

## HPE ArcSight SmartConnectors Known Limitations

### *All SmartConnectors*

If you are using a map file with an expression setter in the `<connector_install_location>`  
`\current\user\agent\map location`, and the connector runs out of memory, then you can add the  
following property to `agent.properties` to work-around the problem:  
`parser.operation.result.cache.enabled=false`

If this problem happens with Windows Event Log Native, and if the above work-around does not completely  
solve the problem, then reduce the value of the Native connector parameter 'eventprocessorthreadcount'.  
You can try to reduce it successively, down to a minimum value of 1, to see which value works best for your  
environment.

Example:

```
agents[0].eventprocessorthreadcount=5 or  
agents[0].eventprocessorthreadcount=1, etc..  
where 0 is the index of the WINC connector in the container. [CON-19234, CON-18977]
```

### *Microsoft Office 365*

When configuring the Office 365 connector, if you get the following error "HTTP/1.1 400 Bad Request"  
with the message: `{"error":{"code":"AF20024","message":" The subscription is  
already enabled. No property change."}}`, you can ignore the error, continue configuration, and then  
run the connector to collect events.

The error is caused by an undocumented change in the Office 365 API response behavior. Before this change,  
when connector requested to start an already started subscription, the API would return a 200 OK response, and  
it would work fine. Office 365 API has changed the behavior to respond with HTTP error 400, instead of 200.  
Neither the change in API behavior, nor the new Error# AF20024, have been documented by Microsoft at:  
<https://msdn.microsoft.com/en-us/office-365/office-365-management-activity-api-reference> [CON-18936]

### *Check Point OPSEC NG*

Check Point has updated their servers to be able to use SHA-256 certificates. A newer LEA client is needed to  
support these SHA-256 certificates. Because the SmartConnector for Check Point OPSEC NG does not use this  
new LEA client, the connector can no longer connect to collect events. The recommendation is to use the  
SmartConnector for Check Point Syslog to collect Check Point events. Note that the R77.30 Add-On on the  
Security Management Server or Multi-Domain Server is required for syslog event collection (see sk105412 at:  
<http://supportcontent.checkpoint.com/solutions?id=sk105412>). [CON-19222]

### *Oracle Audit Syslog*

Time from original event is not parsed. End Time shows as time at which SmartConnector received the event  
and not the time from original event itself. [CON-18619]

### *All JSON FlexConnectors*

The processed file is always renamed despite the correct parameters having been set. This issue will be fixed in  
an upcoming release. [CON-18382]

### *All SmartConnectors using Logger Secure Pool for v7.5 and earlier*

For Logger Secure Pool transport, the current default number of threads is 2, indicating the number of logger  
pool members. When there is a Logger communication error and the connector disconnects from that Logger  
pool member, it may stop sending to any Logger pool member even though some are available. When this  
happens the connector will cache events. Restarting the connector clears the problem. Setting the thread count  
to 1 avoids this problem. [CON-18009]

Workaround: Upgrade to v7.6.0.8009.0 or add the following to `agent.properties`:  
`transport.loggersecurepool.threads=1`

## *All SmartConnectors version 7.5 in FIPS mode with client authentication enabled*

When installing a version 7.5 Connector, in FIPS mode, with client authentication enabled, ESM registration may fail. If agent.log contains certificate errors, such as "Registration failed: Manager certificate not trusted. Please check your SSL configuration.", then follow this workaround. [CON-18847, CON-18819]

Workaround: The workaround is to import the ESM Manager certificate into the Connector's key store. For example:

1. cd <connector installation directory>/current
2. Run one of the following commands:
  - a. For Linux:  
jre/bin/keytool -importcert -file <path to manager certificate> -keystore config/keystore.client.bcfks -storepass <keystore password, default is changeit> -storetype BCFKS -providername BCFIPS -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath lib/agent/fips/bc-fips-1.0.0.jar -J-Djava.security.egd=file:/dev/urandom -alias <an alias, such as esm>
  - b. For Windows:  
jre/bin/keytool -importcert -file <path to manager certificate> -keystore config/keystore.client.bcfks -storepass <keystore password, default is changeit> -storetype BCFKS -providername BCFIPS -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath lib/agent/fips/bc-fips-1.0.0.jar -alias <an alias, such as esm>

## *All SmartConnectors*

When remotely upgrading a SmartConnector with FIPS disabled from SmartConnector release v7.5.0.7983 using an ESM in "password and SSL" mode, the upgrade may fail. The 'upgrade-from' instance will continue to run. [CON-19084]

Workaround: Perform a local upgrade.

## *All SmartConnectors with Logger Destinations*

This issue could affect any connector with a Logger destination using a non-persistent connection. Occasionally, depending on the network, the connector could experience problems sending a batch of events to Logger. During that time, the following symptoms might be noticed in the log: Logger ping test could fail frequently; the EPS could drop down; the heartbeat transport and event transport links could sporadically go up and down. In the statistics, longer roundtrip times might be observed for 'event sent' acknowledgement or events could even fail to be sent and caching may be observed. Some of these symptoms could be related to the JDK bug (see <https://bugs.openjdk.java.net/browse/JDK-8172578>) which will be addressed in an upcoming JRE patch. Use the following workaround if you notice these symptoms. [CON 18602]

Workaround:

Change the connection setting between the connector and Logger from non-persistent to persistent.

1. Edit the agent.properties file by adding the following line:  
transport.loggersecure.connection.persistent=true
2. Restart connector.

## *All SmartConnectors using FIPS mode with Client Authentication enabled*

For the SmartConnector release 7.5.0.7983, the Connector key pair for Client Authorization was not automatically migrated from the legacy FIPS store (NSS) to the new FIPS store (BouncyCastle). This issue has been fixed in the SmartConnector release 7.6.0.8009.[CON-18708]

Workaround:

To manually upgrade to 7.5 from 7.4 or earlier when using FIPS mode with Client Authentication enabled:

1. Stop the connector.
2. If they exist, comment-out or remove any of these properties from the agent.properties file:  
ssl.keystore.path, ssl.keystore.type, ssl.truststore.path, ssl.truststore.type
3. Perform the upgrade. If you see the following certificate error, exit from setup:  
"Failed to login: Couldn't connect to ArcSight Manager:... Received fatal alert: bad\_certificate"
4. cd to current directory.

5. Find the alias used when creating the client key pair. It may be "agent" or "admin". To list the entries:
  - a. Execute:  

```
bin/arcsight runcertutil -L -d <full path to installation directory>/user/agent/nssdb.client_migrated/
```
  - b. On Linux, this may find the one entry:  

```
bin/arcsight runcertutil -L -d <full path to installation directory>/user/agent/nssdb.client_migrated/ | grep "Cu,Cu,Cu"
```
6. Execute:  

```
bin/arcsight runpk12util -o ../clientkey.p12 -n <alias from previous step, such as agent or admin> -d sql: <full path to installation directory>/user/agent/nssdb.client_migrated
```

  - a. Enter passwords as prompted, the NSS DB password, and a password for the clientkey.p12 file.
7. Execute:  

```
bin/jre/keytool -importkeystore -srckeystore ../clientkey.p12 -srcstoretype PKCS12 -srcstorepass <password used for clientkey.p12> -destkeystore config/keystore.client.bcfks -deststorepass <password from agent property, ssl.fips.keystore.password> -deststoretype BCFKS -providername BCFIPS -providerclass org.bouncycastle.jcayce.provider.BouncyCastleFipsProvider -providerpath lib/agent/fips/bc-fips-1.0.0.jar -J-Djava.security.egd=file:/dev/urandom
```
8. Update the agent.properties file by adding this line:  

```
ssl.fips.keystore.path=config/keystore.client.bcfks
```
9. Run the connector (bin/arcsight agents).

#### *All SmartConnectors using FIPS Suite B*

For SmartConnector release 7.5.0.7983, all Suite B certificates must be preloaded into the keystore before configuring multiple Suite B destinations. If certificates are not pre-loaded, you will need to relaunch the setup wizard after adding certificates to add those destinations. This issue is fixed in the 7.6.0.8009 release. [CON-18485]

Best Practice for release 7.5: Import all Suite B certificates before running the configuration wizard.

#### *All SmartConnectors accessing the ArcSight Keytool in SmartConnector release 7.5*

In SmartConnector release 7.5.0.7983, the command line tool, ArcSight Keytool, was not working and was made unavailable. It has been fixed in SmartConnector release 7.6.0.8009. [CON-18636]

Workaround for 7.5: Use the Java keytool executable at <installation directory>/jre/bin/keytool.

EXAMPLES: To import a certificate from ESM:

1. cd to the connector installation directory.
2. jre/bin/keytool -storepass changeit -importcert -file /tmp/esm-15.214.129.5.cer -alias esm

To generate a connector key pair:

1. cd to the connector installation directory.
2. jre/bin/keytool -genkeypair -keystore config/keystore.client -storetype JKS -storepass changeit -dname "cn=admin, ou=ArcSight, o=HP, c=US" -alias admin -validity 365

To export the key pair certificate:

1. cd to the connector installation directory.
2. jre/bin/keytool

To export the key pair certificate:

1. cd to the connector installation directory.
2. jre/bin/keytool -exportcert -keystore config/keystore.client -alias admin -storepass changeit -file agent-certadmin.cer

#### *Check Point OPSEC NG*

Checkpoint OPSEC LEA Client randomly crashes on Windows 2012 R2 platform. [CON-18427]

Workaround: HPE recommends using the SmartConnector for Check Point Syslog or installation of the SmartConnector for Check Point OPSEC NG on a Red Hat Enterprise Linux (RHEL) platform.

#### *Cisco Secure IPS SDEE, Sourcefire Defense Center eStreamer, and HPE Operations Manager Incident Web Service connectors*

FIPS compliance is not supported for these connectors. [CON-18660, CON-18662]

#### *Qualys QualysGuard File*

Currently FIPS is not supported for this connector. [CON-18661]

#### *All SmartConnectors that run in a local container on an ArcMC appliance*

Emergency Restore from ArcMC appliance using 7.4 and 7.5 connectors leaves a blank destination on the GUI.

Workaround: Remove 'NSP' destination from transport.types property in agents.properties file and restart the connector. [CON-18018]

#### *AUP Upload Issue with ConnApp and ArcMC*

Uploading AUP updates for upgrading connectors in ConApp and ArcMC fails when the AUP update file is larger than 600 MB. Workaround: Go to the `logger.default.properties` at

`/opt/arcsight/conapp/current/arcsight/conapp/config/logger`. Change the value of the `AUP.connectorappliance.upgrade.upload.max=600` to `=900` and restart. [CON-16879]

#### *All SmartConnectors using ODBC and Other Databases*

Beginning with SmartConnector release 7.2.1, SmartConnectors are using Java 8. Java 8 does not support ODBC connections; therefore, database connectors using MS SQL databases can only use JDBC connections. For the same reason, the MS Access database and the embedded database for the Symantec Endpoint Protection connector are no longer supported with connector release 7.2.1 or later. If your connector uses an unsupported database, a warning message displays during local upgrades. Remote upgrades will fail, and automatically roll back to the previous version, possibly losing up to five minutes of events. HPE does not recommend upgrading until you are using a database connection supported by Java 8.

#### *All SmartConnectors in FIPS mode*

If you are running a connector in FIPS mode and trying to setup a Logger Secure (Smart Message) destination, it prompts a warning or error message indicating the connection to the destination failed on a ping test even if all the destination parameters are correct and the SSL certificate has been imported correctly into the connector trust store.

Workaround: Ignore the warning and finish the destination setup. The connector will work as expected and communicate with the destination logger at startup. [CON-18584]

#### *Oracle Solaris Basic Security Module*

Solaris BSM connector does not keep up with file rotation, causing the connector to stop processing events. [CON-10510]