Micro Focus Security ArcSight Model Import Connector

Software Version: 1.0

Administration Guide for GTAP 1.0

Document Release Date: May 2022
Software Release Date: May 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

Administration Guide for GTAP 1.0 5

Product Overview 6

Galaxy Threat Acceleration Program 6

GTAP Solution Overview 7

Event Flow Explained 8

GTAP Connector Installation Options 9

Obtaining License Keys 10

Overview of GTAP Active Lists 10

Locating GTAP Active Lists 10

Understanding GTAP Active Lists 11

Fields in Active Lists for GTAP Plus 12

Understanding How Content Leverages GTAP Active Lists 13

Installing and Configuring the Connector 15

Preparing to Install the Connector 16

Downloading the Custom MISP Instance Certificate 16

Installing and Configuring GTAP Plus 17

Installing and Configuring GTAP Basic 19

Installing and Configuring GTAP Custom 20

Completing Installation 22

Increasing the Java Heap Size 22

Setting Up the User in ESM 23

Starting and Stopping Data Import 24

Configuring the Start Date 24

Optimizing Data Transfer by Using a Timer 25

Running the Connectors 25

Running in Standalone Mode 25

Running as a Windows Service 26

Running Connectors as a UNIX Daemon 26

Verifying the Connector Functionality 27

Identifying Basic and Plus Content When GTAP Plus Connector is Installed 29

Troubleshooting 31

Common Causes of Error 31

Errors Specific to GTAP Plus, Basic and Custom MISP versions 32

Connector is unable to receive any events if the /user/ agent/ agentdata folder contains cache 33

Invalid Parameters Error During GTAP Plus Installation 33

Resetting Data Import 34

Send Documentation Feedback 35

Administration Guide for GTAP 1.0

This guide describes the steps to install the CyberRes Galaxy Threat Acceleration Program Model Import Connector and to configure the device for data collection. For more information about the software requirements, see the Technical Requirements for SmartConnectors.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the Connectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectors to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

Product Overview

Threat intelligence is no longer considered as a 'nice to have' option and organizations are looking to implement threat detection mechanisms, which can detect the latest and most notorious attacks as early as possible.

CyberRes Galaxy is an immersive cyberthreat experience that provides actionable and business-centric threat intelligence for security executives. CyberRes Galaxy enables cyber professionals to quickly gain visibility into the most pressing threats to their business and helps organizations secure their value chains so they can focus on driving business growth.

At a high level, Galaxy program is comprised of two main offerings:

• **Galaxy Online:** Provides timely threat briefings through an interactive web-portal, mainly geared towards C-level executives and SOC leaders.

• **Galaxy Commercial (Also Known As Galaxy Threat Acceleration Program - GTAP)** Provides up-to-the-minute threat intelligence (from OSINT -open source- and CyberRes-curated premium intelligence) feed for ArcSight ESM customers.

Galaxy Threat Acceleration Program

At a high level, GTAP comprises of the following two licensing models:

GTAP Basic

- Provides near real-time threat intelligence, by synchronizing an ArcSight ESM Server with CyberRes Galaxy Threat Intelligence (TI) server in the cloud.
- The threat intelligence received is the Open Source Intelligence (OSINT), filtered on `TLP:WHITE` as provided by the public instance of MISP CIRCL TI feed.
- Does not require an access key.

GTAP Plus

- All of the GTAP Basic features.
- Premium threat intelligence feed for ArcSight ESM customers, curated by CyberRes Threat Intelligence Research Team, "very low false positive, high fidelity indicators of compromise" that correlate with the most important threats an organization needs to identify and resolve at the highest urgency level.
- Specific indicator types are added to the ESM Active lists so that more alerts will be triggered for specific attacks.
- High, Medium, and Low confidence level is added to the ESM Active lists.

- Human threat research team as opposed to generically and automatically generated threat feed records.
- Good for use in SOC automation as it provides reliable indicators.
- New added rule for High Confidence Alerts to quickly identify and resolve well known threats.

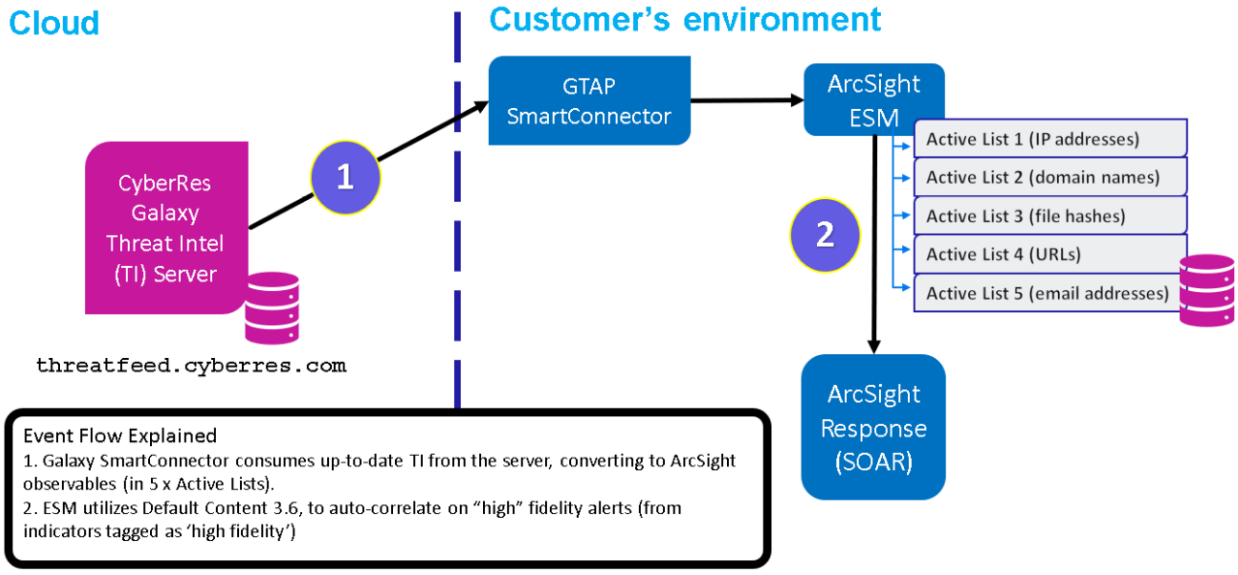
GTAP Solution Overview

As can be seen from the diagram below, GTAP Model Import Connector connects the ArcSight ecosystem to the CyberRes Galaxy Threat Feed server, synchronizing the data multiple times daily. In the 1.0 release, we support the threat feed only into ArcSight ESM.

Galaxy solution provides an end-to-end experience, by also including the ESM content (detection, correlation rules, etc…) as well as integration into SOAR. This GTAP content is embedded into the ArcSight Default Content, available out-of-the-box, as a turnkey solution for today's advanced SOC's.

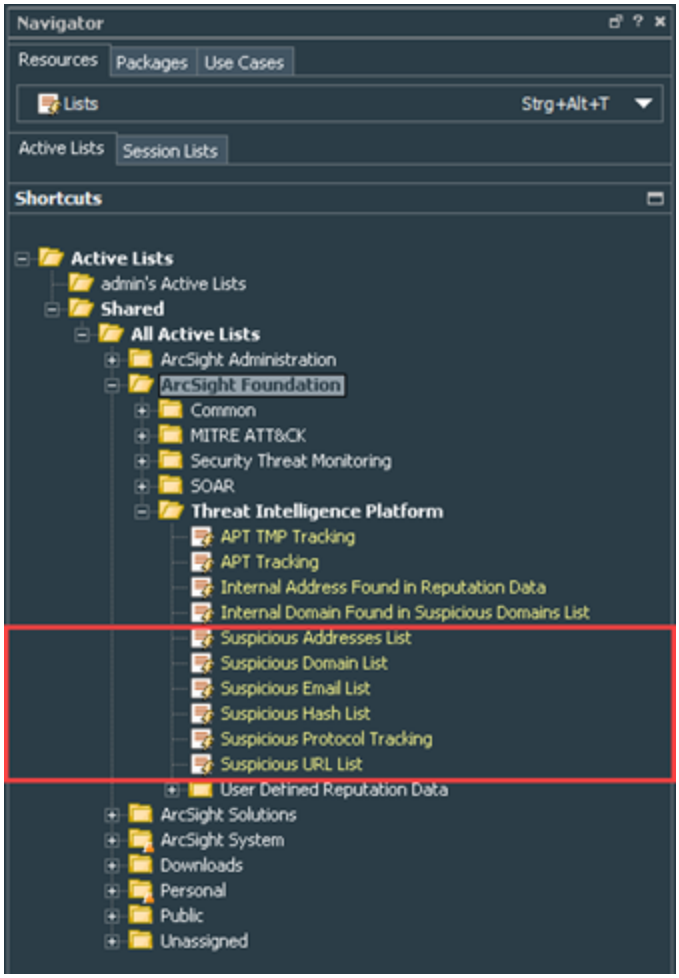
The CyberRes Galaxy Threat Acceleration Program Model Import Connector retrieves threat intelligence events and attribute data and uploads it to ESM Active Lists found under **All Active Lists > ArcSight Foundation > Threat Intelligence Platform**. These entries include, IP addresses, domain names, email addresses, hash values, and URLs.

Galaxy High-Level Architecture



Event Flow Explained

- Galaxy Model Import Connector consumes up-to-date Threat Intelligence from the server, converting to ArcSight observables (in 5 x Active Lists).
  - Suspicious Addresses List
  - Suspicious Domain List
  - Suspicious Email List
  - Suspicious Hash List
  - Suspicious URL List



- ArcSight ESM utilizes Default Content 3.6, to auto-correlate on "High confidence" alerts. The `high confidence` tag is added to description field in the 5 Active Lists, and more attack types are added to `indicatorType` field in order to trigger specific rules (for example phishing attack).

GTAP Connector Installation Options

CyberRes Galaxy Threat Acceleration Program Model Import Connector provides the following three options, as to which threat intelligence feed to synchronize with:

- **CyberRes Galaxy Threat Acceleration Program Plus:**This option is subscription based and unlocks the premium threat intelligence feed for ArcSight ESM customers. This feed is curated by the CyberRes Threat Intel Research Team and it is hosted on the GTAP server **threatfeed.cyberres.com**. This feed is mostly comprised of "zero false positive, high fidelity indicators of compromise" that correlate with the most critical cyber security threats an organization needs to identify and resolve at the highest urgency level.

  This option requires a valid subscription key, to connect to the threat feed server. This subscription key is delivered to all GTAP Plus customers who have purchased 1, 2, or 3-year subscriptions to the GTAP Plus solution. It is compatible with the default content updates packages that are periodically released.

  - As this option requires a connection to GTAP Threat Feed Server, the following firewall port should be opened one-way, from the GTAP Connector host, to the GTAP Threat Intelligence server as follows:

  Protocol/port: TCP port 443

  from: the host machine hosting/running the GTAP Model Import Connector

  to: threatfeed.cyberres.com
- **CyberRes Galaxy Threat Acceleration Program Basic:** All ArcSight ESM customers are entitled to use the GTAP Basic solution free of charge. This option does not require any key. The threat intelligence received is the OSINT (Open Source Intelligence), filtered on `TLP:WHITE` as provided by the public instance of CIRCL MISP TI feed.
  - As this option requires a connection to GTAP Threat Feed Server, the following firewall port must be opened one-way, from the GTAP Model Import Connector host, to the GTAP Threat Intel Server as follows:

    Protocol/port: TCP port 443

    from: the host machine hosting/running the GTAP Model Import Connector

    to: threatfeed.cyberres.com
- **Custom MISP Instance:** This option can be used if you already use a public or private instance of a MISP server as per the needs of your organization. This option does not require a subscription to CyberRes Galaxy solution. However, you must have the authorization key - also known as the MISP API key - for the public or private instance of the MISP server you are connecting to.

Note to Existing ArcSight MISP Connector Users: The CyberRes Galaxy Threat Acceleration Program Model Import Connector is an enhanced version of the previously released ArcSight Model Import Connector for MISP (Open Source Threat Intelligence and Sharing Platform Solution). As upgrading from the Model Import Connector for MISP to GTAP Model Import Connector is not supported, existing users can do a fresh installation of the GTAP Model Import Connector.

Obtaining License Keys

To purchase this pack, contact your account or sales representative.

After you purchase this pack, you can download the package from the Software Licenses and Downloads (SLD) portal.

Log in to the portal using your active service contract ID.

Overview of GTAP Active Lists

The following active lists are being used by GTAP Basic and GTAP Plus:

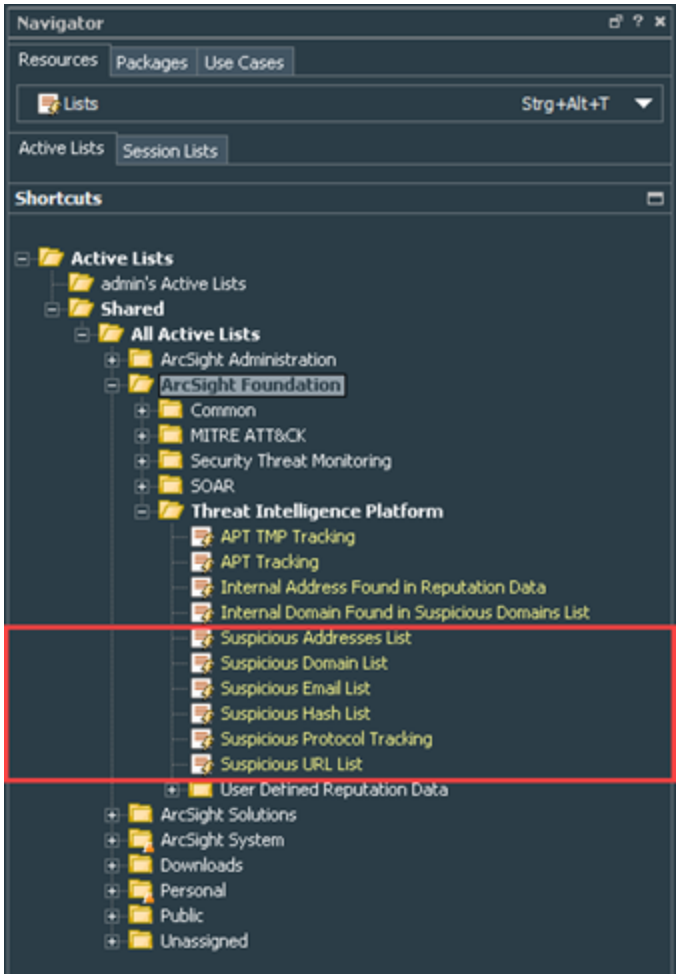
- Suspicious Addresses List
- Suspicious Domain List
- Suspicious Email List
- Suspicious Hash List
- Suspicious URL List

You can adjust the maximum capacity of active lists through manager properties, however, it is not required as per the date of this documents writing.

Note, that GTAP Basic and GTAP Plus use the same active lists.

Locating GTAP Active Lists

ESM Active Lists are located in **All Active Lists** > **ArcSight Foundation** >**Threat Intelligence Platform** folder.



Understanding GTAP Active Lists

Active list entries include, IP addresses, domain names, email addresses, hash values, and URLs.

List	Type of Information	Works With (Example)
Suspicious Addresses	IP Addresses	Proxies, Firewalls, Flows, DNS, EDR
Suspicious Domains	Domain Names	Proxies, Firewalls, EDR, DNS
Suspicious Emails	Email Addresses	E-Mail Gateway, Mail Servers
Suspicious Hashes	Hash Values (various algorithms)	EDR, AV
Suspicious URLs	Full URL being requested	Proxies, Firewalls, EDR

Fields in Active Lists for GTAP Plus

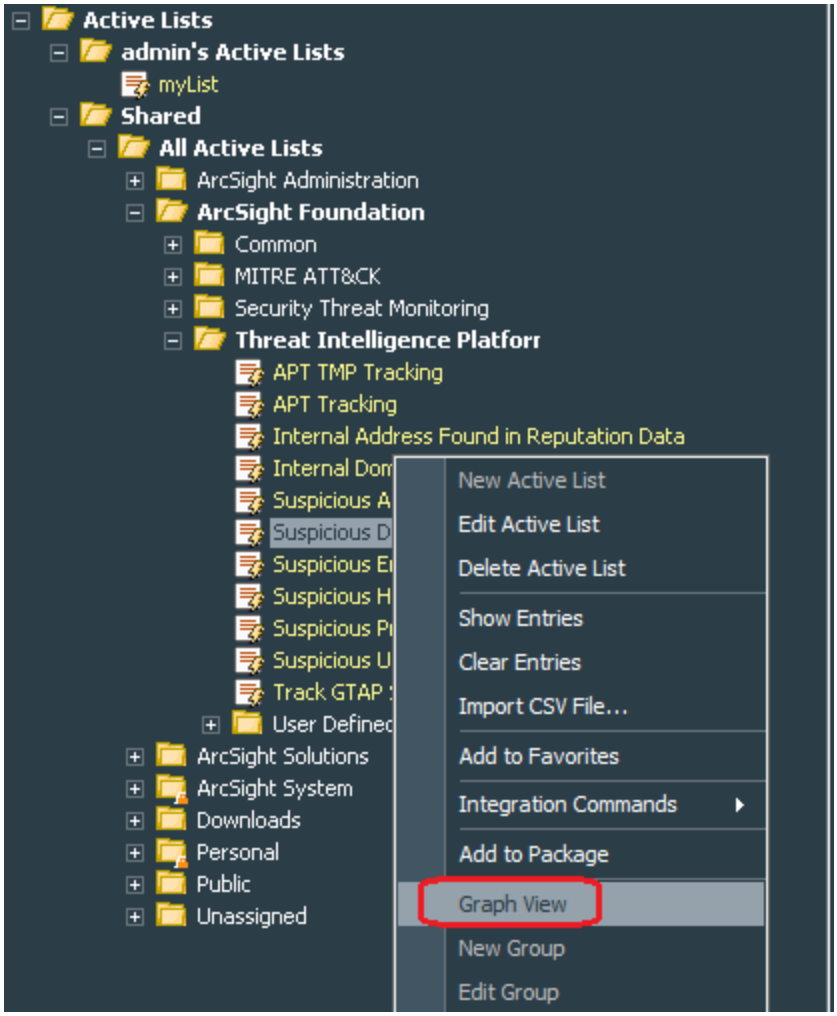
If you subscribe to GTAP Plus, the active lists contain the following fields to ensure that the Plus customers get exclusive premium content to help them quickly identify positive threats:

Active List Fields	Description
address or domain or email or url or hashValue	The suspicious address, domain, email, URL or hashValue found and shared as harmful indicators.
indicatorType	One or more publicly known malware types that are associated with this indicator.
actors	A threat actor is an individual or group involved in malicious cyber activity. This field lists one or more threat actors that are associated with this indicator.
origin	The organization that created the indicator.
cve	A unique and common identifier for a publicly known security vulnerability that is associated with the indicator. When more than one value exists, they are separated by a comma.
virusTotalCount	The number of reliable review committees who consider this indicator harmful.
malwareName	One or more malware names associated with the indicator.
confidence	The confidence level of theindicator. The values for confidence level are: very high, high, medium, and low values.

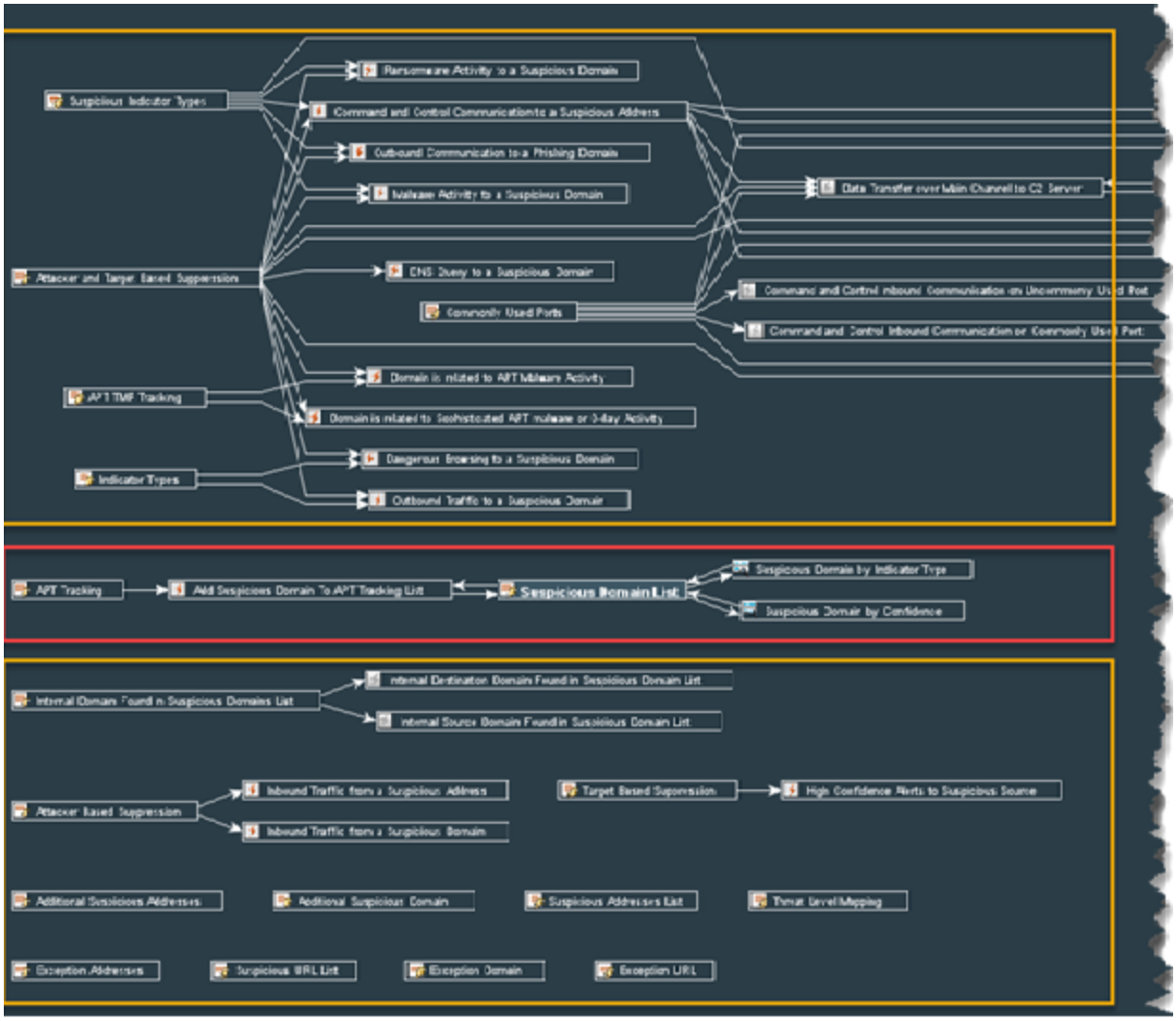
Active List Fields	Description
cyDNA	The Cyber DNA string that relates to the specific ArcSight ESM solution content for the indicator.
galaxyOnlineID	The bulletin identifier that references the bulletin record at https://cyberresgalaxy.com.
avSignatureName	One or more virus signatures that were used to detect malware associated with the indicator.
tiEventID	The unique identifier of the event to avoid collisions between events and attributes across MISP servers.

Understanding How Content Leverages GTAP Active Lists

Various content elements use the lists indirectly. You can generate a graph view of a particular list to understand its indirect usage.



This would look like the following, where YELLOW indicates indirect usage and RED indicates direct usage:



Installing and Configuring the Connector

The following sections provide the steps to install and configure the Connector. It is recommended not to install the Connector on the same machine as ESM.

If you have ArcSight subscription, then select either **CyberRes Galaxy Threat Acceleration Program Plus** or **CyberRes Galaxy Threat Acceleration Program Basic**. However, GTAP Plus is a subscription based license. Before you proceed with this option, make sure that you have purchased the license and have the API key details.

If you have already have an MISP license and want to continue with that, then use the **Custom MISP Instance** option.

Note: Use a non-root account to install the Connector.

Preparing to Install the Connector

Before installing the connector, verify that **ESM** and **Console** have already been installed correctly.

For complete product information, refer to the Administrator's Guide to ArcSight Platform guide, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the ArcSight Management Center Administrator's Guide for instructions.

Note: If you are an existing user who have been using the **CyberRes Galaxy Threat Acceleration Basic** version, and want to upgrade to the **CyberRes Galaxy Threat Acceleration Plus** version, then you must purchase the license, get the valid API Key, and reinstall the connector using the Configuring parameters for CyberRes Galaxy Threat Acceleration Plus option.

Important: It is recommended to clear the data in the Active List.

Before installing the Connector, ensure that you have the following:

- Local access to the machine where you want to install the Connector.
- Additional 2GB memory if the connector is running in a standalone mode.
- Local administrator access to the machine on which the connector will be installed.
- Refer to the Technical Requirements Guide for supported platforms.
- The machine, on which the connector will be installed, has external access over the Internet to any system over port 443 and connectivity to the ESM machine over port 8443 (default) or the configured port if the default was not used.
- ESM IP address, port, administrator user name, and password.
- The Threat Intelligence Platform package, in **All Packages > ArcSight Foundation > Threat Intelligence Platform** is installed.
- If you had installed the ArcSight Model Import Connector for MISP on the machine before, then clear the Active Lists before proceeding to install the CyberRes Galaxy Threat Acceleration Program Connector.

Downloading the Custom MISP Instance Certificate

Note: This step is only applicable for the CyberRes Galaxy Threat Acceleration Custom option and not for the other two options.

You must export the MISP instance certificate from the browser as a DER encoded binary x.509 (.CER) file.

To export the MISP instance certificate:

1. **Open a browser** and **Enter the URL of the MISP** server instance.
2. **Specify** the email and password.
3. Click the **Lock** symbol in the browser next to where you have entered the URL.
4. Click **Connection is Secure**.
5. Click **Certificate is valid** to download and **Save** the certificate.

   Note: It displays the date and validity of the certificate, which is for one year.
6. Navigate to **Details**, then click **Copy to file** by clicking the option to save it in your local.
7. Click **Next**, in the certificate export wizard.
8. The **x.CER** format is automatically selected. Click **Next**.
9. Add the **File Name** and the **Path** where you want to download the certificate.
10. Click **Save**.
11. Click **Finish**.
12. Click **OK** to successfully export the certificate.

Installing and Configuring GTAP Plus

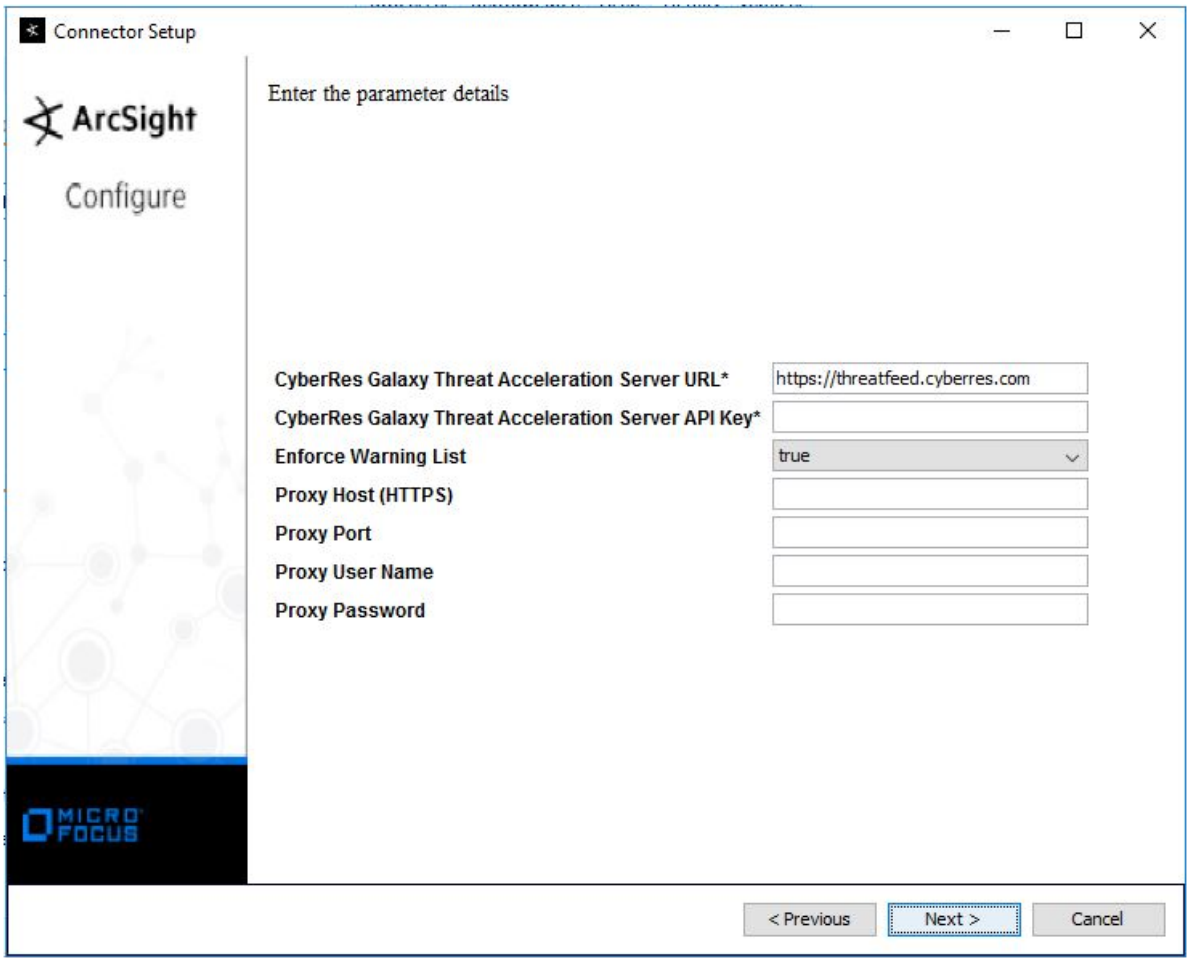
This is a subscription based service. Before you proceed with this option, make sure that you have purchased the license and have the API key details.

Follow the instructions in the wizard to install the core software.

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. (Conditional) If you exit out of the installation wizard after the installation of core software, then use the runagentsetup file in the *./current/bin/* to proceed with the connector installation.
4. Specify the relevant Global Parameters, when prompted.

   Note: Make sure that the FIPS Mode configuration matches with the FIPS mode configuration in the ESM application. For example, if the FIPS mode is enable in ESM, then FIPS mode must be enable in Connectors as well.
5. Select **Galaxy Threat Acceleration Program Model ImportConnector** and click **Next**.
6. Select the **CyberRes Galaxy Threat Acceleration Program Plus** option.

7. Specify the following details:



Parameter Name	Description
CyberRes Galaxy Threat Acceleration Server URL	Specify threatfeed.cyberres.com as the URL for the Galaxy Threat Acceleration server instance.
CyberRes Galaxy Threat Acceleration Server API Key	Specify the API Key that you received after purchasing the license.

8. Click **Next**, then proceed to complete the installation.

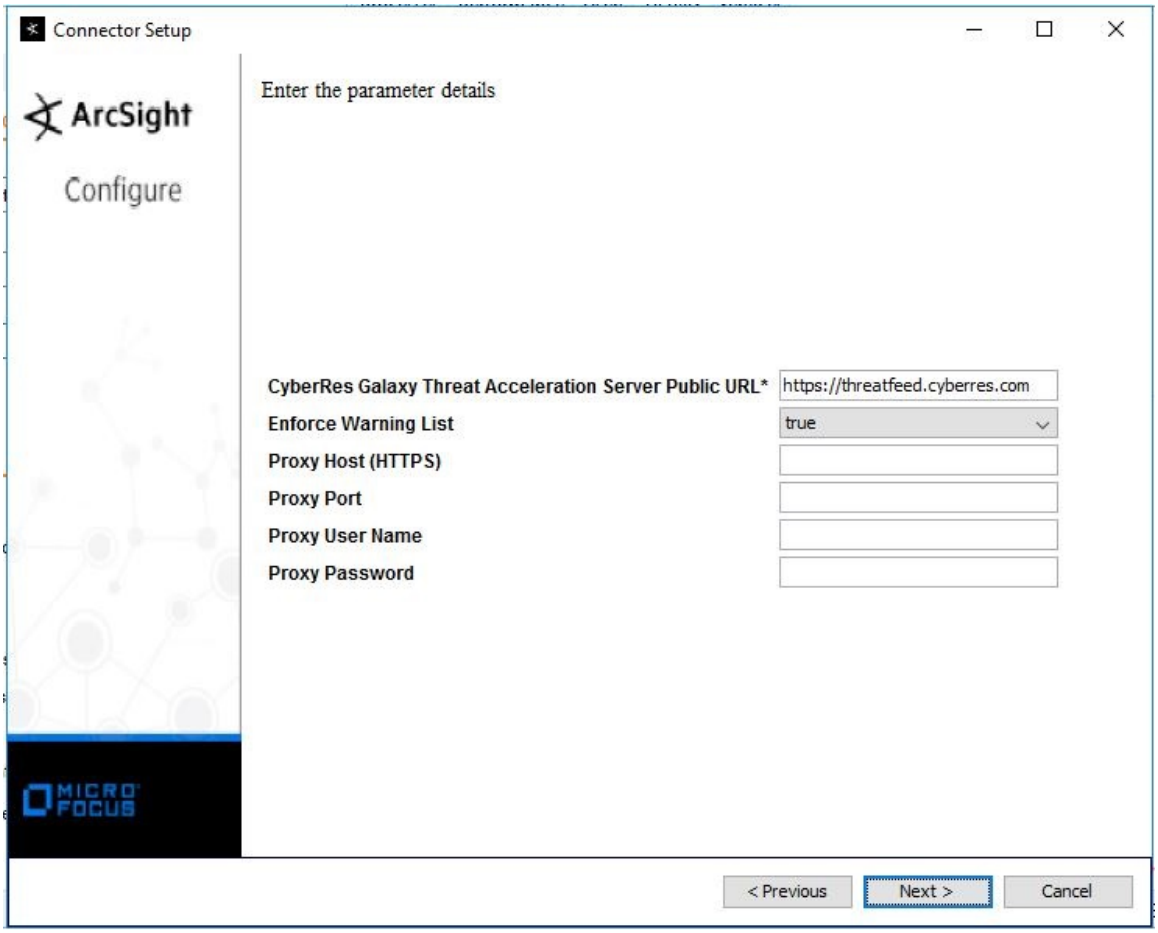
Note: If you get the error message "The parameters are invalid, Do you want to Continue", click **No**. Make sure that you have entered the correct Access Key. If you do not have a valid access key, then purchase the license and get a valid Access Key before proceeding to install CyberRes Galaxy Threat Acceleration Plus.

Installing and Configuring GTAP Basic

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. (Conditional) If you exit out of the installation wizard after the installation of core software, then use the runagentsetup file in the *./current/bin/* to proceed with the connector installation.
4. Specify the relevant Global Parameters, when prompted.

   Note: Make sure that the FIPS Mode configuration matches with the FIPS mode configuration in the ESM application. For example, if the FIPS mode is enable in ESM, then FIPS mode must be enable in Connectors as well.

5. Select **Galaxy Threat Acceleration Program SmartConnector** and click **Next**.
6. Select the **CyberRes Galaxy Threat Acceleration Program Basic** option.
7. Specify the following details:



Parameter Name	Description
CyberRes Galaxy Threat Server Public URL	Specify threatfeed.cyberres.com as the URL for the Galaxy Threat Acceleration Server instance.

8. Click **Next**, then proceed to complete the installation.

Installing and Configuring GTAP Custom

You can configure only one destination per installation.

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Exit the installation wizard.
4. Import the exported certificate into the connector framework FIPS keystore, using a command similar to the following from the current directory: `./jre/bin/keytool -importcert -file /opt/certificate.cer -keystore $ARCSIGHT_HOME/current/user/agent/fips/bcfips_ks -storepass changeit -storetype BCFKS -providername BCFIPS -providerclass`

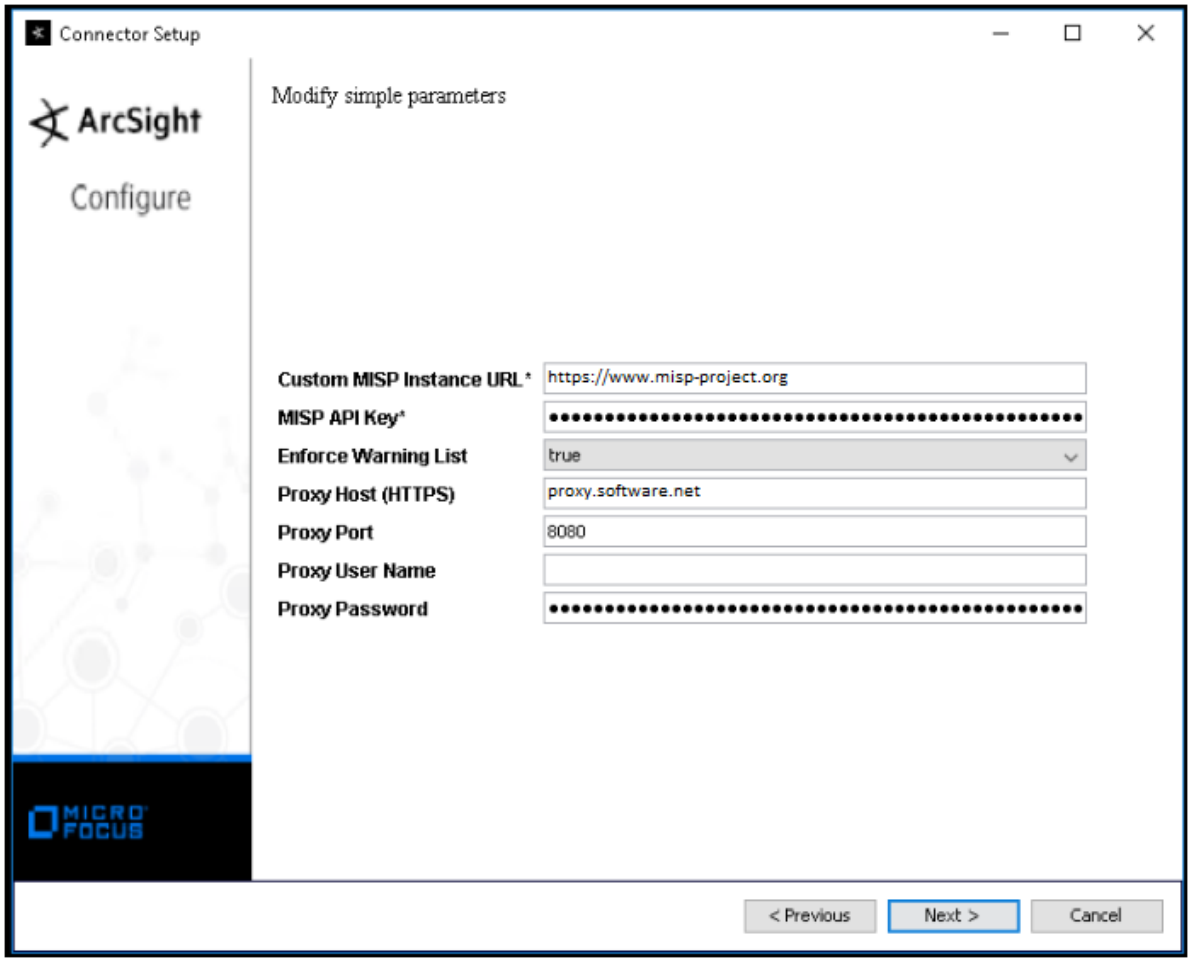
```
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$ARCSIGHT_HOME/current/lib/agent/fips/bc-fips-1.0.2.jar -J-
Djava.security.egd=file:/dev/urandom -alias mispInstance
```

Note: Specify the path to the folder where you have downloaded the certificate file.

5. Use the runagentsetup file in the *./current/bin/* to proceed with the connector installation.
6. Specify the relevant Global Parameters, when prompted.

Note: Make sure that the FIPS Mode configuration matches with the FIPS mode configuration in the ESM application. For example, if the FIPS mode is enable in ESM, then FIPS mode must be enable in Connectors as well.

7. Select **Galaxy Threat Acceleration Program SmartConnector** and click **Next**.
8. Select the **CyberRes Galaxy Threat Acceleration Custom** option.
9. Specify the following details:



Parameter Name	Description
Custom MISP Instance URL	Specify the URL for your MISP instance.
MISP API Key	Specify the API Key for your MISP instance.

10. Click **Next**, then proceed to complete the installation.

Completing Installation

1. Select **ArcSight Manager (Encrypted)**, then click **Next**.
2. Specify the following destination parameters:

Parameter Name	Description
Manager Hostname	Enter the hostname for Manager.
Manager Port	Enter **8443**.
User	Enter the user name
Password	Enter the password for the user.

3. Click **Next** and enter a **Name** for the connector and a description.
4. Click **Next.**
5. Review the **Add connector Summary** and click **Next**.
6. Select either **Install as a service or Leave as a standalone application as the mode to run the connector** and click **Next**.
7. Increase the Java Heap size.
8. Set up the user in ESM.
9. Start the data import.
10. (Optional) If you have installed the connector in the standalone mode, then run the connector manually.

Increasing the Java Heap Size

You can increase the java heap memory for the connector by doing the following:

- If you are running the connector as a **Windows service or Linux daemon**, open the *~../current/user/agent/agent.wrapper.conf* file and set the heap size as follows:

```
#Initial Java Heap Size (in MB)
```

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

```
#Maximum Java Heap Size (in MB)
```

```
wrapper.java.maxmemory=4096
```

- If you are running the connector in a **Standalone mode**:
  - **Linux:** Create an executable shell script *~/ARCSIGHT_HOME/current/user/agent/setmem.sh*, with the following content:

    ```
    ARCSIGHT_MEMORY_OPTIONS=" -Xms1024m -Xmx4096m"
    ```

  - **Windows:** Create the batch file *$ARCSIGHT_HOME\current\user\agent\setmem.bat* with the following content:

    ```
    SET ARCSIGHT_MEMORY_OPTIONS=" -Xms1024m -Xmx4096m"
    ```

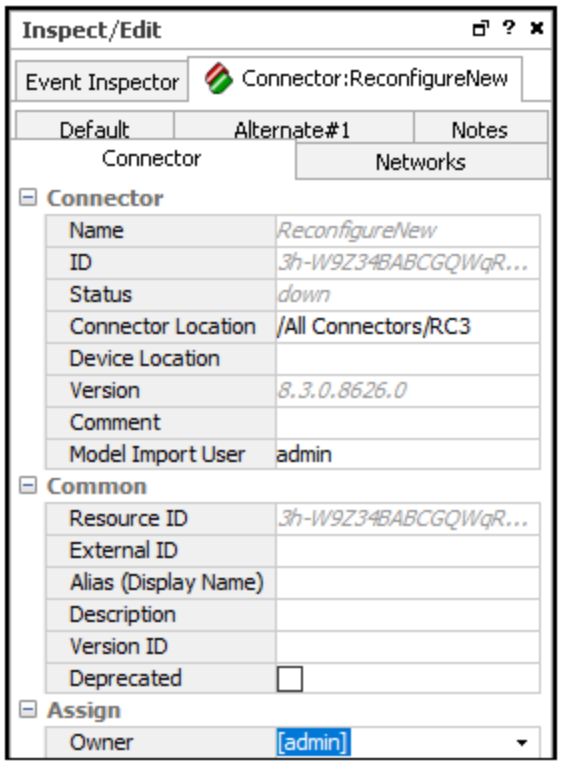
To verify if the connectors are running, select the ArcSight **Console Navigator** in the **Resources** tab, under **Connectors**. If the connector is running, you will see <connector_name> (running) listed. For more information, see Running Connectors.

Setting Up the User in ESM

After installing, configuring, and starting the connector, you must set the user for the connector from the ArcSight Console. Setting the user links the user to the resources, and that user is then treated as the **Creator** of resources. The connector is then run on that user's behalf.

Note: The user must have console administrative privileges. Else, the import fails.

1. From the ArcSight Console, go to the **Navigator** > **Resources** tab.
2. From **All Connectors**, navigate to your **Galaxy Threat Acceleration Program Connector**.
3. Right-click on the connector and select **Configure**.
4. On the **Inspect/Edit** panel, select the **Connector** tab.
5. Enter **Model Import User** as **Admin** and **Owner** as **Admin**.



6. Click **Apply**/ **OK**.

Starting and Stopping Data Import

By default the connector's data import capability is not started. You must start the import manually in the ArcSight Console.

Note: Data import needs to be started only once from the ArcSight Console. Unless it is stopped from the ArcSight Console, there is no need to restart the data import.

To start and stop import data for the GTAP Connector:

1. Select the GTAP connector and right-click.
2. Specify the following commands:
   - **To Start:** Select **Send Command > Model Import Connector > Start Import**
   - **To Stop:** Select **Send Command > Model Import Connector > Stop Import**

Configuring the Start Date

When the GTAP Model Import Connector is installed in **CyberRes Galaxy Threat Acceleration Program Plus** and **CyberRes Galaxy Threat Acceleration Program Custom** options, it starts

retrieving data from a month prior to the date of installation. However, you can configure the connector to retrieve older data as well.

To set data retrieval to a different date, modify the agent.properties as **agent(0).start.date**, then restart the connector.

For **CyberRes Galaxy Threat Acceleration Program Basic** option, after the connector is installed all the events will be downloaded.

Optimizing Data Transfer by Using a Timer

The time interval between archives sent by the connector to ESM can be controlled by the `buildmodeldelay` property. The default value is 1 minute.

To increase or decrease this time interval, you can add the `buildmodeldelay` property to the file `agent.properties` (located at `$ARCSIGHT_HOME\current\user\agent`). The property `buildmodeldelay` is expressed in milliseconds.

For example, the following property sets the time interval to 10 seconds:

```
agent.component[35].buildmodeldelay=10000
```

Running the Connectors

The Connector can be run in stand-alone mode or as a service, depending on the mode selected during installation.

Note: Before you start the Connector, make sure that ArcSight ESM is up and running.

To verify that a connector is running, you can check the **ArcSight Console Navigator** in the **Resources** tab, under **Connectors**. If the connector is running, you will see <connector_name> (running) listed.

Running in Standalone Mode

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted.

- To run all Connectors installed in stand-alone mode on a particular host, open a command window, go to the **$ARCSIGHT_HOME\current\bin** directory and run the following command:

  ```
  arcsight connectors
  ```

- To view the Connector log, read the following file:

```
$ARCSIGHT_HOME/current/logs/agent.log
```

- To stop all Connectors, enter **Ctrl+C** in the command window.

Running as a Windows Service

- To start or stop Connectors installed as services on Windows platforms:
  a. Right-click **My Computer**, then select **Manage** from the **Context** menu.
  b. Expand the **Services and Applications** folder and select **Services**.
  c. Right-click the Connector service name and select **Start** to run the Connector or **Stop** to stop the service.
- To verify that a Connector service has started, view the following file:

```
$ARCSIGHT_HOME/logs/agent.out.wrapper.log
```

- To reconfigure a Connector as a service, open a command window on $ARCSIGHT_HOME/current/bin and run the following command to start the Connector **Configuration Wizard**:

```
runagentsetup
```

Running Connectors as a UNIX Daemon

Note: When installing the connector as a Linux daemon, run the following command as root and ensure the -u parameter is a non-root user:

```
$ARCSIGHT_HOME/current/bin/arcsight agentsvc -i -u user -sn <service_name>
```

Connectors installed as a daemon can be started and stopped manually by using platform-specific procedures.

On UNIX systems, when you configure a Connector to run automatically, ArcSight creates a control script in the /etc/init.d directory.

- To start or stop a particular Connector, find the control script and run it with either a start or stop command parameter.

  For example:

```
/etc/init.d/arc_serviceName {start|stop}
```

- To verify that a Connector service has started, view the file:

```
$ARCSIGHT_HOME/logs/agent.out.wrapper.log
```

- To reconfigure the Connectors as a daemon, run the Connector **Configuration Wizard** again. Open a command window on *$ARCSIGHT_HOME/current/bin* and enter:

```
runagentsetup
```

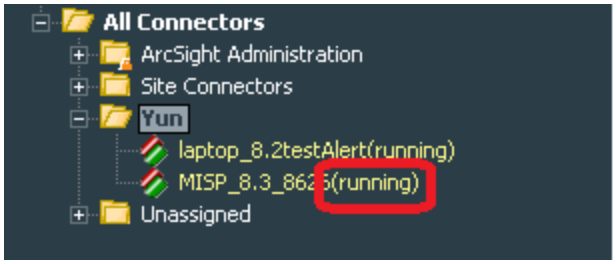
Note: By default, the connector collects events starting from a month prior to the installation day. To start retrieving older events, modify the `start.date` parameter in the `../current/user/agent/agent.properties` file. The format of the field is `YYYY-MM-DD`. The connector can only collect data up to 12 months from the date of installation. If the `start.date` set, is a period longer than 12 months, the default time of one month will be used. The MISP Instance timezone is defined in the PHP.ini file on the MISP Instance host.

Verifying the Connector Functionality

After you have installed and configured the connector, you must verify the connector functionality.

To verify:

1. Log in to the ESM Console.
2. Go to **All Connectors** > ***<installation_folder>*** > ***<connector_name>***, then verify that the status is displayed as *running*.



3. Go to **All Active Lists** > **Threat Intelligence Platform**, then right-click the following active lists and select **Show Entries** to verify if data is populated in the active lists:

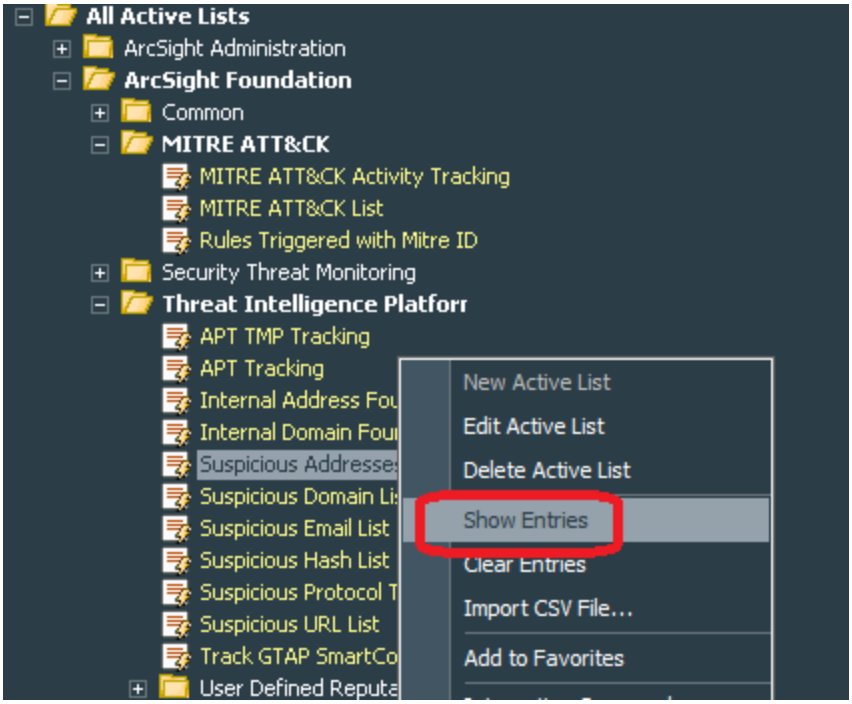
   /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Addresses List

   /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain List

   /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email List

   /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash List

   /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious URL List

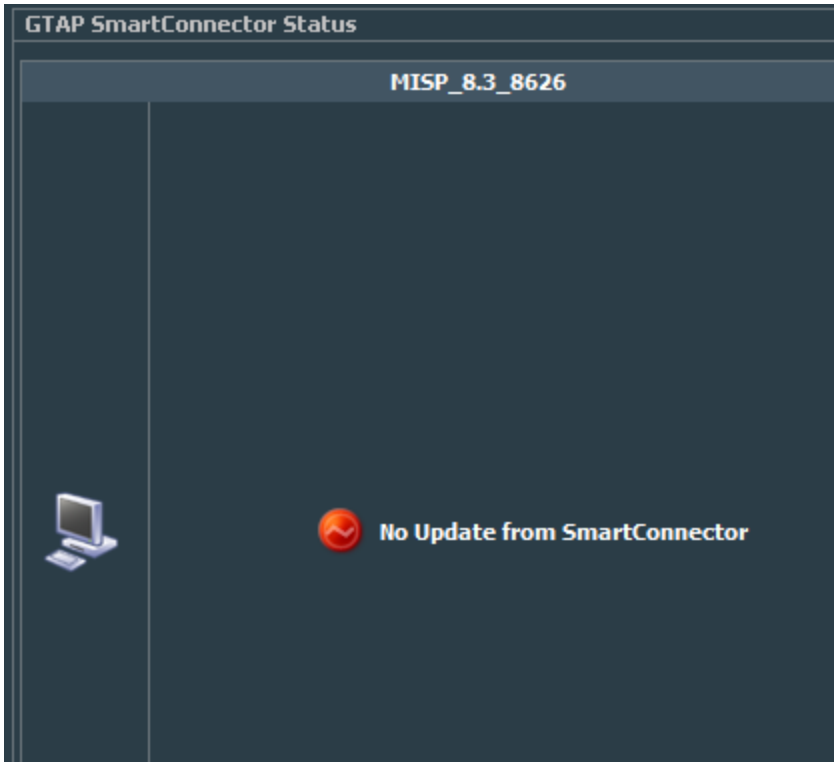


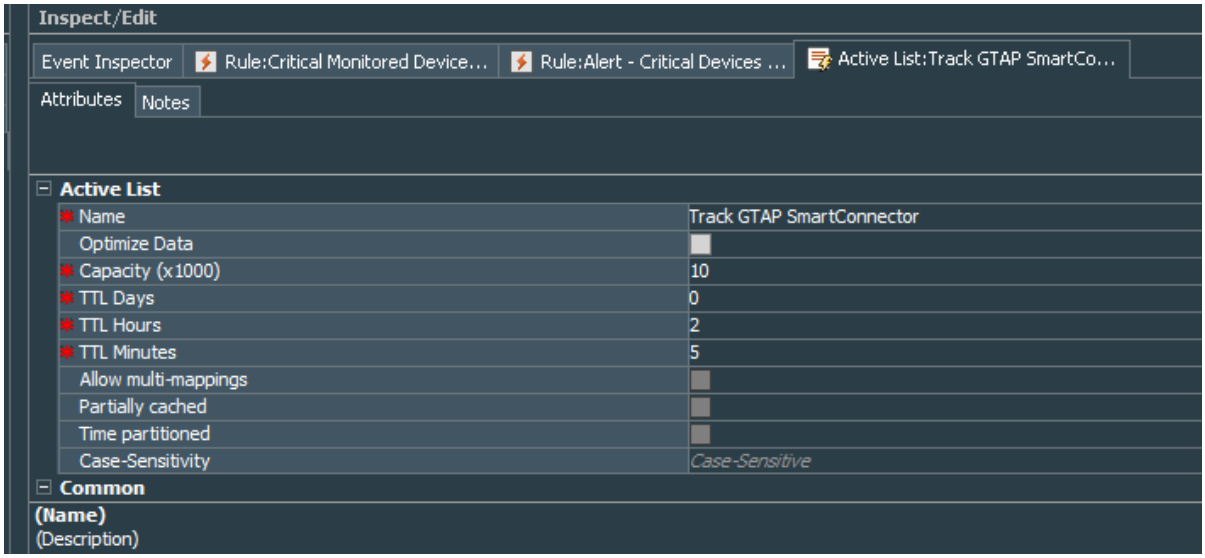
The SmartConnector requires approximately 5-15 minutes to sync data into active lists for the first time after installation.

4. To verify if the SmartConnector works properly, go to **All Dashboards** > **ArcSight Foundation** > **Threat Intelligence Platform**, then check if the GTAP SmartConnector status is green.

   If the status is red, it might indicate one of the following:

   - ESM has received an error message from the SmartConnector.
   - Active lists have not been updated during the time specified in the **All Active Lists** > **ArcSight Foundation** > **Threat Intelligence Platform** > **Track GTAP SmartConnector** > **TTL Hours** field. By default, this value is set to 2 hours.



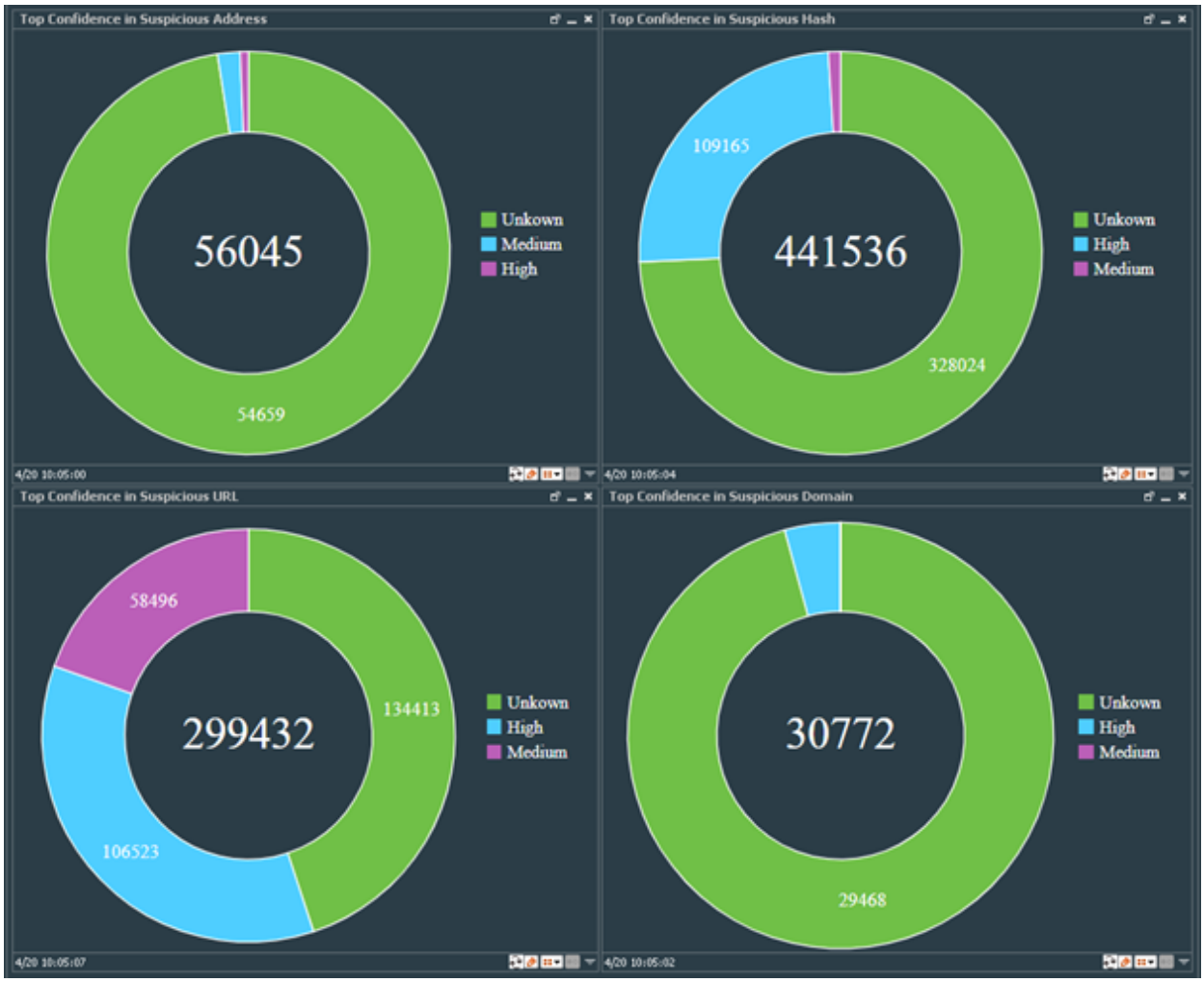


Identifying Basic and Plus Content When GTAP Plus Connector is Installed

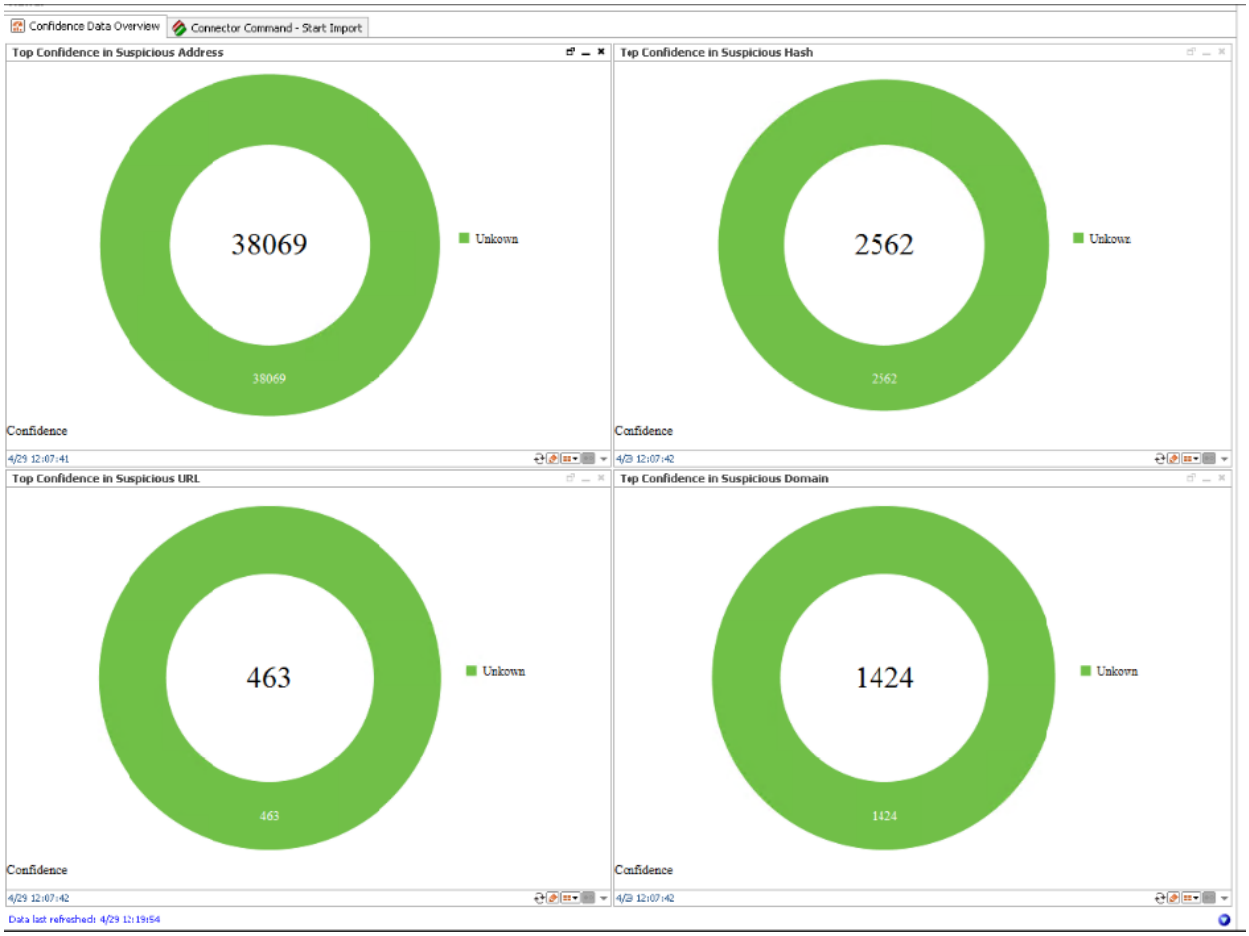
GTAP Basic SmartConnector displays the confidence of threat intelligence feed as "Unknown" whereas the GTAP Plus SmartConnector displays *High/Medium/Low* confidence data for threat intelligence feed so that organizations can identify and resolve threat at the highest urgency level.

To view the threat intelligence feed, go to **All Dashboards** > **ArcSight Foundation** > **Threat Intelligence Platform** > **Confidence Data Overview**.

The GTAP Plus Connector dashboard displays *High/Medium/Low* confidence as shown in the following image:



The Connector dashboard displays *Unknown* confidence, as shown in the following image:



Troubleshooting

This section has the following troubleshooting topics:

Common Causes of Error

Following are some of the typical issues that might be present:

- Communication requirements between the connector and the service address are not met.

  Check for network connectivity and verify if the GTAP Model Import Connector is able to reach the GTAP Server or if the GTAP Model Import Connector is able to connect to the ESM server.
- Model import user is not properly set on ESM. For more information, see Setting the Model Import user on ESM.
- Data import did not start. For more information, see Starting and Stopping Data Import.

- Content pack for “Threat Intelligence Platform” is not installed on ESM. For more information about installing the Threat Intelligence Platform content pack, see ArcSight Marketplace.
- Lower number of records as expected due to the default sync time span of one month.

  Wait until data import has been completed, which might take up to an hour. Check if you have set the "time period" through agent.properties file to a custom, very short time frame.

Errors Specific to GTAP Plus, Basic and Custom MISP versions

Some of the errors that might appear for GTAP Basic, Plus and Custom MISP instance are:

GTAP Plus and Custom MISP

License Key Entered Is Invalid

The following error messages indicate that the license key entered is invalid:

In *$ARCSIGHT_HOME/current/logs/agent.log:*

```
[ERROR] [verifyParameters] Unable to connect to Galaxy Threat Acceleration
Server instance. <Additional data>
```

In *$ARCSIGHT_HOME/current/logs/agentsetup.log*:

```
Unable to connect to Galaxy Threat Acceleration Server instance. Please
provide valid information and try again.
```

Workaround: Verify that the license key that you have entered is valid.

Unable to Retrieve Events

The following error messages might be displayed for both Plus or Custom MISP instances of Model Import Connector in the *agent.log* file in the *$ARCSIGHT_HOME/current/logs* folder:

```
[ERROR] [retrieveEvents] Unable to retrieve response due to <cause>
```

```
[ERROR] [retrieveEvents] <with additional information>
```

Workaround: Check the network connectivity or look for authentication issues. If the Connector is unable to reach the GTAP server, try restarting the server.

GTAP Basic

Following error message might be displayed for the GTAP Model Import Connector in the *agent.log* file in the *$ARCSIGHT_HOME/current/logs* folder.

`[ERROR] [processGTAPEvents] <with additional information>`

Workaround: Check the network connectivity or look for authentication issues. If the Connector is unable to reach the GTAP server, try restarting the server.

In the ESM Console

In ESM Console, look for the connector events "Data received" and "Data processed" Count=<count>" in Message field.

For GTAP Basic version, you must see this event every 60 minutes and for GTAP Plus and Custom MISP, you must see this every 15 minutes. If you do not see this event, then it indicates that the Connector is not working properly.

Workaround: Check the network connectivity or look for authentication issues. If the Connector is unable to reach the GTAP server, try restarting the server.

Connector is unable to receive any events if the /user/ agent/ agentdata folder contains cache

If you had installed MISP Model Import Connector version 8.2, and installed CyberRes Galaxy Threat Model Import Connector on the same machine with the **CyberRes Galaxy Threat Acceleration Plus** option, the connector is unable to send any content to destination after the installation completes.

Workaround: Clear cache from the user/ agent/ agentdata folder, then restart the connector. The connector will now be able to send events to destination.

Invalid Parameters Error During GTAP Plus Installation

You might get the error message "`The parameters are invalid. Do you want to Continue`, while installing the GTAP Plus version.

Workaround: Click **No** to exit installation. Verify that the API key you have entered is correct. If you do not have a valid API key, then purchase the license and get a valid API Key before proceeding to install CyberRes Galaxy Threat Acceleration Plus.

Resetting Data Import

If you are unable to see updated data in active lists or if you suspect that the data is not loading properly, you can stop the connector, delete all the existing files and then restart the connector. The connector will then load all data from the start date set in the agent.properties file.

To reload the Connector:

1. Stop the connector, if active.
2. Remove all files:
   - **Linux:** `~/ARCSIGHT_HOME/current/user/agent/agentdata`
   - **Windows:** `$\ARCSIGHT_HOME\current\user\agent\agentdata`
3. In the ArcSight Console, clear all entries in the **Suspicious Domain List**, **Suspicious Email List**, **Suspicious Hash List** and **Suspicious URL List**. For each Active List:
   a. Under **Threat Intelligence Platform**, select the, **Suspicious Domain List**, **Suspicious Addresses List**, **Suspicious Email List**, **Suspicious Hash List** and/ or the **Suspicious URL List** and right-click.
   b. Select **Clear Entries**.
4. Restart the connector.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Administration Guide for GTAP 1.0 (Model Import Connector 1.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!