Configuration Guide

ArcSight™ Logger Forwarding Connector for HP Network Node Manager i

September, 2012

ArcSight™
An HP Company

SmartConnector™ Guide for ArcSight™ Logger Forwarding Connector for HP Network Node Manager i

Revision History

Date	Product Version	Description
09/28/2012	5.2.3.6287.0	Added support for selected HP H3C and HP ProCurve sub-messages. Added support for HP NNMi 9.20, patch 1 and a new connector installation wizard. Event data is forwarded as CEF Syslog from Logger to the Logger Forwarding Connector for HP NNMi. The parsing is now enabled only in the corresponding release of the SmartConnectors. Forwarding events from supported devices such as Cisco Router, HP H3C, and HP ProCurve directly to the Logger Forwarding Connector without SmartConnectors or Logger is not a supported configuration.
05/15/2012	5.2.1.6206.0	Added support for selected Cisco Router sub-messages.
11/15/2011	5.1.7.6081.0	Added support for JRE 1.6.0_26.
06/15/2011		First release of Logger Forwarding Connector for HP NNMi documentation.

Release Notes template version: 2.1.0

Contact Information

Phone	1-866-535-3285 (North America) +44 203-564-1189 (EMEA) +49 69380789455 (Germany)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

Configuration Guide for HP ArcSight Logger Forwarding Connector for NNMi

This guide provides information on installing and configuring the HP ArcSight Logger Forwarding Connector for NNMi. This Logger Forwarding Connector software supports **Logger 5.1** and **5.2** and **NNMi 9.20, patch 1**.

See Appendix A, Supported Cisco Router, HP H3C, and HP ProCurve Sub-Messages, on page 13 for details on supported Cisco Router sub-messages.

Note the following:

- You must upgrade to HP NNMi 9.20, patch 1 to be able to use the current Logger Forwarding Connector for HP NNMi. If you have a previous version of HP NNMi installed, the current Logger Forwarding Connector for HP NNMi will not function.
- SmartConnector 5.2.3.6281 should always be used with the current Logger Forwarding Connector for NNMi. If you plan to process events from HP ProCurve devices, you must also install the SmartConnector build 5.2.3.6281.0 or a later build.
- SmartConnector 5.2.3.6281 support for syslog events from HP ProCurve devices are limited to the Logger to NNMi integration.

About HP ArcSight Logger and HP NNMi

HP 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 HP ArcSight Logger Forwarding Connector allows you to send these event logs from Logger to the HP Network Node Manager (HP NNMi).

HP Network Node Manager (NNMi) provides continual network discovery using unified fault, availability, and performance monitoring. HP NNMi enables network management teams to detect, locate, and diagnose faults and performance degradations of the network quickly, analyze the business and service impact of outages, and increase network staff efficiency and productivity.

Using the HP ArcSight Logger Forwarding Connector and the HP/ARC NNMi integration install, network staff can view syslog messages from Logger in the NNMi console.

Sending Events From Logger to NNMi

Logger sends events to the Logger Forwarding Connector using CEF Syslog, which then forwards the events to NNMi via SNMP. For Logger to send events to the Logger Forwarding Connector, 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.

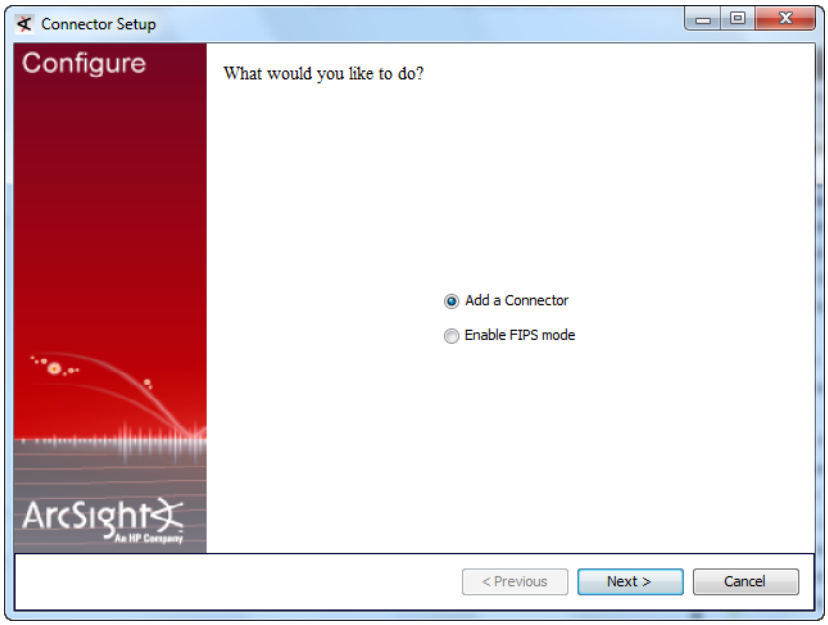
Installing the Connector

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.

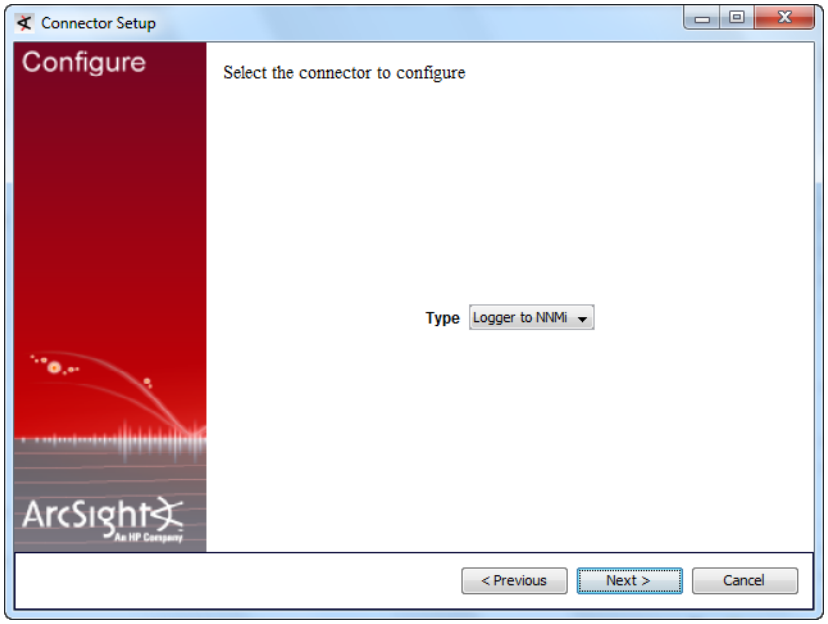
1. Download the HP ArcSight executable for your operating system from **My Updates** on the HP SSO site.
2. Start the HP ArcSight Installer by running the executable.

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

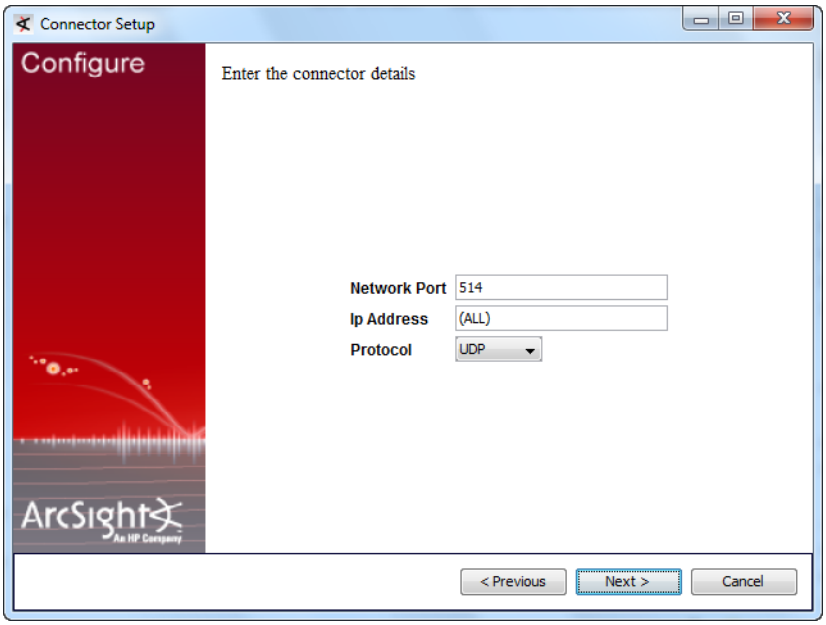
   Introduction
   Choose Install Folder
   Choose Install Set
   Choose Shortcut Folder
   Pre-Installation Summary
   Installing...
3. Select **Add a Connector**.



4 Click **Next**. **Logger to NNMi** is selected by default.

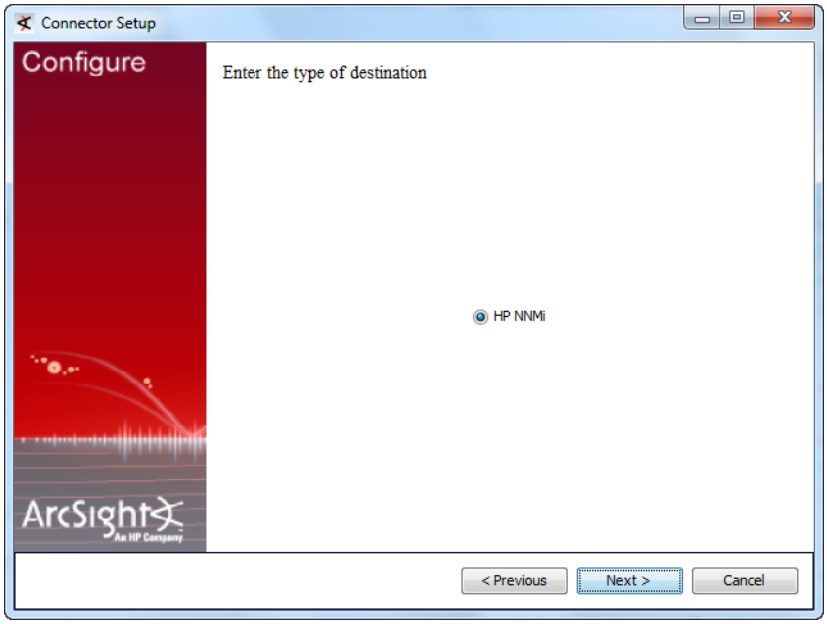


5 Click **Next**. Enter the Logger information.

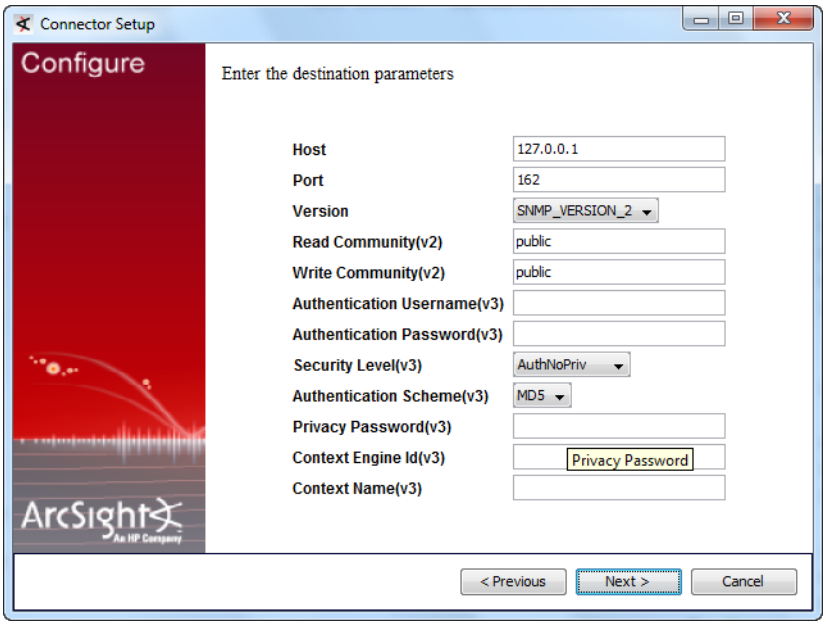


Parameter	Description
Network Port	514 or another port that matches the Receiver (the port to which the forwarding connector sends events)
IP Address	IP or host name of the Logger
Protocol	UDP or Raw TCP **Note**: Whichever protocol you choose, it must match that of the forwarder type chosen during Logger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

6 Click **Next**. **HP NNMi** is selected by default.

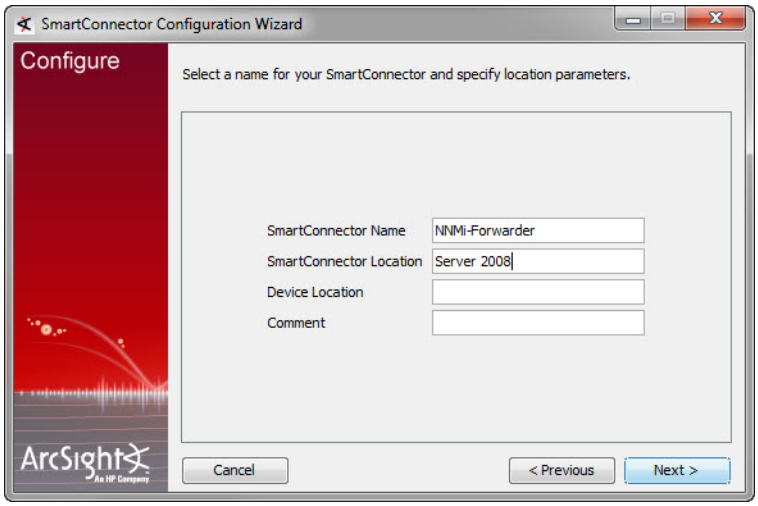


7 Click **Next**. Fill in the parameter information required for connector configuration.



Parameter	Description
Host	Enter the Host name or IP address of the NNMi device.
Port	Enter the port to be used by the adaptor to forward events. The default port is 162. To determine if the trap port monitored by NNMi is other than the default, use the NNMi command: **$NnmInstallDir/bin/nnmtrapconfig.ovpl -showProp** See the *NNMI ArcSight Logger Integration Guide*, HP ArcSight Logger chapter for details on HP NNMI and Logger integration.
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)

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



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

10 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.

11 Click **Next**. Choose **Exit**, to complete the connector installation, or choose **Continue**, to continue to make connector modifications. Click **Next** to exit or continue.

Logger Forwarders

Logger Forwarders allow you to send all events, or events which match a particular filter, to another destination, in this instance to the HP NNMi Logger Forwarding Connector. For more detailed information on Logger Forwarders, see the *HP ArcSight Logger Administrator's Guide*.

You cannot configure a Logger Forwarder to send data to a destination on the same system.

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 NNMi, a Logger Forwarder must be created. To do so, complete the following steps in the 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”.

Whichever forwarder type you choose, it must match that of the SmartConnector protocol and port 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 NNMi, 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.

To create a specific filter for **NNMi**, refer to the HP NNMi documentation.

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.

Appendix A

Supported Cisco Router, HP H3C, and HP ProCurve Sub-Messages

This appendix lists Cisco Router, HP H3C, and HP ProCurve sub-messages for which additional mappings were provided in this release.

Cisco Router Sub-messages

These are the Cisco Router sub-messages for which the mappings are provided:

- BGP-5-ADJCHANGE
- CDP-4-DUPLEX_MISMATCH
- DTP-3-NONTRUNKPORTFAIL
- DTP-3-TRUNKPORTFAIL
- DTP-5-NONTRUNKPORTON
- DTP-5-TRUNKPORTCHG
- DTP-5-TRUNKPORTON
- FR-5-DLCICHANGE
- LINEPROTO-5-UPDOWN
- LINK-3-UPDOWN
- STANDBY-3-DUPADDR
- LINK-4-ERROR
- PAGP-5-PORTFROMSTP
- PAGP-5-PORTTOSTP
- PORT_SECURITY-2-PSECURE_VIOLATION_VLAN
- SNMP-5-MODULETRAP
- SPANTREE-5-PORTLISTEN
- SPANTREE-5-ROOTCHANGE
- SPANTREE-6-PORTFWD
- SPANTREE-6-PORTLISTEN

- STACKMGR-6-MASTER_ELECTED
- STACKMGR-6-MASTER_READY
- STACKMGR-6-STACK_LINK_CHANGE
- STANDBY-6-STATECHANGE
- SYS-3-MOD_CFGMISMATCH1
- SYS-3-MOD_CFGMISMATCH2
- SYS-3-MOD_CFGMISMATCH3
- SYS-3-MOD_CFGMISMATCH4
- SYS-3-PKTBUFBAD
- SYS-3-PORT_COLL
- SYS-3-PORT_COLLDIS
- SYS-3-PORT_IN_ERRORS
- SYS-3-PORT_RUNTS
- SYS-4-SYS_LCPERR4
- SYS-5-MOD_INSERT
- SYS-5-MOD_OK
- SYS-5-MOD_REMOVE
- SYS-5-MOD_RESET
- SYS-5-RELOAD
- SYS-5-RESTART
- SYS-5-SYS_LCPERR5

HP H3C Sub-messages

These are the HP H3C sub-messages for which the mappings are provided:

- CFM/5/CFM_SAVECONFIG_SUCCESSFULLY
- NTP/5/NTP_SOURCE_LOST
- DEV/4/FAN_FAILED
- OSPF/5/OSPF_NBR_CHG
- DEVM/3/BOARD_REMOVED
- DEV/4/FAN_RECOVERED
- DEVM/2/BOARD_STATE_FAULT
- VRRP/6/VRRP_STATUS_CHANGE
- DEV/4/POWER_FAILED
- DEV/4/POWER_RECOVERED
- MSTP/5/MSTP_BPDU_RECEIVE_EXPIRY
- OPTMOD/4/MODULE_IN
- OSPF/6/OSPF_LAST_NBR_DOWN
- ARP/5/ARP_DUPVRRPIP
- ARP/3/ROUTECONFLICT
- BFD/5/BFD_CHANGE_FSM

- BGP/5/BGP_RECHED_THRESHOLD
- DEV/4/BOARD_LOADING
- DEV/4/LOAD_FINISHED
- DEVM/2/POWER_FAILED
- DEVM/5/POWER_RECOVERED
- DEVM/3/RPS_ABSENT
- DEVM/5/RPS_NORMAL
- DEVM/5/SYSTEM_REBOOT
- DEV/4/POWER_ABSENT
- DEV/4/SYSTEM_REBOOT
- LDP/5/LDP_SESSION_DOWN
- OPTMOD/5/CHKSUM_ERR
- OPTMOD/5/IO_ERR
- OPTMOD/5/MOD_ALM_OFF
- OPTMOD/5/MOD_ALM_ON
- OPTMOD/4/MODULE_OUT
- OPTMOD/3/TYPE_ERR
- PIM/5/PIM_NBR_DOWN
- STM/4/LINK_STATUS_CHANGE
- STM/3/STM_LINK_STATUS_DOWN
- STM/6/STM_LINK_STATUS_UP

HP ProCurve Sub-messages

These are the HP ProCurve sub-messages for which the mappings are provided:

- RMON_PMGR_PORT_UP
- RMON_CHASSIS_FAN_STATUS
- RMON_STP_NEW_ROOT
- RMON_LACP_DYNAMIC_TRUNK_OFF_LINE
- RMON_LACP_DYNAMIC_TRUNK_ON_LINE
- RMON_LACP_ERROR_CONDITION_BLOCK
- RMON_POEMGR_PD_DENIED_POWER
- RMON_POEMGR_PD_OVERCURRENT
- RMON_POEMGR_INTERNAL_50V_FAULT
- RMON_BOOT_CRASH_RECORD0
- RMON_BOOT_CRASH_RECORD1
- RMON_BOOT_NO_CRASH_RECORD
- RMON_BOOT_SELFTEST_FAILURE
- RMON_SSH_DISABLED
- RMON_SSH_ENABLED
- RMON_CHASSIS_POWER_STATUS

- RMON_CHASSIS_HEARTBEAT_FAILURE