

ArcSightTM HP OM and HP OMi SNMP Interceptor Policy Readme

November 15, 2011

These release notes contain information about uploading the SNMP Interceptor policies for HP OM and HP OMi. This information applies to these products:

- ArcSight Forwarding Connector for ESM
- ArcSight Logger Forwarding Connector for HP Operations Manager
- ArcSight Logger Forwarding Connector for HP Operations Manager i

For details on the forwarding connectors see the *SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector*, the *SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HP Operations Manager* or the *SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HP Operations Manager i*.

Uploading Policy Files for HP OM and HP OMi

The following sections contain details on uploading policy files for HP OM and HP OMi.

Uploading Policy Files for HP OM

The following sections contain details on uploading policy files for HP OM.

Using Operations Manager for Windows

Policy files are available at the same download site from which you obtained the connector. After obtaining the policy files from ArcSight, use the following command to upload the policy:

```
ovpmutil cfg pol upl <dir>\142714A5-55F4-4722-A393-6D1860D001F8_header.xml
```

The directory where you will place the uploaded policy will depend on your environment. An example of <dir> is:

```
"C:\temp\hpompolicy"
```



Be sure to upload both the header and data file.

You should receive the following message:

```
Policies upload completed successfully.
```

For descriptions of specific HP OM commands, refer to the HP Operations Manager online help and documentation.

Using Operations Manager for UNIX or Linux for HP OM

Policy files are available at the same download site from which you obtained the connector. After obtaining the policy files from ArcSight, use the following command to upload the policy:

```
/opt/OV/bin/OpC/Utils/opcpolicy -upload file=<dir>/142714A5-55F4-4722-A393-6D1860D001F8_header.xml
```

The directory where you will place the uploaded policy will depend on your environment. An example of <dir> is:

```
"/temp/hpompolicy"
```

You should receive the following message:

```
Operation successfully completed.
```

For descriptions of specific HP OM commands, refer to the HP Operations Manager online help and documentation.

Using the HP BSM Adapter to Import and Activate Policy Files for HP OMi

Policy files are available at the same download site from which you obtained the connector. In the BSM Integration Adapter, you must import and activate the policy files. To do so:

- 1 Click the **Import** icon in the BSM Integration Adapter UI.
- 2 Browse to find the policy files.
- 3 Select header and data files and click **Open** to import the files. The files will resolve into a policy listed in the BSM Integration Adapter UI. You must import both files for the policy to function correctly.
- 4 Select the policy and click the **Activate** icon.
- 5 Configure the HP Operations Agent to receive SNMPv2 traps by setting the SNMP_SESSION_MODE variable. Refer to the *Using HP BSM Integration Adapter Guide* for details on the HP BSM Adapter.

Policy Mappings

Event severity and "Security" ETI hint are based on content of `event.agentSeverity`:

- "Very-High" results in "Major" event severity and "Security:Major" for the security ETI hint
- "High" results in "Minor" event severity and "Security:Minor" for the security ETI hint
- "Medium" results in "Warning" event severity and "Security:Warning" for the security ETI hint
- "Low" results in "Normal" event severity and "Security:Normal" for the security ETI hint

Further mappings are provided in the following table. <\$#> indicates the index of the variable binding in the SNMP trap.

Name	Value
NODE IP 0.0.0.0	<\$6>
APPLICATION	ArcSight ESM/Logger

Name	Value
MSGKEY	<\$1>
event.eventId	<\$1>
event.name	<\$2>
event.message	<\$3>
event.deviceEventCategory	<\$4>
event.deviceEventClassId	<\$5>
event.targetHostName	<\$6>
event.targetAddress	<\$7>
event.originalAgentHostName	<\$8>
event.deviceSeverity	<\$9>
event.agentSeverity	<\$10>
event.severity	<\$11>
event.priority	<\$12>
event.type	<\$13>
event.externalId	<\$14>
event.deviceReceiptTime	<\$15>
event.startTime	<\$16>
event.endTime	<\$17>
event.transportProtocol	<\$18>
event.applicationProtocol	<\$19>
event.targetZoneURI	<\$20>
event.targetPort	<\$21>
event.targetUserName	<\$22>
event.targetProcessName	<\$23>
event.targetServiceName	<\$24>
event.attackerHostName	<\$25>
event.attackerAddress	<\$26>
event.attackerPort	<\$27>
event.attackerUserName	<\$28>
event.attackerProcessName	<\$29>
event.attackerServiceName	<\$30>
event.agentHostName	<\$31>

Name	Value
event.agentType	<\$32>
event.deviceAddress	<\$33>
event.deviceAction	<\$34>
event.deviceVendor	<\$35>
event.deviceProduct	<\$36>
event.deviceVersion	<\$37>
event.deviceExternalId	<\$38>
event.deviceCustomString1	<\$39>
event.deviceCustomString2	<\$40>
event.deviceCustomString3	<\$41>
event.deviceCustomString4	<\$42>
event.deviceCustomString5	<\$43>
event.deviceCustomString6	<\$44>
event.categoryBehavior	<\$45>
event.categoryDeviceGroup	<\$46>
event.categoryObject	<\$47>
event.categoryOutcome	<\$48>
event.categorySignificance	<\$49>
event.categoryTechnique	<\$50>
Description	<\$3>
SubCategory	<\$4>
EtiHintSecurity	<event severity dependent>
NodeHint	<\$7>
RelatedCiHint	<\$7>:<\$6>
SourceCiHint	<\$8>
TEXT or Title	<\$2>

For further assistance, contact ArcSight Customer Support at <https://support.arcsight.com>.

© Copyright 2011 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP 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.

The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.arcsight.com/copyrightnotice>

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

This document is confidential.

