Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

Enterprise System Connector for HP Service Manager REST 7.1.7.7612.0

Configuration Guide

February 15, 2016

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Contact Information

Phone	A list of phone numbers for HP ArcSight Technical Support is available on the HP Enterprise Security contacts page: www.hpe.com/software/support/contact_list
Support Web Site	www.hpe.com/software/support
Protect 724 Community	https://protect724.hp.com

Revision History

Date	Product Version	Description
02-15-2016	7.1.7.7612.0	• Updated the build number. • ESM 6.9.1c support.
09-11-2015	7.1.5.7512.0 Beta	• HP Service Manager REST version 9.4, ESM 6.8c, and ESM Express 6.9.0c support. • Added information for Service Manager mapping and values. • Added graphic to illustrate the HP SM and ESM severity rule. • Added HP SM setting for REST integration.
05-15-2014	7.0.3.7043.0	Initial release of this connector.

Contents

Enterprise System Connector for HP Service Manager REST

This guide provides information for installing the Enterprise System Connector for HP Service Manager REST, and configuring the device for data collection.

Product Overview

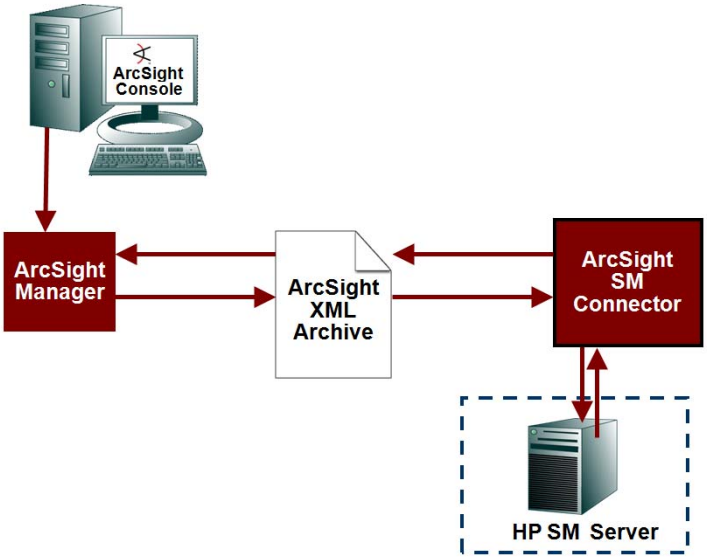
ArcSight Manager communicates with HP Service Manager using the Enterprise System Connector for HP Service Manager REST. HP Service Manager is an incident tracking and case management system. HP Service Manager can be used in addition to or as an alternative to ESM case management to use for incident creation, tracking, and workflow support for ArcSight security event data. ESM cases and their associated events can be exported to HP Service manager incidents. The status of HP Service Manager incidents can be exported back to ESM and reflected there as the status of the associated case. This is useful for customers already using HP Service Manager as their centralized incident tracking system.

The Enterprise System Connector for HP Service Manager REST can send events and cases exported from ESM to HP Service Manager. The connector runs in the background, as a service, transferring the case data from ESM to HP Service Manager. Cases are reflected as incidents in HP Service Manager. The Enterprise System Connector for HP Service Manager can also be configured to update the ESM database with case status of HP Service Manager incidents.

Features and Functional Summary

When the export is triggered by a command or a rule, ArcSight security cases and associated events (or single event) are transferred by ESM to the HP Service Manager using the Enterprise System Connector for HP Service Manager REST. The connector parses the XML archive file and prepares the data to submit to HP Service Manager Web Services for transfer. The Manager exports event and case data in ArcSight XML archive format in the Manager's `archive/exports` directory. The Manager imports data from

any ArcSight XML archive format files it finds in the `archive/imports` directory (the incident ID and the incident status. The Manager checks for the import and export files every minute (60 seconds), by default.



The `archive/exports` directory and the `archive/imports` directory are system-created and do not have to be created manually. These directories are found, by default, in `<MANAGER_HOME>`.

The connector sends the HP Service Manager incident ID back to ESM, where it is stored as the case `External ID` field. Also, the connector tracks the HP Service Manager incident's status changes and sends the status back to ESM, where it is displayed in the `Stage` field for the case, which has been mapped by default to show the status. This and other mappings can be changed as needed.

The exported and imported XML archive files are identified by a time stamp (which displays both time and date), in this format:

`ExternalEventTrackingData_<timestamp>.xml`

For example:

`ExternalEventTrackingData_10_19-10_15-27-19.692.xml`

The ESM schema DTDs for the XML files are located in `schema/xml/archive` on the Manager, and you can use these DTDs for reference for field mappings.

HP Service Manager Setting

Your HP Service Manager integration must have REST capability enabled. Starting with release 9.34, for REST to work you need to add the following parameter in **sm.ini**:

`restaccessviabrowser:1`

XML File Examples - Imports

These are examples of XML files in the `archive/imports` directory. The first is an XML file used to provide ESM with the External ID (the incident ID from HP Service Manager) of an exported case:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE archive SYSTEM <archive version="2.0">
<Case externalID="IM10497" id="79gcxzyoBABCOWTV7XFFrLA=="
name="_system_case_Event_Export_Request_9-1-10_14-25-51.222"/>
</archive>
```

This is an example of XML in the `archive/imports` directory used to provide ESM with the status of a previously exported case:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE archive SYSTEM
<archive version="2.0">

<Case externalID="IM10341" name="IM10341">
<stage>Queued</stage>
</Case>

<Case externalID="IM10408" name="IM10408">
<stage>Queued</stage>
</Case>

<Case externalID="IM10340" name="IM10340">
<stage>Queued</stage>
</Case>
</archive>
```

XML File Examples - Exports

This is an example of a portion of an XML file in the `archive/exports` directory.

```
<Case id="79gcxzyoBABCOWTV7XFFrLA=="
name="_system_case_Event_Export_Request_9-1-10_14-25-51.222"
action="insert" >
<action>B-Block/Shutdown</action>
<associatedImpact>A-Availability</associatedImpact>
<attackAgent>I-Insider</attackAgent>
<attackMechanism>P-Physical</attackMechanism>


<caseEvents>
<list>
<ref type="SecurityEvent" uri="/All Events/80001320358"
id="80001320358"/>
<ref type="SecurityEvent" uri="/All Events/80001320359"
id="80001320359"/>
<ref type="SecurityEvent" uri="/All Events/80001320360"
id="80001320360"/>
</list>
</caseEvents>
```

```
…
<SecurityEvent id="80001320358" name="New subagent [generic_syslog]
detected for device [127.0.0.1]" action="insert" >

<agent>
<map>
<address>127.0.1.1</address>
<assetId>43u1n1igBABCebzetu2dMIA==</assetId>
<descriptorId>1400001</descriptorId>
<hostName>tantoine-desktop</hostName>
<id>3Rt0mzyoBABCOJzV7XFFrLA==</id>
<timeZone>America/Los_Angeles</timeZone>
<type>syslog</type>
<version>5.0.2.0.0</version>
<zone>
<ref type="Zone" uri="/All Zones/ArcSight System/Private Address
Space Zones/RFC1700 Zones/RFC1700: 127.0.0.0-127.255.255.255"
id="M77cj2AABABCCz1pYAT3UdQ==">
</zone>
</map>
</agent>
<agentReceiptTime>2010-09-01 14:18:45.344</agentReceiptTime>
<agentSeverity>High</agentSeverity>
```

Set Up Task Overview

To use the Enterprise System Connector for HP Service Manager REST to send case and event data and receive HP Service Manager incident IDs and status, you must:

1. Install the connector. See “Installing the SmartConnector” on page 9.
2. Familiarize yourself with the fields in the schema for ESM and HP Service Manager.
3. Examine the connector properties file, `servicemanager.properties`, to understand what data fields will be transferred by default to HP Service Manager. There are default mappings in this file, and you can modify these mappings as needed.
4. Decide if there are any additional fields you want to send to HP Service manager, and add those mappings to `servicemanager.properties`. “Mapping the HP Service Manager Properties” on page 14.
5. Trigger the export of event and case data from ESM to HP Service Manager by command or rule. “Using the ArcSight Console to Export” on page 18.
6. Check the ArcSight Console for incident information (external incident ID and status in the Stage field, or as mapped).

Supported Versions and Platforms

The supported platforms for the Enterprise System Connector for HP Service Manager REST are:

- Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012 R2, both 64-bit
- Red Hat Enterprise Linux (RHEL) 6.6, 7.1 all 64-bit

Versions Supported:

- HP Service Manager versions 9.32 and 9.4

ESM Certification:

- ESM 5.5, 5.6, 6.8c, 6.9.1c
- AE 4.0 P1, ESM Express 6.9.0c

Additionally, the Enterprise System Connector for HP Service Manager REST can support cross-platform implementations as follows:

- ESM installed on Linux and the Enterprise System Connector for HP Service Manager REST installed on Microsoft Windows (using the Samba Server to achieve the connection)
- ESM installed on Microsoft Windows and the Enterprise System Connector for HP Service Manager REST installed on Linux (using the NFS Server to achieve the connection)

Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected connector.

Prepare to Install Connector

Before you install the connector, make sure that the ESM Manager has already been installed correctly.ArcSight products with which the connectors will communicate have already been installed correctly. This configuration guide takes you through the installation process with **ArcSight Manager (encrypted)** as the destination.

The Enterprise System Connector for HP Service Manager can be installed on the same machine as ESM, or on another machine.

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords
- Access to the Manager's installation folder (by default, `<MANAGER_HOME>`)
- You must have read/write access to the `archive/exports` and the `archive/imports` directories and the files in these directories. These directories are located in `<MANAGER_HOME>`. When ESM is running on Linux and the connector is running on Windows, set up a read/write file share between Linux and Windows using Samba; also configure SELINUX.
- HTTP access to HP Service Manager, either directly or through a proxy

Also, review the "Installation Troubleshooting Tips" to ensure you complete the steps described in those installation scenarios (if needed).

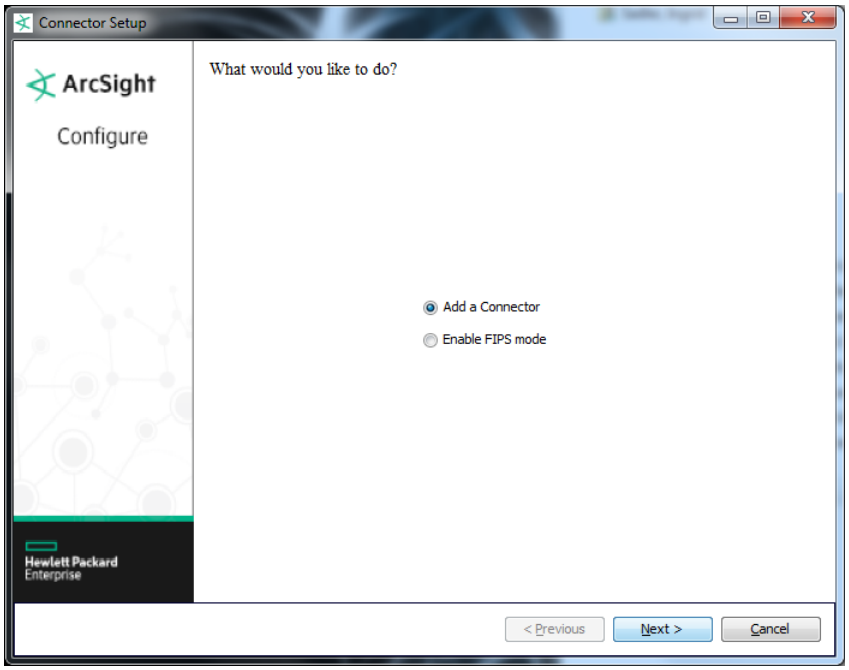
Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HP SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the HP SSO site.
2. Start the SmartConnector Installer by running the executable.

   Follow the installation wizard through the following folder selection tasks and installation of the core connector software:

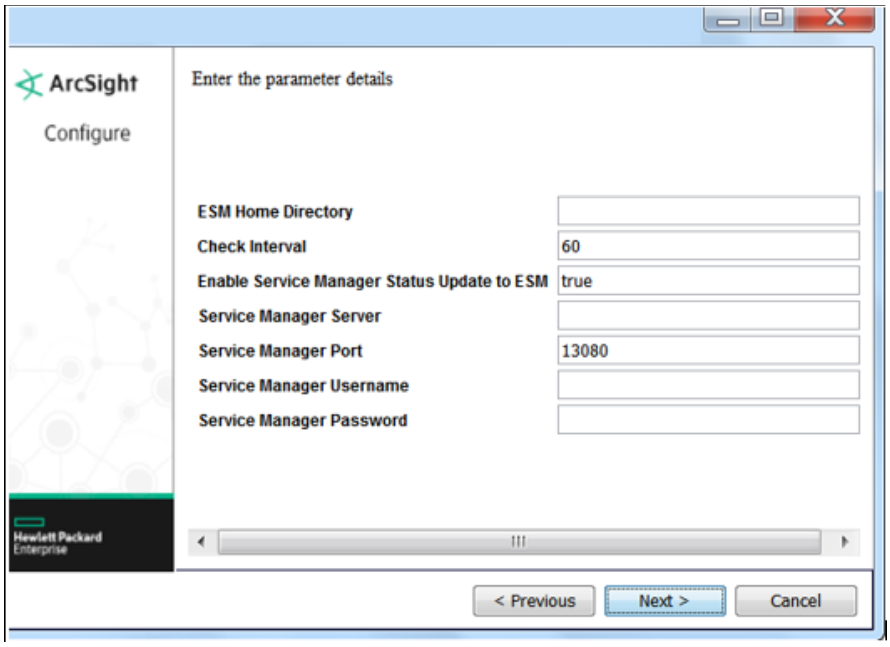
   Introduction
   Choose Install Folder
   Choose Install Set
   Choose Shortcut Folder
   Pre-Installation Summary
   Installing...
3. When the installation of SmartConnector core component software is finished, the following window is displayed:



Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**.
2. The connector type **Enterprise System Connector for HP Service Manager REST** is pre-selected; click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
ESM Home Directory	The path to the ESM Manager home directory.
Check Interval	Interval at which the connector checks for updates. The default is **60** (seconds). The value must be 1 or larger, and in whole numbers. Zero (0) is invalid. The default is recommended for performance reasons. This field is required.
Enables Service Manager Status Update to ESM	Determines whether the HP Service Manager incident status will be updated in the `Stage` field for the case. The default is **true**. This is the same setting as the value of the `downlink.enabled` parameter in `$ARCSIGHT_HOME\current\user\agent\agent.properties` file. HP recommends that you run both the connector and the Manager as the same network user, since both processes need write access to the same files. If you notice issues in either export or import even though the files are created correctly, check the owner and permissions attached to them.
Service Manager Server	The IP address or host name of the HP Service Manager server.
Service Manager Port	Port to use to connect to HP Service Manager. Default is 13080. This default works for a relatively small implementation, for example for one HP Service Manager servlet. For that reason, HP recommends that you set up a dedicated HP Service Manager servlet. See the HP Service Manager documentation for details. Also, note that HP Service Manager Load Balancer often uses port 13080. Do not connect to HP Service Manager Load Balancer because of potential HTTP redirect issues.

Parameter	Description
Service Manager Username	Enter the HP Service Manager user name. It is recommended that you create a user dedicated to the Enterprise System Connector for HP Service Manager REST. This is to ensure that the user associated with the integration with ESM has the permissions appropriate to that integration, and that integration alone.
Service Manager Password	Enter the HP Service Manager password (can be optional, depending on the HP Service Manager requirements).

Select a Destination

1. The next window asks for the destination type; select **ArcSight Manager (encrypted)** and click **Next**. (For information about this destination or any of the other destinations listed, see the *ArcSight SmartConnector User Guide*.)
2. Enter values for the **Manager Host Name, Manager Port, User,** and **Password** required parameters. This is the same ArcSight user name and password you created during the ArcSight Manager installation. Use a fully qualified domain name as the Manager Host Name; this name and the certificate common name must be the same. Click **Next**.
3. Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.
4. The certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.
2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.
3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.
4. Click **Next** on the summary window.
5. To complete the installation, choose **Exit** and Click **Next**.

Installation Troubleshooting Tips

This section contains troubleshooting information for specific installations.

- For a remote installation on the Windows platform (with the connector running as a service) the default user is System account. The System account user has limited

capability. To ensure the needed capability, change the owner of the service to a local user account. The user default is not an issue for installations where the connector is running standalone on Windows.

- For a remote installation on the Linux platform (either with the connector running as a service, or running standalone), be sure that the user ID (UID) and group ID (GID) on the system where the connector is installed matches the values for UID and GID on the ESM Manager.

Parameter Modifications

This section highlights some of the properties for you to adjust in your environment as needed.

Rerun agent.setup

Run the wizard again after first installing a SmartConnector to modify the settings:

From `$ARCSIGHT_HOME\current\bin`, execute:

```
runagentsetup
```

1. To make changes to the initial values set during connector installation and configuration, select **Modify Connector**.
2. Click **Next**. Select **Modify connector parameters** and click **Next.**
3. Modify the parameters as needed in the parameters window.
4. Click **Next** to continue. Modify table parameters (if they exist; many connectors have no table parameters) as needed.
5. Click **Next**. The connector parameters changes are processed and the connector configuration is modified. When the configuration changes are complete, you will receive the message **Successfully updated parameters**.
6. Click **Next**. Choose **Exit**, to complete the connector modification. Click **Next** to exit or continue.

After running the SmartConnector `agent.setup`, you can access the connector's parameters as follows:

1. From the `$ARCSIGHT_HOME\current\user\agent` directory open the file `agent.properties` in a pure ASCII text editor (such as Notepad++).
2. In the `agent.properties` file, locate the parameters whose values you want to modify.
3. Enter the property values as needed for the properties described below.
4. Save the exit the `agent.properties` file.
5. Restart the connector.

You can reset mapping of the fields back to default by deleting `user/agent/servicemanager.properties` file and restarting the connector. The default properties are then copied into the `$ARCSIGHT_HOME\current\user\agent\servicemanager.properties` file.

To adjust connector to your environment, you might want to modify the value for the following properties:

Property and Default Value	Use
max.events.per.case	Use to control the maximum number of events per case. This determines how many events are included in each HP Service Manager incident. Default is 100.
max.record.transfer	Use to control the maximum number of records transferred. This can be useful if a rule triggers a large number of records to transfer, and you want to limit the number. Default is 100.
override.default.properties	Indicates that `user/agent/servicemanager.properties` can (and will be) overwritten if not found in the directory on connector restart, with default `servicemanager.properties` file.
servicemanager.proxy.host	Use to point to web proxy (if used). Enter the proxy host IP address or name.
servicemanager.proxy.port	Enter the proxy port. Default is 80.
servicemanager.service.uri	Part of the URL; shows the web service. Do not change if default web service is used. Modify to create your own URL for web service.

Run the Connector

Connectors can be installed and run in standalone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, connectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in standalone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the ArcSight SmartConnector User's Guide.

To run all connectors installed in standalone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the connector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all connectors, enter `Ctrl+C` in the command window.

Mapping the HP Service Manager Properties

You use the mappings in the `$ARCSIGHT_HOME\current\user\agent\servicemanager.properties` file to choose which ArcSight event and case field attributes to send to HP Service Manager. There can be several events per case. Map the fields in the HP Service Manager Incident Management Schema to the fields in the ESM schema by defining them in the `servicemanager.properties` file. Mandatory fields (and the defined values for the fields that require them, such as drop-down lists) are specified in HP Service Manager. The values translated by the mapping have to be accepted and writable on both sides (ESM and

HP Service Manager) for full mapping to occur. Only values that are validated by ESM are transmitted by HP Service Manager to ESM.

The entire content of each event (values of all of the fields) is represented in ESM as a row of data in the Description field for the incident. You can control the fields shown in the data strings by modifying mappings in the `servicemanager.properties` file.

The default fields for data transfer to HP Service Manager are defined in the `servicemanager.properties` file. In general, you can use the default fields for your transfer. If additional fields are added to the HP Service Manager schema, you might have to add more field mappings to accommodate those added fields. If you need to specify additional ArcSight security event fields whose values you want to transfer to HP Service Manager, edit the `servicemanager.properties` file.

The `servicemanager.properties` file has three sections, containing field mappings for case content, event content, and downlink. Examples of these sections are shown below.

1 Case content; for example:

```
# ------------------------------------------------------------------------
# Enterprise System Connector for HP Service Manager mapping configuration
# ------------------------------------------------------------------------
# ========================================================================================

# ----------------------------------------------------------------------------------------
# HP Service Manager field mappings for case content (see DTD below)
# ----------------------------------------------------------------------------------------

# Set the number of fields to set in the incident
servicemanager.case.incident.fields=10

# Set the Service Manager field names to arcsight attribute names mapping
servicemanager.case.incident.field[0].name=Title
arcsight.case.attribute[0].name=description

servicemanager.case.incident.field[1].name=ProblemType
arcsight.case.attribute[1].name=ticketType

servicemanager.case.incident.field[2].name=Category
arcsight.case.attribute[2].name="incident"

servicemanager.case.incident.field[3].name=Status
arcsight.case.attribute[3].name="Open"

servicemanager.case.incident.field[4].name=Impact
arcsight.case.attribute[4].name=operationalImpact

servicemanager.case.incident.field[5].name=Urgency
arcsight.case.attribute[5].name=consequenceSeverity

servicemanager.case.incident.field[6].name=AssignmentGroup
arcsight.case.attribute[6].name="Application"
```

On the ESM side:

Operational Impact: Impact of reported issue. Values assigned are **0** (no impact), **1** (no immediate impact), **2** (low priority impact), **3** (high priority impact), **4** (immediate impact).

Consequence Severity: Values assigned are **0** (None), **1** (Insignificant), **2** (Marginal), **3** (Critical), **4** (Catastrophic).

On the HP SM side:

Impact: The Service Desk Agent populates this field with the impact the interaction has on the business. The impact and the urgency are used to calculate the priority. The impact is based on how much of the business is affected by the issue.

The stored value can be 1-4, as follows:

1 - Enterprise

2 - Site/Dept.

3 - Multiple Users

4 - User

This is a required field.

Urgency: The urgency indicates how pressing the issue is for the service recipient. The urgency and the impact are used to calculate the priority.

The stored value can be 1-4, as follows:

1 - Critical

2 - High

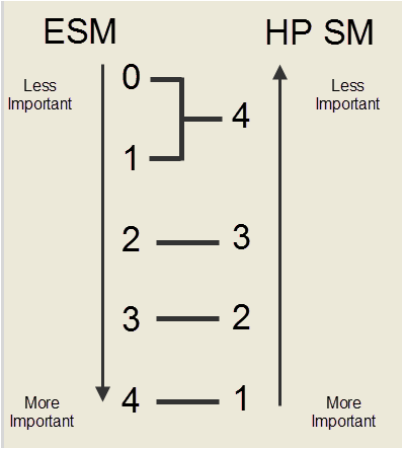
3 - Average

4 - Low

This is a required field.

The mapping for fields 4 and 5 follow this rule:

On the ESM side, values **0**,**1** are mapped to **4** on HP SM incident; **2** to **3**; **3** to **2**; **4** to **1**. See the illustration for clarity.



2 Event content; for example:

```
# ------------------------------------------------------------------------------
# HP Service Manager field mappings for event content (see DTD below)
# ------------------------------------------------------------------------------

# Set the number of fields to set in the incident description
servicemanager.event.incident.fields=14

# Set the Service Manager field names to Arcsight attribute names mapping
# NOTE: these fields will appear as key=value pairs in the Incident description.
#
servicemanager.event.incident.field[0].name=Event Name
arcsight.event.attribute[0].name=name

servicemanager.event.incident.field[1].name=Event ID
arcsight.event.attribute[1].name=id
```

3 Downlink; these are mappings that determine which field in ESM will show the incident status from HP Service Manager, that the update query is based on a timestamp, and the case attribute used to get HP Service Manager updates. For example:

```
# ------------------------------------------------------------------------------
# HP Service Manager field mappings for downlink (from SM to Arcsight)
# ------------------------------------------------------------------------------

# Set the HP Service Manager field name that should be propagated to Arcsight
remote.downlink.field=Status

# Update Timestamp field
remote.downlink.timestamp.field=UpdatedTime
remote.downlink.timestamp.format=yyyy-MM-dd'T'HH:mm:ssZ

# Extra query parameters for the REST service
remote.downlink.extraquery=
remote.downlink.maxcount=25

# Set the Arcsight case attribute to be used to get Service Manager updates
arcsight.downlink.attribute=stage
```

When downlink is enabled, import will update all ESM case fields that are listed in the mapping with the corresponding value from HP Service Manager. Valid field names can be found in the ESM DTD and the HP Service Manager WSDL.

Note the extra query parameters for the REST service. The `remote.downlink.extraquery` parameter allows searches based on queries in addition to the timestamp (the default) as long as the queries follow the REST HTTP query syntax. For example, you might want to filter for a specific createdBy or AssignmentGroup value when retrieving incidents. The `remote.downlink.max` parameter (default 25) controls the maximum number of incidents that can be returned for each query.

Be sure that the date format set in HP Service Manager matches date format in the connector.

Use internal names in the `servicemanager.properties` file rather than the display names shown for the fields in the Event Inspector. For example, use "attackerAddress" for the field that is shown in the Event Inspector as "Attacker Address."

Internal field names can differ from the field labels displayed in the ArcSight Console or the HP Service Manager interface.

To convert a display name to an internal name, remove all spaces and start the field name with a lowercase letter. HP Service Manager fields also use internal names instead of display names. The ESM fields you add must exist in the ESM schema.

1 Check the HP Service Manager schema to verify the fields you need to map.

2 Specify the ESM field names as needed in the `servicemanager.properties` file. See the `servicemanager.properties` file installed with the connector for the default property mappings and values.

3 Restart the HP Service Manager Enterprise System connector.

Using the ArcSight Console to Export

The Enterprise System Connector for HP Service Manager REST initiates the creation of a new HP Service Manager incident for each exported case found in the files in the Manager's `archive/exports` directory. When HP Service Manager creates the new incident, the Enterprise System Connector for HP Service Manager notifies the Manager of the new incident ID, which is then stored in the External ID field of the case.

ESM exports data to HP Service Manager once per case; HP Service Manager can update the data and send these updates to ESM indefinitely.

The HP Service Manager status of the incident is mapped by default to display in the `Stage` field for the case in the ArcSight Console. The Enterprise System Connector for HP Service Manager REST sends incident information to the Manager to update the status of the incident in ESM.

When case data is imported from HP Service Manager, the value shown in the Name field for a case is the HP Service Manager incident ID. To be able to track the case, you can override the `Name` field value by entering a name of your choice in the `Alias (Display Name)` field for the case.

Events that have been successfully sent to HP Service Manager are marked with a red flag in the ArcSight Console Event Inspector. Cases successfully sent to HP Service Manager are flagged with a red case in the Navigator panel.

Be sure to have a description for your case in ESM. Otherwise, data substitution can cause event data to be written to the description.

To send an event to HP Service Manager manually

1 Right-click one or more selected events in the ArcSight Console.

2 Choose **Export > Export to Event Tracking System** from the context menu.

To send an event to HP Service Manager automatically

Use the rule action **Export to External System** on any rule.

To send a case to HP Service Manager manually

1 Right-click a case in the ArcSight Console.

2 Choose **Export > Export to External System** from the context menu.

To send a case to HP Service Manager automatically

1 Create a new rule in the ArcSight Console under `/All Cases/Public`. For the example, the rule named is “HPSMExportCase”.

2 In the Inspect/Edit area, in the actions tab for the rule, choose **Add > Case > Add to Existing Case** from the context menu.

3 Create a new search group in the Resources area. Select a case and right-click to choose New Search Group. For this example, the search group is called “ForExport”.

Create a condition for this new search group using `$generatorName_$endTime`. This condition must have the same name as the rule created in step 1. In this example, that rule name is “HPSMExportCase”.

4 Add this entry to the `server.properties` file:

```
external.export.querygroup.uri=/All Cases/All
Cases/Public/ForExport
```

The path is the path to the search group created in step 3.

5 Restart the ESM server so the new property is implemented.

Exporting Events

If **one** ArcSight event is selected and exported to HP Service Manager, **one** ArcSight case is generated, **one** HP Service Manager incident is created and **one** HP Service Manager incident ID is added to the External ID field of the ArcSight case. If 10 events are selected and exported together in an export request, one ArcSight case is generated to track the export, one HP Service Manager incident is created, that accounts for all of the 10 events in that case.

When directly exporting events to HP Service Manager (either interactively or automated using Rule action), keep in mind that one ArcSight case is automatically created per export request to track the export. Be careful in using the Rule action for Export to External System. If the rule fires export requests too often, it will create a large number of auto-generated cases in ESM. You may have to manually delete these cases periodically.

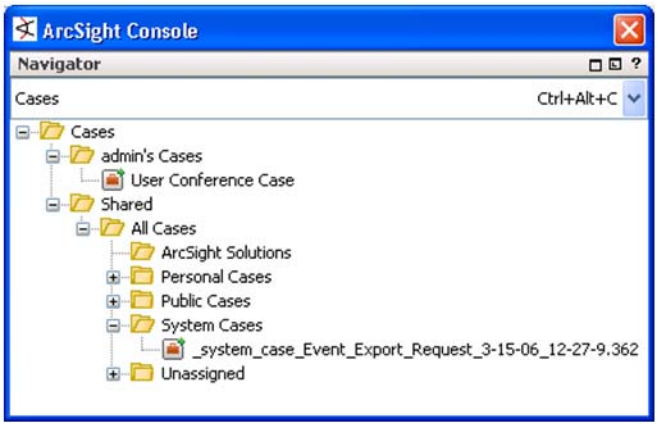
Exporting Cases

If **one** ArcSight case has multiple events, and that case is exported to HP Service Manager, **one** HP Service Manager incident is created that accounts for all events in that case. After creating the incident in HP Service Manager, the connector places the HP Service Manager incident ID in the ArcSight case’s `ExternalID` field. For example, if one ArcSight case has 10 events and is exported to HP Service Manager, one HP Service Manager incident is created and one HP Service Manager incident ID is subsequently sent back from HP Service Manager and added to the **one** ArcSight case.

Tracking Event and Case Exports

The export of data to the XML archive can be tracked using cases. A case exists for any export, whether it is a case or a single event. A case is created automatically if the export was for a single event rather than a case.This applies both to exports that are performed

manually or by rule action. Exported cases are tracked under `Cases/Shared/All Cases/System Cases`.



Troubleshooting Using the Log Files and Product Log

Check the `$ARCSIGHT_HOME\current\logs\agent.log` as needed to verify the cycle of data transferred and data received. Check to see if there were any exceptions, or to verify the number of cases exported to ensure that the export is what you expect.

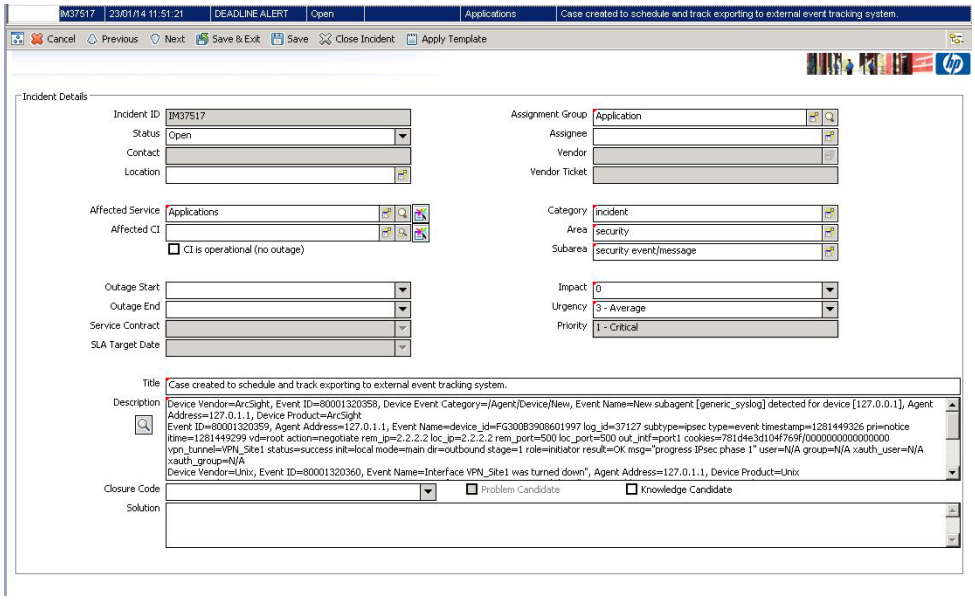
Also, you can monitor the connector output log a command window to check the success of various connector operations. This is an example of a portion of an output log:

```
Output in console:
[Tue Jan 28 11:16:03 PST 2014] [INFO ] .... waking up ....
[Tue Jan 28 11:16:03 PST 2014] [INFO ] Checking for updates from ESM...
[GC 104942K->12766K(245760K), 0.0182364 secs]
[Tue Jan 28 11:16:05 PST 2014] [INFO ] Now Parsing [ExternalEventTrackingData_9-20-10_12-49-56.795.xml]
[Tue Jan 28 11:16:05 PST 2014] [INFO ]    Event ID [80001320358] mapped
[Tue Jan 28 11:16:05 PST 2014] [INFO ]    Event ID [80001320359] mapped
[Tue Jan 28 11:16:05 PST 2014] [INFO ]    Event ID [80001320360] mapped
[Tue Jan 28 11:16:05 PST 2014] [INFO ]    Event ID [80001320361] mapped
[Tue Jan 28 11:16:05 PST 2014] [INFO ]    Event ID [80001320362] mapped
[Tue Jan 28 11:16:05 PST 2014] [INFO ]    Event ID [80001320363] mapped
[Tue Jan 28 11:16:05 PST 2014] [INFO ]    Event ID [80001320594] mapped
[Tue Jan 28 11:16:06 PST 2014] [INFO ] Message from web service: [US/Pacific 28/01/14 11:10:35:  Incident IM375
[Tue Jan 28 11:16:06 PST 2014] [INFO ] Enterprise System Connector exported 1 file(s) from ArcSight ESM.
[Tue Jan 28 11:16:06 PST 2014] [INFO ] Checking for updates from external system...
[Tue Jan 28 11:16:06 PST 2014] [INFO ]    incident ID [IM37518] Status => case stage is now [Open]
[Tue Jan 28 11:16:06 PST 2014] [INFO ] Found 1 record(s) updated since [Thu Jan 23 11:51:21 PST 2014].
[Tue Jan 28 11:16:06 PST 2014] [INFO ] Imported the updated content of 1 case(s) to ESM!
[Tue Jan 28 11:16:06 PST 2014] [INFO ] .... going to sleep ....
[Tue Jan 28 11:16:53 PST 2014] [INFO ] Shutting Down Agent Framework Version [6.0.8.23521.0]
```

Working with the HP Service Manager New Incident Tab

HP Service Manager displays ArcSight security event data within a defined schema, that displays in the New Incident tab as Incident Details and attachments. Fields that are displayed in the default version of the Incident Management Web Services are the only fields for which connector mappings can be provided. Do not modify these Web Services fields.

This is an example of the New Incident tab showing an imported incident using default mappings:



HP Service Manager provides a default version of the New Incident tab.The fields available on this tab depend on what was set up in HP Service Manager. The `servicemanager.properties` file must map these fields to fields in the ESM schema. Mandatory fields (and the defined values for the fields that require them, such as drop-down lists) are specified in HP Service Manager.

ESM DTDs Location and Example

The DTDs used to define the events and cases used by the Enterprise System Connector for HP Service Manager REST is located in the ESM environment in `<MANAGER_HOME>\schema\xml\archive\`. These DTDs are:

- arcsight-case.dtd
- arcsight-event.dtd
- arcsight-event-common.dtd

This is an example of a portion of a DTD used to define cases:

```
<!ELEMENT Case ANY>
<!ATTLIST Case
id CDATA #IMPLIED
externalID CDATA #IMPLIED
name CDATA #REQUIRED
alias CDATA #IMPLIED
versionID CDATA #IMPLIED
deprecated (true | false) "false"
action (insert | update | remove) "insert"
>
<!ELEMENT displayId (#PCDATA)>
<!ELEMENT caseId (#PCDATA)>
<!ELEMENT attackMechanism (#PCDATA)>
<!ELEMENT attackAgent (#PCDATA)>
```

```
<!ELEMENT createTime (#PCDATA)>
<!ELEMENT ticketType (#PCDATA)>
<!ELEMENT caseEvents (list)>
```