
Sentinel™ 5

3rd Party Integration Guide v5.1.2

- Remedy Help Desk (v4.2 and v5)
- HP Service Desk (v4.2 and v5)

Volume V of V

May 2006
www.esecurity.net

Preface

The e-Security 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 e-Security's Enterprise Security Management System. There is additional documentation available on the e-Security web portal.

e-Security Technical documentation is broken down into five different volumes. They are:

- Volume I – Sentinel™ 5 Install Guide
- Volume II – Sentinel™ 5 User's Guide
- Volume III – Sentinel™ 5 Wizard User's Guide
- Volume IV – Sentinel™ 5 User's Reference Guide
- Volume V – Sentinel™ 5 3rd Party Integration Guide

Volume I – Sentinel Install Guide

This guide explains how to install:

- Sentinel Server
- Sentinel Console
- Sentinel Correlation Engine
- Sentinel Crystal Reports
- Wizard Agent Builder
- Wizard Agent Manager
- Advisor

Volume II – Sentinel User's Guide

This guide discusses:

- Sentinel Console Operation
- Sentinel Features
- Sentinel Architecture
- Sentinel Communication
- Vulnerability assessment
- Event monitoring
- Event filtering
- Event correlation
- Sentinel Data Manager
- Event Configuration for Business Relevance
- Mapping Service
- Historical reporting
- Wizard Host Management
- Incidents
- Cases
- User management
- Workflow

Volume III – Wizard User's Guide

This guide discusses:

- Wizard Agent Builder Operation
- Wizard Agent Manager
- Agents
- Wizard Host Management
- Building and maintaining agents

Volume IV - Sentinel User's Reference Guide

This guide discusses:

- Wizard scripting language
 - User Permissions
-

- Wizard parsing commands
- Wizard administrator functions
- Wizard and Sentinel meta-tags
- Sentinel correlation engine
- Correlation command line options
- e-Security database schema

Volume V - Sentinel 3rd Party Integration Guide

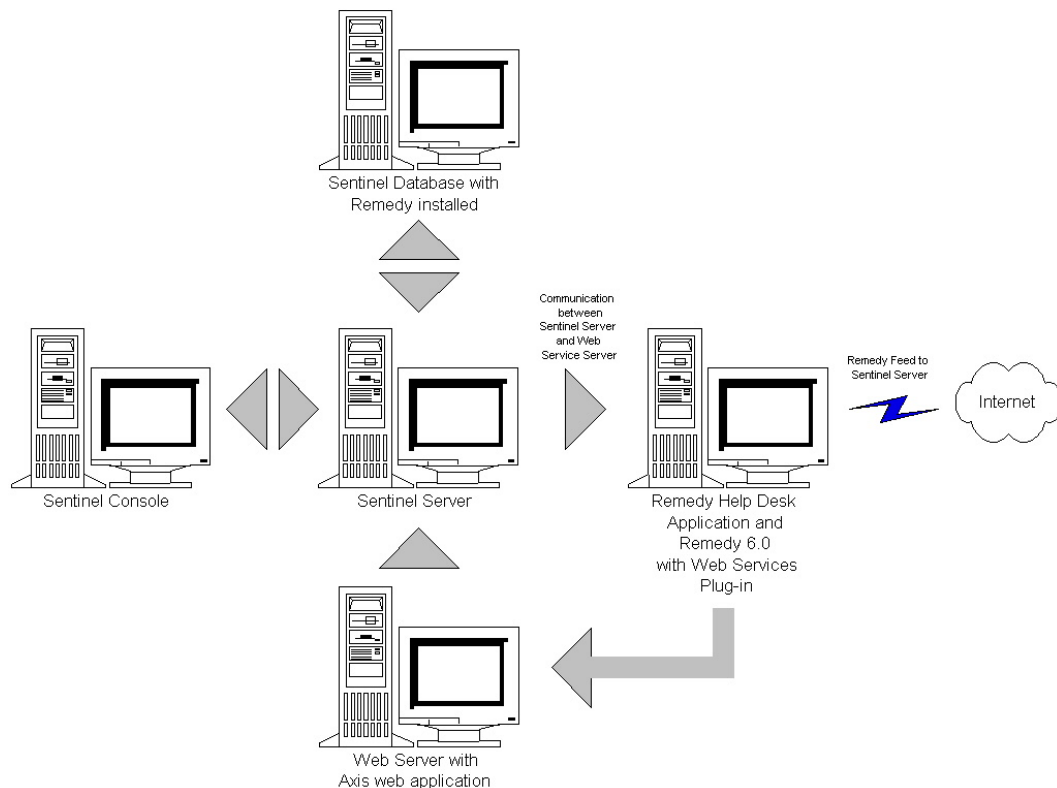
- Remedy
- HP OpenView Operations
- HP Service Desk

Chapter 1 – Remedy Integration	1-1
Configuration.....	1-1
Remedy to e-Security Sentinel Data Flow.....	1-5
Installing Sentinel	1-9
Remedy to Sentinel Data Flow Configuration	1-9
Chapter 2 – Remedy Help Desk Operations	2-1
Remedy Help Desk Operations.....	2-1
Manually Reconfiguring the Remedy Interface Settings	2-1
Remedy Settings.....	2-1
Resetting the Remedy Password	2-2
Chapter 3 – Installing HP OpenView Service Desk for Windows.....	3-1
System Requirements	3-1
Installation	3-2
Configuring HP OpenView Service Desk	3-2
Enabling Service Desk to Sentinel (bi-directional) Interface	3-3
Chapter 4 – HP OpenView Service Desk Integration	4-1
HP OpenView Service Desk	4-1
Sending Incidents to HP OpenView Service Desk	4-2
HP OpenView Service Desk Client	4-3
HP OpenView Service Desk – Bi-Directional Interface	4-5
Manually Reconfiguring the HP OpenView Service Desk Interface Settings	4-6
Appendix A – Sentinel Copyright Information.....	A-1

Chapter 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 e-Security Sentinel.
- Ability to update a related case in Help Desk, when e-security Sentinel incident is updated.
- Ability to update an e-security 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 e-Security 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 on the '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 the '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.

Creating the 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.

The screenshot shows the 'Modify Web Service - EsecToHelpDesk' dialog box. The 'Basic Info' tab is active, showing the following fields:

- Name:** EsecToHelpDesk
- Base Form:** HPD:HelpDesk
- Service Type:** document - literal
- XML Schema:** (empty field with a folder icon, Load... button, and Options button)

The 'Additional Info' section contains:

- Label:** (empty field)
- Description:** (empty field)

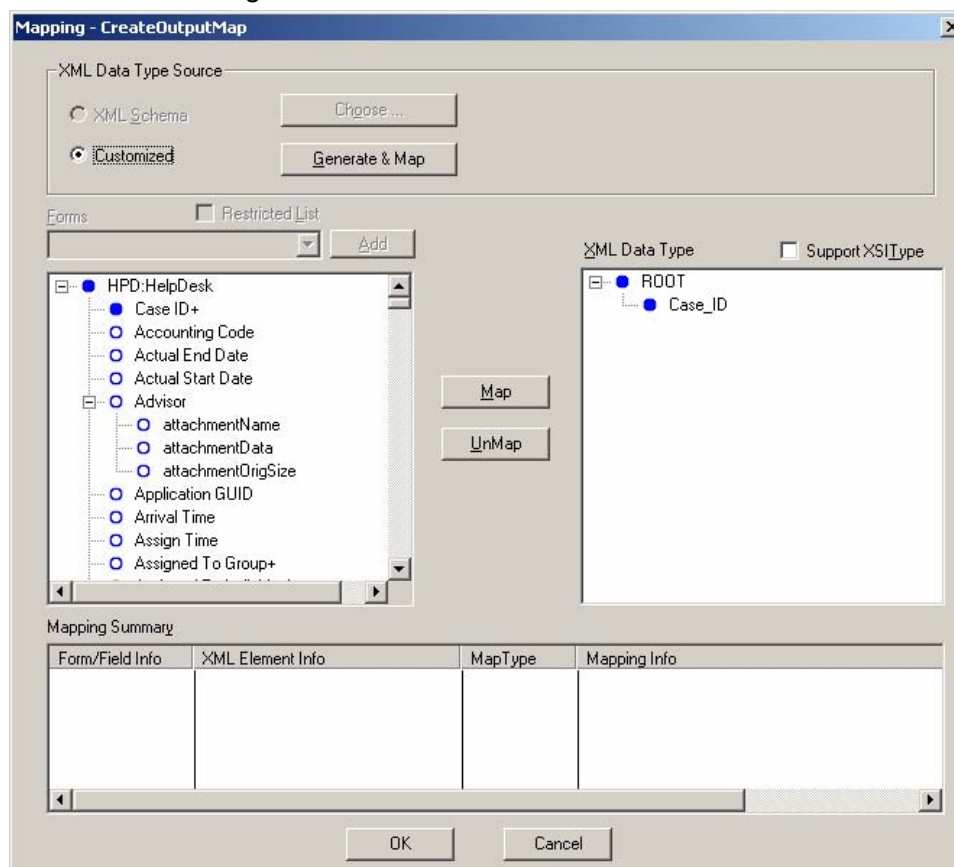
The 'Operations' section includes an 'Operations List' with 'OpCreate' and 'OpSet' (selected). To the right of the list are buttons: New, Copy, Modify, and Remove. Below the list, the 'Name' field is 'OpSet' and the 'Type' is 'Set'. There is an 'Options...' button next to the Type field.

The 'Mappings' section has 'Input Mapping...' and 'Output Mapping...' buttons.

At the bottom, the 'Qualification' section has a text box containing 'Case ID+' and a button to open the XPath editor.

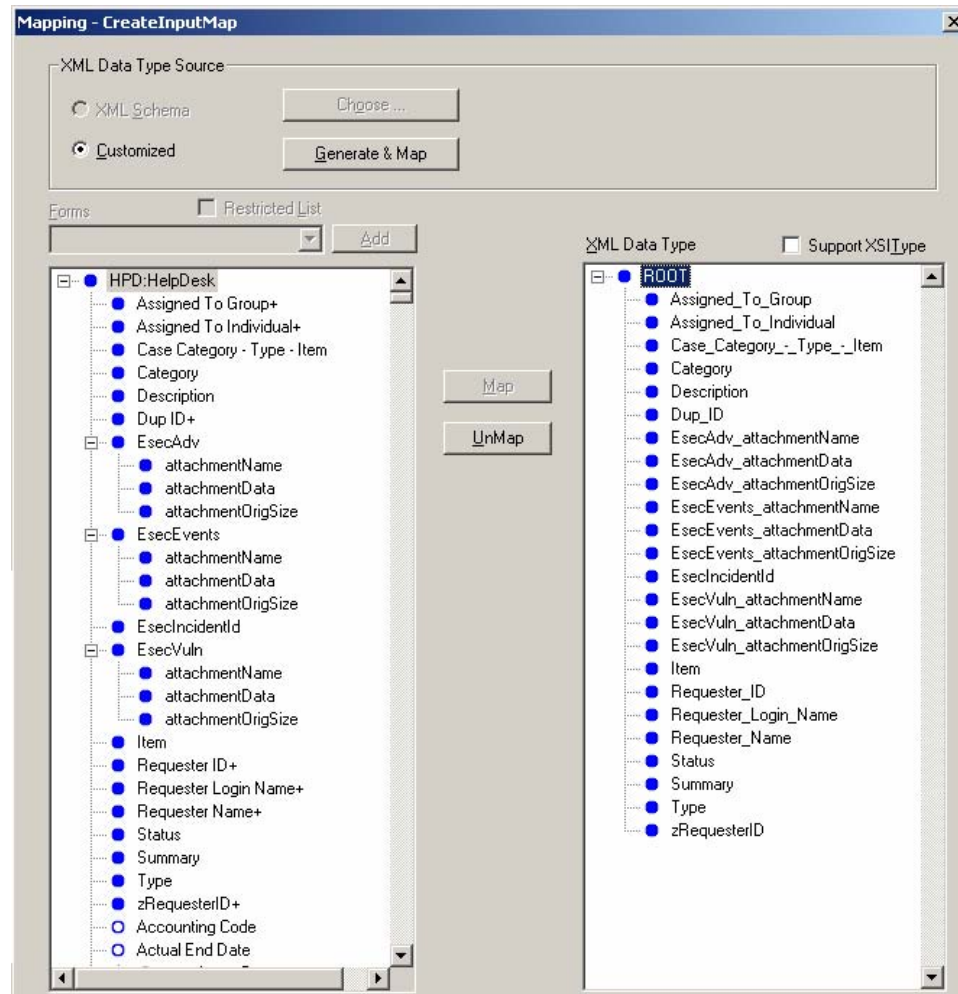
2. Using the Help Desk Case as a base form, create a WebService called 'EsecToHelpDesk' and select Base Form 'HPD HelpDesk'.

3. Make two operations for this web service called:
 - opCreate
 - opSetby removing the other operations.
4. Select OpCreate and click the Output Mapping button. Make the screen match the following illustration.



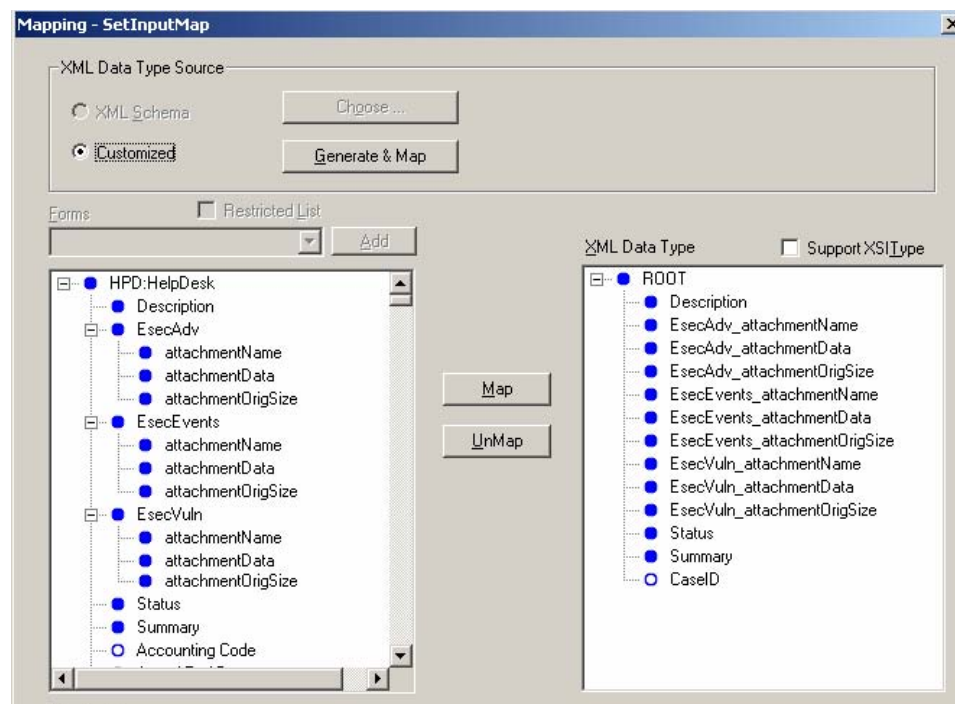
Select Input Mapping button for opCreate. Make the screen match the following illustration.

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

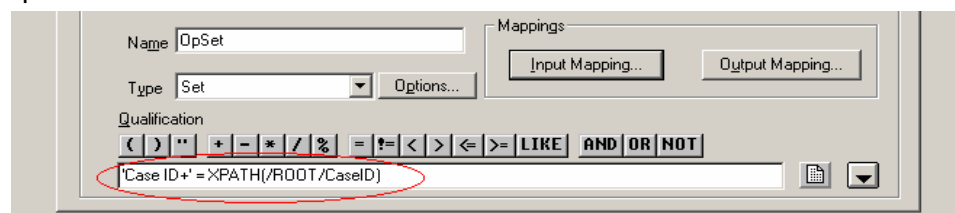


Click Save.

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 e-Security Sentinel Data Flow

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

Remedy to e-Security 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.

Modify Filter - EsecUpdate2

Basic | If Action - (1) | Else Action | Change History | Help Text

Filter

Name: EsecUpdate2

☒ Enable Execution Order: 500

Form Name: HPD:HelpDesk ☐ Restricted List

☒ **HPD:HelpDesk**

☐ Alert Events

☐ Alert List

☐ Application Pending

☐ Application Statistics

☐ Application Statistics Configuration

☐ AR System Administrator Preference

☐ AR System Application State

☐ AR System Currency Codes

☐ AR System Currency Label Catalog

☐ AR System Currency Localized Labels

☐ AR System Currency Ratios

Execute On:

☐ Submit ☒ Modify ☐ Delete ☐ Get Entry ☐ Merge

Run If:

() " + - * / % = != < > <= >= LIKE AND OR NOT EXTERNAL

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 e-Sentinel WebService (<http://<webserver IP or DNS name>:8080/axis/services/EsecWebService?wsdl>).

Create Filter

Basic | If Action | Else Action | Change History | Help Text

New Action: Set Fields

Current Actions:

Move

Add Action

Delete Action

Set Field

Server Name: <Your Server Name>

Read Value for Field From: WEB SERVICE

Choose Wsdl

http://<webserver>:8080/axis/services/EsecWebService?wsdl

Load

Web Service:

SetExternalDataWsvcService

Choose Operation

updateEsecIncident

Mapping Info

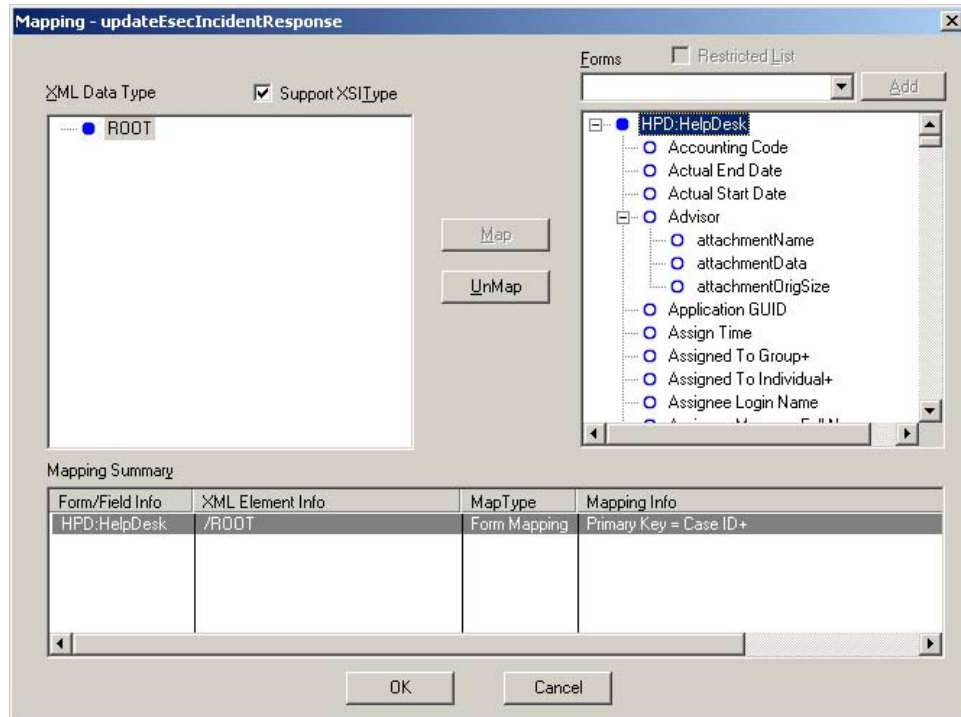
Input Mapping...

Output Mapping...

☐ Restricted List ☐ Advanced

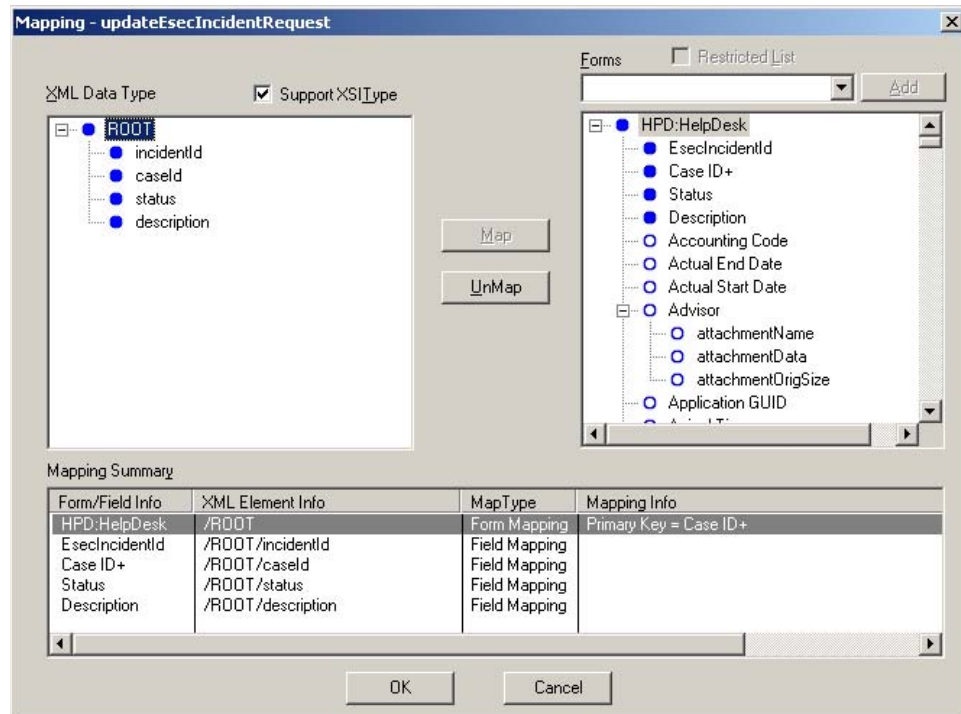
4. In the 'Choose Operation' drop down menu, select select 'updateEsecIncident' method and set the Input and Output mapping.

Click the 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 (i.e. incidentId), select an item on the right (i.e. 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 | ▪ Group Name (may be left blank) |
| ▪ Password | ▪ Individual Name (may be left Blank) |
| ▪ Requestor Name | ▪ Server Name |
| ▪ Requester ID | ▪ Service Name |
| ▪ Requestor Login | |

For Remedy to e-Security 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:

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

In order to have Remedy to e-Security 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 e-Security web server.

Modify Filter - EsecUpdate2

Basic | If Action - (1) | Else Action | Change History | Help Text

New Action: [Dropdown]

Current Actions: Set Fields

[Move] [Modify Action] [Delete Action]

Set Field

Server Name: <Your remedy server>

Read Value for Field From: WEB SERVICE

Choose Wsdl

http://<Your web server and port>/axis/services/EsecWebService?wsdl

[Load]

Web Service: SetExternalDataWSvcService

Choose Operation: updateEsecIncident

Mapping Info

[Input Mapping...] [Output Mapping...]

☐ Restricted List ☐ Advanced

Chapter 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 e-Security Sentinel.
- Ability to update a related case in Help Desk, when e-security Sentinel incident is updated.
- Ability to update an e-security Sentinel incident when a related Case in Help Desk is updated.

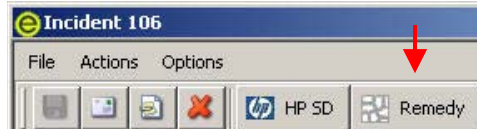
Remedy Help Desk Operations

How to send an Incident for Remedy Help Desk (v5.0.1 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.



How to update an Incident to Remedy Help Desk (v5.0.1. 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. `cd %ESEC_HOME%/sentinel/bin/`
2. Enter:

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

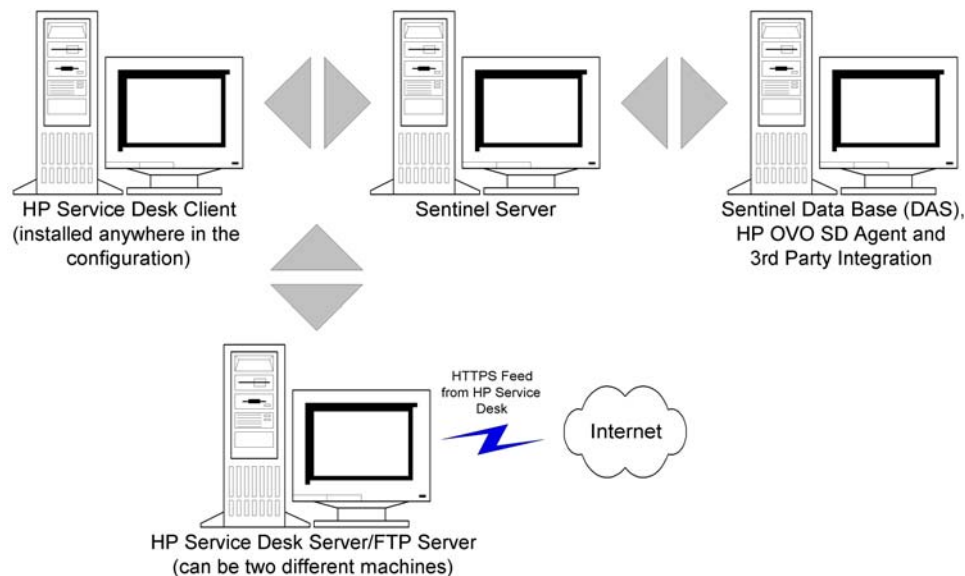
 - `-r` is the Remedy password

Chapter 3 – Installing HP OpenView Service Desk for Windows

e-Security's bi-directional integration with HP OpenView Service Desk, which is licensed separately, provides new valuable features to the Sentinel Console. e-Security 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 e-security Security's Sentinel Console Incident and SD
- Round Trip Integration: SD send updates to e-security and e-security sending updates to SD
- Update SD Incident Status from e-Security's Sentinel Console
- Update e-Security'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.

e-Security supports the following versions of HP OpenView Service Desk:

- 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
- e-Security 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 e-Security 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.

The screenshot shows the 'Attachment Settings' dialog box with the 'General' tab active. The 'Attachment Server' section includes text boxes for 'Name' (containing '<IP address of your FTP Server>'), 'User name' (containing '<your user name>'), 'Password' (empty), and 'Target folder' (containing './'). Below these is an unchecked checkbox for 'Use Passive FTP' and a 'Test Connection...' button. At the bottom, the checkbox for 'Save attachment in background' is checked.

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 e-Security's Sentinel (das_cmd.bat) is installed. This allows HP Service Desk to execute Sentinel's das_cmd utility.

Enabling 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.

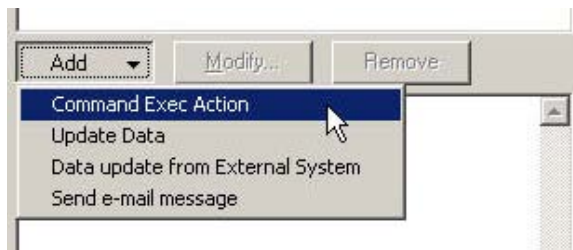
When incident is created or modified
When incident is created
When incident is modified
When incident is deleted

8. Click the Condition... button.
9. Click the Add Criterion... button.
10. Click the 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]"
```

Command Exec Action

Name:

Description:

Host:

This command will be executed on the following host:

☐ Blocked

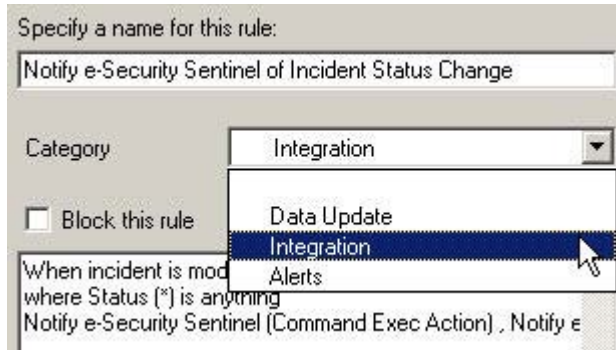
Command line:

Parameters:

Insert at cursor position:

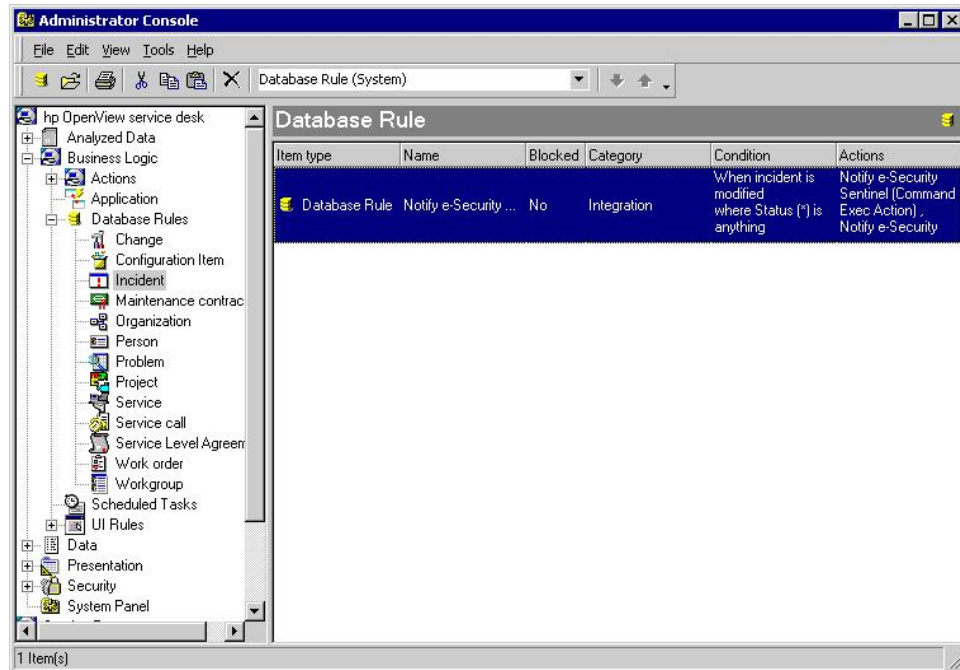
Give the new Database Rule any name you want with a description. Click OK and then click Next.

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.



Chapter 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

e-Security 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 e-Security's Sentinel Console
- Update SD Incident Status from e-Security's Sentinel Console
- Update e-Security's Incident Status from HP SD

e-Security 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

Service Desk Status	Sentinel State
Closed	Closed

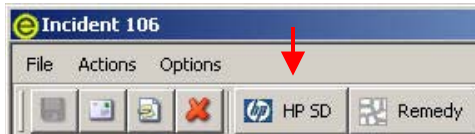
Sending Incidents to HP OpenView Service Desk

How to send an Incident to HP OpenView Service Desk

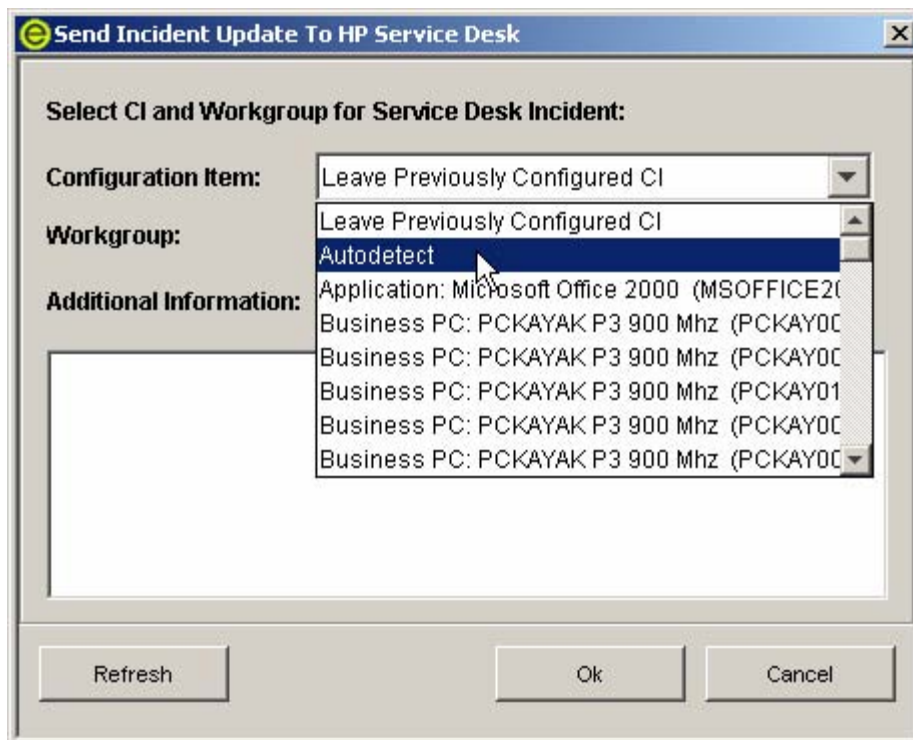
1. Click the Incidents tab.
2. In the navigator pane, expand the Incident Views folder and high light Incident View Manager.

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 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 Auto-detect option is available in the Configuration Item selection list. If you select Auto-detect, 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.

Incident 105

File Actions Options

HP SD

Incident ID: 105

Title: 6

State: OPEN

Severity: Trivial (1)

Priority: None (0)

Category:

Originator: esecadm

Responsible:

Description:

Resolution:

Events Assets Vulnerability Advisor iTRAC History Attachments **External Data**

External Data Source: HP Service Desk

External Data ID: 171

External Data:

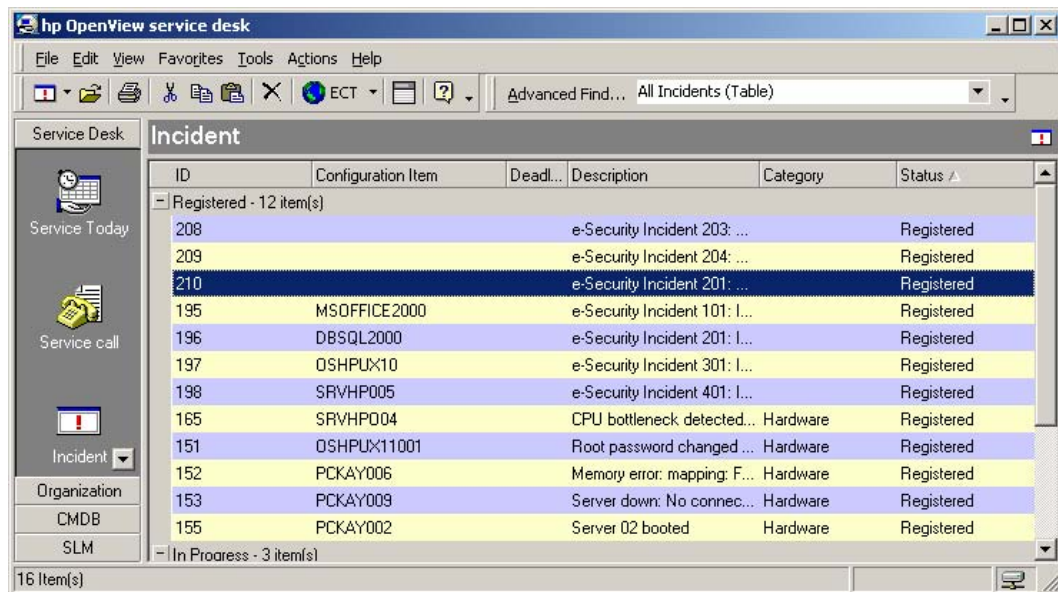
ASSIGNED CONFIGURATION ITEM:
 Configuration Item: PCKAY007
 Name: PCKAYAK P3 900 Mhz
 IP Address: 127.0.0.1
 Category: Business PC
 Location: USA
 Service Level: Bronze (8 x 5)

RELATED CONFIGURATION ITEM(S):
 No CI information found for IP Address(es): 192.168.76.61, 192.168.131.135, 192.168.85.86, 192.168.148.64

Save Cancel

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)

210 - Incident

File Edit View Tools Actions Help

Save and Close Main Incident template

Due in 4 days.

ID: 210

Status: Registered

Configuration: DBSQL2000

Description: e-Security Incident 201: Correlation

Information: Fri May 07 06:21:00 EDT 2004 (ESEC_CORR) - <empty>.

Solution:

Workaround:

General Work orders Subcontract calls Relations Time/Cost History

Severity:

Impact: None

Priority: 5 None

Deadline: 23/07/04 17:00

Actual Finish:

Assignment:

To workgroup:

To person:

More:

Service:

Service Level: Bronze (8 x 5)

Folder:

Category:

Classification:

Closure code:

Attachments: Incident-201... Incident-201... Incident-201...

HP OpenView Service Desk – Bi-Directional Interface

If this option is enabled, (see e-Security 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.

210 - Incident

File Edit View Tools Actions Help

Save and Close Main Incident template

Due in 4 days.

ID: 210

Status: In Progress

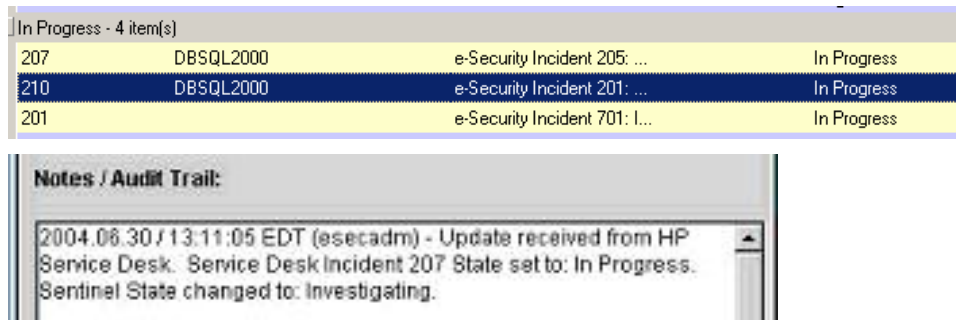
Configuration: DBSQL2000

General Work orders Subcontract calls Relations Time/Cost History

Severity:

Impact: None

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)

Appendix A – Sentinel Copyright Information

e-Security Sentinel™ 5

Copyright © 1999-2006, e-Security, Inc. All rights reserved.

Sentinel 5 may contain the following third-party technologies:

- **Apache Axis** and **Apache Tomcat**, Copyright © 1999 to 2005, Apache Software Foundation. For more information, disclaimers and restrictions, see <http://www.apache.org/licenses/>
- **ANTLR**. For more information, disclaimers and restrictions, see <http://www.antlr.org>
- **Boost**, Copyright © 1999, Boost.org.
- **Bouncy Castle**, Copyright © 2000-2004, the Legion of Bouncy Castle. For more information, disclaimers and restrictions see <http://www.bouncycastle.org>.
- **Checkpoint**. Copyright © Check Point Software Technologies Ltd.
- **Concurrent**, utility package. Copyright © Doug Lea. Used without CopyOnWriteArrayList and ConcurrentReaderHashMap classes.
- **Crypto++ Compilation**. Copyright © 1995-2003, Wei Dai, incorporating the following copyrighted work: **mars.cpp** by Brian Gladman and Sean Woods. For more information, disclaimers and restrictions see <http://www.eskimo.com/~weidai/License.txt>.
- **Crystal Reports Developer and Crystal Reports Server**. Copyright © 2004 Business Objects Software Limited.
- **DataDirect Technologies Corp.** Copyright © 1991-2003.
- **edpFTPj**, licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see <http://www.enterprisedt.com/products/edftpj/purchase.html>.
- **Enhydra Shark**, licensed under the Lesser General Public License available at: <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 and/or Macrovision Europe Ltd.
- **Java 2 Platform, Standard Edition**. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt.

The Java 2 Platform may also contain the following third-party products:

- CoolServlets © 1999
- DES and 3xDES © 2000 by 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, a registered trademark or trademark of Bigelow and Holmes

- Taligent, Inc.

- IBM, some portions available at: <http://oss.software.ibm.com/icu4j/>

For more information regarding these third-party technologies and their associated disclaimers and restrictions, see:

http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt.

- **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.
- **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.
- **Java Ace**, by Douglas C. Schmidt and his research group at Washington University and **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>
- **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>.
- **Java Network Launching Protocol (JNLP)**. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions, please see <http://www.java.sun.com/products/javawebstart/download-jnlp.html> and click download > license.
- **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.
- **jTDS** 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>.
- **Monarch Charts**. Copyright © 2005, Singleton Labs.
- **Net-SNMP**. Portions of the code are copyrighted by various entities, which reserve all rights. Copyright © 1989, 1991, 1992 by Carnegie Mellon University; Copyright © 1996, 1998 to 2000, the Regents of the University of California; Copyright © 2001 to 2003 Networks Associates Technology, Inc.; Copyright © 2001 to 2003, Cambridge Broadband, Ltd.; Copyright © 2003 Sun Microsystems, Inc. and Copyright © 2003 to 2004, Sparta, Inc. For more information, disclaimers and restrictions, see <http://net-snmp.sourceforge.net>.
- **The OpenSSL Project**. Copyright © 1998-2004. the Open SSL Project. For more information, disclaimers and restrictions, see <http://www.openssl.org>.
- **Oracle Help for Java**. Copyright © 1994-2006, Oracle Corporation.
- **RoboHELP Office**. Copyright © Adobe Systems Incorporated, formerly Macromedia.

- **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/>.
- **Sonic Software Corporation.** Copyright © 2003-2004. The SSC software contains security software licensed from RSA Security, Inc.
- **Tinyxml.** For more information, disclaimers and restrictions see <http://grinninglizard.com/tinyxmldocs/index.html>.
- **SecurityNexus.** Copyright © 2003 to 2006. SecurityNexus, LLC. All rights reserved.
- **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>.
- **yWorks.** Copyright © 2003 to 2006, yWorks.

<p>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 webpages are inactive, please contact e-Security's Office of the Counsel at 1921 Gallows Road, Vienna, VA 22182. 703-852-8000.</p>

bi-directional interface		HP OpenView Service Desk 3-2	
HP OpenView Service Desk	3-4	Sentinel.....	1-9
HP - Service Desk.....	4-1	installing Sentinel.....	1-9
HP OpenView Service Desk	3-1, 4-1	Remedy	1-1
configuring to FTP Server	3-2	Remedy Help Desk.....	2-1
installation	3-2	changing the case form	1-1
sending an Incident (v5.0).....	4-2	creating the web service	1-2
to set attachment settings	3-3	data flow	1-5
HP SD	4-1	data flow - input mapping.....	1-8
HP Service Desk.....	3-1, 4-1	data flow - output mapping	1-8
configuring to FTP Server	3-2	Incident Setup (v5.0.1 and later)....	2-1
installation	3-2	installing Sentinel.....	1-9
sending an Incident (v5.0).....	4-2	opCreate - input.....	1-4
to set attachment settings	3-3	opCreate - output.....	1-3
HP-OpenView Operations.....	4-1	opSet - input	1-5
HP-OVO	4-1	sending an Incident to Remedy Help	
installation		Desk (v5.0.1 and later)	2-1