Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for IBM Tivoli Access Manager XML File

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for IBM Tivoli Access Manager XML File

November 30, 2016

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://www.protect724.hpe.com/docs/DOC-13026.

Revision History

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/15/2013	Added support for version 6.1.
05/15/2012	Added new installation procedure.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
09/30/2009	Added section about increasing memory size for XML reports.
06/30/2009	Global update to installation procedure for FIPS support.
02/11/2009	Updated field mappings for Destination User Name.

SmartConnector for IBM Tivoli Access Manager XML File

This guide provides information for installing the SmartConnector for IBM Tivoli Access Manager XML File for event collection. This SmartConnector is supported for installation on UNIX platforms. IBM Tivoli Access Manager versions 5.1 and 6.1 are supported.

Product Overview

IBM Tivoli Access Manager is an authentication and authorization solution for corporate Web, client/server, and existing applications. Tivoli Access Manager lets you control user access to protected information and resources and supports authentication, authorization, data security, and resource management capabilities. When using native Tivoli Access Manager auditing, audit events are captured in the audit trail in a standard format using the Extensible Markup Language (XML) elements. The XML file is in ASCII format.

Configuration

Assumptions

Installation instructions for Tivoli Access Manager can be found in the *IBM Tivoli Access Manager for e-business Web Security Installation Guide Version 5.1*.

It is assumed that IBM's recommendations have been followed in deploying the IBM Tivoli Access Manager system as described in this section.

The following servers have been installed on separate, standalone servers:

- Registry Server
- Policy Server
- WebSeal
- WebPortal

The following prerequisite software products are installed on these servers:

- Global Security Kit
- IBM JRE
- IBM Tivoli Directory

The following products (which can be installed together in one machine) have been installed:

- Authorization Server
- ADK System

- Java Run Time Environment
- Policy Proxy Server
- Run Time System
- Web Portal Manager
- WebSEAL

Logging Events

This section provides instructions for enabling auding, sending events to a log file, changing the message log files location, and logging messages in log XML format. Note that these instructions are for version 5.1; instructions may vary for version 6.1. See your IBM Tivoli documentations for complete information.

Enabling Auditing

To configure Tivoli Access Manager server audit trail files:

1. Edit the appropriate server configuration file. Each server provides its own stanza entry values in its configuration file.
2. Locate the `[aznapi-configuration]` stanza.
3. Enable auditing by specifying **yes** or **true**: `logaudit = {yes|true}`. By default, auditing is disabled. When enabled, the auditcfg and auditlog stanza entries are also required.
4. Select the component-specific type of audit records that you want to capture:

   auditcfg = azn
   #auditcfg = authn
   #auditcfg = mgmt

   By default, when auditing is enabled for a process with no configured audit tags, all auditable events are captured. Another stanza entry is auditcfg=http, which is used for components other than the Base, such as WebSEAL. Each server provides its own value in its configuration file.
5. Specify the name and location of the audit trail file for the local client:

   ```
   auditlog = fully_qualified_path
   ```

   If no location and name are supplied, auditing will not be performed.
6. Save and exit the configuration file.

Sending Events to a Log File

To configure Tivoli Access Manager to send event records to a log file:

1. Edit the appropriate server configuration file. Each server provides its own stanza entry values in its configuration file. Locate the `[aznapi-configuration]` stanza.

2 Specify that the category is to send event records to a log file using the format *category*:file. For example, a category might be to audit authorization events (audit.azn):
`logcfg=audit.azn:file`

3 Specify the log file location: `path=`*fully_qualified_path*. The default directories are:

UNIX `/opt/PolicyDirector/log`

Windows `C:\Program Files\Tivoli\Policy Director\log`

The default file name depends upon the type of logging being performed, such as `audit.log`.

4 Specify the log file ID: `log_id=`*logid*

Use the `log_id` option to set the log file identifier (ID) explicitly; otherwise, it is given a default value. If the `path=` option is specified, the default value is the configured path name. If `path=` is not specified, the log ID defaults to the domain component of the event category being captured. For example, `logcfg = audit.azn:file` implies `log_id=audit`.

Changing the Message Log Files Location

To change the directory for the Tivoli Access Manager server-specific message log files:

1 Go to the directory where the routing files are located. The default directory location is one of the following:

a UNIX: `/opt/PolicyDirector/etc/`

b Windows: `C:\Program Files\Tivoli\Policy Director\etc\`

2 Select one of the appropriate server-related routing files to edit:

pdmgrd_routing for the Tivoli Access Manager Policy Server
pdacld_routing for the Tivoli Access Manager authorization server
pdmgrproxyd_routing for the Tivoli Access Manager policy proxy server
routing for Tivoli Access Manager general serviceability information

3 Edit the file and locate the section entitled `Sequential Logging`.

4 Change the default location for the message log files, as appropriate. In the following proxy server (pdmgrd) example, you can change from the default *routing_path* installation location of `/var/PolicyDirector/log/`:

```
FATAL:STDOUT:-;UTF8FILE;/var/PolicyDirector/log/msg_pdmrd_utf8.log
    :644:ivmgr:ivmgr
ERROR:STDOUT:-;UTF8FILE:/var/PolicyDirector/log/msg_pdmgrd_utf8.log
    :644:ivmgr:ivmgr
WARNING:STDOUT:-;UTF8FILE:/var/PolicyDirector/log/msg_pdmrd_utf8.log
    :644:ivmgr:ivmgr
NOTICE:STDOUT:-;UTF8FILE:/var/PolicyDirector/log/msg_pdmgrd_utf8.log
    :644:ivmgr:ivmgr
```

```
#NOTICE_VERBOSE:STDOUT:-;/var/PolicyDirector/log/
    msg_pdmgrd_utf8.log:644:ivmgr:ivmgr
```

To a different directory location of /myTAMlogs/:

```
FATAL:STDOUT:-;UTF8FILE:/myTAMlogs/msg_pdmgrd_utf8.log:644:ivmgr:ivmgr
ERROR:STDOUT:-;UTF8FILE:/myTAMlogs/msg_pdmgrd_utf8.log:644:ivmgr:ivmgr
WARNING:STDOUT:-;UTF8FILE:/myTAMlogs/msg_pdmgrd_utf8.log:644:ivmgr:ivmgr
NOTICE::STDOUT:-;UTF8FILE:/myTAMlogs/msg_pdmgrd_utf8.log:644:ivmgr:ivmgr
#NOTICE_VERBOSE:STDOUT:-;/myTAMlogs/msg_pdmgrd_utf8.log
    :644:ivmgr:ivmgr
```

5 Exit and save the routing file.

Remember to prune log files periodically to prevent them from becoming too large.

Logging Messages in Log XML Format

To log messages in XML format:

1 Go to the directory where the routing files are located. The default directory location is one of the following:

UNIX: `/opt/PolicyDirector/etc/`
Windows: `C:\Program Files\Tivoli\Policy Director\etc\`

2 Select one of the appropriate server-related routing files to edit:

pdmgrd_routing for the Tivoli Access Manager policy server
pdacld_routing for the Tivoli Access Manager authorization server
pdmgrproxyd_routing for the Tivoli Access Manager policy proxy server
routing for Tivoli Access Manager general serviceability information

3 Find a line similar to the following in the routing file:

```
ERROR:STDOUT:-;XMLFILE:%PDDIR%/log/msg_error.log
```

For example, to change the line to specify that ERROR messages should be logged in XML format instead of text format to both STDOUT and to the file `msg_error.log`:

```
ERROR:XMLSTDOUT:-;XMLFILE:%PDDIR%/log/mes_error.log
```

where %PDDIR% is the Tivoli Access Manager UNIX directory variable.

Increase Memory Size for XML Reports

The connector cannot process reports that are too lengthy. With the default 256M memory setting, the connector can safely process reports up to 250K in length. If memory is increased to the maximum limit of 1024M, the connector can process reports up to a million lines in length. Longer reports cannot be processed. ArcSight's recommendation for long reports is to split the scan into multiple smaller reports and import them individually.

To increase the memory size for stand-alone connectors from the command line, change the following line in `$ARCSIGHT_HOME\current\bin\scripts\connectors.bat` (Windows) or `$ARCSIGHT_HOME/current/bin/scripts/connectors.sh` (Unix)

```
ARCSIGHT_MEMORY_OPTIONS="  -Xms256m -Xmx256m "
```

to

```
ARCSIGHT_MEMORY_OPTIONS="  -Xms1024m -Xmx1024m "
```

To increase the memory size for connectors being run as a service, change the following lines in `user/agent/agent.wrapper.conf` from:

```
wrapper.java.initmemory=256
wrapper.java.maxmemory=256
```

to:

```
wrapper.java.initmemory=1024
wrapper.java.maxmemory=1024
```

To increase the memory size for connectors managed by the Connector Appliance/ArcSight Management Center, the heap size can be set using a container level command.

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). This configuration guide takes you through the installation process with **ArcSight Manager (encrypted)** as the destination.

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.

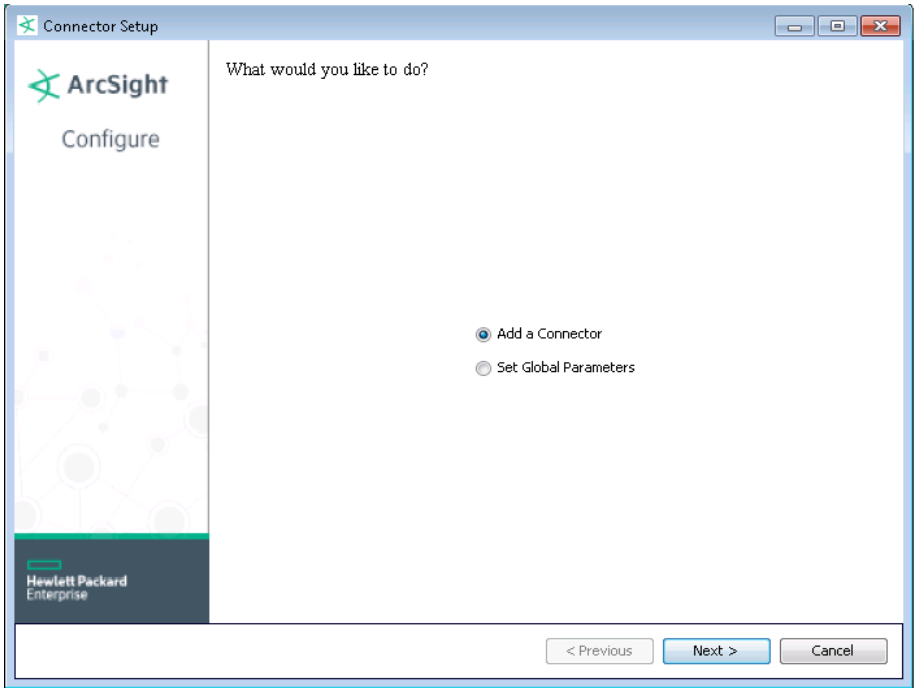
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

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. After installing core software, you can set the following parameters:

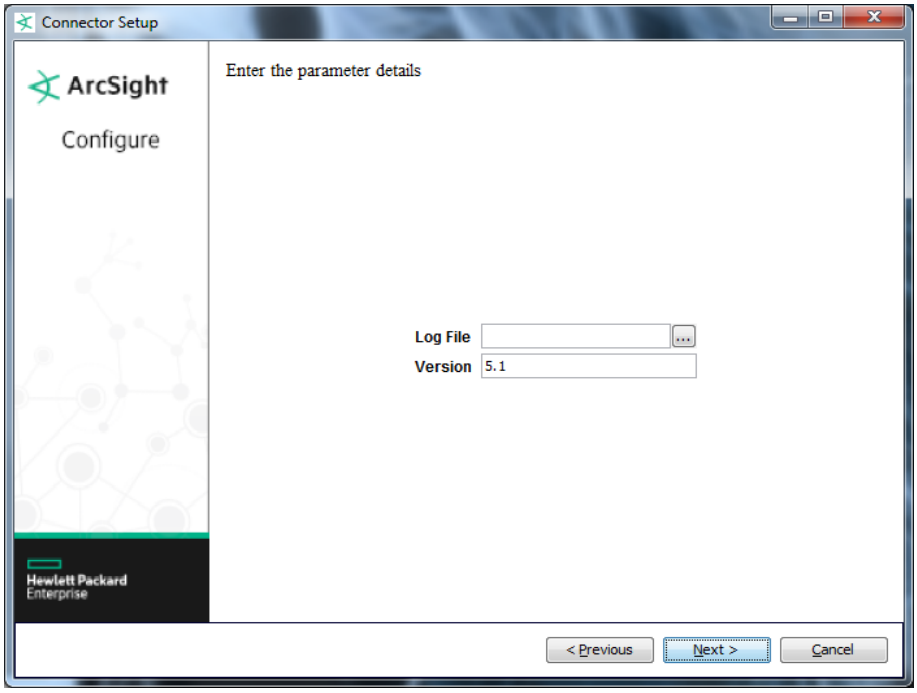
Global Parameter	Setting
Set FIPS mode	Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'.

Global Parameter	Setting
Set Remote Management	Set to 'Enable' 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 'Disable'.
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	If 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. When both values are present, the initial setting is 'IPv4'.

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 the "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 **IBM Tivoli Access Manager XML File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Log File	Enter the complete path to the XML log files.

Parameter	Description
Version	Enter the version of Tivoli Access Manager or its components (5.1 is entered by default).

Select a Destination

1. The next window asks for the destination type; make sure **ArcSight Manager (encrypted)** is selected and click **Next**. (For information about this destination or any of the other destinations listed, see the *ArcSight SmartConnector User Guide*.)

2. Enter values for the **Manager Host Name**, **Manager Port**, **User** and **Password** required parameters. This is 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. 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 some SmartConnectors, a system restart is required before the configuration settings you made take effect. If a **System Restart** window is displayed, read the information and initiate the system restart operation.

Save any work on your computer or desktop and shut down any other running applications (including the ArcSight Console, if it is running), then shut down the system.

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.

IBM Tivoli Access Manager Audit XML 6.1 Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = Failure, Low = Success, Pending, Unknown
Destination Host Name	location
Destination User Name	One of (principal, accessor, accessor_name)
Device Action	outcome (0=Success, 1=Failure, 2=Pending, 3=Unknown)
Device Custom IPv6 Address 2	user_location (Source IPv6 Address)
Device Custom String 1	principal_auth
Device Custom String 2	target_resource (0=AUTHORIZATION, 1=PROCESS, 2=TCB, 3=CREDENTIAL, 5=GENERAL, 6=APPLICATION, 7=AUTHENTICATION)
Device Custom String 3	object
Device Custom String 4	All of (policy_name, policy_type, Policy_descr)
Device Custom String 5	All of (attribute_name, attribute_type, attribute_source, attribute_value)
Device Custom String 6	audit_event
Device Event Category	component
Device Process Name	originator_blade
Device Product	'Tivoli Access Manager'
Device Receipt Time	date
Device Severity	outcome (0=Success, 1=Failure, 2=Pending, 3=Unknown)
Device Vendor	'IBM'
Device Version	'6.1'
External ID	action
Name	action (0=Authentication or authorization, 1=Change password, 2=WebSEAL, 'Management')
Source Address	user_location
Source Domain	principal_domain

IBM Tivoli Access Manager Audit XML 5.1 Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	Location
Destination User Name	Principal, Accessor, or Accessor_name
Device Action	Outcome (0=Success, 1=Failure, 2=Pending, 3=Unknown)
Device Custom Number 1	Outcome status
Device Custom String 1	principal_auth
Device Custom String 2	Target_resource (0=AUTHORIZATION, 1=PROCESS, 2=TCB, 3=CREDENTIAL, 5=GENERAL, 6=APPLICATION, 7=AUTHENTICATION)
Device Custom String 3	Object
Device Custom String 4	Policy name type description
Device Custom String 5	Attribute name plus attribute type plus attribute_source, plus attribute_value
Device Custom String 6	Audit event
Device Event Category	Component
Device Event Class Id	outcome_status
Device Process Name	originator_blade
Device Product	Tivoli Access Manager
Device Receipt Time	Date
Device Severity	Outcome (0=Success, 1=Failure, 2=Pending, 3=Unknown)
Device Vendor	IBM
Device Version	5.1
External Id	Action
Message	Data
Name	One of (action, "0=Authentication or authorization", "1=Change password", "2=WebSEAL") "Management"
Source Domain	principal_domain