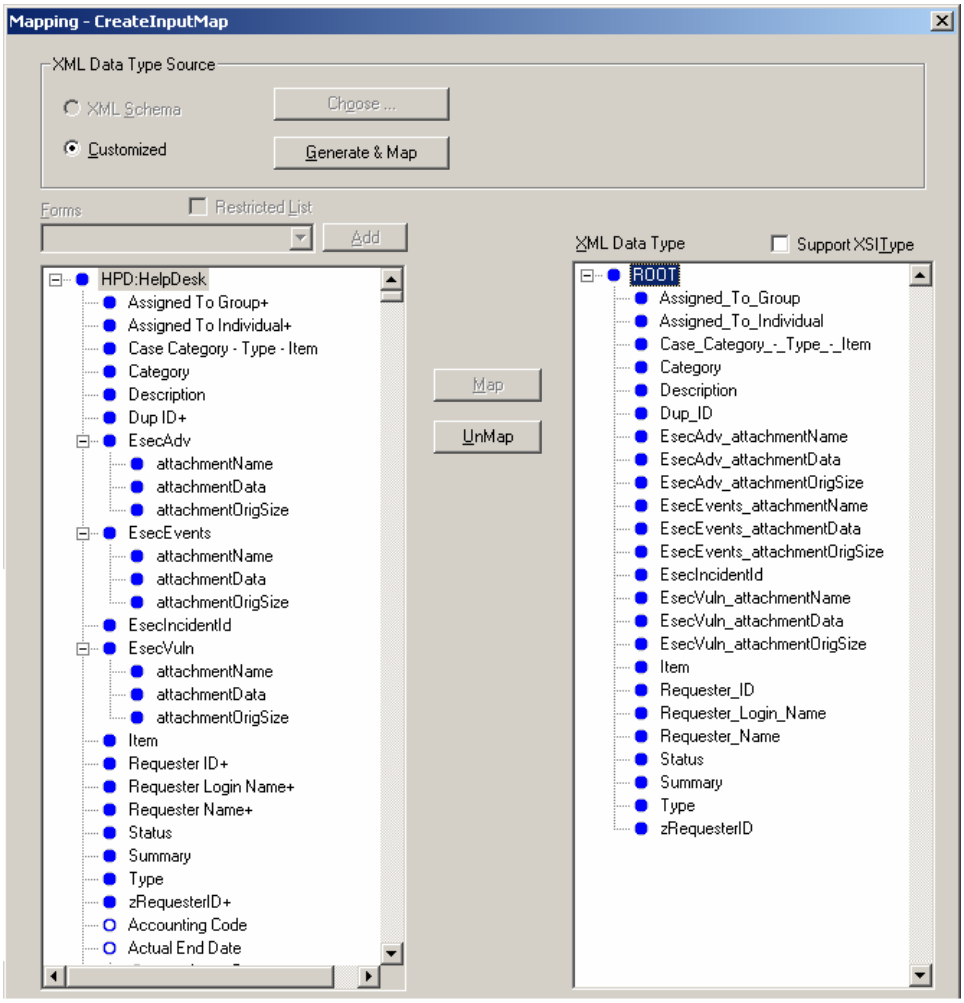
   y elimine el resto de operaciones.

4. Seleccione OpCreate y haga clic en el botón Output Mapping (Asignación de salida). Haga que las opciones de la pantalla coincidan con las de la ilustración siguiente.



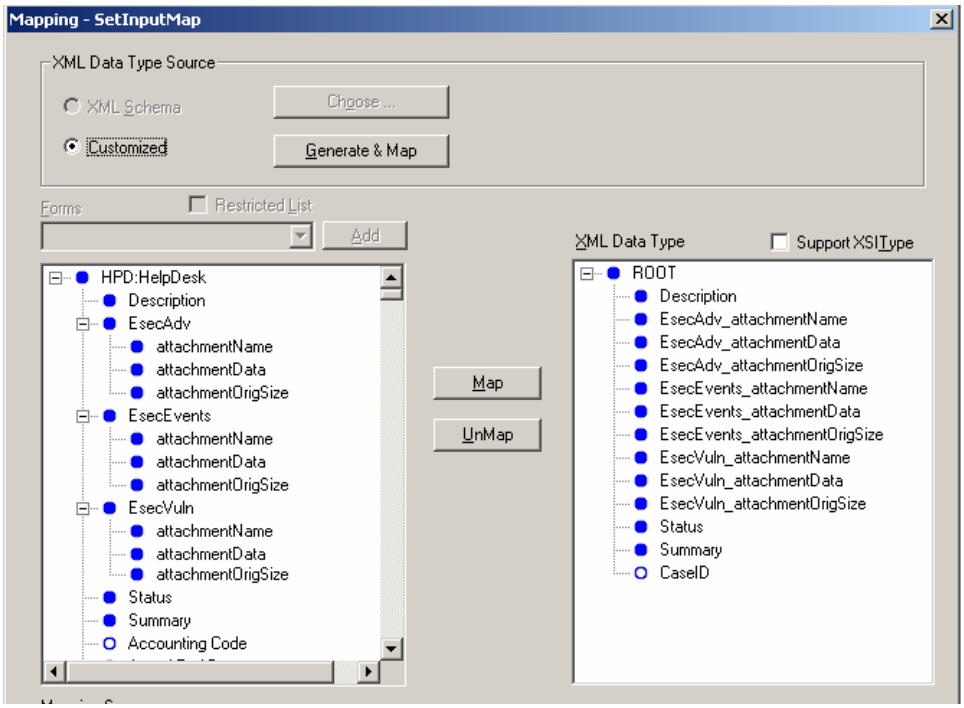
Seleccione el botón Input Mapping (Asignación de entrada) para opCreate. Haga que las opciones de la pantalla coincidan con las de la ilustración siguiente.

NOTA: Para eliminar un elemento, resáltelo > haga clic con el botón derecho del ratón > cortar.

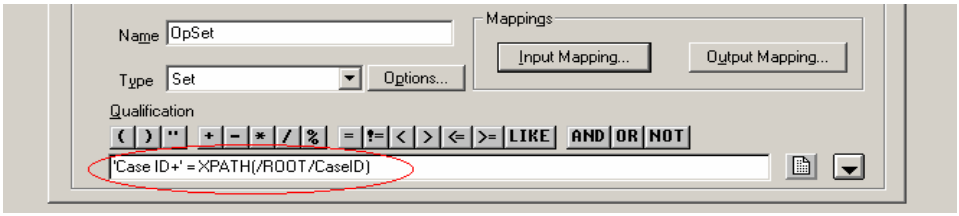


Haga clic en *Guardar*.

Seleccione el botón Input Mapping (Asignación de entrada) para opSet. Haga que las opciones de la pantalla coincidan con las de la ilustración siguiente.



No existe ninguna asignación de salida para opSet. Para opSet, es necesario especificar una cualificación:



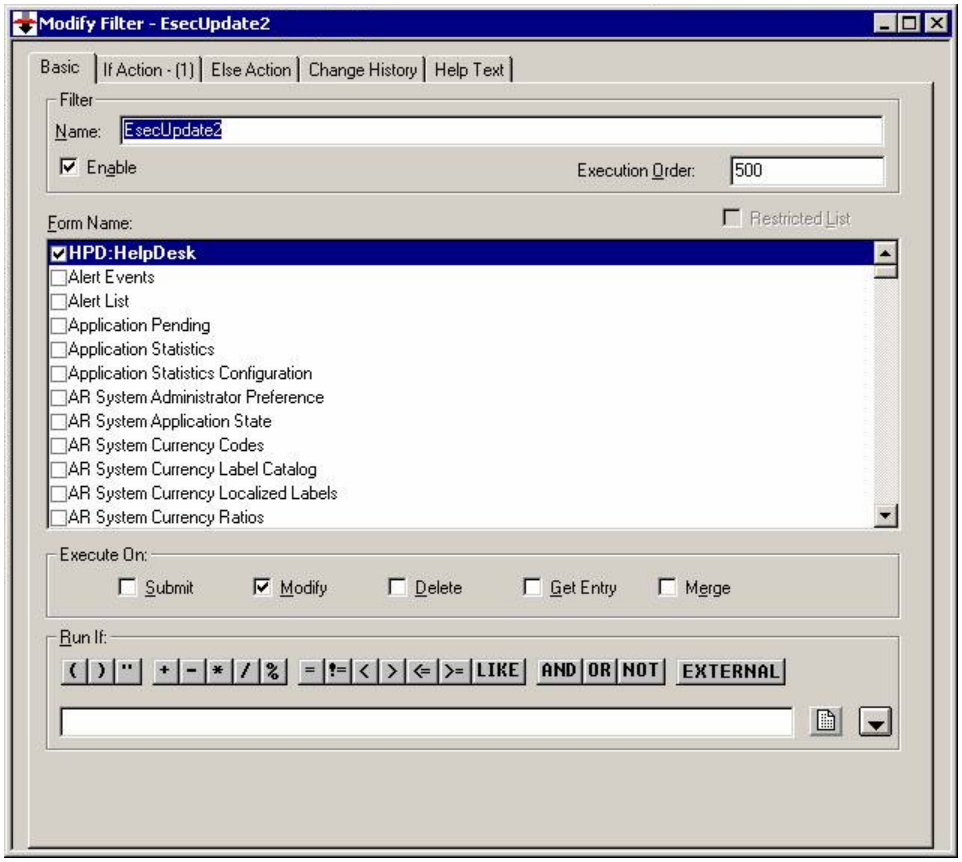
5. Vaya a la pestaña Permissions (Permisos) y cambie el servicio a Public (Público) desplazando Public (Público) de izquierda a derecha. Haga clic en *Guardar*.

De Remedy al flujo de datos de Sentinel

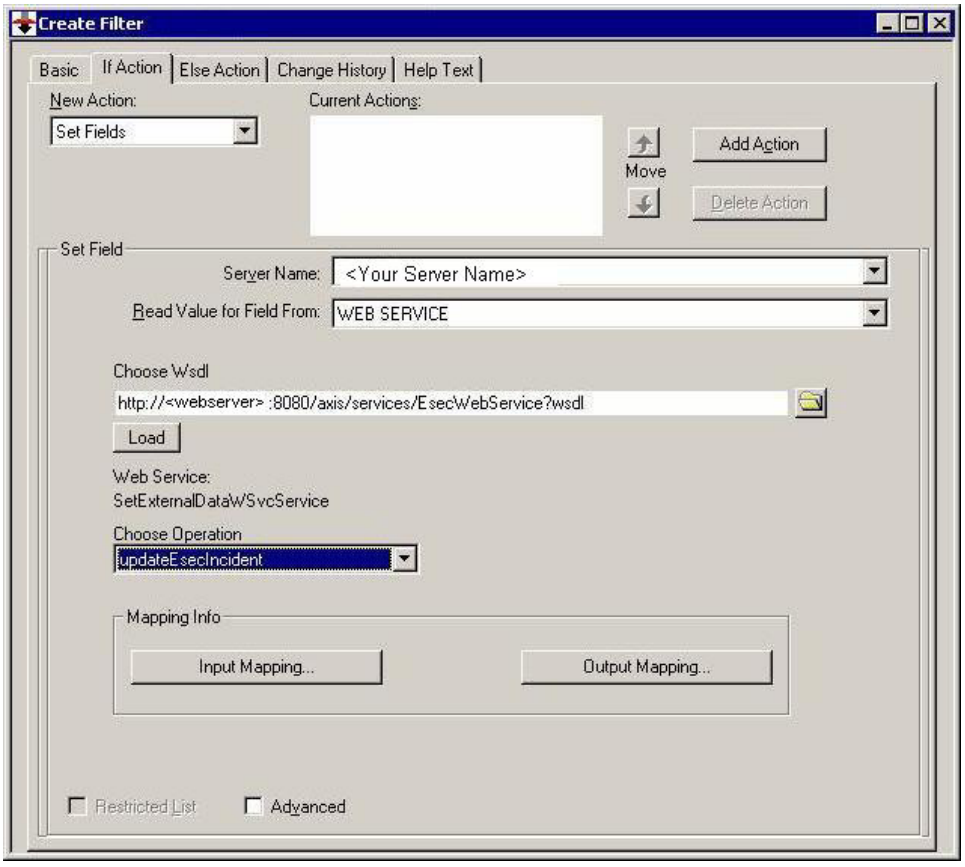
Para poder acceder al servicio Web de Sentinel, es necesario disponer de un servidor Web que esté ejecutando la aplicación Web Axis en el momento del inicio del servidor de Sentinel.

De Remedy al flujo de datos de Sentinel

1. En el Administrador de Remedy, resalte Filters (Filtros) y haga clic con el botón derecho del ratón en *Add Filter* (Añadir filtro).
2. Cree un filtro para el formulario de Help Desk Case (Caso de ayuda técnica) que se ejecuta en un evento modificado. Asegúrese de que las opciones de la pantalla coinciden con las de la ilustración siguiente.

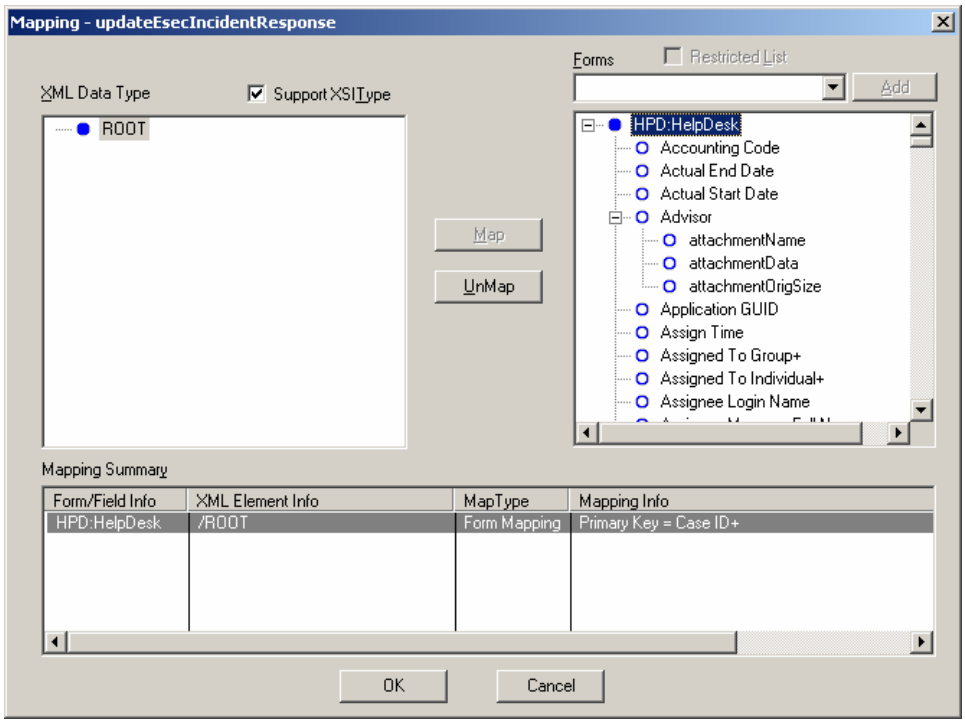


3. En la pestaña '*If Action*' (En caso de acción) del menú desplegable '*New Action*' (Nueva acción), seleccione la acción 'Set Field' (Establecer campo); en el panel 'Set Field' (Establecer campo) seleccione 'SERVICIO WEB' y proporcione la URL del servicio Web de Sentinel (http://<IP del servidor Web o nombre DNS>:8080/axis/services/EsecWebService?wsdl).



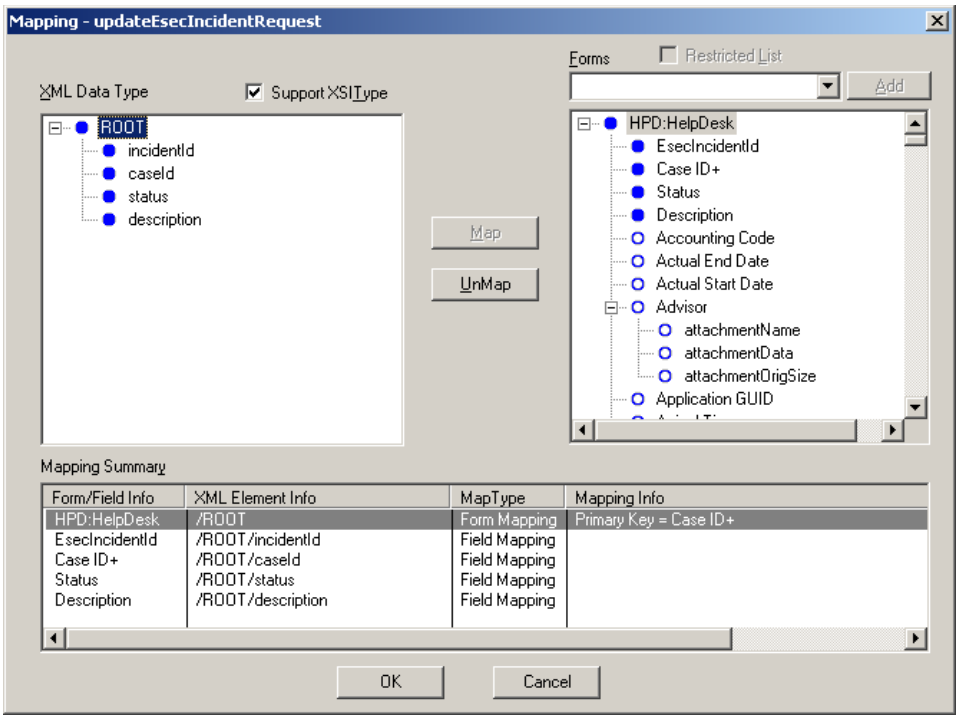
4. En el menú desplegable '*Choose Operation*' (Seleccionar operación), seleccione el método '*updateEsecIncident*' y defina la asignación de entrada y de salida.

Haga clic en el botón Output Mapping (Asignación de salida). Asegúrese de que las opciones de la pantalla coinciden con las de la ilustración.



Haga clic en el botón Input Mapping (Asignación de entrada). Asegúrese de que las opciones de la pantalla coinciden con las de la ilustración siguiente.

NOTA: Para establecer la asignación, seleccione un elemento de la izquierda (p. ej. incidentId), uno de la derecha (p. ej. EsecIncidentId) y haga clic en el botón Map (Asignar).



NOTA: Tras el inicio, cada vez que se guarda un cambio en el formulario de Help Desk Case (Caso de ayuda técnica), éste se enviará a un servicio de Sentinel.

5. Haga clic en *Guardar*.

Instalación de Sentinel

Para instalar Sentinel con Remedy, es necesario disponer de una cuenta en Remedy. Desde dicha cuenta se solicitará al usuario la información siguiente.

NOTA: Es necesario disponer de un permiso de integración con Remedy.

- Nombre de usuario
- Contraseña
- Nombre del peticionario
- ID del peticionario
- Entrada a la sesión del peticionario
- Nombre del grupo (se puede dejar en blanco)
- Nombre individual (se puede dejar en blanco)
- Nombre del servidor
- Nombre del servicio

Para Remedy al flujo de datos de Sentinel, se le solicitará:

- Servidor Web de Sentinel (<nombre de equipo:puerto>)
- Nombre de usuario de Sentinel (como, por ejemplo, esecadm)
- ID de usuario de Sentinel
- UUID de Sentinel
- ID de bloqueo de Sentinel (generalmente establecido en 1 ó 2, se trata de....

1. Seleccione la integración con Remedy durante la instalación.
2. Tenga a mano la información anterior durante el proceso de instalación.

Configuración de Remedy al flujo de datos de Sentinel

Si va a utilizar la integración con otros fabricantes (integración con Remedy), es recomendable realizar la instalación y la configuración en el orden siguiente:

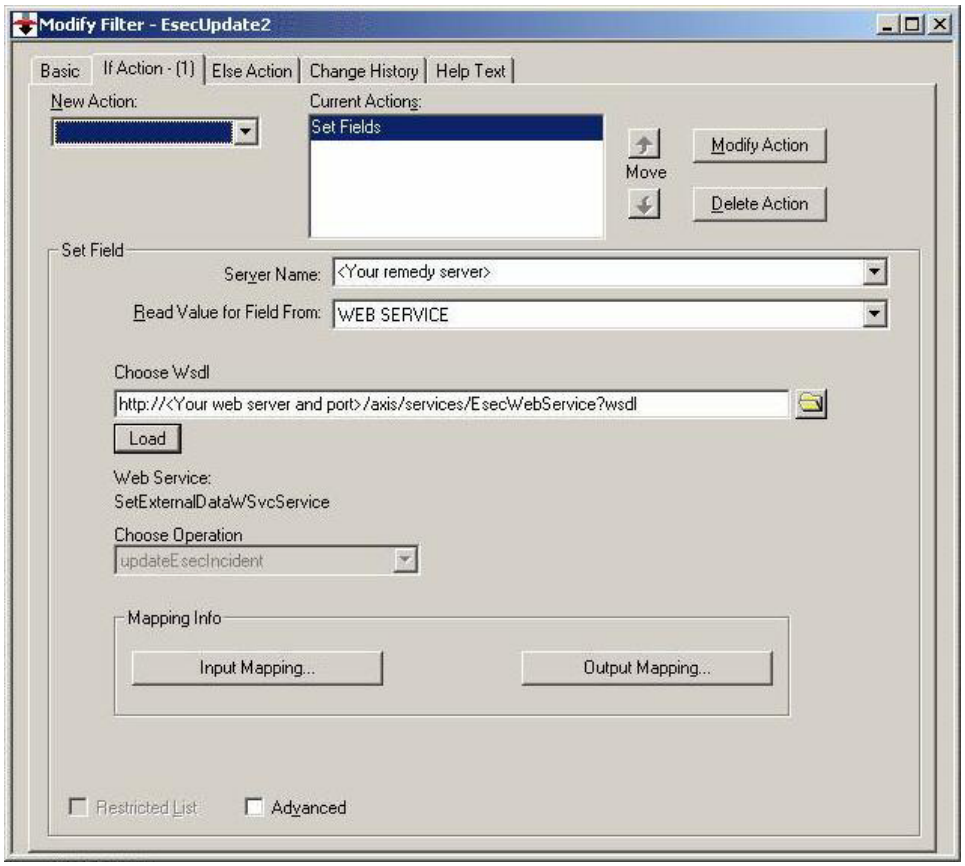
- Instalación de la aplicación Remedy Help Desk y Remedy 6.0 con el módulo auxiliar de servicios Web.
- Configuración de nuevos filtros y servicios Web en la aplicación Remedy Help.
- Instalación de Sentinel.

Para disponer de Remedy al flujo de datos de Sentinel, es necesario:

- Para poder acceder al servicio Web de Sentinel, es necesario disponer de un servidor Web que ejecute la aplicación Web Axis antes de iniciar el servidor de Sentinel.
- Copiar todos los archivos jar de la ubicación siguiente al servidor de Sentinel en <aplicación Web axis>\webclient\lib.
  - %ESEC_HOME%\lib
  - %ESEC_HOME%\sentinel\console
  - %ESEC_HOME%\communicator (sólo para v4.2)
- Copiar los archivos configuration.xml y keystore del servidor de Sentinel a la ubicación que desee de su servidor Web. Ambos archivos se encuentran en %ESEC_HOME%.
  - Editar configuration.xml en su servidor Web para que apunte al archivo. keystore.
  - Añadir la siguiente opción JVM al servidor Web,

```
Dcom.esecurity.configurationfile=<vía a
   configuration.xml>\configuration.xml
```

- Es necesario crear un filtro para el formulario de Help Desk Case (Caso de ayuda técnica) para que se ejecute en un evento “Modificado”. Este filtro llama el servidor Web de Sentinel.



2 Operaciones de Remedy Help Desk (Ayuda técnica de Remedy)

La integración de soluciones se puede utilizar para crear aplicaciones de flujo de trabajo. Las características de la integración con Remedy son:

- Posibilidad de crear un nuevo caso en Remedy Help Desk (Ayuda técnica de Remedy) basado en una incidencia de Sentinel.
- Posibilidad de actualizar un caso relacionado en Help Desk (Ayuda técnica), cuando se actualice una incidencia de Sentinel.
- Posibilidad de actualizar una incidencia de Sentinel, cuando se actualice un caso relacionado en Help Desk (Ayuda técnica).

Operaciones de Remedy Help Desk (Ayuda técnica de Remedy)

Envío de incidencias a Remedy Help Desk (Ayuda técnica de Remedy) (v5.0.1 y posterior)

1. Haga clic en la pestaña *Incidencias*.
2. En el panel del navegador, expanda la carpeta Vistas de la incidencia y resalte el Gestor de vistas de incidencias.

   NOTA: Si ya se ha establecido una incidencia para otro sistema externo, no será posible modificarla.

3. Expanda una de las vistas de incidencias y haga doble clic en la incidencia. La incidencia se abrirá.
4. Haga clic en el botón Remedy.

   La incidencia se actualizará con una pestaña Datos externos y el botón Remedy.

Actualización de incidencias en Remedy Help Desk (Ayuda técnica de Remedy) (v5.0.1. y posterior)

1. Haga clic en la pestaña *Incidencias*.
2. Expanda el panel del navegador de la izquierda y haga doble clic en una incidencia establecida para Remedy Help Desk (Ayuda técnica de Remedy).
3. Haga clic en el botón Remedy de la incidencia. Se añadirá una anotación en la ficha Externa.

Reconfiguración manual de los valores de la interfaz de Remedy

Durante la instalación inicial de la interfaz de Remedy Help Desk (Ayuda técnica de Remedy), los valores de Remedy se almacenan en el archivo das_query.xml. Utilice la información de esta sección de la documentación si desea modificar estos valores tras la instalación.

Valores de Remedy

Los valores de Remedy se almacenan en el archivo das_query.xml en el componente RemedyARServerService del modo siguiente:

Restauración de la contraseña de Remedy

Las contraseñas de Remedy se almacenan en formato codificado en el archivo das_query.xml. Por lo tanto, si desea restaurar las contraseñas almacenadas en dicho archivo, deber_ utilizar la utilidad que se describe a continuación.

Para restaurar la contraseña de la interfaz de Remedy:

1. Cambie al directorio %ESEC_HOME%/sentinel/bin/
2. Introduzca:

```
extconfig -n das_query.xml [-r contraseña_de_remedy]
```

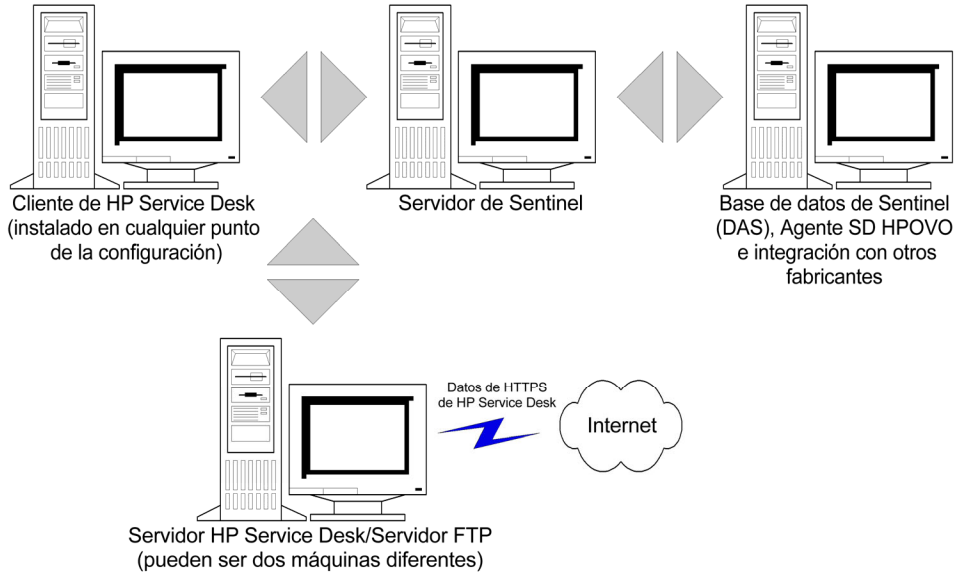
   - -r es la contraseña de Remedy

3 Instalación de HP OpenView Service Desk para Windows

La integración bidireccional de Sentinel con el Servicio de atención al cliente de HP OpenView, que tiene una licencia distinta, ofrece funciones nuevas y útiles a la consola de Sentinel. Sentinel aprovecha las funciones de Asset Management (Gestión del activo) de HP OpenView Service Desk para proporcionar información de referencia útil para responder a ataques y amenazas de seguridad. Estas nuevas funciones permiten:

- Enviar incidencia(s) a HP Service Desk (SD)
- Adjuntar evento(s) a una incidencia de HP SD
- Adjuntar información de vulnerabilidades a una incidencia de HP SD
- Solicitar e incorporar información del elemento de configuración (activo) tanto al incidente de la consola de Sentinel como a SD
- Integración recíproca: SD envía actualizaciones a Novell y Novell envía actualizaciones a SD
- Actualizar el estado de la incidencia de SD desde la consola de Sentinel de Novell
- Actualizar el estado de la incidencia de Sentinel desde HP SD

A continuación se muestra la configuración de instalación típica. Es posible que su configuración sea distinta.



Requisitos del sistema

Para obtener información acerca de los requisitos de software y hardware del agente, el servidor y el cliente de HP OpenView Service Desk consulte la HP OpenView Service Desk Installation Guide (Guía de instalación de HP OpenView Service Desk).

Sentinel es compatible con las versiones siguientes de HP OpenView Service Desk:

- Servidor de HP OpenView Service Desk - Versión 4.5 con Service Pack 8 (4.5.0588.0802 SP 8)
- Cliente de HP OpenView Service Desk - Versión 4.5 con Service Pack 8
- Agente de HP OpenView Service Desk - Versión 4.5 con Service Pack 8
- Sentinel 4.2.1.8 ó 4.2.1.15 para Windows
- Cualquier servidor FTP de otros fabricantes

El cliente y el servidor de HP OpenView Service Desk deben estar instalados en una máquina designada como servidor de Service Desk. Consulte la HP OpenView Service Desk Installation Guide (Guía de instalación de HP OpenView Service Desk) para obtener más información acerca de la instalación de Service Desk.

Para poder activar esta interfaz bidireccional, es necesario tener instalado un agente de HP OpenView en la misma máquina en la que se ha instalado das_cmd.bat. La interfaz bidireccional permite a HP Service Desk notificar a Sentinel todas las modificaciones realizadas en el estado de una incidencia originada en Sentinel por parte de un usuario de Service Desk. Estas incidencias deben originarse en la consola de Sentinel.

Para que Service Desk pueda manipular los adjuntos, es necesario tener instalado un servidor FTP (normalmente en el servidor de Service Desk), y Service Desk debe estar configurado de forma que pueda comunicarse con él. Se puede utilizar un servidor FTP de cualquier fabricante. Consulte la guía de instalación de su servidor FTP para obtener más información acerca de la instalación del servidor FTP.

Instalación

Si también está instalando HP OpenView Operations, es recomendable instalar HP OpenView Operations antes que HP OpenView Service Desk.

NOTA: Durante la instalación inicial de la interfaz de HP OpenView Service Desk de otros fabricantes, los valores de Service Desk y OpenView se almacenan en el archivo das_query.xml. Para modificar cualquiera de estos valores (como, por ejemplo, el nombre de usuario o la contraseña), consulte *Operation - HP OpenView and Service Desk for Windows 2000 (Operación - HP OpenView y Service Desk para Windows 2000)*.

Es recomendable realizar la instalación en el orden siguiente:

- Servidor FTP

  NOTA: Consulte la guía de instalación de su servidor FTP para obtener más información acerca de la instalación del servidor FTP.

- Servidor de HP OpenView Service Desk con Service Pack 8; en el mismo lugar que el servidor FTP
- Cliente de HP OpenView Service Desk con Service Pack 8
- Agente de HP OpenView Service Desk con Service Pack 8 (para activar la interfaz bidireccional); debe instalarse en la máquina en la que se ha instaladoDAS.

  NOTA: Consulte la HP OpenView Service Desk Installation Guide (Guía de instalación de HP OpenView Service Desk) para obtener más información acerca de la instalación del software HP OpenView Service Desk.

- Instalación de la integración con otros fabricantes de Sentinel
  - HP OpenView Service Desk

  NOTA: Para obtener información acerca de la instalación, consulte las Notas de la versión de Sentinel v4.2.1.8 y la Guía de instalación de Sentinel v4.2 para Windows y Solaris.

Configuración de HP OpenView Service Desk

La configuración del Servicio de atención al cliente de HP OpenView se realiza a través del cliente de Service Desk. Antes de modificar la configuración de HP Service Desk para que se comunique con el servidor FTP, tenga a mano la información siguiente:

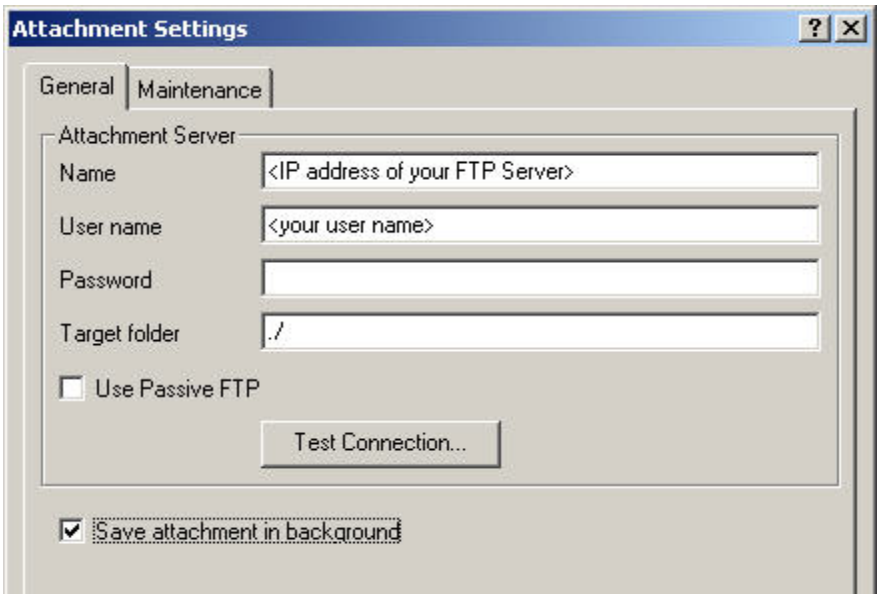
- Nombre: dirección IP del servidor FTP.
- Nombre de usuario/Contraseña: cualquier usuario definido en el servidor FTP.
- Target Folder (Carpeta de destino): se recomienda introducir "./". De este modo, el directorio FTP se colocará en el directorio FTP actual.
- Desmarque la casilla 'Use Passive FTP' ('Usar FTP pasivo').
- Marque la casilla 'Save attachment in background' (Guardar adjunto en segundo plano).

  NOTA: Para obtener más información, consulte la sección Post Installation Tasks (Tareas posteriores a la instalación) de la HP OpenView Service Desk Installation Guide (Guía de instalación de HP OpenView Service Desk), donde encontrará descritos de forma detallada los pasos de la configuración.

Para establecer los valores del adjunto

1. Inicie el cliente de HP Service Desk.
2. Haga clic en *Tools* (Herramientas) > *System* (Sistema).
3. Haga clic en *System Panel* (Panel del sistema) en el panel del navegador de la izquierda.
4. Haga doble clic en *Attachment Settings* (Valores del adjunto). Introduzca:
   - Name (Nombre): dirección IP del servidor FTP
   - Username/Password (Nombre de usuario/Contraseña): cualquier usuario definido en el servidor FTP.
   - Target Folder (Carpeta de destino): se recomienda introducir "./". De este modo, el directorio FTP se colocará en el directorio FTP actual.
   - Desmarque la casilla '*Use Passive FTP*' ('Usar FTP pasivo').
   - Marque la casilla '*Save attachment in background*' (Guardar adjunto en segundo plano).

NOTA: Para obtener más información, consulte la sección Post Installation Tasks (Tareas posteriores a la instalación) de la HP OpenView Service Desk Installation Guide (Guía de instalación de HP OpenView Service Desk), donde encontrará descritos de forma detallada los pasos de la configuración.



5. Haga clic en *Test Connection* (Probar conexión).
6. Haga clic en *Aplicar* y, a continuación, en *Aceptar*.

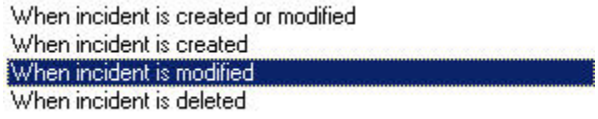
Activación de la interfaz de Service Desk a Sentinel (bidireccional)

Esta opción permite a HP OVO OpenView Service Desk notificar las modificaciones realizadas en el estado de una incidencia (originada en Sentinel) por parte de un usuario de Service Desk. Esto permite realizar un seguimiento del estado actual de cada incidencia enviada previamente a HP OVO OpenView Service Desk.

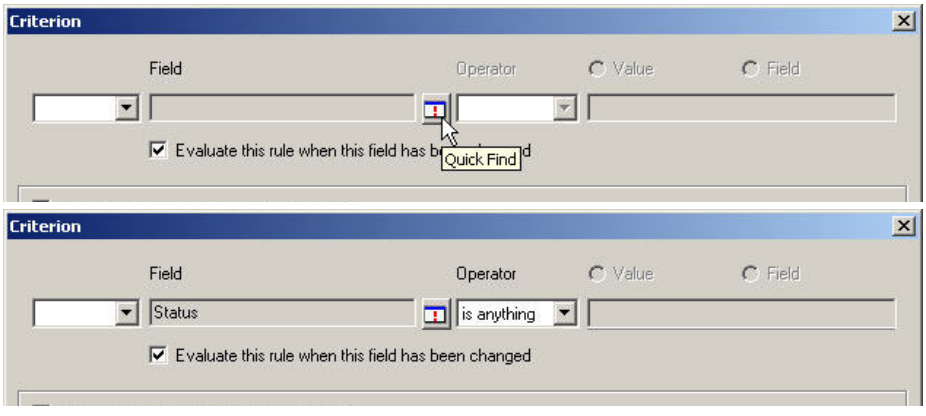
Para poder activar esta función, es necesario que el agente de HP OVO OpenView Service esté instalado en la misma máquina en la que se encuentra instalado Sentinel (das_cmd.bat). Esto permite que HP Service Desk pueda ejecutar la utilidad das_cmd de Sentinel.

Activación de la interfaz bidireccional

1. Inicie el cliente de Service Desk.
2. Visualice la consola del administrador seleccionando *Tools* (Herramientas) > *System* (Sistema).
3. Haga clic en Business Logic (Lógica empresarial) en el panel del navegador de la izquierda.
4. Haga doble clic en *Database Rules* (Reglas de base de datos).
5. Haga doble clic en *Incident* (Incidencia). Aparecerá la ventana con la lista de reglas de la base de datos.
6. Haga clic con el botón derecho del ratón en el panel Database Rules (Reglas de base de datos) > *New Database Rule* (Nueva regla de base de datos).
7. Resalte 'When incident is modified' ('Cuando se modifique una incidencia') y haga clic en Next (Siguiente).

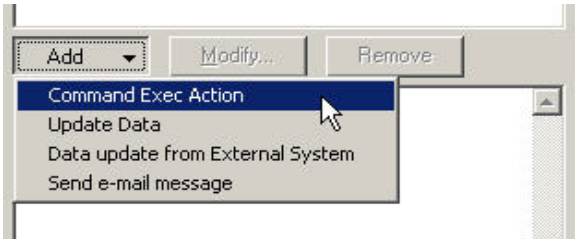


8. Haga clic en el botón *Condition...* (Condición).
9. Haga clic en el botón *Add Criterion...* (Añadir criterio).
10. Haga clic en el botón *Quick Find* (Búsqueda rápida), seleccione *Status* (estado) y seleccione '*is anything*' ('es cualquiera') en el campo del operador.



Haga clic en *Aplicar* y, a continuación, en *Aceptar*.

11. Haga clic en *Añadir*. Seleccione *Command Exec* Action (Acción ejec. comando).



12. Añada una nueva "Acción ejec. comando" de modo que el guión "das_cmd.bat" se ejecute en el servidor de Sentinel cada vez que se evalúe la regla.

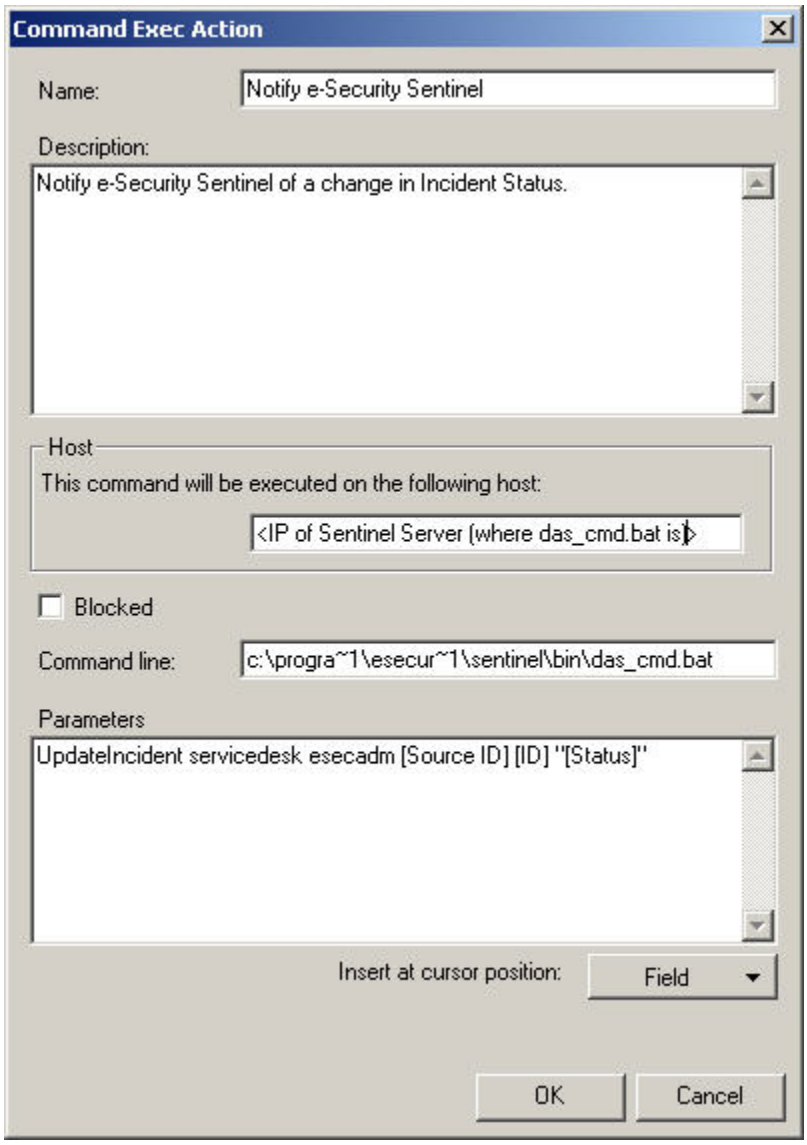
    Al configurar la acción, asegúrese de especificar el nombre (o dirección IP) del servidor de Sentinel (la máquina en la que se encuentra das_cmd.bat) como el "Host". No olvide tampoco especificar la vía completa del archivo "das_cmd.bat" en el servidor de Sentinel, en "Command Line" ("Línea de comando"), como:

    ```
    c:\progra~1\esecur~1\sentinel\bin\das_cmd.bat
    ```

NOTA: Utilice la convención de nombres DOS 8.3 para especificar los nombres de directorios con espacios. Por ejemplo, utilice "progra~1" en lugar de "Archivos de programa".

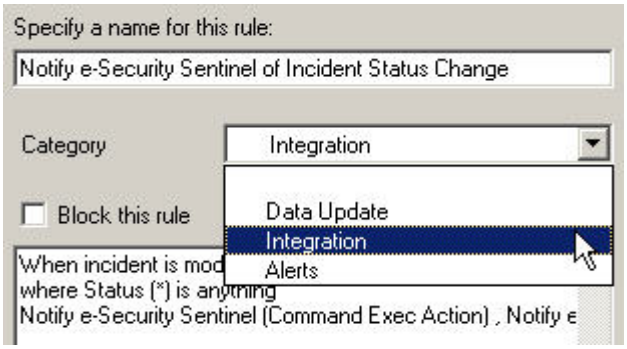
Y, por último, especifique la acción “Parameters” (“Parámetros”) como:

```
UpdateIncident servicedesk esecadm [Source ID] [ID]
   "[Status]"
```



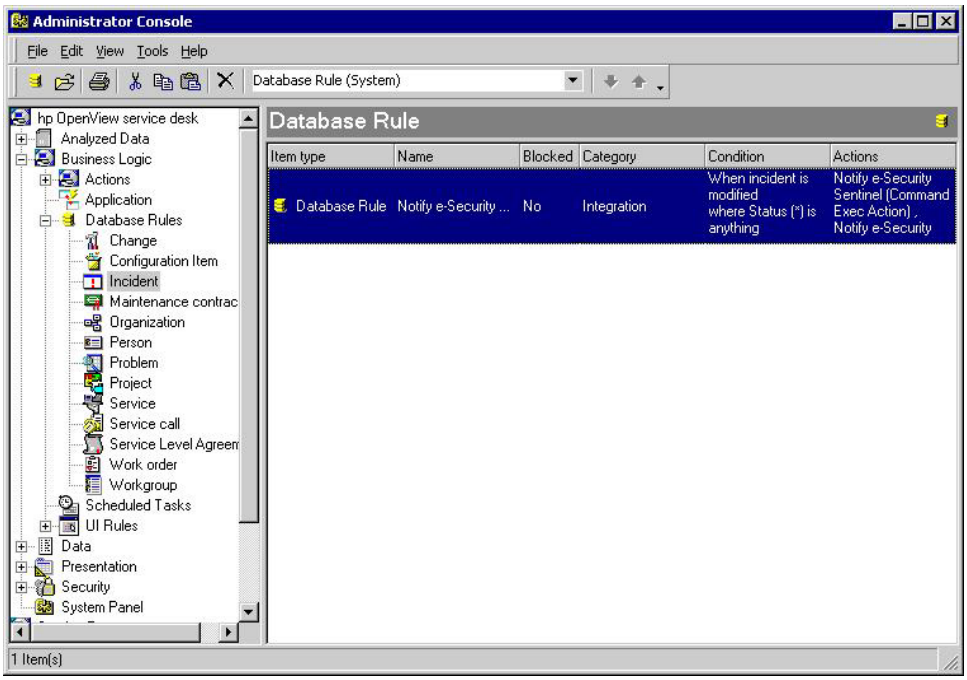
Otorgue a la nueva regla de la base de datos el nombre que desee con una descripción. Haga clic en *Aceptar* y, a continuación, en *Siguiente*.

13. En el campo Category (Categoría), seleccione Integration (Integración) y especifique un nombre para esta regla. No seleccione '*Block this rule*' ('Bloquear esta regla').



Haga clic en *Finalizar*.

14. Al finalizar la nueva regla de la base de datos, aparecerá una nueva regla en la lista Regla de base de datos.



4 Integración con HP OpenView Service Desk

HP OpenView Service Desk para Sentinel permite enviar eventos desde cualquier pantalla en la que se visualicen incidencias y eventos a HP OpenView Service Desk.

HP OpenView Service Desk

La integración de Sentinel con el Servicio de atención al cliente de HP OpenView permite disponer de funciones adicionales de gestión del activo. Esta función adicional de gestión del activo permite:

- Enviar incidencia(s) a HP Service Desk (SD).
  - Adjuntar evento(s) a una incidencia de HP SD.
  - Adjuntar información de vulnerabilidades a una incidencia de HP SD.
  - Adjuntar información del asesor a una incidencia de HP SD.
  - Solicitar e incorporar información del elemento de configuración (activo) a la consola control de Sentinel.
- Actualizar el estado de la incidencia de SD desde la consola de control de Sentinel.
- Actualizar el estado de la incidencia de Sentinel desde HP SD.

La información de la incidencia de Sentinel que se envía a HP OpenView Service Desk incluye:

- ID de la incidencia de Sentinel
- Estado
- Título
- Anotaciones/Historial
- Eventos (adjunto)
- Información de vulnerabilidades (adjunto)
- Información del asesor (adjunto)

Al enviar o recibir información desde HP OpenView Service Desk, se produce un estado automático, una asignación de estado y una conversión.

La asignación y conversión del estado de Sentinel al estado de Service Desk es como se muestra a continuación:

Estado de Sentinel	Estado de Service Desk
Abierto	Registrado
Reconocido	En espera
Asignado	Informado
Investigando	En proceso
Positivo falso	Cerrado
Verificado	Completado
Aprobado	En proceso
Cerrado	Cerrado

La asignación y conversión del estado de Service Desk al estado de Sentinel es como se muestra a continuación:

Estado de Service Desk	Estado de Sentinel
Registrado	Abierto
En proceso	Investigando
En espera	Reconocido
Completado	Verificado
Informado	Asignado
Cerrado	Cerrado

Envío de incidencias a HP OpenView Service Desk

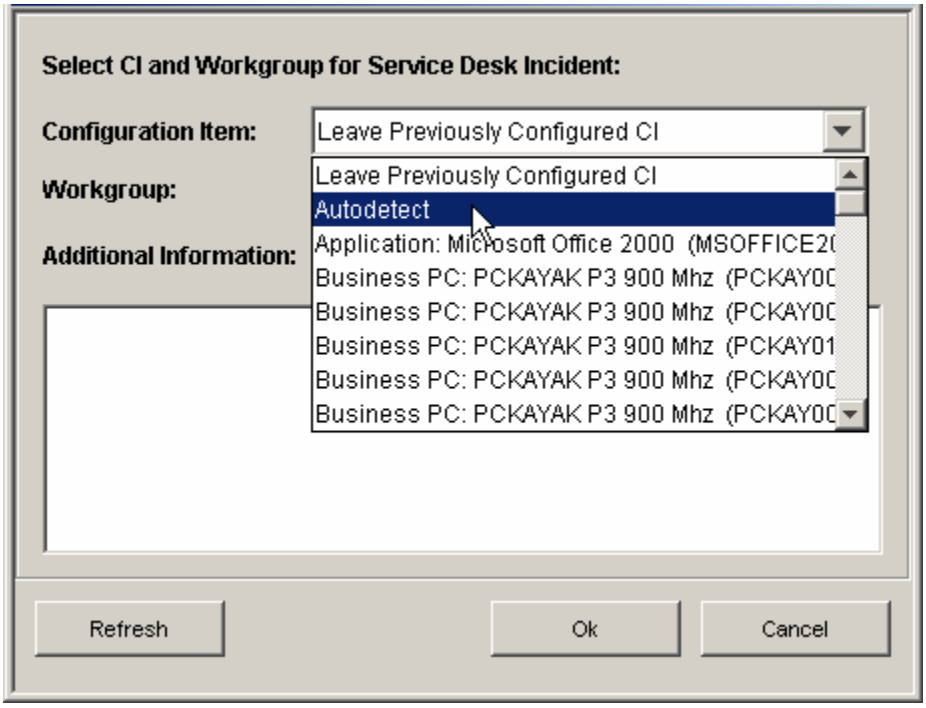
Para enviar una incidencia a HP OpenView Service Desk

1. Haga clic en la pestaña *Incidencias*.
2. En el panel del navegador, expanda la carpeta Vistas de la incidencia y resalte el Gestor de vistas de incidencias.

   NOTA: Si ya se ha establecido una incidencia para otro sistema externo, no será posible modificarla.

3. Expanda una de las vistas de incidencias y haga doble clic en la incidencia. La incidencia se abrirá.
4. Haga clic en el botón *HP SD*.

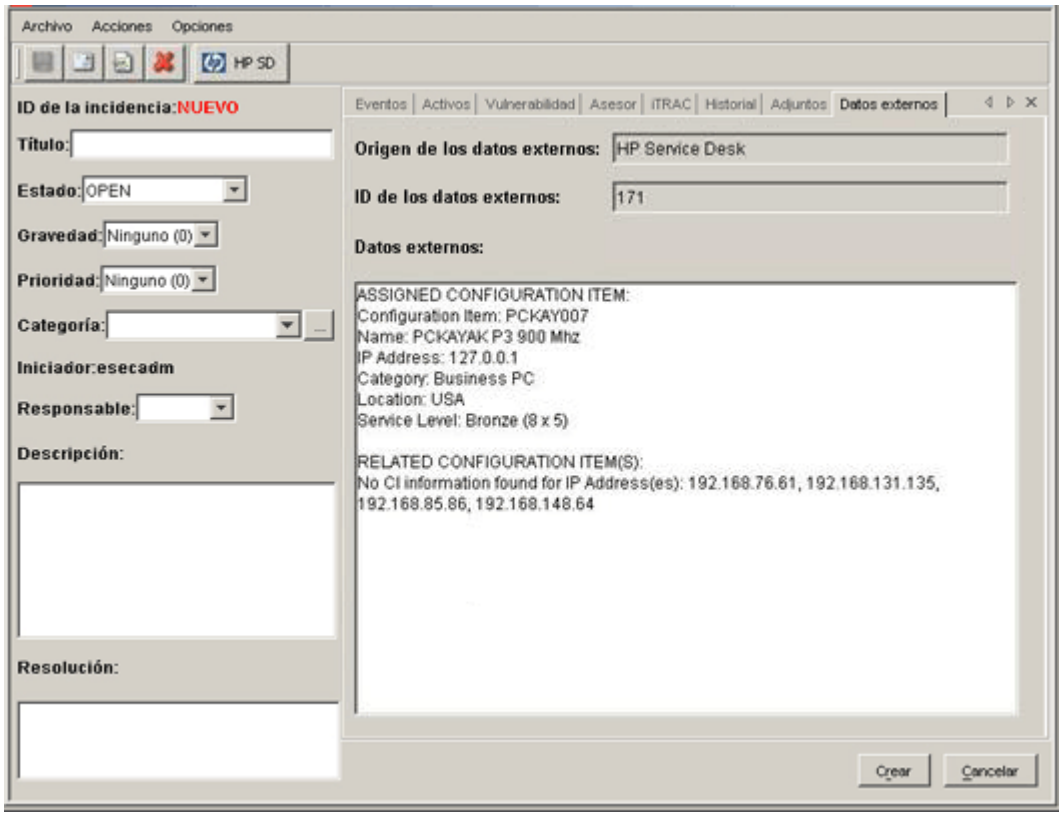
5. Aparecerá la ventana Enviar incidencia a *HP Service Desk*. El menú desplegable Enviar a Service Desk ofrece una lista de selección de elementos de configuración en la que se encuentran los elementos de configuración consultados desde HP Service Desk.



En la lista de selección Elemento de configuración existe una opción Autodetectar. Si se selecciona Autodetectar, Sentinel intentará utilizar las direcciones IP de destino de los eventos asociados con la incidencia de Sentinel para determinar automáticamente el EC de Service Desk.

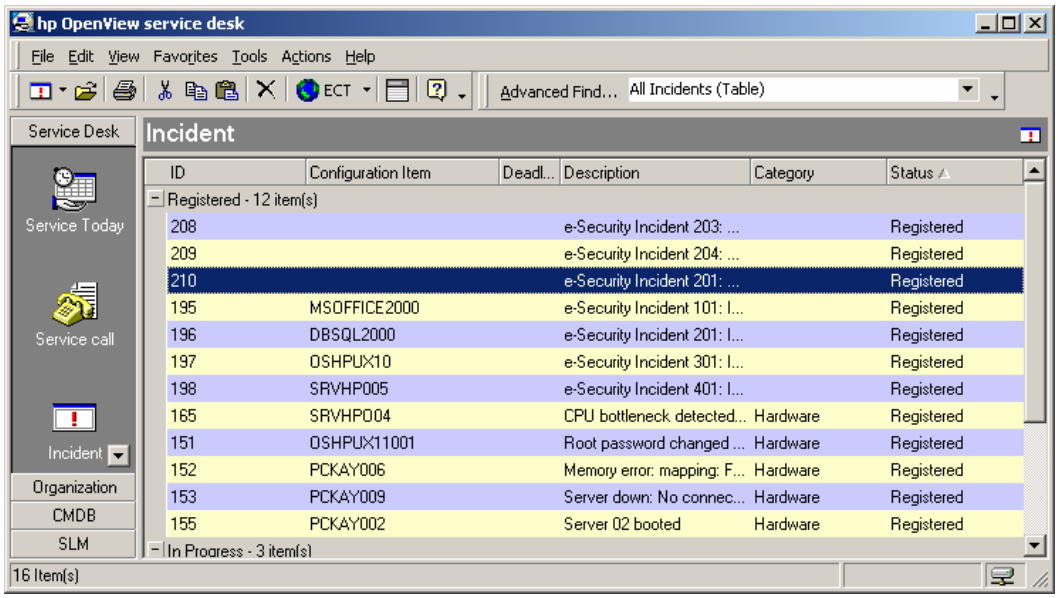
6. (opcional) El cuadro de diálogo Enviar a Service Desk también proporciona una lista de selección de grupos de trabajo en la que se encuentran los grupos de trabajo consultados desde Service Desk.
7. Haga clic en *Aceptar* y el incidente se remitirá a HP *OpenView Service Desk*.

NOTA: La pantalla de incidencias de Sentinel se actualiza con una pestaña Datos externos. La pestaña Datos externos indica el ID de la incidencia de Service Desk y el elemento de configuración de Service Desk al que se ha asignado la nueva incidencia de Service Desk.



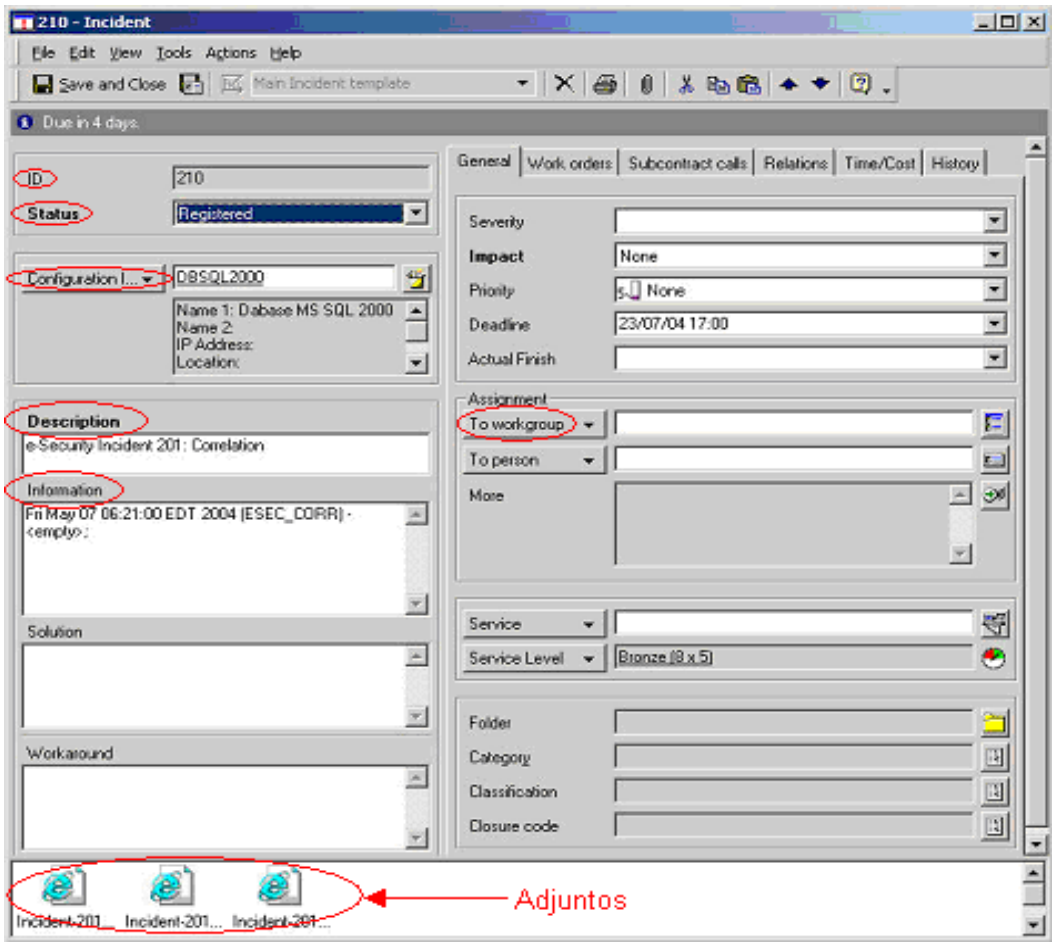
Cliente de HP OpenView Service Desk

Tras el envío de una incidencia a HP OpenView Service Desk, ésta aparecerá en el cliente de HP OpenView Service Desk. En el cliente de Service Desk, la incidencia aparece clasificada por su ID de datos ampliados, no por su número de ID de incidencia.



Al hacer doble clic en una incidencia aparece la visualización detallada de la misma.

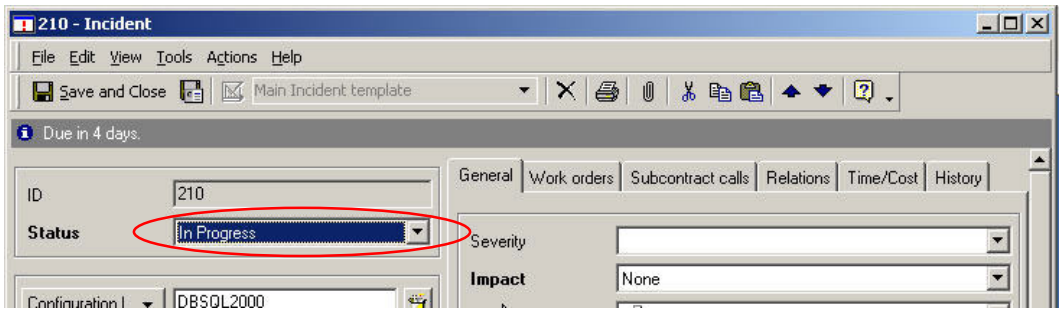
- ID de origen ampliado
- Estado
- Elemento de configuración
- Descripción
- Información
- Grupo de trabajo
- Información del evento (adjunto)
- Información de vulnerabilidades (adjunto)
- Información del Asesor (adjunto)



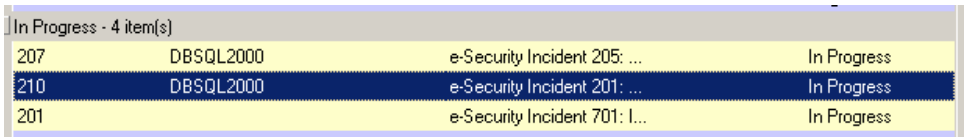
HP OpenView Service Desk: Interfaz bidireccional

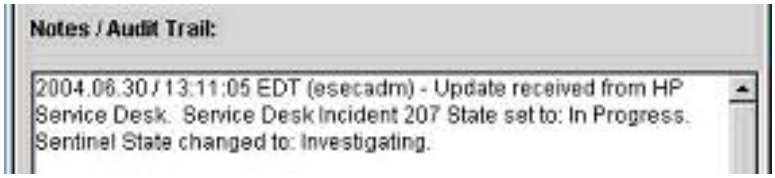
Si se activa esta opción, (consulte la Guía de instalación de Sentinel) Service Desk notificar_ a Sentinel todas las modificaciones realizadas en el estado de una incidencia (originada en Sentinel) por parte de un usuario de Service Desk. Esto permite a los usuario de Sentinel realizar un seguimiento del estado actual de cada incidencia enviada a Service Desk.

Si se visualiza una pantalla detallada, se modifica y se guarda, la pantalla detallada indicará un estado En progreso.



Esta actualización también puede visualizarse en el cliente de HP OpenView Service Desk y en la ventana de la incidencia de la consola de Sentinel.





Reconfiguración manual de los valores de la interfaz de HP OpenView Service Desk

Durante la instalación inicial de la interfaz de HP OpenView Service Desk de otros fabricantes, los valores de Service Desk se almacenan en el archivo das_query.xml. Utilice la información de esta sección de la documentación si desea modificar estos valores tras la instalación.

Valores de HP OpenView Service Desk

Los valores de HP OpenView Service Desk se almacenan en el archivo das_query.xml, en el componente HpServiceDeskService, del modo siguiente:

- server: ajustado a la dirección IP/nombre de host de Service Desk.
- username: ajustado al nombre de usuario del servidor de Service Desk.
- password: ajustado a la contraseña cifrada del servidor de Service Desk mediante la utilidad descrita en la sección Restauración de las contraseñas de HP OpenView.
- attachment_path: ajustada automáticamente al directorio "attach" de otros fabricantes.
- ftp_server: ajustado a la dirección IP/nombre de host del servidor FTP (que utilizará Service Desk para los adjuntos).
- ftp_username: ajustado al nombre de usuario de FTP (que utilizará Service Desk para los adjuntos).
- ftp_password: ajustado a la contraseña de usuario de FTP codificada (que utilizará Service Desk para los adjuntos) mediante la utilidad descrita en la sección Restauración de las contraseñas de HP OpenView.
- ftp_user_home: ajustado a la vía completa del directorio del usuario FTP.
- attachment.events: ajustada en "sí" para indicar que se utilizarán los adjuntos de eventos.
- attachment.events.filename: nombre de archivo que se utiliza para los archivos adjuntos de eventos.
- attachment.vuln: ajustado en "sí" para indicar que se utilizará el adjunto Vulnerabilidad.
- attachment.vuln.filename: nombre de archivo que se utilizará para los archivos adjuntos de Vulnerabilidad.
- attachment.adv.attack: ajustado en "sí" para indicar que se utilizará el adjunto Ataque del asesor.
- attachment.adv.attack.filename: nombre de archivo que se utiliza para los archivos adjuntos Ataque del asesor.

Restauración de las contraseñas de HP OpenView

Las contraseñas de HP OpenView se almacenan en formato codificado en el archivo das_query.xml. Por lo tanto, si desea restaurar las contraseñas almacenadas en dicho archivo, deber_ utilizar la utilidad que se describe a continuación.

Para restaurar los valores de la interfaz de HP OpenView Service Desk

1. Cambie al directorio %ESEC_HOME%/sentinel/bin/
2. Introduzca:

```
extconfig -n das_query.xml [-s sd_password] [-f
   sd_ftp_password]
```

   - -s es la contraseña del servidor de HP OpenView Service Desk
   - -f es la contraseña del servidor FTP (del servidor FTP que Service Desk utilizar_ para los adjuntos)

Índice