Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for JBoss Security Audit File

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for JBoss Security Audit File

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.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/15/2015	Added parameter screen image and description of parameters.
11/15/2012	First edition of this guide.

SmartConnector for JBoss Security Audit File

This guide provides information for installing the SmartConnector for JBoss Security Audit File and enabling the JBoss security auditing feature. JBoss Application Server 7.1 is supported.

Product Overview

Government regulations require auditing in enterprise applications to ensure that the software components of an implementation are traceable and operating within their design parameters. Government regulations and standards also require audit controls in addition to standard application auditing. JBoss Application Server security event auditing provides for constant monitoring of the security domain, and deployed Web and EJB applications.

JBoss Security Auditing

Security event auditing may introduce a performance impact on servers that manage high event volumes. Auditing is deactivated by default, and should be configured to be available on-demand. Web container event auditing can expose sensitive user information. Administrators must ensure appropriate data protection procedures such as password hashing are implemented when configuring security auditing for Web container events.

Configuration

Configure the Security Audit Feature

To configure the security audit feature, perform the following procedure:

1. Open the `jboss-log4j.xml` file using a text editor.

   The `jboss-log4j.xml` file is located in the `$JBOSS_HOME/server/$PROFILE/conf/` directory.

2. By default, the Security Audit Provider category definition in the `jboss-log4j.xml` file is commented out. Uncomment the category definition as shown below:

```
 <!-- Category specifically for Security Audit Provider -->
 <category name="org.jboss.security.audit.providers.LogAuditProvider"
additivity="false">
 <priority value="TRACE"/>
   <appender-ref ref="AUDIT"/>
 </category>
```

3. Specify the auditing levels system property.

   The auditing levels for Web applications must be specified using the `org.jboss.security.web.audit` system property in the `run.sh` (Linux) or `run.bat`

(Microsoft Windows) script. Alternatively, you can specify the system property in the jboss-as/server/$PROFILE/deploy/properties-service.xml file.

```
<!-- Security AUDIT Appender -->
 <appender name="AUDIT"
  class="org.jboss.logging.appender.DailyRollingFileAppender">
   <errorHandler class="org.jboss.logging.util.OnlyOnceErrorHandler"/>
   <param name="File" value="${jboss.server.log.dir}/audit.log"/>
   <param name="Append" value="true"/>
   <param name="DatePattern" value="'.'yyyy-MM-dd"/>
   <layout class="org.apache.log4j.PatternLayout">
     <param name="ConversionPattern" value="%d %-5p [%c] (%t:%x) %m%n"/>
   </layout>
 </appender>
```

4 Save the jboss-log4j.xml file and restart the JBoss server so the new security policy takes effect.

5 Once the audit service is configured and deployed, audit log entries will verify the audit service and EJB invocation success. The audit.log file is located in the jboss-as/server/$PROFILE/log/ directory.

Configure Security Auditing for Web Containers

To configure the security audit feature for Web containers, configure the security audit feature (see "Configure the Security Audit Feature" above) and then perform the following procedure:

1 Web container auditing must first be activated in the server realm of the server.xml file. The server.xml file is located in the jboss-as/server/$PROFILE/deploy/jbossweb.sar/ directory. The Realm element must have enableAudit set to **True** as shown in the following example:

```
<Realm className="org.jboss.web.tomcat.security.JBossWebRealm"
 certificatePrincipal="org.jboss.security.auth.certs.SubjectDNMapping"
  allRolesMode="authOnly"
  enableAudit="true"/>
```

2 Specify the auditing levels system property.

The auditing levels for Web applications must be specified using the org.jboss.security.web.audit system property in the run.sh (Linux) or run.bat (Microsoft Windows) script. Alternatively, you can specify the system property in the jboss-as/server/$PROFILE/deploy/properties-service.xml file.

- Linux: Add the system property into the jboss-as/bin/run.sh file.

```
## Specify the Security Audit options
 #System Property setting to configure the web audit:
 #* off = turn it off
 #* headers = audit the headers
```

```
 #* cookies = audit the cookie
 #* parameters = audit the parameters
 #* attributes = audit the attributes
 #* headers,cookies,parameters = audit the headers,cookie and parameters
 #* headers,cookies = audit the headers and cookies
 JAVA_OPTS="$JAVA_OPTS -
Dorg.jboss.security.web.audit=headers,cookies,parameter"
```

- Windows: Add the system property into the `jboss-as/bin/run.bat` file.

```
rem Specify the Security Audit options
 rem System Property setting to configure the web audit
 rem * off = turn it off
 rem * headers = audit the headers
 rem * cookies = audit the cookie
 rem * parameters = audit the parameters
 rem * attributes = audit the attributes
 rem * headers,cookies,parameters = audit the headers,cookie and
parameters
 rem * headers,cookies = audit the headers and cookies
 set JAVA_OPTS=%JAVA_OPTS% " -
Dorg.jboss.security.web.audit=headers,cookies,parameter"
```

- properties-service.xml: Update the SystemPropertiesService class MBean in the `jboss-as/server/$PROFILE/deploy/properties-service.xml` file, and declare the java property as an <attribute>. You can uncomment the relevant operating system block in the code sample below:

```
...
  <mbean code="org.jboss.varia.property.SystemPropertiesService"
name="jboss:type=Service,name=SystemProperties">
     <!-- Linux Attribute Declaration -->
    <!-- <attribute name="Properties">JAVA_OPTS="$JAVA_OPTS -
Dorg.jboss.security.web.audit=headers,cookies,parameter" </attribute>  --
>
     <!-- Windows Attribute Declaration -->
    <!--  <attribute name="Properties">JAVA_OPTS=%JAVA_OPTS% " -
Dorg.jboss.security.web.audit=headers,cookies,parameter"  </attribute>  -
->
  </mbean>
 ...
```

3 Verify that security auditing is functioning correctly.

After the system property is specified in the files, audit log entries will verify Web invocation success. The `audit.log` file is located in `jboss-as/server/$PROFILE/log/` directory.

Install the SmartConnector

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

Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

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

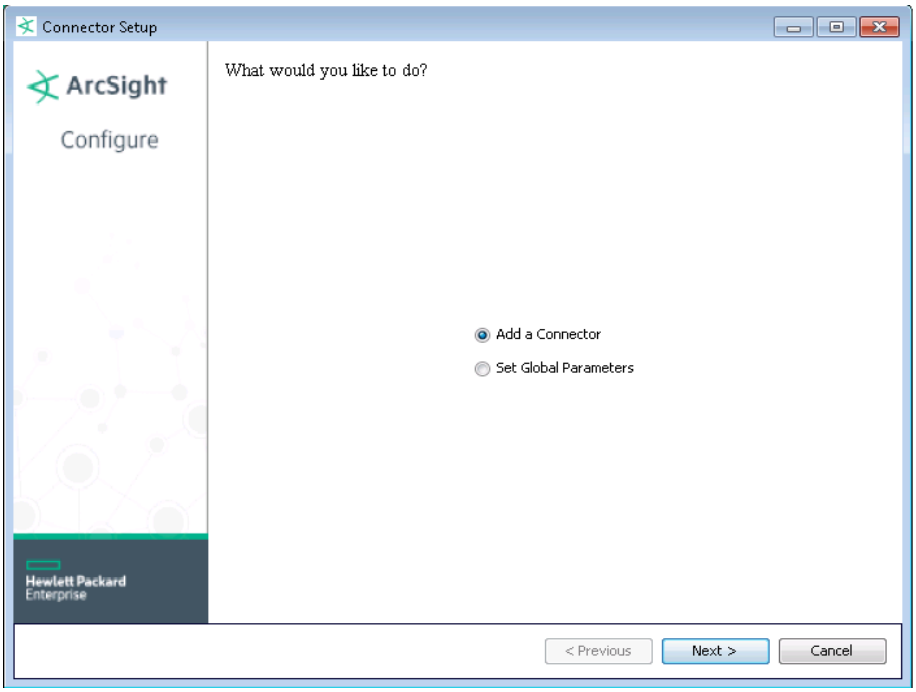
Install Core Software

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:



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.

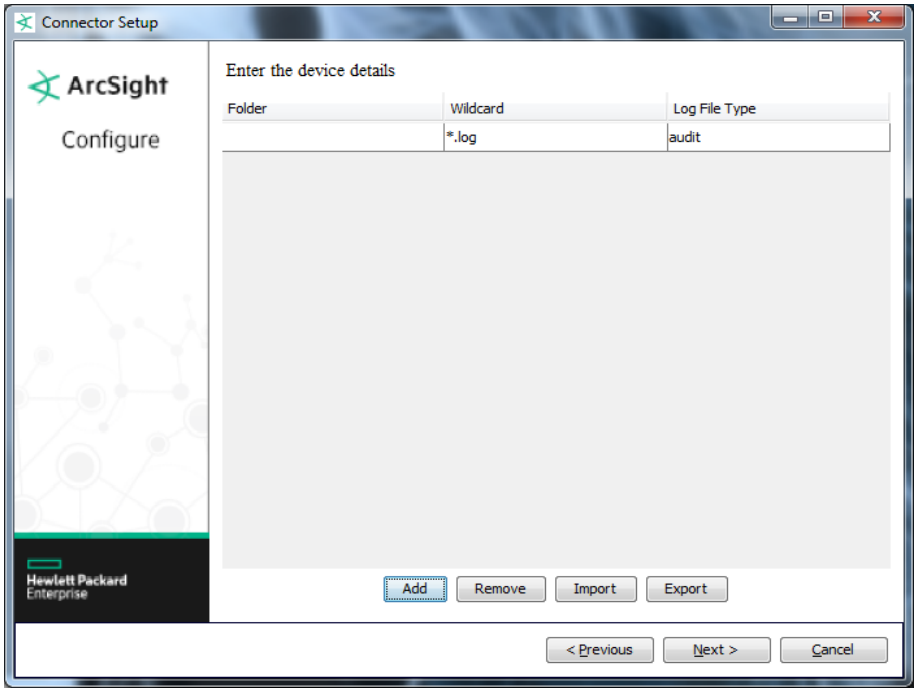
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of 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.

Parameter	Setting
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.
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 **JBoss Security Audit File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Folder	Enter the absolute path to the location of the log file.

Parameter	Description
Wildcard	Enter a wildcard that identifies the files to process. For example, if the access log file is 'access1003o21405.log', use wildcard 'access*.log'.
Log File Type	Accept the default value of audit for log file type.

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*.

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.

JBoss Security Audit File Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = ERROR,Fatal; Medium = WARN,DEBUG; Low = TRACE,INFO
Application Protocol	Protocol
Device Custom IPv6 Address 1	"Device IPv6 Address"
Device Custom IPv6 Address 3	"Destination IPv6 Address"
Device Custom String 1	DetectTime
Device Custom String 3	ClassName
Device Event Class ID	Key
Device Product	JBoss
Device Receipt Time	FullDetectTime
Device Severity	Severity
Device Vendor	RedHat
Message	Message