SmartConnector™ Configuration Guide for

ArcSight™ Logger Forwarding Connector for HP Operations Manager

June, 2011

ArcSight™
An HP Company

SmartConnector™ Guide for ArcSight™ Logger Forwarding Connector for HP Operations Manager

Revision History

Date	Description
06/2011	Second release of Logger Forwarding Connector for HP OM documentation.
05/2011	First release of Logger Forwarding Connector for HP OM documentation.

Release Notes template version: 2.1.0

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	http://www.arcsight.com/supportportal
Customer Forum	https://forum.arcsight.com

Contents

Configuration Guide for Logger Forwarding Connector for HP OM

This guide provides information on installing and configuring the Logger Forwarding Connector for HP OM. This software supports Logger versions **5.0** and **5.1**.

ArcSight Logger is a log management solution that is optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis. Logger receives and stores events; supports search, retrieval, and reporting; and can forward selected events.The ArcSight Logger Forwarding Connector allows you to send these event logs from Logger to the HP Operations Manager (HP OM).

HP Operations Manager (HP OM) provides comprehensive event management, proactive performance monitoring, and automated alerting, reporting, and graphing for operating systems, middleware, and applications. It is designed to provide service-driven event and performance management of business-critical enterprise systems, applications, and services.

Supported Versions of HP OM

The supported versions of HP OM include

- HP OM for Windows v9.0 and 8.16 (patch level 90)
- HP OM for UNIX v9.10
- HP OM for Linux v9.10

Sending Events From Logger to HP OM

ArcSight Logger sends events to the Logger Forwarding Connector using CEF Syslog, then forwards the events to HP OM via SNMP. A Logger forwarder must be created to send these events. For instructions on how to create a forwarder to send the events, see "Creating a Forwarder to Forward Events" on page 10.

HP OM uses an SNMP interceptor policy to allow ArcSight events to be accepted within the HP OM environment. For instructions on how to create an SNMP interceptor policy, see "Creating an SNMP Interceptor Policy" on page 11.

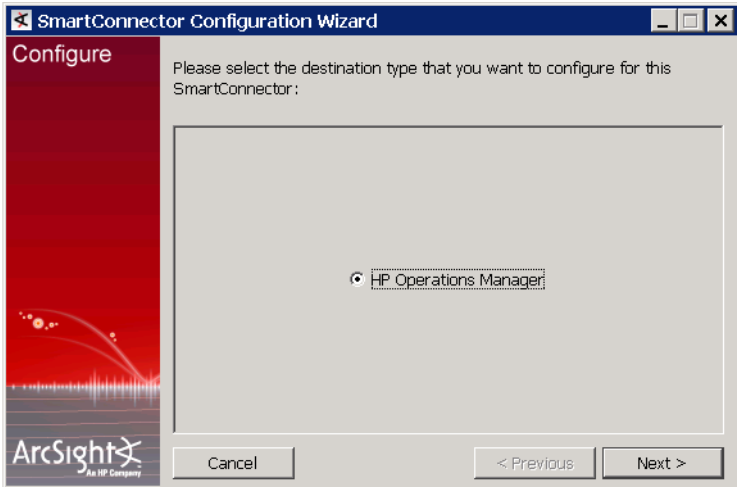
Installing the Connector

Before you install the connector, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (the ArcSight Logger, for example) and you have assigned appropriate privileges. For data security, ArcSight recommends that you install the connector and the HP Operations Agent on the same system.

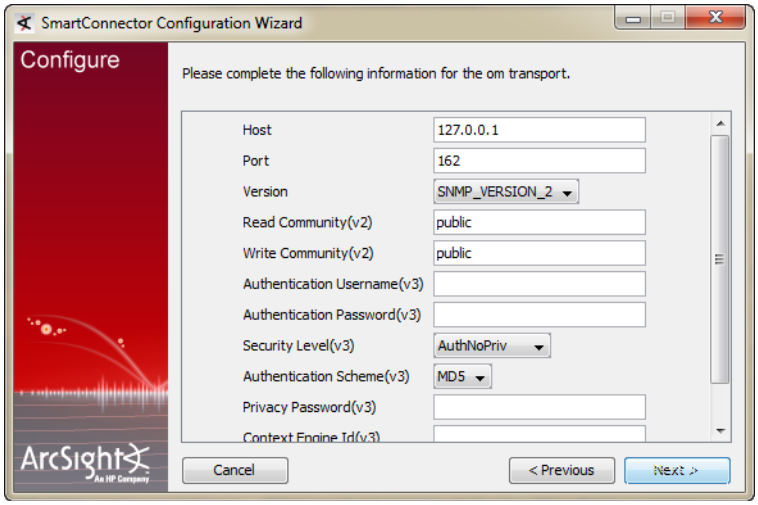
1. Download the ArcSight executable for your operating system from the ArcSight Customer Support Site.
2. Start the ArcSight Installer by running the executable.

   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. The following destination window is displayed; click **Next** to continue.

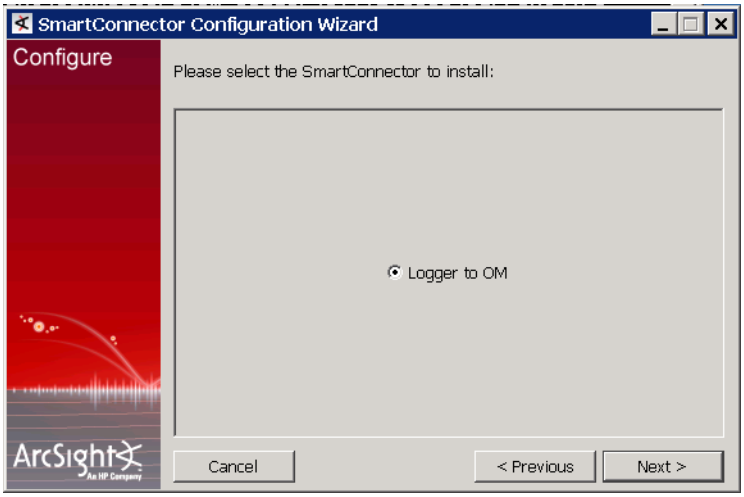


4 Fill in the parameter information required for connector configuration, then click **Next**.

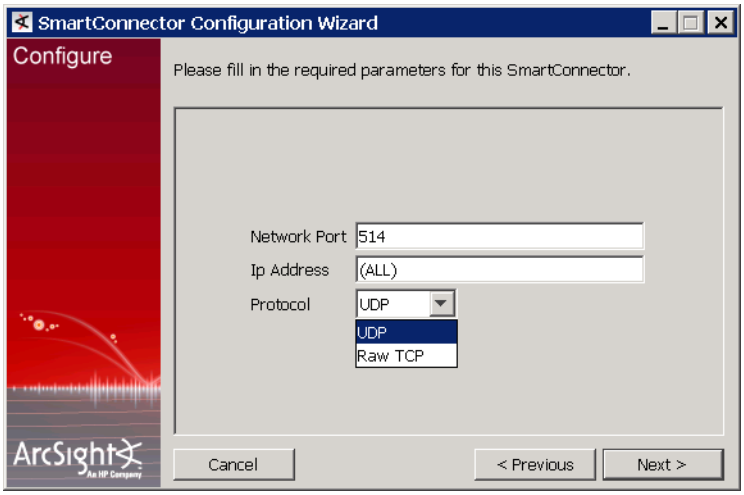


Parameter	Description
Host	Enter the Host name or IP address of the HP OM device. This is the HP OM managed node (the system where the HP Operations Agent is installed, and to which the SNMP interceptor policy is deployed).
Port	Enter the port to be monitored for events by the HP Operations Agent.
Version	Accept the default value of **SNMP_VERSION_2**. **SNMP_VERSION_3** is not available at this time.
Read Community(v2)	Enter the SNMP Read Community name.
Write Community(v2	Enter the SNMP Write Community name.
Authentication Username(v3)	For use with SNMP v3; not available at this time.
	Authentication Password(v3)
	Security Level(v3)
	Authentication Scheme(v3)
	Privacy Password(v3)
	Context Engine Id(v3)
	Context name(v3)

5 Click **Logger to OM**, then click **Next**.

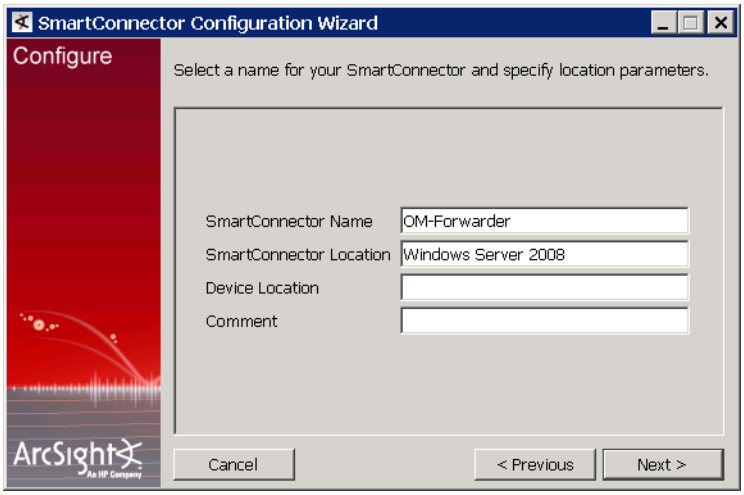


6 Enter the Logger information, then click **Next**.



Parameter	Description
Network Port	514 or another port that matches the Receiver
IP Address	IP or host name of the Logger
Protocol	UDP or Raw TCP **Note**: Whichever protocol you choose, it must match that of the forwarder type chosen during Logger Forwarder configuration.

7 Enter a name for the connector and provide other information identifying the connector's use in your environment. Click **Next**.



8 Read the installation summary and click **Next**. If the summary is incorrect, click **Previous** to make changes.

9 When the connector completes its configuration, click **Next**. The Wizard now prompts you to choose whether you want to run the connector as a process or as a service.

If you choose to run the connector as a service, the Wizard prompts you to define service parameters for the connector.

10 After making your selections, click **Next**. The Wizard displays a dialog confirming the connector's setup and service configuration.

11 Click **Finish**.

12 Click **Done**.

Logger Forwarders

Logger **forwarders** allow you to send all events, or events which match a particular filter, to another destination, in this instance, to HP OM. However, the ability to define a different filter for each forwarder allows Logger to divide traffic among several destinations or limit the events sent to a single destination. For example, because Logger can handle higher event rates, it might be used to forward events to another HP OM management server and/or an ArcSight ESM Manager. Forwarder query filters make it possible to split the flow between the different devices, using one forwarder for each.

Logger forwarding uses several forwarder types, but the Logger Forwarding Connector operates with UDP and TCP forwarder types only.

- **UDP Forwarders** forward events as User Datagram Protocol messages, such as Syslog format datagrams.
- **TCP Forwarders** forward events as Transmission Control Protocol messages.

Creating a Forwarder to Forward Events

In order to successfully forward events from Logger to HP OM, a forwarder must be created. To do so, complete the following steps within the ArcSight Logger web application.

1 Click **Configuration** from the top-level menu bar.

2 Click **Event Input/Output** in the left panel.

3 Click the **Forwarder** tab, then click **Add**. The **Add Forwarder** page appears.

4 Enter a name for the new forwarder and choose either “UDP Forwarder” or “TCP Forwarder”.

> **Caution** Whichever forwarder type you choose, it must match that of the SmartConnector protocol chosen during installation.

5 Click **Next**.

6 The **Edit Forwarder** page appears.

7 Within the **Query** field, create a query to filter the events sent to HP OM, or leave the default, **NONE**, to send all events.

8 Continue to fill in the remaining parameters, ensuring that the **Ip/Host** field contains the correct Logger Forwarding Connector IP address and that the **Port** number matches that of the connector.

9 Click **Save**. The following page appears.

10 New forwarders are initially disabled, so click the disabled icon ( ) to enable the new forwarder.

The forwarder is now enabled.

11 Start the Logger Forwarding Connector.

For more detailed information on Logger forwarders, see the *ArcSight Logger Administrator’s Guide.*

> **Tip** Wait a few minutes after enabling a forwarder before disabling it. Likewise, wait before enabling a forwarder that has just been disabled. Background tasks initiated by enabling or disabling a forwarder can produce unexpected results if they are interrupted.

Creating an SNMP Interceptor Policy

An SNMP interceptor policy is a type of HP OM policy, with rules, conditions, and actions. Rules define what a policy should do in response to a specific type of event. Each rule consists of a condition and an action. SNMP interceptor policies monitor SNMP events, and can start actions when an SNMP event contains a specified character pattern. The Logger Forwarding Connector sends security events as SNMP traps to an HP OM SNMP interceptor policy that you will create.

SNMP interceptor policies can be configured on either HP OM UI, HP OM for Windows, or HP OM for UNIX or Linux. ArcSight provides a template interceptor policy for use in creating your own customized SNMP interceptor policy. This template policy should be customized and enhanced to satisfy different needs and requirements with HP OM's powerful policy edit features. You can upload the ArcSight SNMP interceptor policy template to HP OM for Windows (using the **ovpmutil** command line tool) and to HP OM for UNIX or Linux (using the **opcpolicy** command line tool).

Uploading Interceptor Template

After you have completed the connector installation, navigate to **$ARCSIGHT_HOME\current\user\agent\hpompolicy**. This folder provides policy files as a basic SNMP interceptor template.

Using Operations Manager for Windows

Copy the **hpompolicy** folder from **$ARCSIGHT_HOME\current\user\agent\hpompolicy** to the destination HP OM for Windows machine's `C:\temp` directory. Then use the following command to upload the policy:

```
"%OvBinDir%\ovpmutil" CFG POL UPL "C:\temp\hpompolicy"
```

You should receive the following messages:

```
Root policy group "for ArcSight Integration" uploading:
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

Copy the **hpompolicy** folder from **$ARCSIGHT_HOME\current\user\agent\hpompolicy** to the destination HP OM machine's `/tmp` directory. Then use the following command to upload the policy:

```
/opt/OV/bin/OpC/utils/opcpolicy -upload
dir=/tmp/hpompolicy/"ArcSight Events"
```

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.

Deploying the Policy

Once you have created your customized SNMP interceptor policy, deploy or assign the policy through the HP OM for Windows or HP OM for UNIX or Linux Administration UI. For details, refer to the HP Operations Manager online help and documentation.

The systems that send the SNMP traps to the logger must also be set up as nodes in HP OM, because HP OM discards messages from unknown systems. Set up an external node or an SNMP node. For details, refer to the HP Operations Manager online help and documentation.

Also, configure the HP Operations Agent for SNMPv2 by setting the **SNMP_SESSION_MODE** variable using the **ovconfchg** command line tool. Refer to the HP Operations Manager or HP Operations Agent online help and documentation for more information.

Troubleshooting Tips

Duplicate Events

If there appear to be duplicate events forwarded to the HP OM console:

1. Check and modify suppression options as needed.
2. If, after modifying suppression options, there still appear to be duplicate events, check the Custom Message Attributes (event details and data), and apply rules to differentiate the events.

   Refer to the HP Operations Manager online help for details.

Dropped Events

If you notice that some events forwarded from ArcSight ESM/Logger are dropped, verify whether the Agent Severity is set correctly in those events. The default SNMP interceptor policy provided by ArcSight in the connector distribution has rules to pick up and forward SNMP Traps from ArcSight ESM/Logger based on the Agent Severity. Events that do not have Agent Severity set are dropped and not forwarded by the SNMP interceptor policy. If the dropped events are correlated events from ESM, make sure that the rules on ESM are set for the correct Agent Severity in the correlated events they generate. If the dropped events are normalized events from devices, then verify that the originating connector that

has normalized the event has mapped the Agent Severity correctly from the Device Severity. If the originating connector (that is not setting the Agent Severity) is a FlexConnector, review the mappings and map all of the device severities to one of these Agent Severity values: Low, Medium, High, or Very-High. If the connector is a supported connector, contact customer support.

Adjusting the Event Processing Rate

The default event processing rate for forwarding events from Logger to HP OM is **50 eps**. If this rate proves excessive for your system, HP OM may queue some incoming events and affect the rate at which these events are processed.

If this occurs, you can adjust the rate at which events are forwarded to HP OM. To do so, you will need to change the event processing rate within your XML properties file.

To adjust the event processing rate,

1. Stop the currently running SmartConnector from operating.
2. From a Windows command line, access your XML properties file using the command

   ```
   cd %ARCSIGHT_HOME%/current/user/agent
   ```

3. Use WordPad or any XML Editor to open the .xml file for your HP OM destination, similar to the example below:

   ```
   0Ajv5S8BABCAAeabNXP5Rw==.xml
   ```

4. From within the .xml file, search for the following:

   ```
   ProcessingSettings.ThrottleRate="50"
   ```

   This value controls the current processing event rate, and has a default value of 50 eps.

5. Change this value to the desired rate of events per second. For example, to lower the rate of events to 10 eps, change the value after the string to 10:

   ```
   ProcessingSettings.ThrottleRate="10"
   ```

   If there are multiple destinations, repeat the steps above to change the rate for each destination, as required.

6. Save the .xml file and exit the XML editor.
7. Restart the SmartConnector.