Novell® Sentinel™

6.0.2

www.novell.com

Volume V – 3RD PARTY INTEGRATION GUIDE

January 2008

Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to any and all parts of Novell software, to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to http://www.novell.com/info/exports/ for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at http://www.novell.com/company/legal/patents/ and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products and to get updates, see www.novell.com/documentation.

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Third Party Legal Notices

This product may include the following open source programs that are available under the LGPL license. The text for this license can be found in the Licenses directory.

- edtFTPj-1.2.3 is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, licensed under the Lesser General Public License available at: http://shark.objectweb.org/license.html.
- Esper. Copyright © 2005-2006, Codehaus.
- FESI is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions, see http://www.lugrin.ch/fesi/index.html.
- jTDS-1.2.2.jar is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, licensed under the Lesser General Public License. For more information, disclaimers and restrictions see http://web.ukonline.co.uk/mseries.
- Tagish Java Authentication and Authorization Service Modules, licensed under the Lesser General Public License. For more information, disclaimers and restrictions see http://free.tagish.net/jaas/index.jsp.

This product may include the following software developed by The Apache Software Foundation (http://www.apache.org/) and licensed under the Apache License, Version 2.0 (the "License"); the text for this license can be found in the Licenses directory or at http://www.apache.org/licenses/LICENSE-2.0. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

- Apache Axis and Apache Tomcat, Copyright © 1999 to 2005, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/.
- Apache FOP.jar, Copyright 1999-2007, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/.
- Apache Lucene, Copyright © 1999 to 2005, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/.
- Bean Scripting Framework (BSF), licensed by the Apache Software Foundation Copyright © 1999-2004. For more information, disclaimers and restrictions see http://xml.apache.org/dist/LICENSE.txt.
- Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Licensed under the Apache Software License. For more information, disclaimers and restrictions see https://skinlf.dev.java.net/.
- Xalan and Xerces, both of which are licensed by the Apache Software Foundation Copyright © 1999-2004. For more information, disclaimers and restrictions see http://xml.apache.org/dist/LICENSE.txt.

This product may include the following open source programs that are available under the Java license.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://www.java.sun.com/products/javabeans/glasgow/jaf.html and click download > license.

- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://java.sun.com/j2se/1.5.0/docs/relnotes/SMICopyright.html.
- JavaMail. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://www.java.sun.com/products/javamail/downloads/index.html and click download > license.

This product may include the following open source and third party programs.

- ANTLR. For more information, disclaimers and restrictions, see http://www.antlr.org.
- Boost. Copyright © 1999, Boost.org.
- Concurrent, utility package. Copyright © Doug Lea. Used without CopyOnWriteArrayList and ConcurrentReaderHashMap classes.
- ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003-2004.
- ILOG, Inc. Copyright © 1999-2004.
- Java Ace, by Douglas C. Schmidt and his research group at Washington University. Copyright © 1993-2005. For more information, disclaimers and restrictions see http://www.cs.wustl.edu/~schmidt/ACE-copying.html and http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html.
- Java Service Wrapper. Portions copyrighted as follows: Copyright © 1999, 2004 Tanuki Software and Copyright © 2001 Silver Egg Technology. For more information, disclaimers and restrictions, see http://wrapper.tanukisoftware.org/doc/english/license.html.
- JIDE. Copyright © 2002 to 2005, JIDE Software, Inc.
- JLDAP. Copyright © 1998-2005 The OpenLDAP Foundation. All rights reserved. Portions Copyright © 1999 - 2003 Novell, Inc. All Rights Reserved.
- Monarch Charts. Copyright © 2005, Singleton Labs.
- OpenSSL, by the OpenSSL Project. Copyright © 1998-2004. For more information, disclaimers and restrictions, see http://www.openssl.org.
- Oracle Help for Java. Copyright © 1994-2006, Oracle Corporation.
- Rhino. Usage is subject to Mozilla Public License 1.1. For more information, see http://www.mozilla.org/rhino/.
- SecurityNexus. Copyright © 2003 to 2006. SecurityNexus, LLC. All rights reserved.
- Sonic Software Corporation. Copyright © 2003-2004. The SSC software contains security software licensed from RSA Security, Inc.
- Tao (with ACE wrappers) by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine and Vanderbilt University. Copyright © 1993-2005. For more information, disclaimers and restrictions see http://www.cs.wustl.edu/~schmidt/ACE-copying.html and http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html.
- Tinyxml. For more information, disclaimers and restrictions see http://grinninglizard.com/tinyxmldocs/index.html.
- yWorks. Copyright © 2003 to 2006, yWorks.

NOTE: As of the publication of this documentation, the above links were active. In the event you find that any of the above links are broken or the linked web pages are inactive, please contact Novell, Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 U.S.A.

Preface

The Sentinel Technical documentation is general-purpose operation and reference guide. This documentation is intended for Information Security Professionals. The text in this documentation is designed to serve as a source of reference about Sentinel's Enterprise Security Management System. There is additional documentation available on the Novell web portal (http://www.novell.com/documentation/).

Sentinel Technical documentation is broken down into six different volumes. They are:

- Volume I – Sentinel Install Guide
- Volume II – Sentinel User Guide
- Volume III – Sentinel Collector Builder User Guide
- Volume IV – Sentinel User Reference Guide
- Volume V – Sentinel 3rd Party Integration
- Volume VI – Sentinel Patch Installation Guide

Volume I – Sentinel Install Guide

This guide explains how to install:

- Sentinel Server
- Sentinel Console
- Sentinel Correlation Engine
- Sentinel Crystal Reports
- Collector Builder
- Collector Manager
- Advisor

Volume II – Sentinel User Guide

This guide discusses:

- Sentinel Console Operation
- Sentinel Features
- Sentinel Architecture
- Sentinel Communication
- Shutdown/Startup of Sentinel
- Vulnerability assessment
- Event monitoring
- Event filtering
- Event correlation
- Sentinel Data Manager
- Event Configuration for Business Relevance
- Mapping Service
- Historical reporting
- Collector Host Management
- Incidents
- Cases
- User management
- Workflow
- Solution Packs

Volume III – Collector Builder User Guide

This guide discusses:

- Collector Builder Operation
- Collector Manager
- Collectors
- Collector Host Management
- Building and maintaining Collectors

Volume IV - Sentinel User Reference Guide

This guide discusses:

- Collector scripting language
- Collector parsing commands
- Collector administrator functions
- Collector and Sentinel meta-tags
- Sentinel correlation engine
- User Permissions
- Correlation command line options
- Sentinel database schema

Volume V - Sentinel 3rd Party Integration Guide

- Remedy
- HP OpenView Operations
- HP Service Desk

Volume VI - Sentinel Patch Installation Guide

- Patching from Sentinel 4.x to 6.0
- Patching from Sentinel 5.1.3 to 6.0

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation and enter your comments there.

Additional Documentation

The other manuals on this product are available at http://www.novell.com/documentation. The additional documentation available on Sentinel:

- Sentinel 6.0 Installation Guide
- Sentinel 6.0 Patch Installation Guide
- Sentinel 6.0 Reference Guide

Documentation Conventions

The following are the conventions used in this manual:

- Notes and Warnings

  NOTE: Notes provide additional information that may be useful or for reference.

  WARNING:

  Warnings provide additional information that helps you identify and stop performing actions in the system that cause damage or loss of data.

- Commands appear in courier font. For example:

```
useradd –g dba –d /export/home/oracle –m –s /bin/csh
oracle
```

- Go to *Start* > *Program Files* > *Control Panel* to perform this action: Multiple actions in a step.
- References
  - For more information, see “Section Name” (if in the same Chapter).
  - For more information, see “Chapter Name” (if in the same Guide).
  - For more information, see Section Name in Chapter Name, *Name of the Guide* (if in a different Guide).

Other References

The following manuals are available with the Sentinel install CDs.

- Sentinel User Guide
- Sentinel Collector Builder User Guide
- Sentinel User Reference Guide
- Sentinel 3rd Party Integration Guide
- Release Notes

Contacting Novell

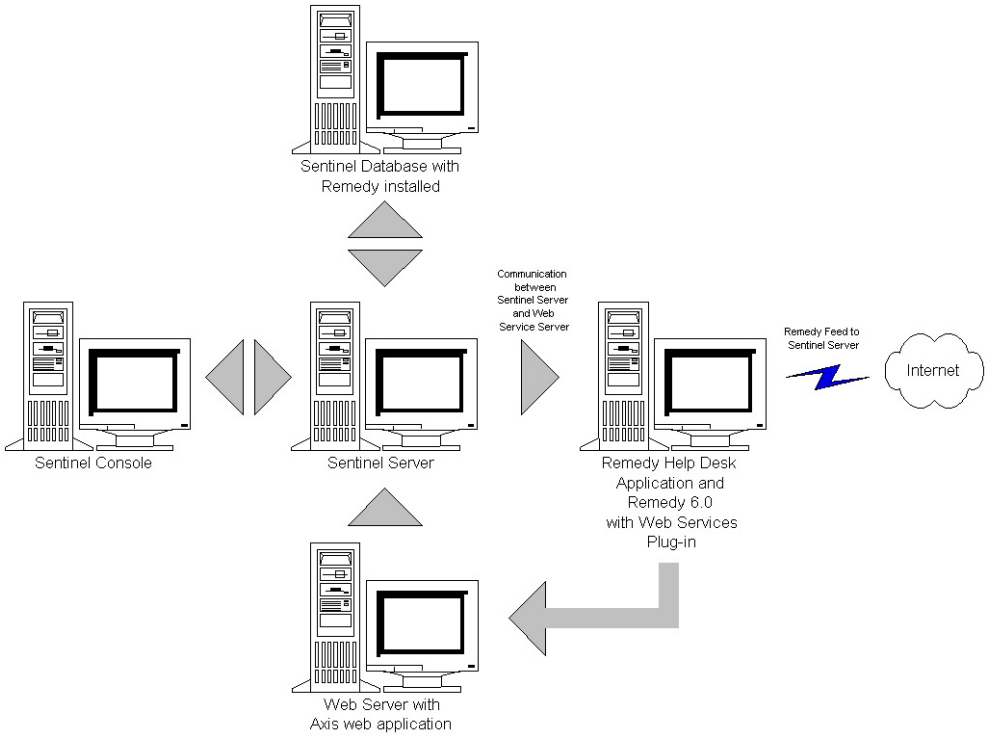
- Website: http://www.novell.com
- Novell Technical Support: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Self Support: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Patch Download Site: http://download.novell.com/index.jsp
- 24x7 support: http://www.novell.com/company/contact.html.
- For Collectors/Connectors/Reports/Correlation/Hotfixes/TIDS: http://support.novell.com/products/sentinel.

Contents

1 Remedy Integration

Remedy integration for Sentinel v4.2 or v5 can be used to create workflow applications that are integrated with both the Remedy Trouble Ticketing System and Sentinel system. Key features with the Remedy integration are:

- Ability to create a new case in Remedy Help Desk based on an incident in Sentinel.
- Ability to update a related case in Help Desk, when a Sentinel incident is updated.
- Ability to update a Sentinel incident when a related Case in Help Desk is updated.



Configuration

To change the Remedy Help Desk Case form:

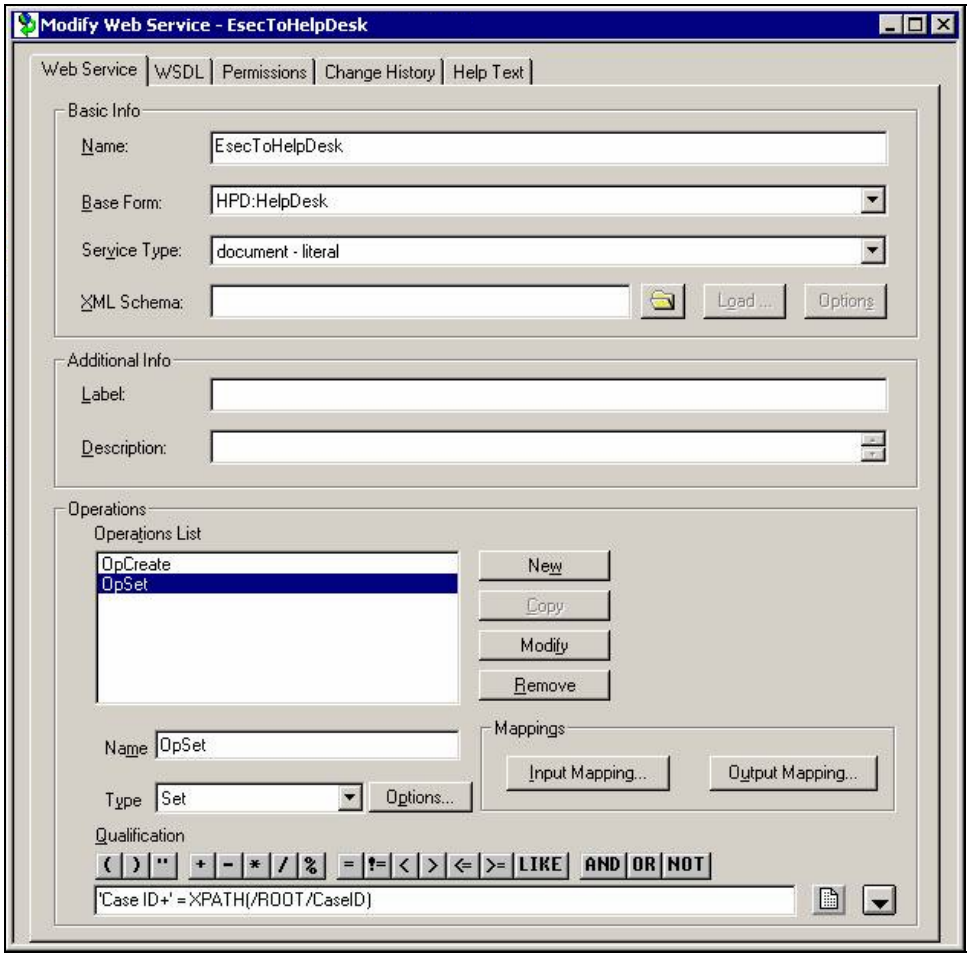
1. Login into *Remedy Administrator > Forms*, double-click on *HPD HelpDesk*.
2. In order to support integration with Sentinel, the Help Desk Case form needs a character (EsecIncidentId) and attachment pool (Attachment Pool) field to be added. These field entries will be used to add incident attachments to the form.
3. To add the EsecIncidentId character field:

- Click *New Character Field* button and place it somewhere on the form.
- Under the Display tab, set a label.
- Under the Database tab, in the Name field set the name to EsecIncidentID.

4. To add the Attachment Pool character field with the following three fields: EsecEvents, EsecVuln and EsecAdv.
   - Click *Create Attachment Pool* button.
   - Under the Display tab, in the label field enter a label name (ex: esec attachments).
   - Under *Attach Fields*, in the *Enter Attachments Field Label*, enter:
     - EsecEvent and click Add
     - EsecVuln and click Add
     - EsecAdv and click Add
5. Click *Save*.

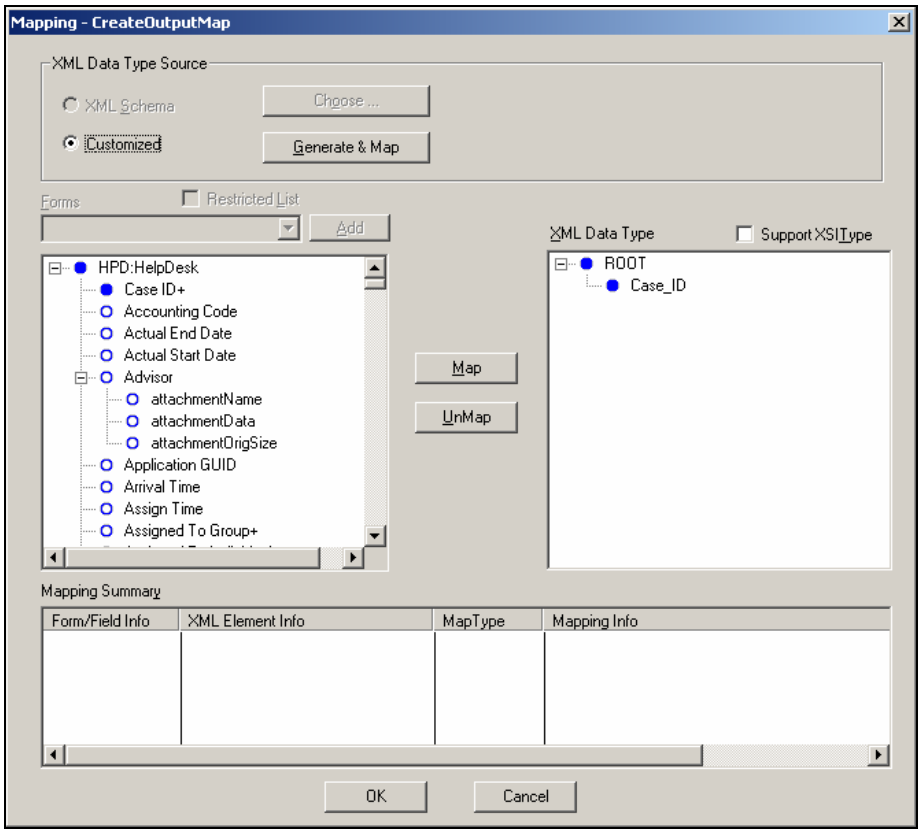
To create a web service:

1. In Remedy Administrator, in the navigation pane high-light *Web Services*. Right-click *New Web Services* and click the *Web Services* tab.



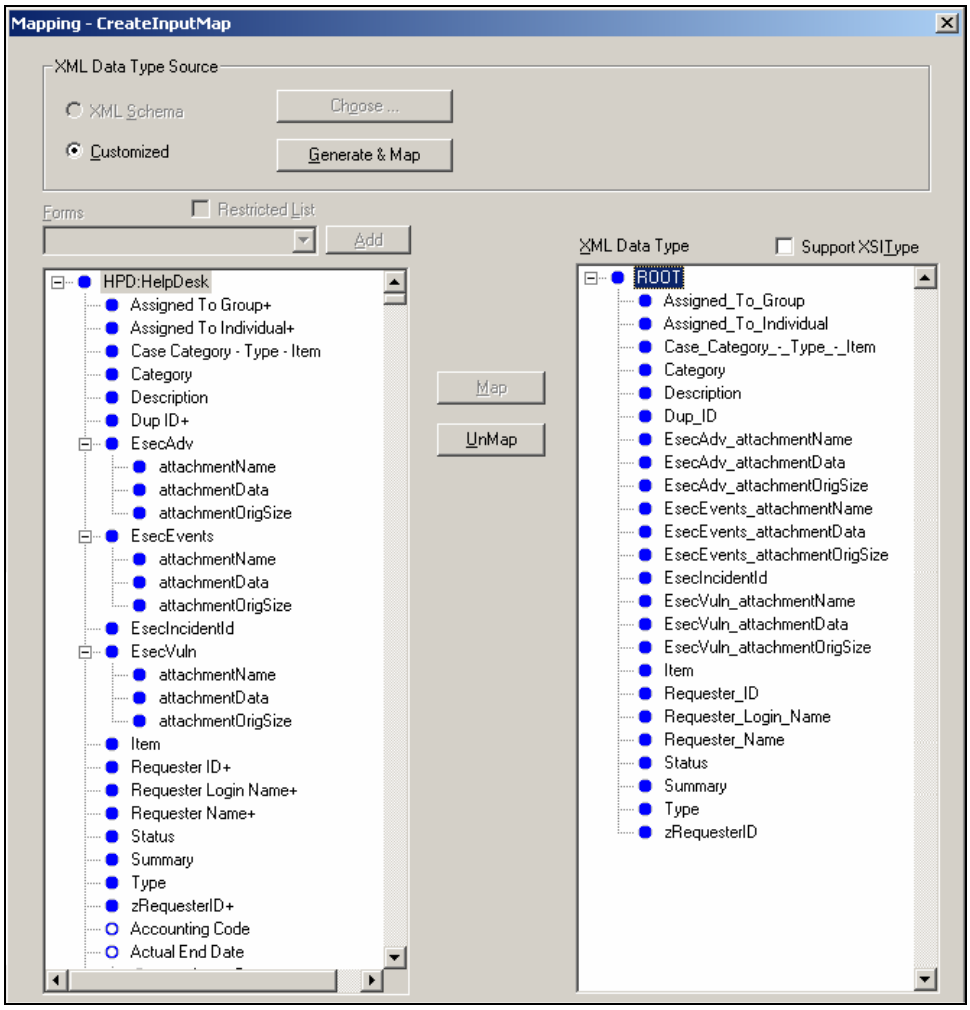
2. Using the Help Desk Case as a base form, create a Web Service called *EsecToHelpDesk* and select Base Form HPD HelpDesk.
3. Make two operations for this web service called:
   - opCreate
   - opSet

   You can do so by removing the other operations.
4. Select OpCreate and click *Output Mapping* button. Make the screen match the following illustration.



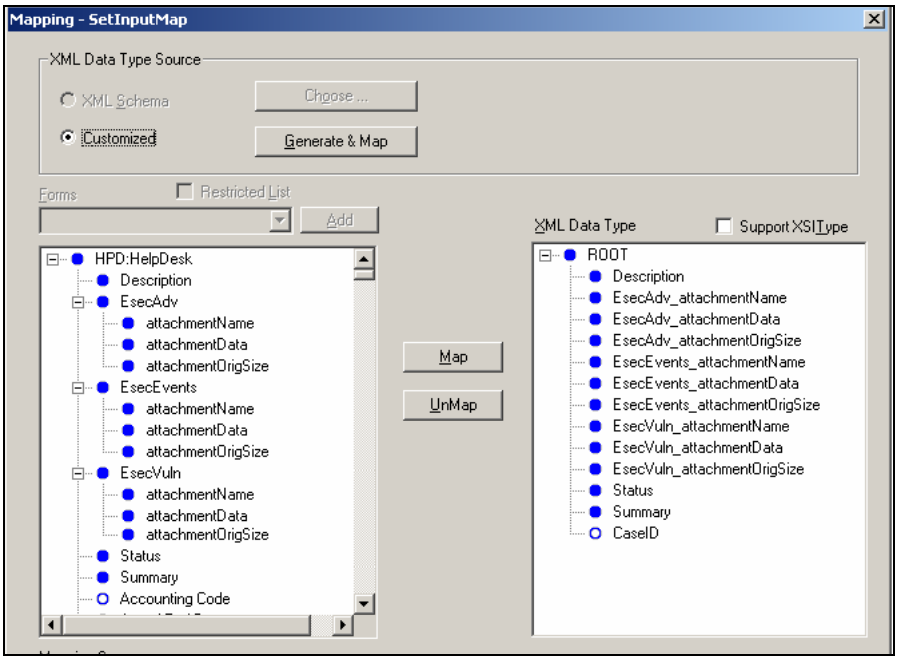
Select *Input Mapping* button for opCreate. Make the screen match the following illustration.

NOTE: To remove an item, high-light it > *right-click* > *cut*.

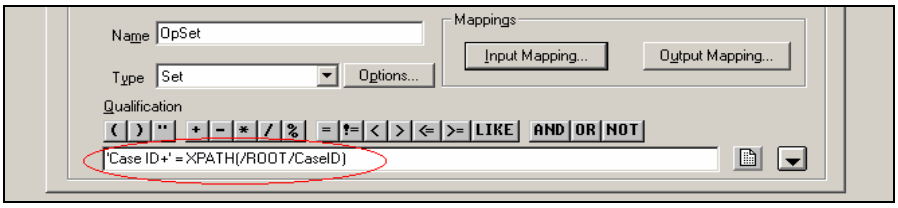


Click *Save*.

Select *Input Mapping* button for opSet. Make the screen match the following illustration.



There is no output mapping for opSet. For opSet, you have to specify a qualification:



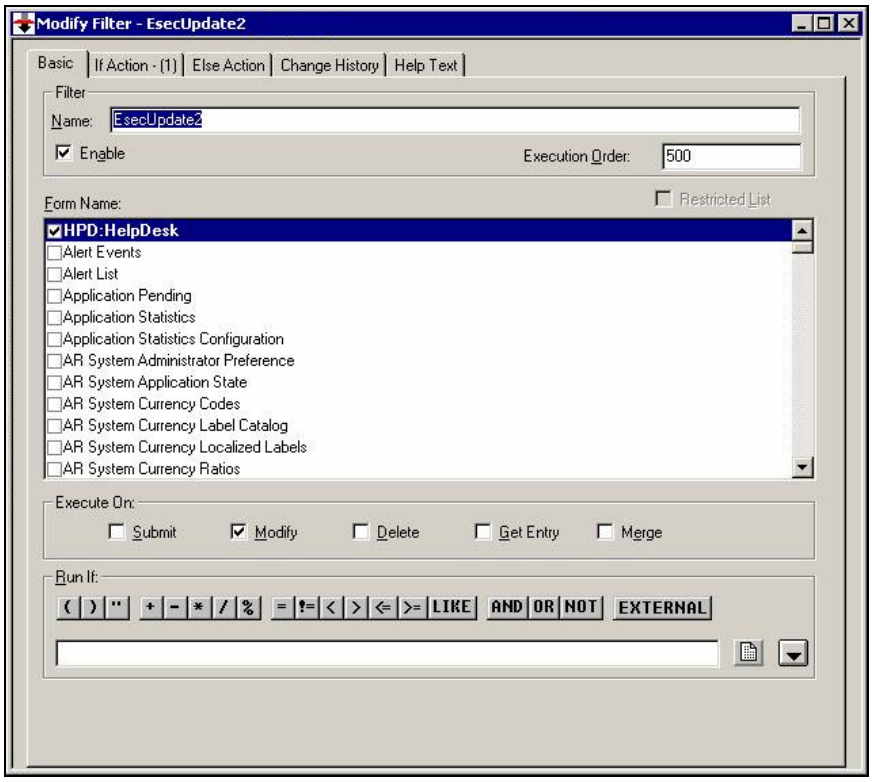
5. Go to the *Permissions* tab and move the service to Public by moving Public from left to right. Click *Save*.

Remedy to Sentinel Data Flow

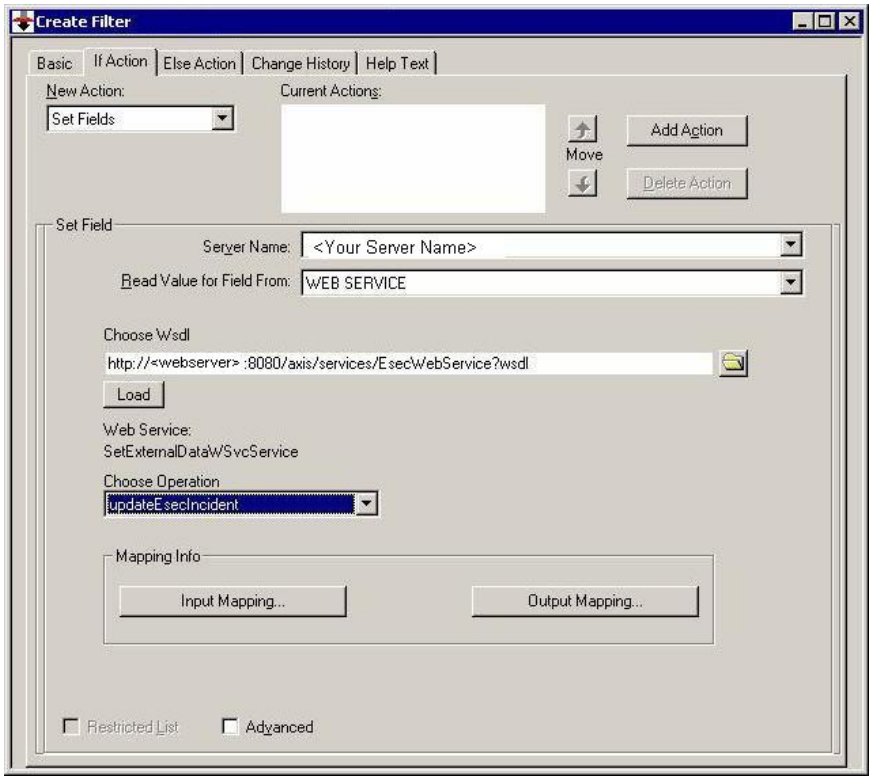
In order for Sentinel Web Service to be accessible, you must have a web server with Axis web application running by the time of Sentinel Server startup.

Remedy to Sentinel Data Flow:

1. In the Remedy Administrator, high-light Filters and right-click *Add Filter*.
2. Create a filter for Help Desk Case form that is executed on a modified event. Make sure your screen matches the following illustration.

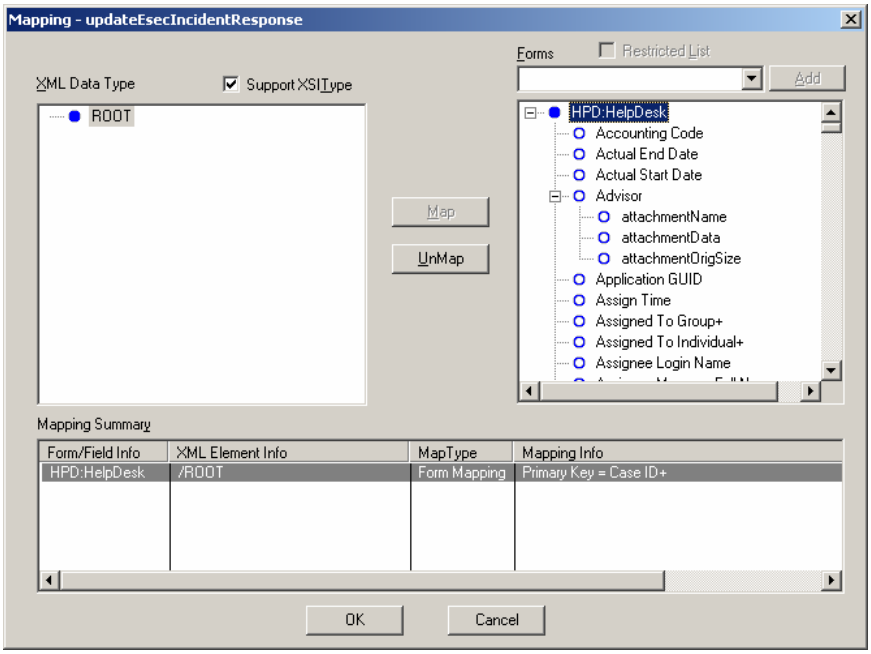


3. Under the *If Action* tab, in the *New Action* drop down menu select *Set field* action, in the *Set Field* pane select *WEB SERVICE* and provide the URL for Sentinel Web Service (http://<webserver IP or DNS name>:8080/axis/services/EsecWebService?wsdl).



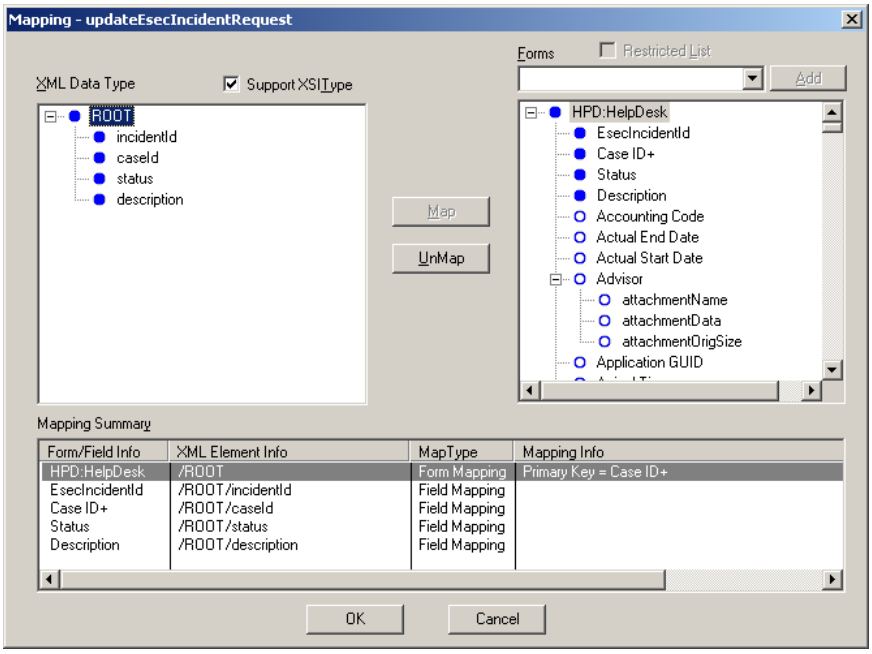
4. In the *Choose Operation* drop down menu, select *updateEsecIncident* method and set the Input and Output mapping.

   Click *Output Mapping* button. Make your screen match the following illustration:



   Click the *Input Mapping* button. Make your screen match the following illustration.

NOTE: To set your Map, select an item on the left (that is, incidentId), select an item on the right (that is, EsecIncidentId) and click the Map button.



NOTE: After setup, whenever you save a change in Help Desk Case form, the change will be submitted to a Sentinel service.

5. Click *Save*.

Installing Sentinel

When installing Sentinel with Remedy, you will need to have an account with Remedy. From this account you will be prompted for the following information.

NOTE: You must have Remedy Integration permission.

- Username
- Password
- Requestor Name
- Requester ID
- Requestor Login
- Group Name (may be left blank)
- Individual Name (may be left Blank)
- Server Name
- Service Name

For Remedy to Sentinel Data Flow, you will be prompted for:

- Sentinel Webserver (<machine name:port>)
- Sentinel Username (such as esecadm)
- Sentinel UserID
- Sentinel UUID
- Sentinel Lock ID (usually set to 1 or 2, this is....

Installing Sentinel:

1. Select Remedy integration during install.
2. Have the above information available during the install process.

Remedy to Sentinel Data Flow Configuration

If you will be using the 3rd Party Integration (Remedy Integration), it is recommended to install and configure in the following order:

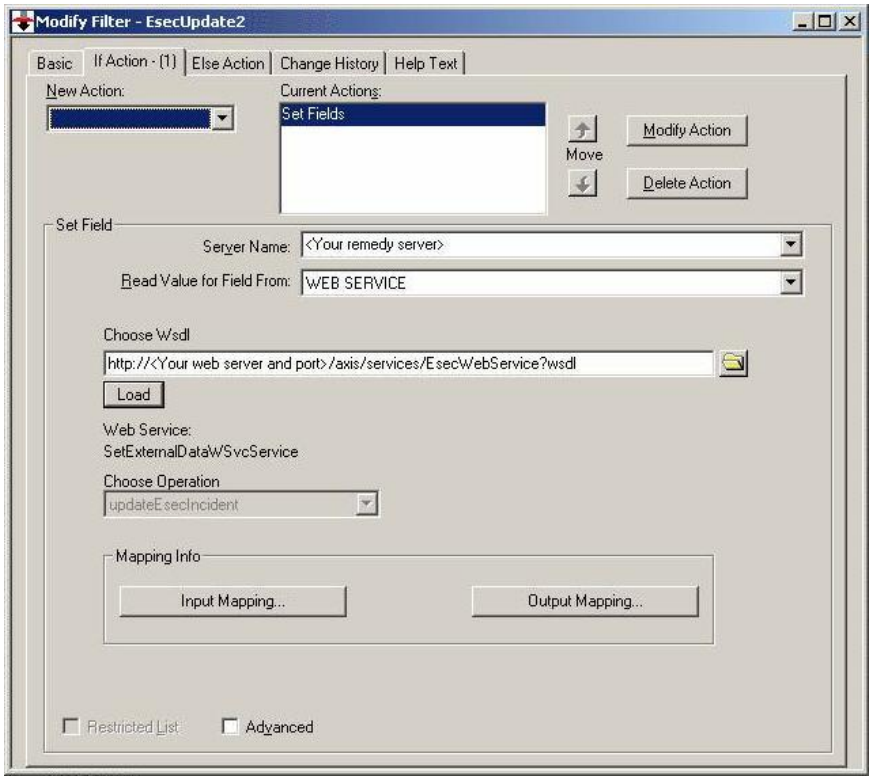
1. Install Remedy Help Desk Application and Remedy 6.0 with Web Services Plug-in.
2. Configure new Filters and Web services in the Remedy Help Application.
3. Install Sentinel

In order to have Remedy to Sentinel data flow, you must:

- In order for Sentinel WebService to be accessible, you must have a web server with Axis web application running before sentinel server is started.
- Copy all the jar files from the following location on your Sentinel Server to <axis web application>\webclient\lib.
  - %ESEC_HOME%\lib
  - %ESEC_HOME%\sentinel\console
  - %ESEC_HOME%\communicator (for v4.2 only)
- Copy your Sentinel Server configuration.xml and .keystore file to a location of your choice to your webserver. Both files are located at %ESEC_HOME%.
  - Edit the configuration.xml on your web server to point to the .keystore file.
  - Add the following JVM option to your webserver,

```
Dcom.esecurity.configurationfile=<path to
   configuration.xml>\configuration.xml
```

- You must create a filter for the Help Desk Case form that is executed on a "Modified" event. This filter calls the Sentinel web server.



2 Remedy Help Desk Operations

Remedy integration can be used to create workflow applications. Features with the Remedy integration are:

- Ability to create a new case in Remedy Help Desk based on an incident in Sentinel.
- Ability to update a related case in Help Desk, when Sentinel incident is updated.
- Ability to update a Sentinel incident when a related Case in Help Desk is updated.

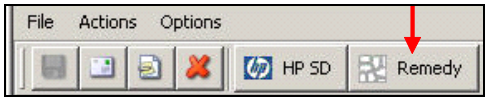
Remedy Help Desk Operations

To send an Incident for Remedy Help Desk (v4.5.x and later):

1. Click the *Incidents* tab.
2. In the navigator pane, expand the *Incident Views* folder and high light *Incident View Manager*.

   NOTE: If you already have an incident set for another external system, you cannot change it.

3. Expand one of the incident views and double-click on your incident. Your incident will open.
4. Click the *Remedy* button.



The Incident will be updated with an External Data tab and Remedy button.

To update an Incident to Remedy Help Desk (v4.5.x and later):

1. Click the *Incidents* tab.
2. Expand the navigator pane on the left and double-click an incident that is set to Remedy Help Desk.
3. Click the *Remedy* button in the Incident. Annotation will be added under the External tab.

Manually Reconfiguring the Remedy Interface Settings

During the initial installation of the Remedy Help Desk Interface, the Remedy settings are stored in the das_query.xml file. Use the information in this section of the documentation if you need to modify these settings after installation.

Remedy Settings

Remedy settings are stored in the das_query.xml file under the `RemedyARServerService` component as follows:

Resetting the Remedy Password

The Remedy passwords are stored in an encrypted format in the das_query.xml file. Therefore, if you need to reset the passwords stored in this file, you must use the utility described below.

To reset the Remedy interface password:

1. Go to `%ESEC_HOME%/sentinel/bin/.`
2. Enter:

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

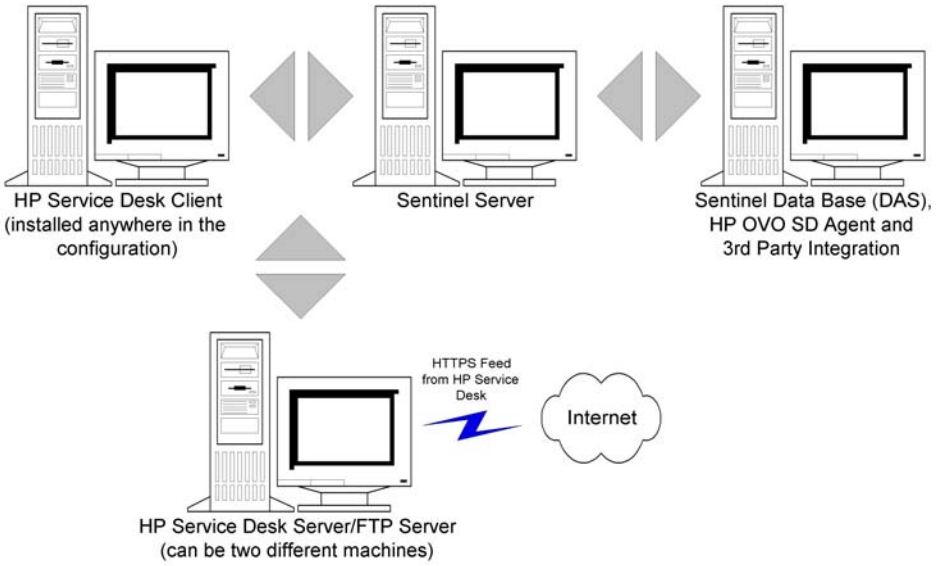
   - -r is the Remedy password

3 Installing HP OpenView Service Desk for Windows

Sentinel's bi-directional integration with HP OpenView Service Desk, which is licensed separately, provides new valuable features to the Sentinel Console. Sentinel leverages HP OpenView Service Desk's Asset Management capabilities to provide referential information to aide in the response to security threats and attacks. These new features provide the ability to:

- Send Incident(s) to HP Service Desk (SD)
- Attach Event(s) to a HP SD Incident
- Attach Vulnerability Information to a HP SD Incident
- Query and Populate Configuration Item (Asset) information both in Sentinel Console Incident and SD
- Round Trip Integration: SD send updates to Novell and Novell sending updates to SD
- Update SD Incident Status from Novell's Sentinel Console
- Update Sentinel's Incident Status from HP SD

Below is a typical installation configuration. Your configuration may be different.



System Requirements

For hardware and software requirements for HP OpenView Service Desk Client, Server and Agent, see HP OpenView Service Desk Installation Guide.

Sentinel supports the following versions of HP OpenView Service Desk:

NOTE: Sentinel supports HP OpenView Service Desk Server version 4.5.x only. HP Service Desk version 5.x is not currently supported by Sentinel.

- HP OpenView Service Desk Server - Version 4.5 with Service Pack 8 (4.5.0588.0802 SP 8)
- HP OpenView Service Desk Client - Version 4.5 with Service Pack 8
- HP OpenView Service Desk Agent - Version 4.5 with Service Pack 8
- Sentinel 4.2.1.8 or 4.2.1.15 for Windows
- Any 3rd Party FTP Server

HP OpenView Service Desk Server and Client must be installed on a machine that is to be designated as the Service Desk Server. Consult the HP OpenView Service Desk Installation Guide for assistance with installing Service Desk.

To enable this bi-directional interface, a HP OpenView Agent must be installed on the same machine where das_cmd.bat is installed. The Bi-directional interface allows HP Service Desk to notify Sentinel whenever the Status of an Incident that originated from Sentinel has been changed by a Service Desk user. These incidents must originate from the Sentinel Console.

In order for Service Desk to handle attachments, an FTP server must be installed (typically on the Service Desk Server), and Service Desk must be configured to communicate with it. Any third party FTP server can be used. Consult the Installation Guide of your FTP server for assistance installing the FTP server.

Installation

If you are also installing HP OpenView Operations, it is recommended to install HP OpenView Operations before HP OpenView Service Desk.

NOTE: During initial installation of the 3rd Party HP OpenView Service Desk Interface, the Service Desk and OpenView settings are stored in the das_query.xml file. To change any of these settings (such as username or password), see *Operation - HP OpenView and Service Desk for Windows 2000*.

It is recommended to install in the following order:

- FTP Server

NOTE: See the Installation Guide of your FTP server for assistance in installing your FTP server.

- HP OpenView Service Desk Server with Service Pack 8 – can the same as the FTP server
- HP OpenView Service Desk Client with Service Pack 8
- HP OpenView Service Desk Agent with Service Pack 8 (to enable bi-directional interface) – must on a the machine where DAS is installed

NOTE: See HP OpenView Service Desk Installation Guide for assistance in installing the HP OpenView Service Desk software.

- Install Sentinel 3rd Party Integration
  - HP OpenView Service Desk

NOTE: For installation information, see the Sentinel v4.2.1.8 Release Notes and Sentinel Installation Guide v4.2 for Windows and Solaris.

Configuring HP OpenView Service Desk

Configuration of HP OpenView Service Desk is accomplished through the Service Desk Client. Before modifying the configuration of HP Service Desk to communicate to the FTP Server, have the following information available:

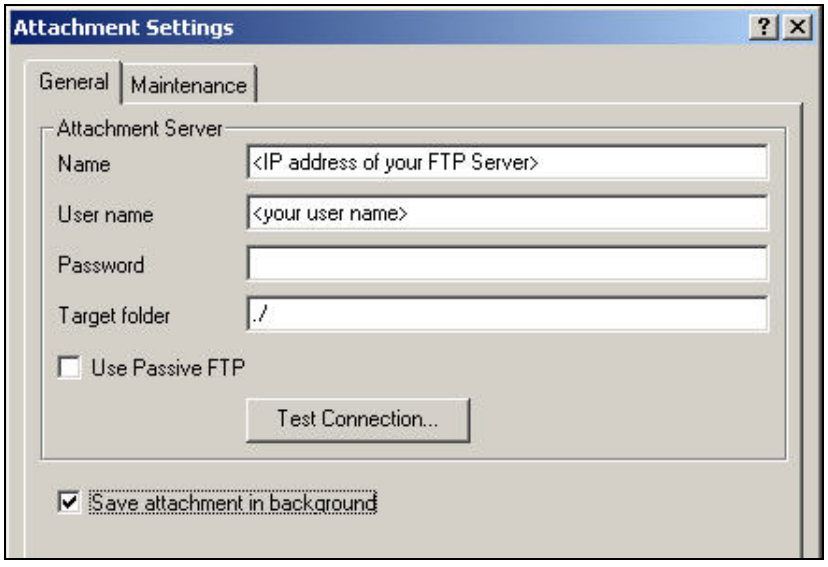
- **Name:** IP address of your FTP Server
- **Username/Password:** any user set in the FTP Server
- **Target Folder:** recommend entering "./". This places your FTP directory to the current FTP directory.
- Uncheck *Use Passive FTP*
- Check *Save attachment in background*

NOTE: For more information, see the Post Installation Tasks section of the HP OpenView Service Desk Installation Guide for detailed configuration steps.

To set Attachment Settings:

1. Start the HP Service Desk Client.
2. Click *Tools* > *System*.
3. Click *System Panel* in the navigator pane on the left.
4. Double-click *Attachment Settings*. Enter:
   - Name – IP address of your FTP Server
   - Username/Password – any user set in the FTP Server
   - Target Folder – recommend entering "./". This places your FTP directory to the current FTP directory.
   - Uncheck *Use Passive FTP*
   - Check *Save attachment in background*

NOTE: For more information, see the Post-Installation Tasks section of the HP OpenView Service Desk Installation Guide for detailed configuration steps.



5. Click *Test Connection.*
6. Click *Apply* and then *OK*.

Enabling Service Desk to Sentinel (bi-directional) Interface

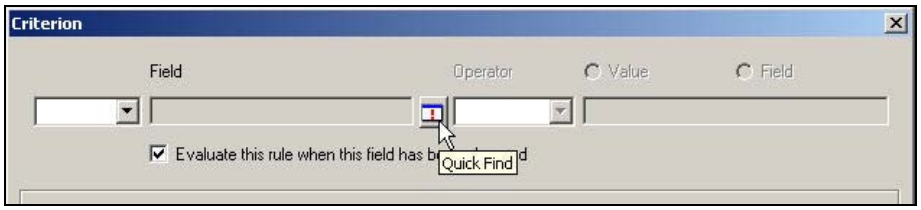
This option allows HP OVO OpenView Service Desk to notify Sentinel whenever the Status of an Incident (that originated from Sentinel) has been changed by a Service Desk user. This allows you to provide the ability to track the current state of each Incident that has been previously sent to HP OVO OpenView Service Desk.

To have enable this feature, you must install a HP OVO OpenView Service Agent must be installed on the same machine where as Sentinel (das_cmd.bat) is installed. This allows HP Service Desk to execute Sentinel's das_cmd utility.

To enable bi-directional interface:

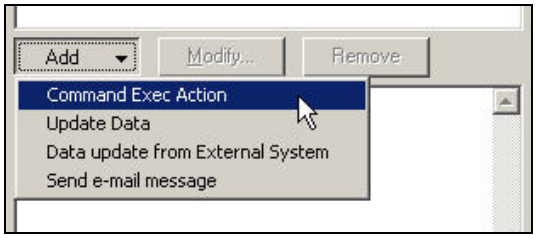
1. Start the Service Desk Client.
2. Bring up the Administrator's Console by selecting the *Tools* > *System*.
3. Click Business Logic in the navigator pane on the left.
4. Double-click *Database Rules*.
5. Double-click *Incident*. The Database Rules list window will appear.
6. Right-click in the Database Rules pane > *New Database Rule*.
7. Highlight *When incident is modified* and click *Next*.

8. Click *Condition...* button.
9. Click *Add Criterion...* button.
10. Click *Quick Find* button, select *Status* and select *is anything* in the operator field.



Click *OK* and Click *OK* again.

11. Click *Add*. Select *Command Exec Action*.



12. Add a new “Command Exec Action” such that the “das_cmd.bat” script is executed on the Sentinel Server whenever the rule is evaluated.

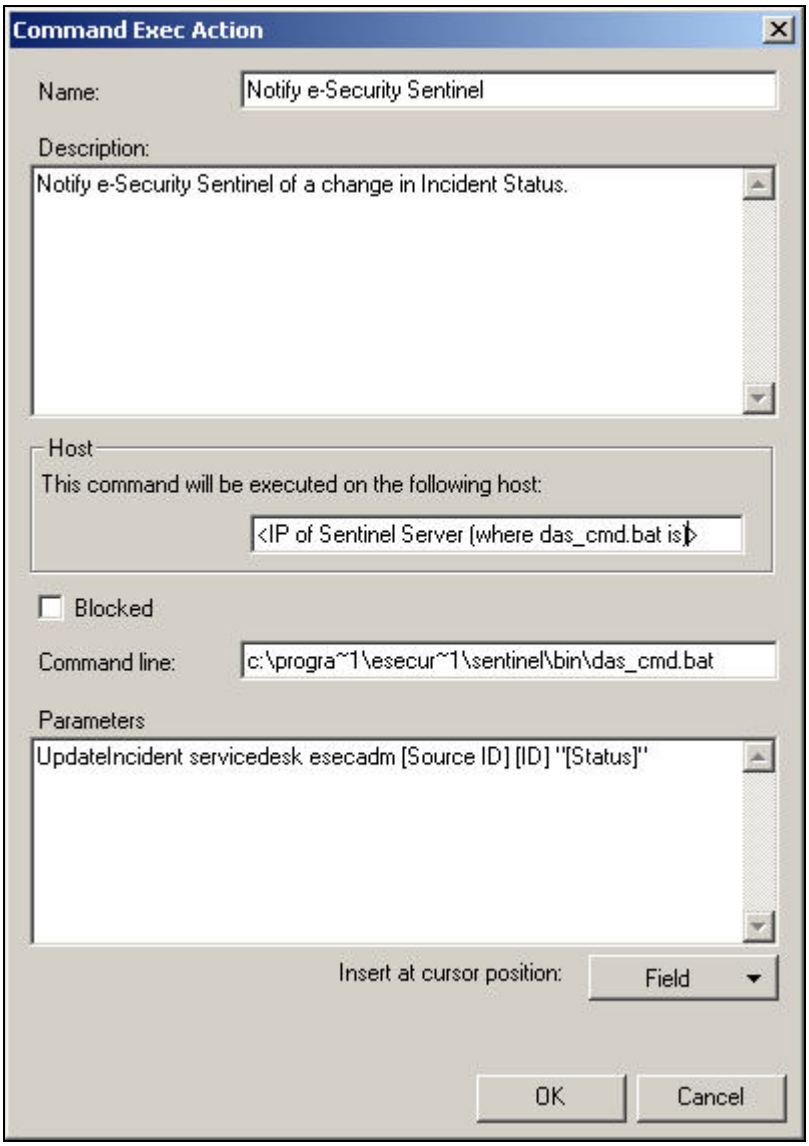
    When configuring the action, be sure to specify the name (or IP address) of your Sentinel Server (machine where das_cmd.bat is located) as the “Host”. Also be sure to specify the full path of the “das_cmd.bat” file on the Sentinel Server in the “Command Line”, such as:

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

    NOTE: You must use the DOS 8.3 naming convention to specify directory names with spaces. For example, use “progra~1” instead of “Program Files”.

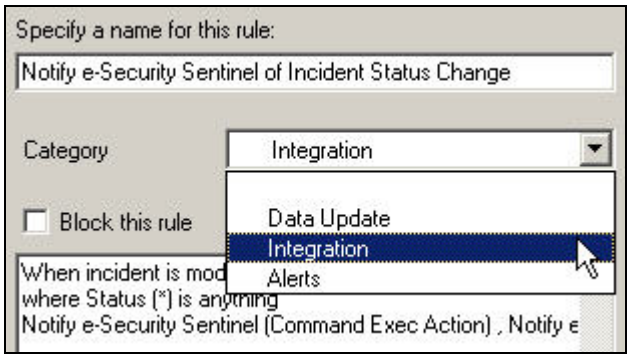
    And finally, be sure to specify the action “Parameters” as:

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



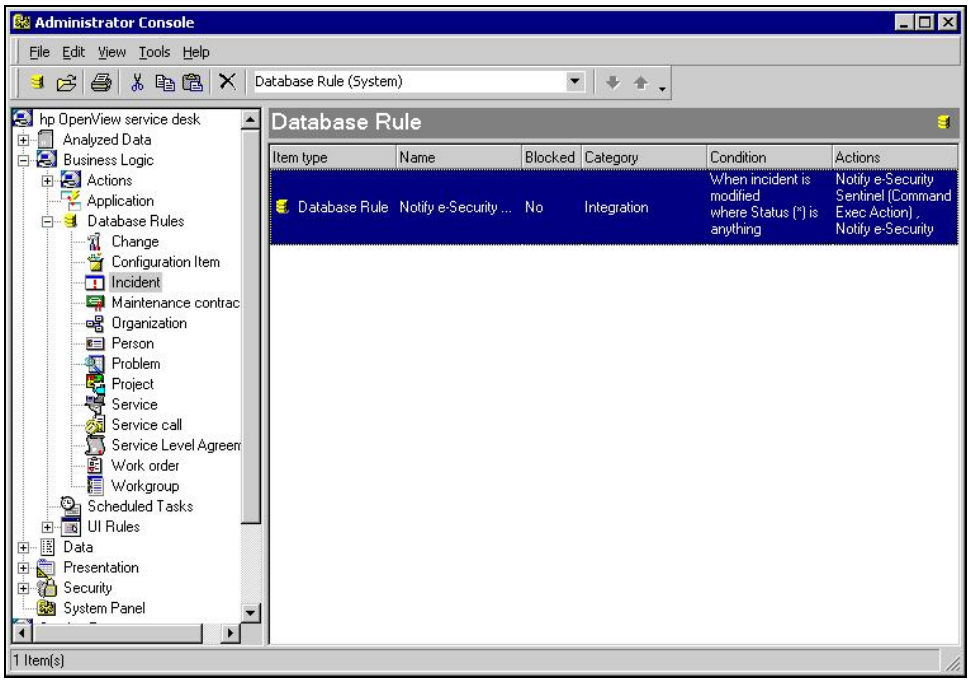
    Give the new Database Rule any name you want with a description. Click *OK* and then click *Next*.

13. In the Category field, select Integration and specify a name for this rule. Do not select *Block this rule*.



Click *Finish*.

14. Upon completion of the new Database Rule, a new rule should be listed in the Database Rule list.



4 HP OpenView Service Desk Integration

HP OpenView Service Desk for Sentinel allows you to send events from any screen displaying incidents and events to HP OpenView Service Desk.

HP OpenView Service Desk

Sentinel integration with HP OpenView Service Desk enables you to have additional asset management capability. This additional asset management capability allows:

- Send Incident(s) to HP Service Desk (SD)
  - Attach Event(s) to a HP SD Incident
  - Attach Vulnerability Information to a HP SD Incident
  - Attach Advisor Information to a HP SD Incident
  - Query and Populate Configuration Item (Asset) information in Sentinel Control Console
- Update SD Incident Status from Sentinel Control Console
- Update Sentinel's Incident Status from HP SD

Sentinel Incident information sent to HP OpenView Service Desk includes:

- Sentinel Incident ID
- State
- Title
- Annotations/History
- Events (attachment)
- Vulnerability Information (attachment)
- Advisor Information (attachment)

When sending or receiving information from HP OpenView Service Desk, there is an automatic state, status mapping, and conversion that takes place.

The Sentinel State to Service Desk Status mapping and conversion is as follows:

Sentinel State	**Service Desk Status**
Open	Registered
Acknowledged	Waiting
Assigned	Informed
Investigating	In Progress
False Positive	Closed
Verified	Completed
Approved	In Progress
Closed	Closed

The Service Desk Status to Sentinel State mapping and conversion is as follows:

Service Desk Status	**Sentinel State**
Registered	Open
In Progress	Investigating
Waiting	Acknowledged
Completed	Verified
Informed	Assigned
Closed	Closed

Sending Incidents to HP OpenView Service Desk

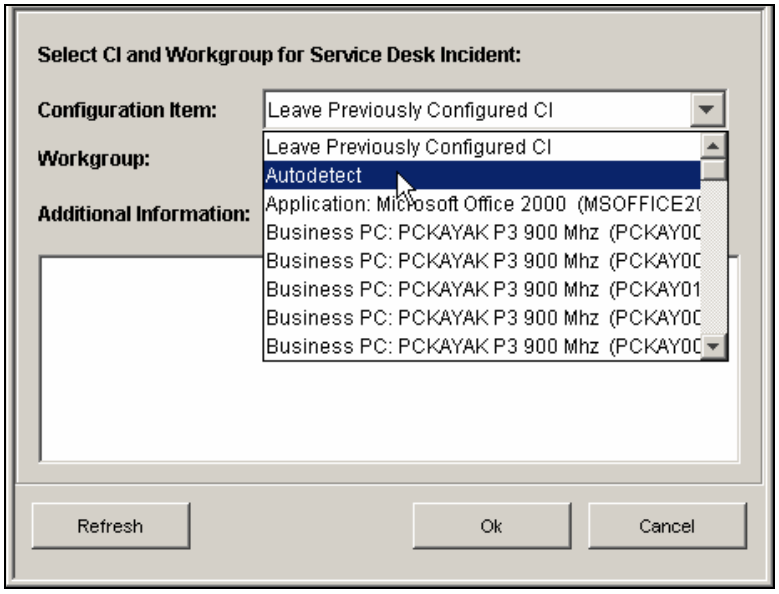
How to send an Incident to HP OpenView Service Desk

1. Click *Incidents* tab.
2. In the navigator pane, expand the *Incident Views* folder and high light *Incident View Manager*.

NOTE: If you already have an incident set for another external system, you cannot change it.

3. Expand one of the incident views and double-click on your incident. Your incident will open.
4. Click the *HP SD* button.

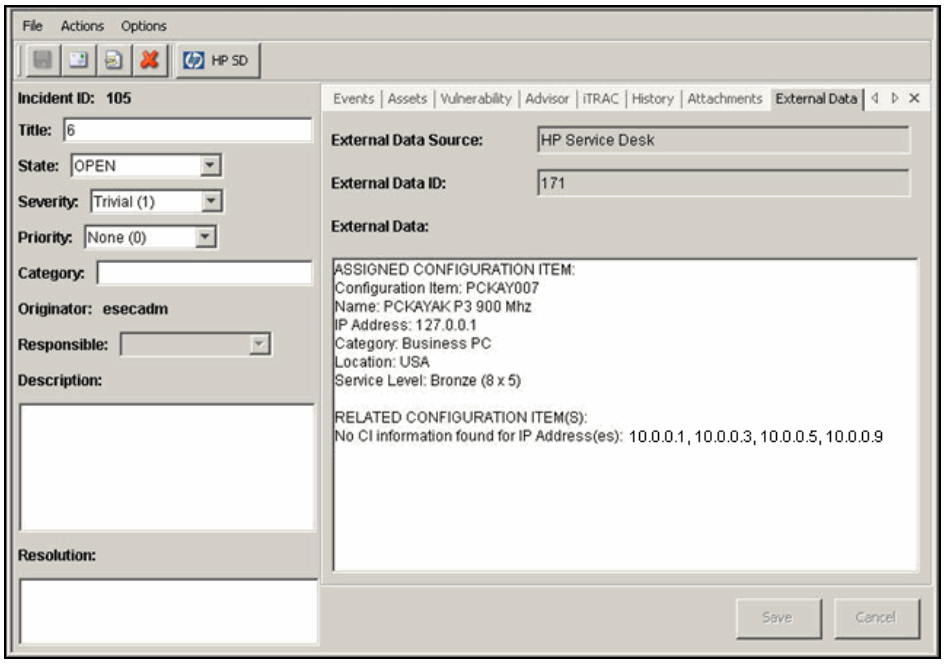
5. The *Send Incident to HP Service Desk* window will appear. The *Send To Service Desk* drop down menu provides a Configuration Item selection list, populated with Configuration Items queried from HP Service Desk.



An *Autodetect* option is available in the Configuration Item selection list. If you select *Autodetect*, Sentinel will attempt to use the Destination IP addresses of the Events associated with the Sentinel Incident to automatically determine the related Service Desk CI.

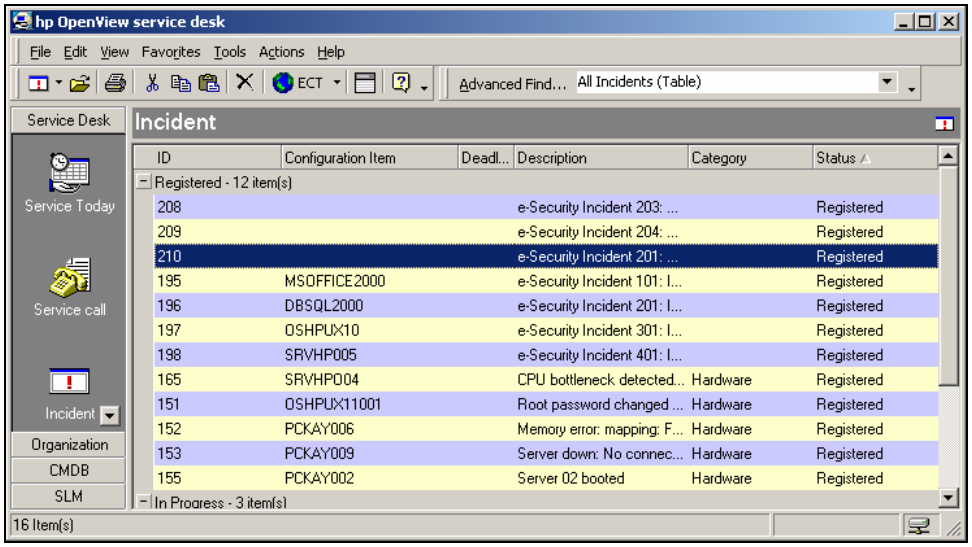
6. (optional) The *Send To Service Desk* dialog also provides a Workgroup selection list populated with Workgroups queried from Service Desk.
7. Click *OK* and the incident is forwarded to *HP OpenView Service Desk*.

NOTE: The Sentinel's Incident display is updated with an External Data tab. The External Data tab indicates the Service Desk Incident ID and the Service Desk Configuration Item to which the new Service Desk Incident was assigned.



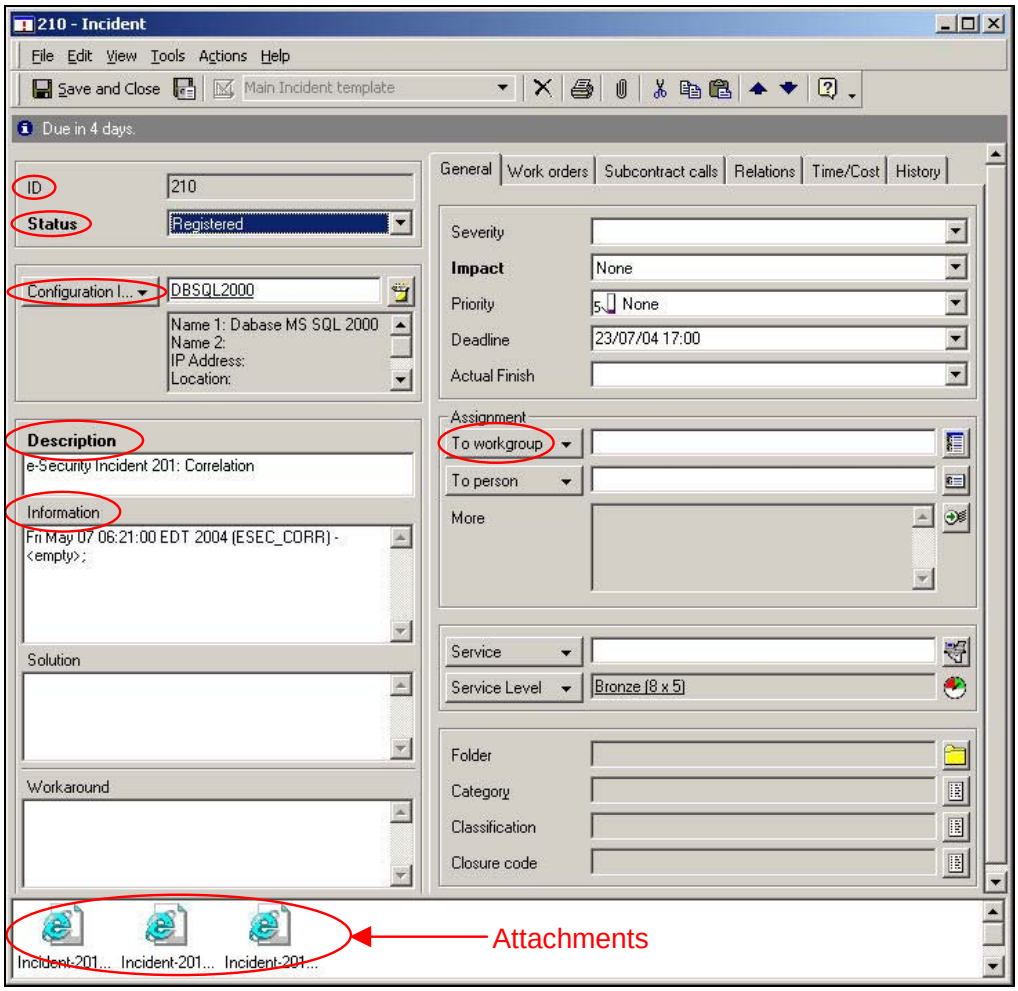
HP OpenView Service Desk Client

After sending an incident to HP OpenView Service Desk, the incident will appear in the HP OpenView Service Desk Client. In the Service Desk Client, the incident is listed by the Extended Data ID, not the Incident ID number.



Double clicking on an incident and the detail display for that incident will appear.

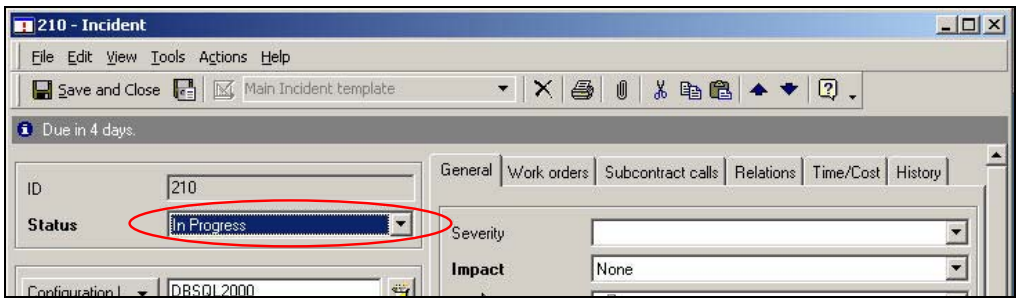
- Extended Source ID
- Status
- Configuration Item
- Description
- Information
- Workgroup
- Event Information (attachment)
- Vulnerability Information (attachment)
- Advisor Information (attachment)



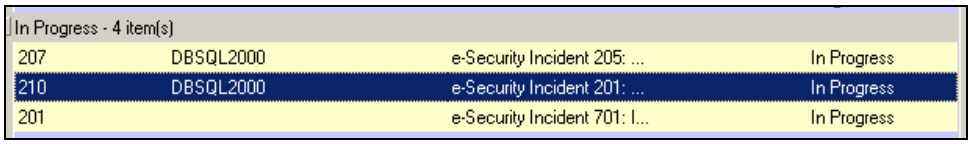
HP OpenView Service Desk – Bi-Directional Interface

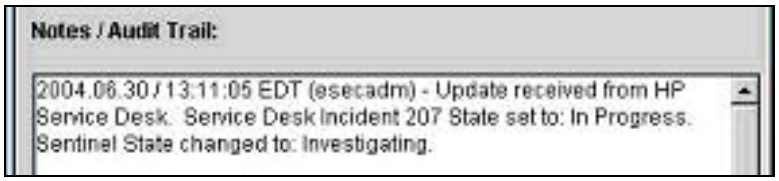
If this option is enabled, (see Sentinel Installation Guide) Service Desk will notify Sentinel whenever the Status of an Incident (that originated from Sentinel) has been changed by a Service Desk user. This allows Sentinel users to track the current state of each Incident that has been sent over to Service Desk.

If you bring up a detail display, change it and then save, the detail display will indicate an in-progress status.



This update can also be seen in the HP OpenView Service Desk Client and the Incident window in the Sentinel Console.





Manually Reconfiguring the HP OpenView Service Desk Interface Settings

During the initial installation of the 3rd Party HP OpenView Service Desk Interface, the Service Desk settings are stored in the das_query.xml file. Use the information in this section of the documentation if you need to modify these settings after installation.

HP OpenView Service Desk Settings

HP OpenView Service Desk settings are stored in the das_query.xml file under the HpServiceDeskService component as follows:

- **server:** Set to the Service Desk Server hostname/ip address.
- **username:** Set to the Service Desk Server username.
- **password:** Set to the encrypted Service Desk Server password using the utility described in the section Resetting the HP OpenView Passwords.
- **attachment_path:** Automatically set to the "attach" 3rd party directory.
- **ftp_server:** Set to the FTP Server hostname/ip address (that Service Desk will use for attachments).
- **ftp_username:** Set to the FTP username (that Service Desk will use for attachments).
- **ftp_password:** Set to the encrypted FTP user's password (that Service Desk will use for attachments) using the utility described in the section Resetting the HP OpenView Passwords.
- **ftp_user_home:** Set to the full directory path of the FTP user.
- **attachment.events:** Set to "yes" to indicate that the Events attachment will be used.
- **attachment.events.filename:** The file name used for Event attachment files.
- attachment.vuln - Set to "yes" to indicate that the Vulnerability attachment will be used.
- **attachment.vuln.filename:** The file name used for Vulnerability attachment files.
- **attachment.adv.attack:** Set to "yes" to indicate that the Advisor Attack attachment will be used.
- **attachment.adv.attack.filename:** The file name used for Advisor Attack attachment files.

Resetting the HP OpenView Passwords

The HP OpenView passwords are stored in an encrypted format in the das_query.xml file. Therefore, if you need to reset the passwords stored in this file, you must use the utility described below.

To reset the HP OpenView Service Desk interface settings:

1. cd %ESEC_HOME%/sentinel/bin/
2. Enter:

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

   - -s is the HP OpenView Service Desk server password
   - -f is the FTP server password (for FTP server that Service Desk will use for attachments)