Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for HPE Operations Manager i Web Services

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for HPE Operations Manager i Web Services

October 17, 2017

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP 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.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:
https://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228.

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
06/15/2017	Updated mappings.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
08/30/2016	HP has changed to HPE, including Device Vendor.
11/17/2015	Added support for OMi version 10.
05/15/2012	Added new installation procedure.
05/15/2011	First edition for this new SmartConnector.

Contents

SmartConnector for HPE Operations Manager i Web Services

This guide provides information for installing the SmartConnector for HPE Operations Manager i Web Services and configuring the device for event collection. This connector supports HPE Operations Manager *i* versions 9.01 and 10.

Product Overview

BSM Operations Management is the event management foundation for a complete BSM monitoring solution. As the operations bridge, it consolidates all IT infrastructure monitoring in a central event console, and relates the events to the IT services that depend on that infrastructure.

BSM Operations Management links infrastructure management with application and business service management. It combines events from HPE Business Service Management components, such as Business Process Monitor (BPM), Real User Monitor (RUM), and Service Level Management (SLM), with events from the operations management components of the BSM solution, such as HPE Operations Manager (HPEOM) and HPE Network Node Manager *i*i (NNMi), letting you keep track of all the events that occur in your monitored environment.

The messages generated by BSM OMi are retrieved through HPE's OMi Web Services and forwarded into the ArcSight System.

Configure BSM OMi for SmartConnector Event Collection

The SmartConnector can validate OMi's authentication certificate. To operate in this configuration, first get the certificate from Operations Manager i, then import it into the SmartConnector Java Runtime Environment (JRE) during the connector installation process, prior to running the SmartConnector.

The following steps presume you have configured Operations Manager i to let the SmartConnector communicate with it. If you have not done so, see your HPE documentation for information about the configuration of access lists or allowed hosts.

Obtain the Authentication Certificate

HPE recommends that you connect to the BSM OMi Web Services using HTTPS connections, which require a suitable certificate on the server. Although the Web Services can listen to both HTTP and HTTPS at the same time, the SmartConnector always attempts to connect through HTTPS. Both BSM OMi Web Services and its certificate are components generally installed on the BSM OMi server by default. The port that the service uses by default for HTTPS communication is 443. The default port for HTTP communication is 80.

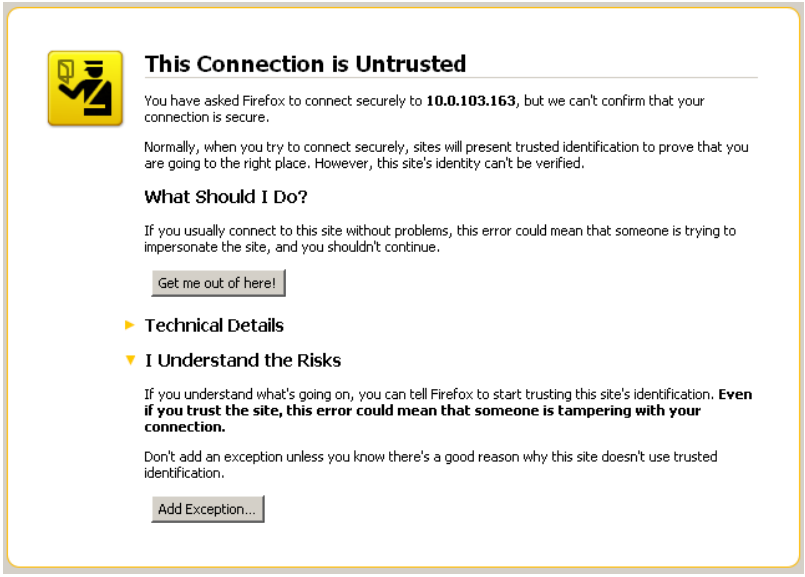
For further security, HPE recommends you verify the hostname and certificate for each HTTPS connection. To verify the certificate for an HTTPS connection, the client system must trust the server's certificate. You will export the server's certificate and import it to the SmartConnector system.

The examples in the following procedure use Mozilla Firefox.

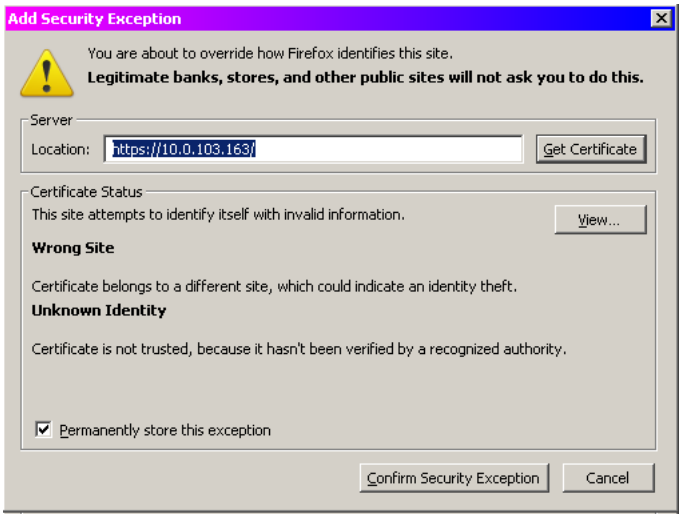
To export the OMi Web Services certificate:

1 Enter the BSM server IP address in your browser.

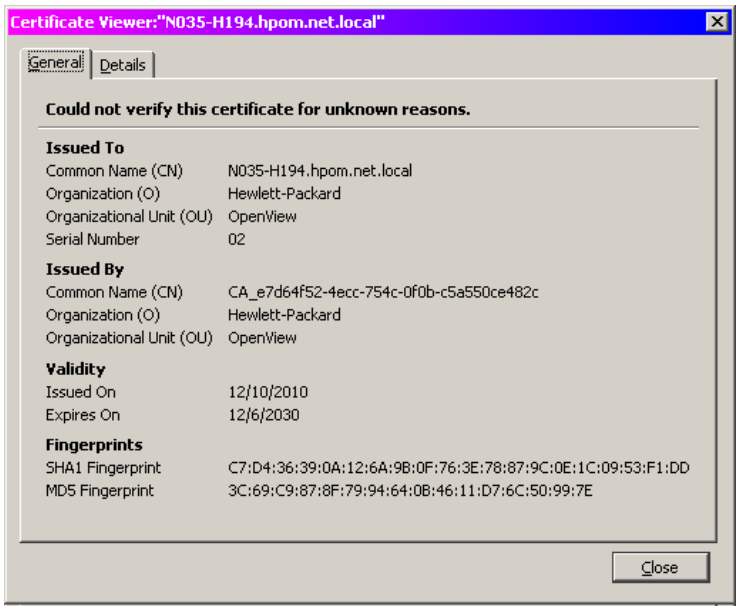
2 Click **I Understand the Risks**.



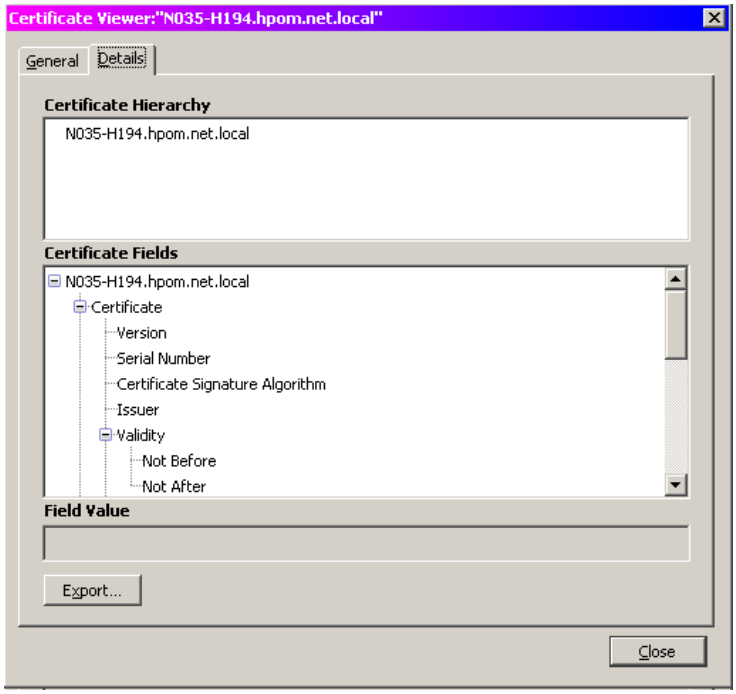
3 Click **Add Exception...**.



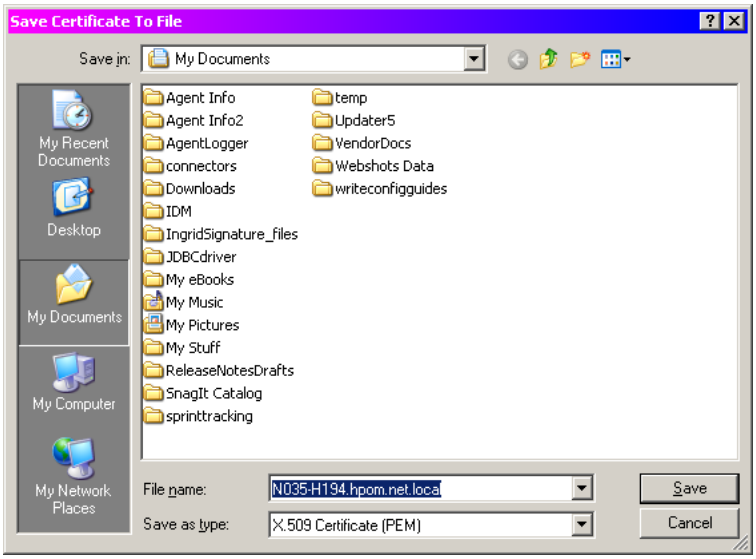
4 Click **View...**.



5 Click the **Details** tab.



6 Click **Export...**.



7 Navigate to the folder into which you want to save the certificate; click **Save**.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

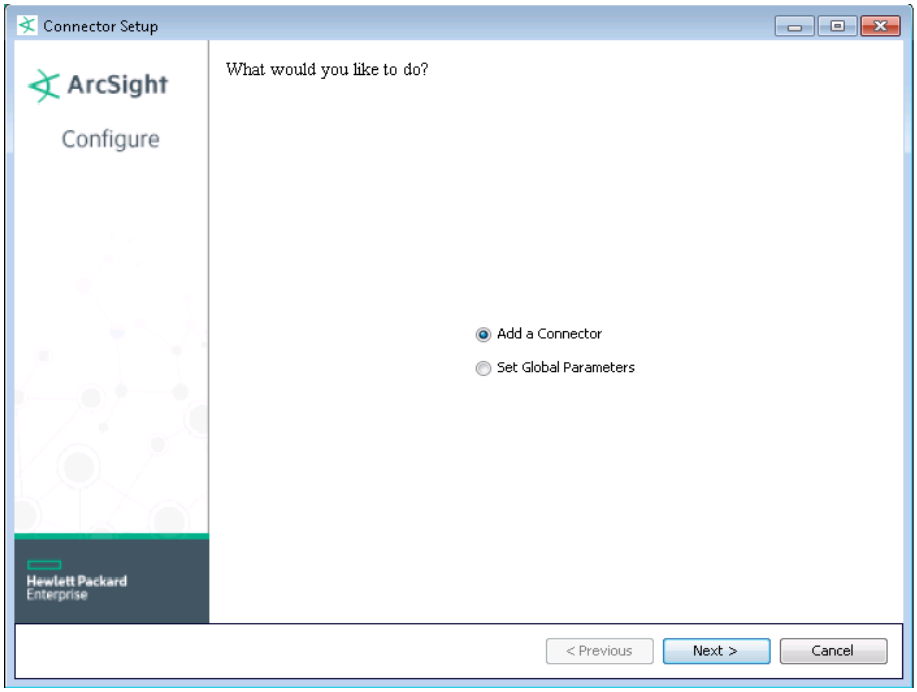
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

2 Start the SmartConnector installation and configuration wizard by running the executable.

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

Introduction
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...

3 When the installation of SmartConnector core component software is finished, the following window is displayed:



The following steps are for importing the server certificate to the connector's Local Java Run Environment; this example is for Windows systems. If you are making use of Linux or Unix, change the command to reflect your $ARCSIGHT_HOME and change \ to /.

A Click **Cancel** to exit the configuration wizard.

B From `$ARCSIGHT_HOME\current\user\agent`, create an `hpeomi` subdirectory; copy the certificate file you obtained during HPE OMi configuration (for example, `server.cer`) and save it into this subdirectory.

C From `$ARCSIGHT_HOME\current\bin`, execute the **keytool** application to import the `server.cer` certificate. Enter this **keytool** command on a single line.

```
arcsight agent keytool -import -alias server_1_1_1_1 -file
<\user\agent\hpeomi\server.cer> -store clientcerts
```

where `<\user\agent\hpeom\server.cer>` is the path and name of the HPE OMi Web Services' certificate file.

D Following the prompts, answer **yes** for the prompt **Trust this certificate?**.

```
Trust this certificate? [no]: yes
```

The certificate is added to keystore.

E Verify the imported certificate by entering the following command from `$ARCSIGHT_HOME\current\bin`:

```
arcsight agent keytool -list -store clientcerts
```

The new certificate (for example, alias=server_1_1_1_1) is displayed in the list.

F From `$ARCSIGHT_HOME/current/bin`, double-click `runagentsetup` to return to the SmartConnector Configuration Wizard.

Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the HPE SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The HPE SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE SecureData to use for encryption.

Parameter	Setting
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

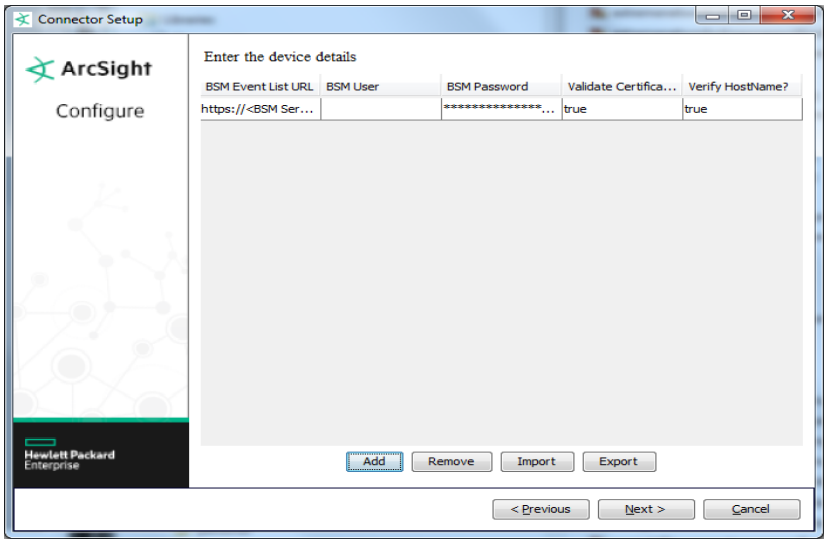
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1 Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.

2 Select **HPE Operations Manager i Web Services** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
BSM Event List URL	Specify the port to which OMi Web Services is listening. To detect whether Web Services is listening, enter the following URL in your browser. You should receive a response from the service. https://<BSM Server>/opr-console/rest/event_list
BSM User	Enter the user name for the BSM user.
BSM Password	Enter the password for the BSM user.
Validate Certificate	Specify whether the SmartConnector is to enable the validation of the BSM OMi SSL certificate for the client. Certificate validation is enabled (true) by default.
Verify HostName	Specify whether the SmartConnector is to enable the validation of the BSM OMi hostname. Hostname validation is enabled (true) by default.

Select a Destination

1. The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2. Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3. Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4. Click **Next** on the summary window.

5. To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Additional Configuration

Read Older Events from HPE OMi

By default, the connector reads only live events starting from the time the connector is up. You can set the advanced parameter `watermark` to an older date and time in the format `<yyyy-MM-ddTHH:mm:ssZ>` (for example, 2010-12-23T00:00:00-08:00) before starting the connector. This tells the connector to read events from a specific time in history. *Make sure to unset this parameter after reading the older events.* Otherwise, the connector will read older events every time it is intentionally or unintentionally restarted. See "Access Advanced Parameters" for how to change these parameters.

Filter the Event Types to Import from OMi

By default, the connector reads all types of events from OMi, including those that have been closed by the operator, and does not perform any filtering. You can, however, choose not to import closed events by setting the advanced parameter `include_closed` to `false`. You can also limit the types of events imported by configuring a value for the advanced parameter `query`. The value for the query should follow the Event Web Service Query Language described in the *BSM OMi Extensibility Guide*. See "Access Advanced Parameters" for how to change these parameters.

Access Advanced Parameters

After SmartConnector installation, you can change parameter values by editing the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`. Change values, save the file, and restart the connector for your changes to take effect.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Operations Manager i Web Services Mappings

ArcSight ESM Field	Device-Specific Field
Additional data	community
Additional data	component
Additional data	enterprise
Additional data	exit_code
Additional data	original_event
Additional data	policy_id
Additional data	specific_trap_type
Additional data	trap_type
Additional data	variables
Additional data	eventNumber

ArcSight ESM Field	Device-Specific Field
Additional data	parameterId
Additional data	Self-Monitoring
Agent (Connector) Severity	Very High = critical; High = major; Medium = warning, minor; Low = normal
Aggregated Event Count	duplicate_count
Destination Address	node_hints_node_ip_address
Destination Host Name	node_hints_node_dns_name
Device Custom Date 1	time_state_changed
Device Custom Date 2	Date Expired
Device Custom Number 1	sequence_number
Device Custom String 1	match_info_policy_name
Device Custom String 2	state
Device Custom String 3	application
Device Custom String 4	source_ci_hints_node_dns_name
Device Custom String 5	originating_server_dns_name
Device Custom String 6	sending_server_dns_name
Device Event Category	match_info_policy_type
Device Event Class ID	eti_hint
Device Host Name	drilldown_url
Device Product	'Operations Manager i'
Device Receipt Time	time_received
Device Severity	severity (critical, major, warning, minor, normal)
Device Vendor	'HPE'
End Time	time_changed
External ID	id
Message	title
Request URL	drilldown_url
Source User ID	assigned_user_login_name
Source User Name	assigned_user_user_name
Source User Privileges	assigned_group_name
Start Time	time_created