

Configuration Guide

ArcSight™ Logger Forwarding Connector for
HP Network Node Manager i

June, 2012



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

Copyright © 2012 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.

Revision History

Date	Product Version	Description
06/30/2012	5.2.1.6206.0	Added support for HP NNMi 9.20. 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 (0)870 141 7487 (EMEA)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

- Configuration Guide for Logger Forwarding Connector for HP NNMI 5**
 - About ArcSight Logger and HP NNMI 5
 - Sending Events From Logger to NNMI 6
 - Installing the Connector 6
 - Logger Forwarders 9
 - Creating a Forwarder to Forward Events 10
- Appendix A: Supported Cisco Router Sub-Messages 11**
 - Cisco Router Sub-messages 11

Configuration Guide for Logger Forwarding Connector for HP NNMi

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

[“About ArcSight Logger and HP NNMi” on page 5](#)

[“Sending Events From Logger to NNMi” on page 6](#)

[“Installing the Connector” on page 6](#)

[“Logger Forwarders” on page 9](#)



You must upgrade to HP NNMi 9.20 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.

See [Appendix A, Supported Cisco Router Sub-Messages, on page 11](#) for details on supported Cisco Router sub-messages.

About ArcSight Logger and HP NNMi

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

Sending Events From Logger to NNMi

ArcSight Logger sends events to the Logger Forwarding Connector using CEF Syslog, which then forwards the events to NNMi 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](#).

Installing the Connector

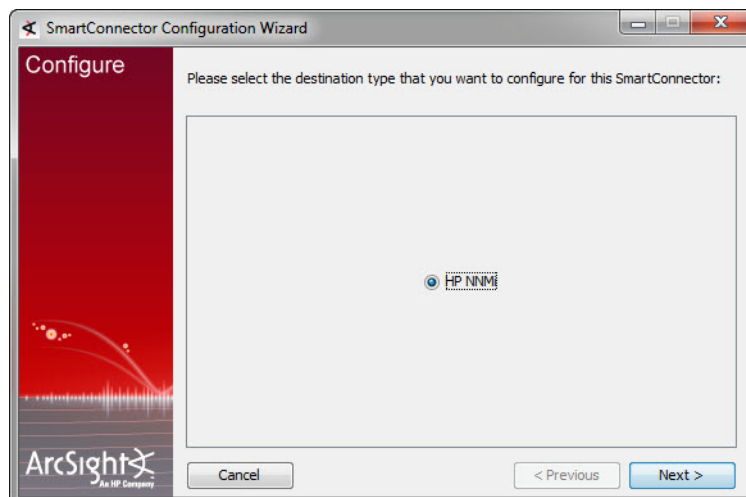
Before you install the connector, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (the ArcSight Logger, for example) and you have assigned appropriate privileges.

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

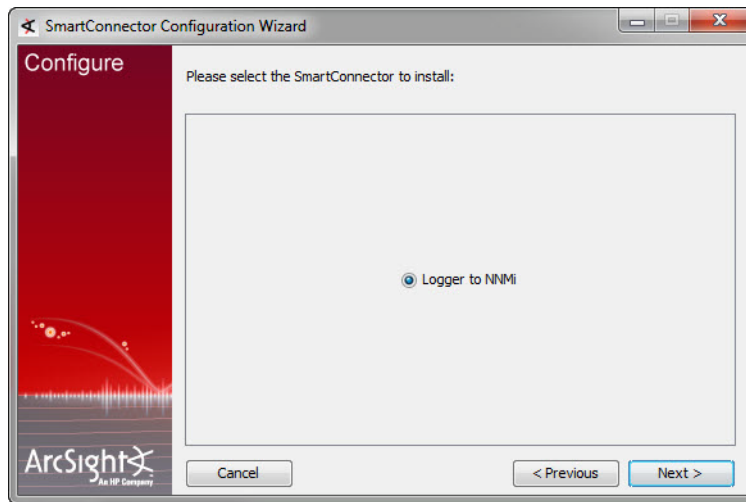
- 3 The following destination window is displayed; click **Next** to continue.



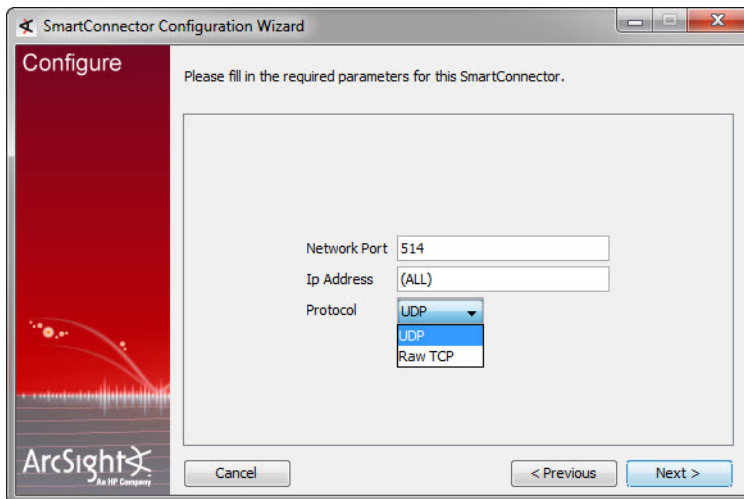
- 4 Fill in the parameter information required for connector configuration, then click **Next**.

Parameter	Description
Host	Enter the Host name or IP address of the 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: \$NnmiInstalldir/bin/nnmtrapconfig.ovpl -showProp See the <i>HP Network Node Manager I Software Deployment Reference Guide</i> , ArcSight Logger chapter for details on HP NNMI and ArcSight 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)

- 5 Click **Logger to NNMi**, then click **Next**.

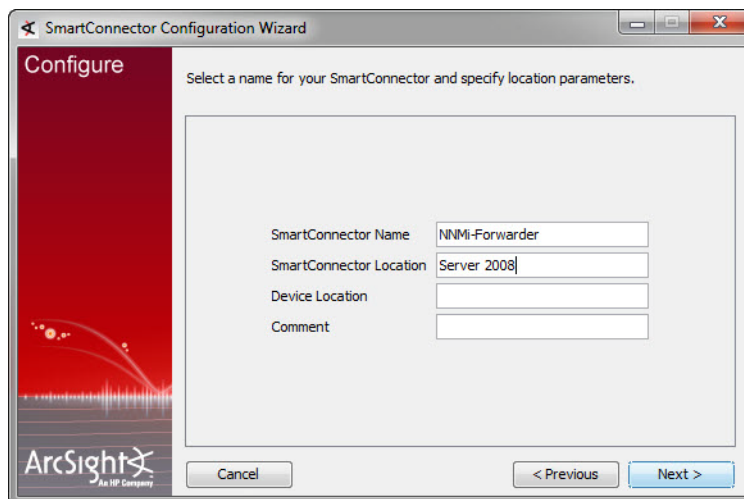


- 6 Enter the Logger information, then click **Next**.



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.

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



The image shows a screenshot of the 'SmartConnector Configuration Wizard' window. The title bar reads 'SmartConnector Configuration Wizard'. The main window has a red sidebar on the left with the 'Configure' tab selected and the 'ArcSight' logo at the bottom. The main content area has a light gray background with the instruction 'Select a name for your SmartConnector and specify location parameters.' Below this instruction are four text input fields: 'SmartConnector Name' (containing 'NNMi-Forwarder'), 'SmartConnector Location' (containing 'Server 2008'), 'Device Location' (empty), and 'Comment' (empty). At the bottom of the window are three buttons: 'Cancel', '< Previous', and '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 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 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”.



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.

Add						
Name	Type	IP/Host	Port	Query		
SMTP FWD	TCP Forwarder	10.0.202.116	515	NONE		

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



The forwarder is now enabled.

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



Note

To create a specific filter for **NNMi**, refer to the *NNMi Deployment Reference 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.

Supported Cisco Router Sub-Messages

This appendix lists Cisco Router sub-messages for which additional mappings are provided.

The Cisco Router Syslog SmartConnector parser supports mappings of [mnemonic](#), [networkTopologyType](#), [networkTopologyValue](#) for SNMP traps for NNMI for the Cisco Router and supports the subset of sub-messages listed in this appendix.

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