SmartConnector™ Configuration Guide for

ArcSight™ Logger Forwarding Connector for HP Network Node Manager i

June, 2011

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

Revision History

Date	Description
06/2011	First release of Logger Forwarding Connector for HP NNMi 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 NNMi

This guide provides information on installing and configuring the Logger Forwarding Connector for NNMi. This software supports **Logger v5.0** and **5.1,** and **NNMi v9.10, patch 1,** also known as **NNMi v9.11**.

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 integration patch, 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, 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 9.

NNMi requires a patch to allow ArcSight events to be accepted within the NNMi environment. For instructions on how to install this patch, see "Installing NNMi 9.10, Patch 1 (also known as NNMi 9.11)" on page 11.

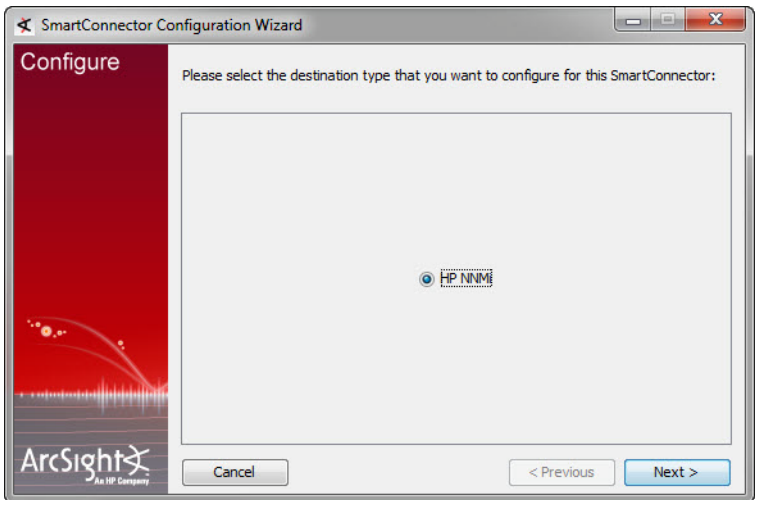
Installing the Connector

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.

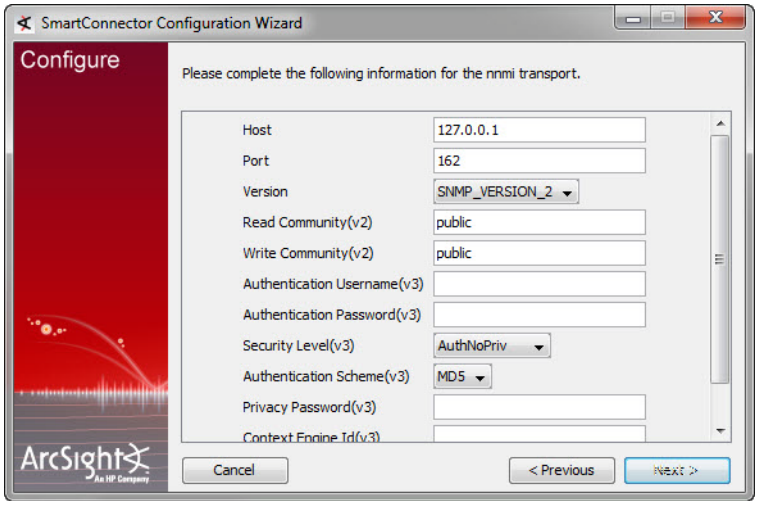
1. Download the ArcSight executable for your operating system from the ArcSight Customer Support Site.
2. Start the ArcSight Installer by running the executable.

   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.

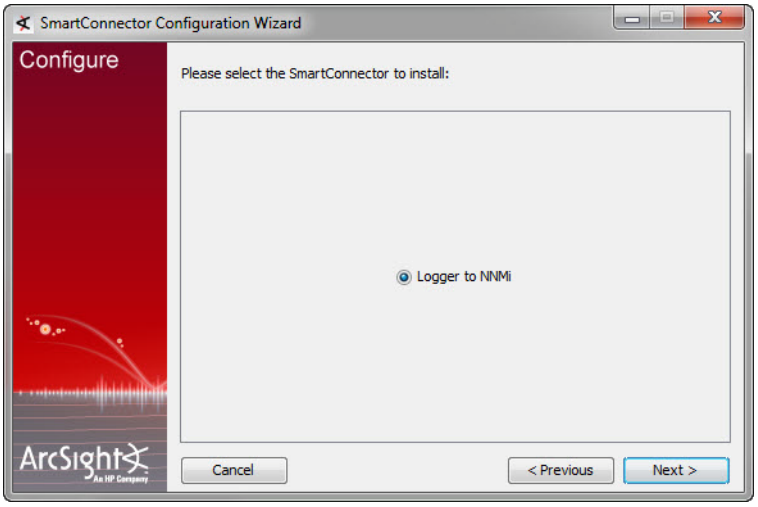


4 Fill in the parameter information required for connector configuration, then click **Next**.

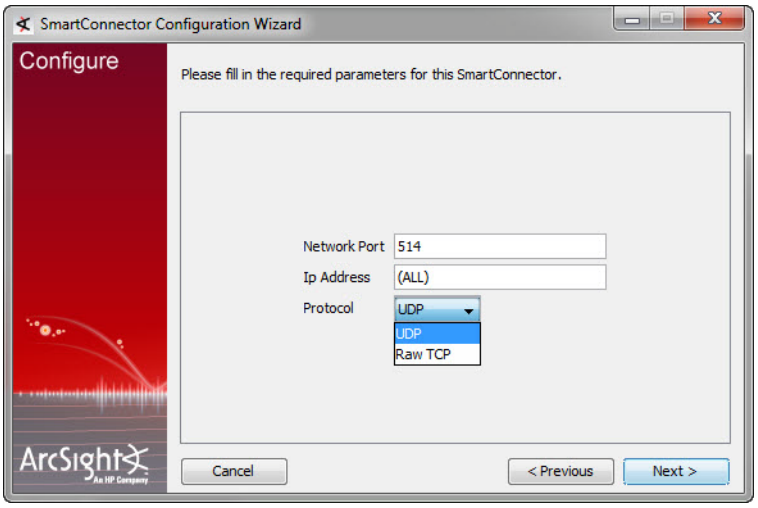


Parameter	Description
Host	Enter the Host name or IP address of the NNMi device.
Port	Enter the port to be used by the adaptor to forward events. The default port is 162. To determine if the trap port monitored by NNMi is other than the default, use the NNMi command: **$NnmInstallDir/bin/nnmtrapconfig.ovpl -showProp** See the *HP Network Node Manager i Software Deployment Reference Guide*, 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**.

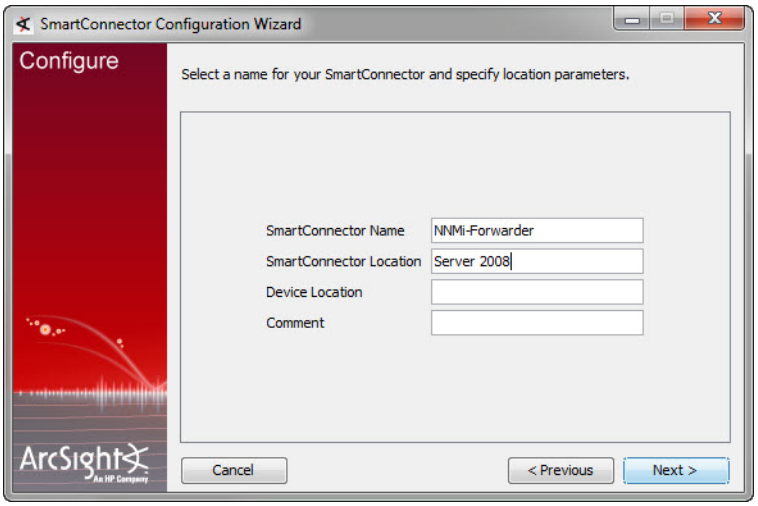


6 Enter the Logger information, then click **Next**.



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**.



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 NNMi. 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 NNMi 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 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 chosen during installation.

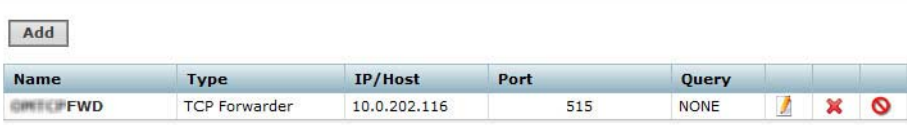
5 Click **Next**.

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.

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

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

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.

Installing NNMi 9.10, Patch 1 (also known as NNMi 9.11)

To obtain and install NNMi 9.10 patch 1, also known as NNMi 9.11, do the following:

1. Point your browser to http://support.openview.hp.com/selfsolve/patches.
2. Search for **“NNMI 9.10 patch 1”** or **“NNMI 9.11”** for your operating system, then download the patch.
3. Install the patch according to the NNMi 9.10 patch 1 (or NNMi 9.11) installation instructions.