Micro Focus Security ArcSight SmartConnector

Software Version: 1.0

Configuration Guide for CyberRes Galaxy Threat Intelligence Program SmartConnector

Document Release Date: March 2022
Software Release Date: March 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

Configuration Guide for CyberRes Galaxy Threat Acceleration Program 1.0 SmartConnector

This guide describes the steps to install the CyberRes Galaxy Threat Acceleration Program SmartConnector 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 ArcSight SmartConnectors.

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

CyberRes Galaxy

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.

CyberRes Galaxy Components

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

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

• **Galaxy Commercial:** Provides up-to-the-minute threat intelligence (from OSINT -open source- and CyberRes-curated premium intelligence) feed for ArcSight ESM customers.

CyberRes Galaxy Commercial (Also Known As Galaxy Threat Acceleration Program)

At a high level, Galaxy Threat Acceleration Program (GTAP) is comprised of two main components.

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 to be received is the Open Source Intelligence (OSINT), as provided by the public instance of MISP CIRCL TI feed.

GTAP Plus

- GTAP Plus offers the same features of "GTAP Basic" as above.
- In addition, it also offers Premium threat intelligence feed for ArcSight ESM customers, curated by CyberRes Threat Intelligence Research Team, mostly comprised of "zero 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.

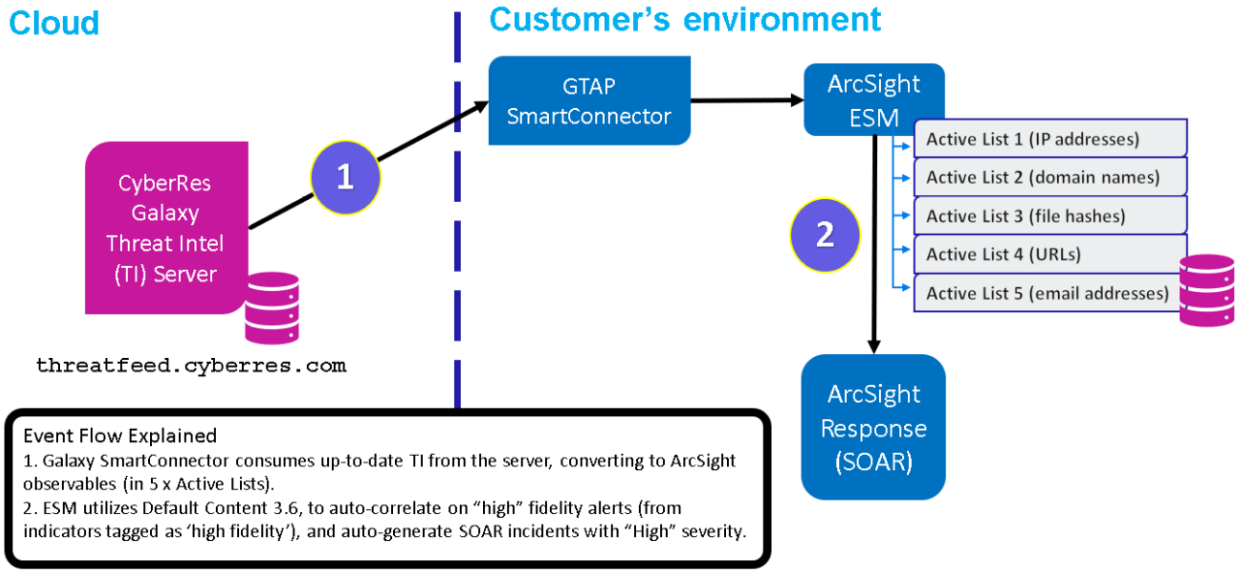
CyberRes Galaxy Threat Acceleration Program SmartConnector

As can be seen from the diagram below, GTAP SmartConnector connects the ArcSight ecosystem* to the CyberRes Galaxy Threat Feed server, synchronizing the data multiple times daily.

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.

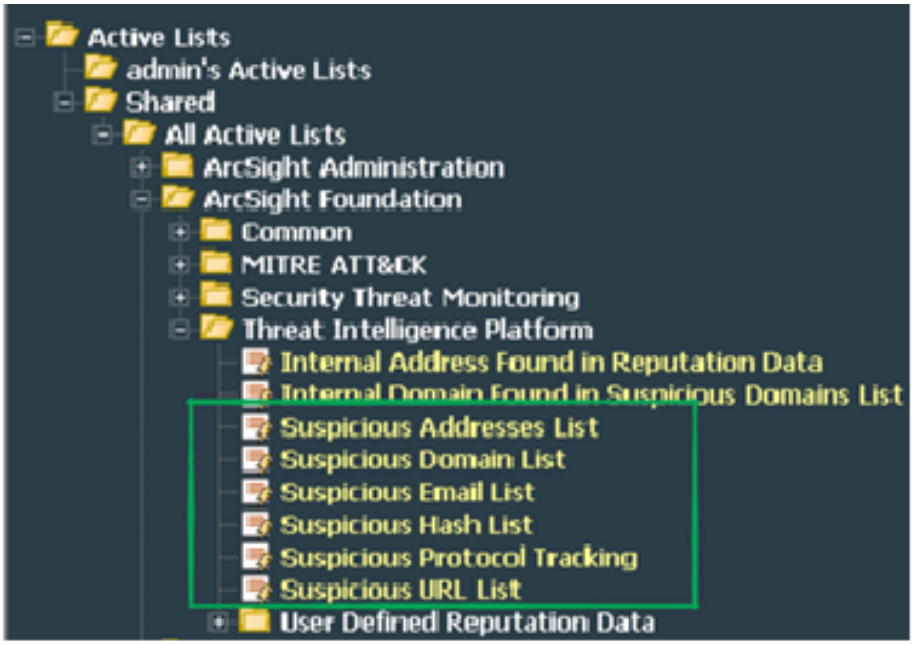
The CyberRes Galaxy Threat Acceleration Program SmartConnector retrieves threat intelligence events and attribute data and uploads it to ESM Active Lists found under /All Active Lists/ ArcSight Foundation/ Threat Intelligence Platform. These entries include, IP addresses, domain names, email addresses,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

Galaxy High-Level Architecture



Event Flow Explained

- Galaxy SmartConnector 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 ("high confidence" tag is added to description field in the 5 Active Lists above), and more attack types are added to indicatorType field as well so that more specific rules (for example phishing attack) can be triggered.

GTAP Installation Options

CyberRes Galaxy Threat Acceleration Program SmartConnector 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 SmartConnector host, to the GTAP Threat Intelligence server as follows:

Protocol/port: TCP port 443

from: the host machine hosting/running the GTAP SmartConnector

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 to be received is the OSINT (Open Source Intelligence), 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 should be opened one-way, from the GTAP SmartConnector host, to the GTAP Threat Intel Server as follows:

    Protocol/port: TCP port 443

    from: the host machine hosting/running the GTAP SmartConnector

    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 SmartConnector 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 SmartConnector is not supported, existing users can do a fresh installation of the GTAP SmartConnector.

Obtaining License Keys

To purchase this pack, please 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.

* (as of version 1.0, GTAP is only supported for ArcSight ESM customers)

Installing and Configuring the SmartConnector

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

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

Preparing to Install the SmartConnector

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 SmartConnector, ensure that you have the following:

- Local access to the machine where you want to install the SmartConnector.
- 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.

  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>
  ```

- 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 SmartConnector.

Installing the SmartConnector

To install the Connector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Exit the installation wizard.

Downloading the Certificate

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

Export the MISP Instance certificate from the browser as a DER encoded binary x.509 (.CER) file:

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.

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.

Configuring the SmartConnector

You can select one of the following options. If you have ArcSight subscription, then select either of the first two options, that is, **CyberRes Galaxy Threat Acceleration Program Plus** or **CyberRes Galaxy Threat Acceleration Program Basic**. Or if you have opted for a customized option then you can select the **Custom MISP Instance** which is the third option. The choices are:

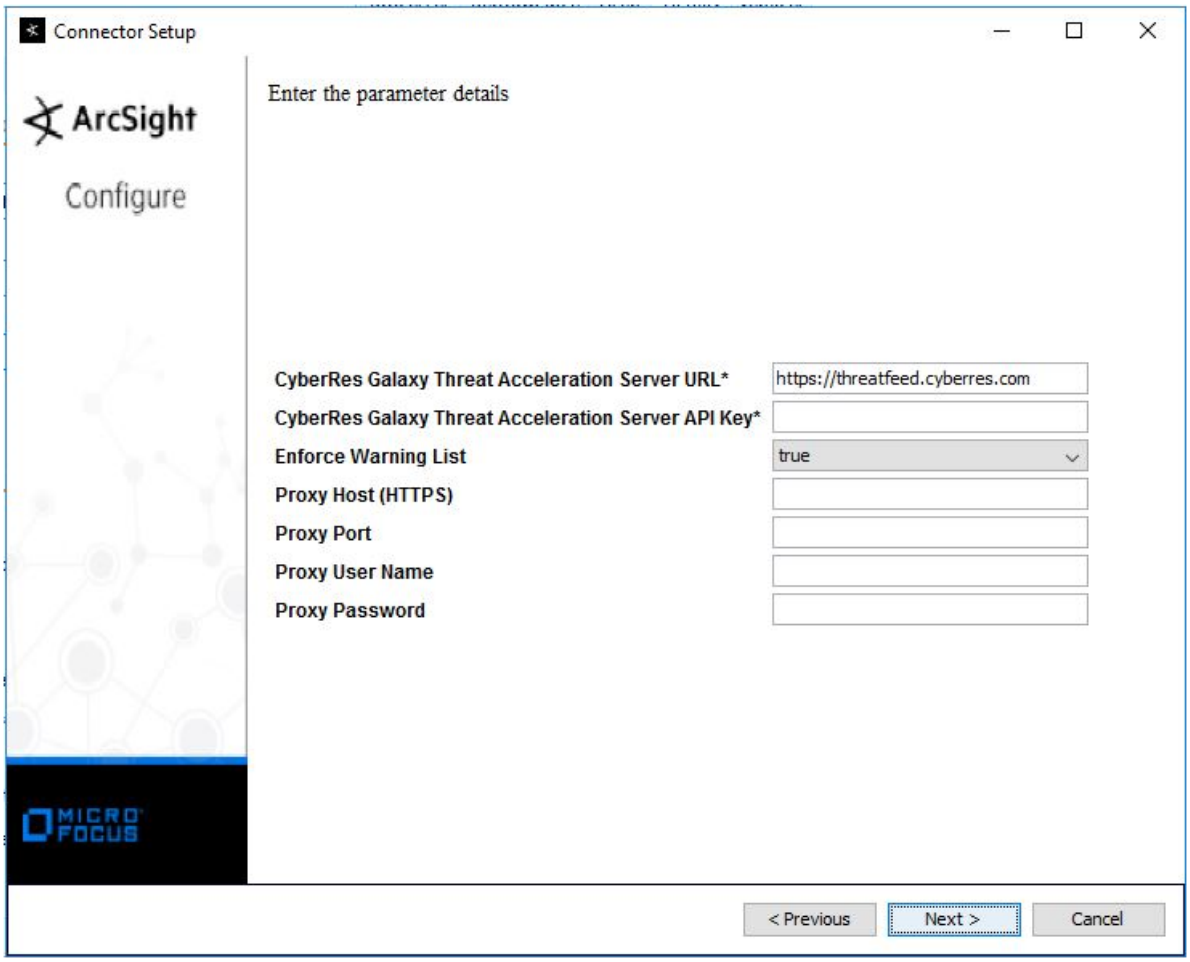
Configuring Parameters for CyberRes Galaxy Threat Acceleration Program Plus

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.

1. Use the runagentsetup file in the *./current/bin/* to proceed with the connector installation.
2. 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 SmartConnectors as well.

3. Select **Galaxy Threat Acceleration Program SmartConnector** and click **Next**.
4. Select the **CyberRes Galaxy Threat Acceleration Program Plus** option.
5. 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.
Enforce Warning List	Select **True**.
Proxy Host (HTTPS)	Specify a URL of the proxy host without https://. For example: web-proxy.am.example.net.
Proxy Port	Enter the port number for the proxy.
Proxy User Name	Enter the name of the proxy user.
Proxy Password	Enter the password of the proxy user. This value is populated when the proxy requires an authentication and if you have specified a proxy user name.

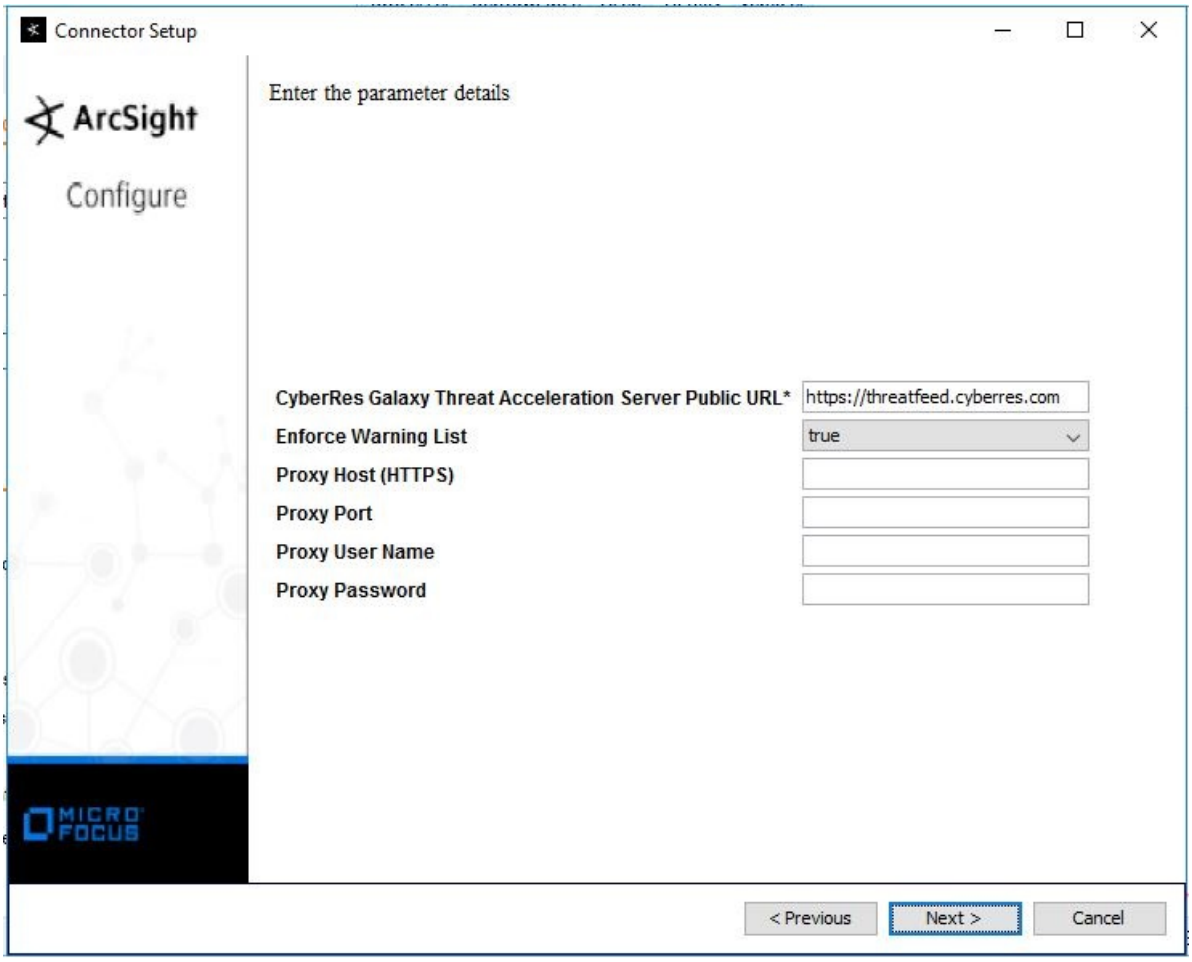
6. Click **Next**, then proceed to complete the installation.

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.

Configuring Parameters for CyberRes Galaxy Threat Acceleration Program Basic

1. Use the runagentsetup file in the *./current/bin/* to proceed with the connector installation.
2. 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 SmartConnectors as well.
3. Select **Galaxy Threat Acceleration Program SmartConnector** and click **Next**.
4. Select the **CyberRes Galaxy Threat Acceleration Program Basic** option.
5. 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.
Enforce Warning List	Select **True**.
Proxy Host (HTTPS)	Specify a URL of the proxy host without https://. For example: web-proxy.am.example.net.
Proxy Port	Enter the port number for the proxy.
Proxy User Name	Enter the name of the proxy user.
Proxy Password	Enter the password of the proxy user. This value is populated when the proxy requires an authentication and if you have specified a proxy user name.

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

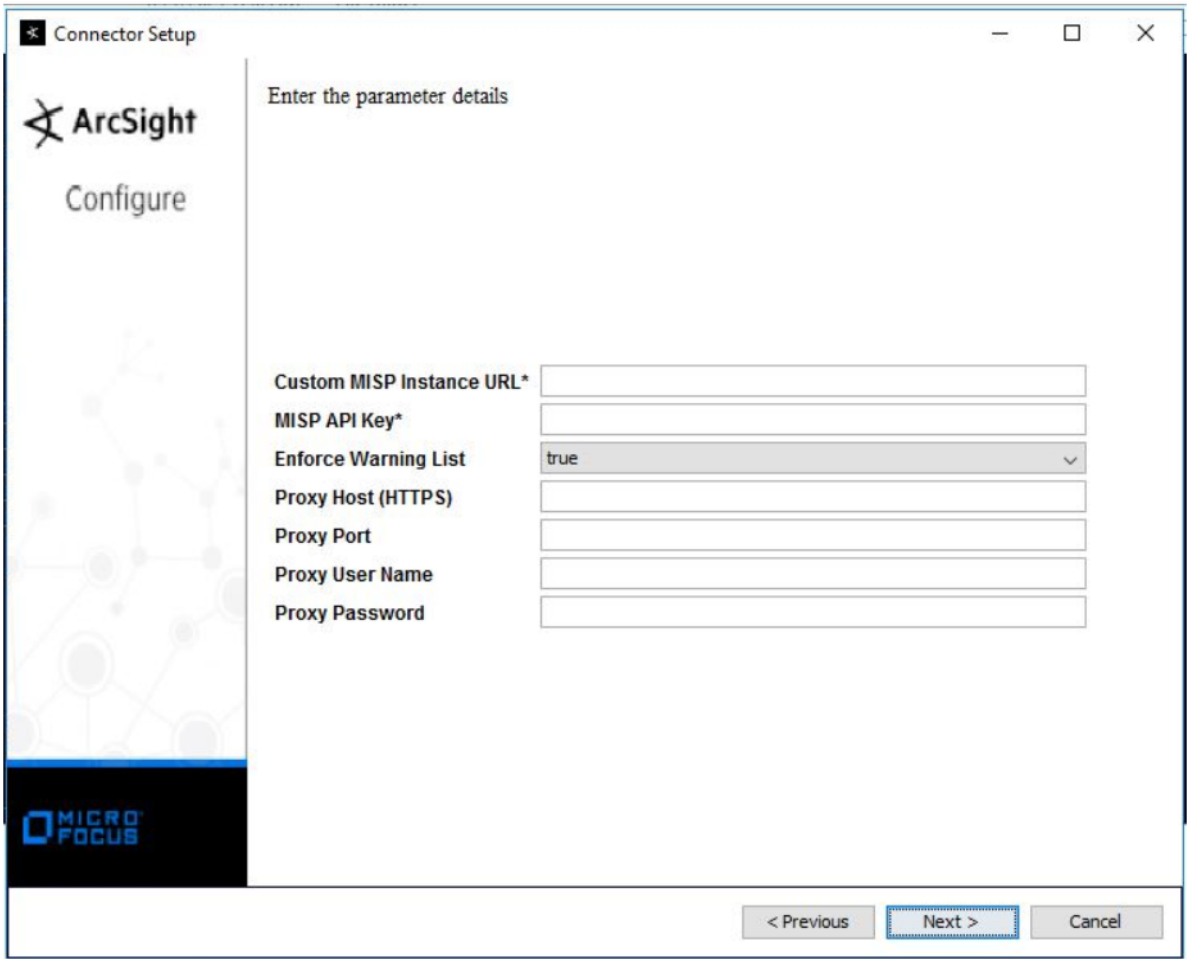
Configuring Parameters for CyberRes Galaxy Threat Acceleration Custom

You can configure only one destination per installation.

1. Use the runagentsetup file in the *./current/bin/* to proceed with the connector installation.
2. 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 SmartConnectors as well.

3. Select **Galaxy Threat Acceleration Program SmartConnector** and click **Next**.
4. Select the **CyberRes Galaxy Threat Acceleration Custom** option.
5. 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.
Enforce Warning List	Select **True** to remove warning list attributes in the result.
Proxy Host (HTTPS)	Specify a URL of the proxy host without https://. For example: web-proxy.am.example.net.
Proxy Port	Enter the port number for the proxy.
Proxy User Name	Enter the name of the proxy user.
Proxy Password	Enter the password of the proxy user. This value is populated when the proxy requires an authentication and if you have specified a proxy user name.

6. 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. Set up the user in ESM.
8. (Optional) If you have installed the connector in the GTAP Plus mode, do the following:
   a. Open the `agent.properties` file from `<install_directory>/current/user/agent/`
   b. Look for the following line:

```
agents[0].regular.confidence_
tags=mispreputationhighconfidence\=Confidence\:High,mispreputationlowco
nfidence\=Confidence\:Low,mispreputationmediumconfidence\=Confidence\:M
edium,manualoverride_mispreputationhighconfidence\=Confidence\:Very
High,manualoverride_mispreputationmediumconfidence\=Confidence\:Medium
```

   c. Append the following line:

```
,manualoverride_mispreplowconfidence\=Confidence\:Low,manualoverride_
misprepmediumconfidence\=Confidence\:Medium,manualoverride_
misprephighconfidence\=Confidence\:High
```

   For example:

```
agents[0].regular.confidence_
tags=mispreputationhighconfidence\=Confidence\:High,mispreputationlowco
nfidence\=Confidence\:Low,mispreputationmediumconfidence\=Confidence\:M
edium,manualoverride_mispreputationhighconfidence\=Confidence\:Very
High,manualoverride_
mispreputationmediumconfidence\=Confidence\:Medium,manualoverride_
mispreplowconfidence\=Confidence\:Low,manualoverride_
```

```
misprepmediumconfidence\=Confidence\:Medium,manualoverride_
misprephighconfidence\=Confidence\:High
```

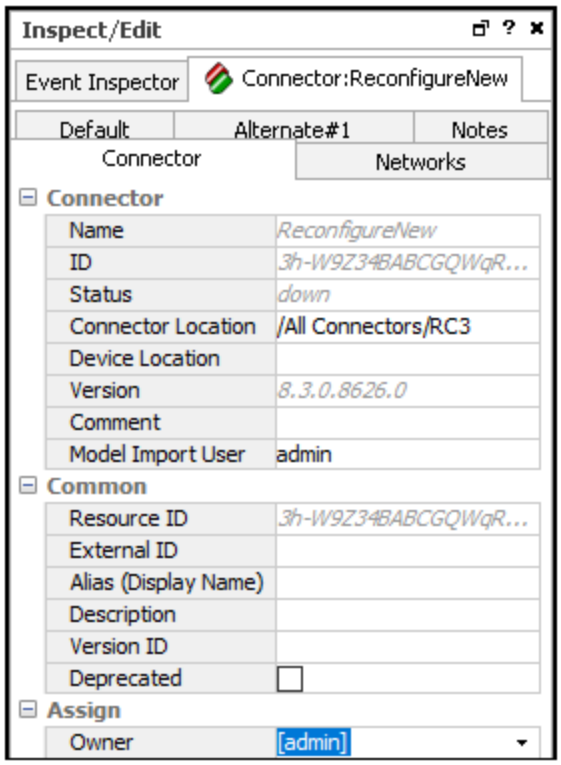
9. Start the data import.
10. Run the Connector.

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 **Micro Focus Galaxy Threat Acceleration Program SmartConnector**.
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 for the Connector for Galaxy Threat Acceleration Program SmartConnector:

1. Select the **Galaxy Threat Acceleration Program (GTAP) SmartConnector** 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

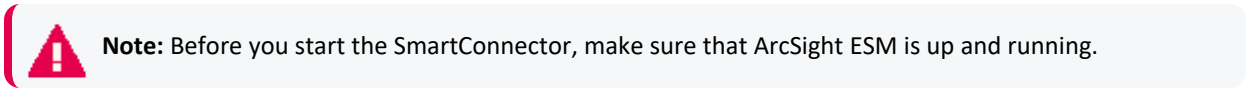
When you install the Galaxy Threat Acceleration Program SmartConnector, is installed in **CyberRes Galaxy Threat Acceleration Program Plus** and **CyberRes Galaxy Threat Acceleration Program Custom** options, it starts retrieving data from a month prior to the date of installation. However, you can configure 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.

Running the SmartConnectors

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



Note: Before you start the SmartConnector, 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 SmartConnector 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 SmartConnector log, read the following file:

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

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

Running as a Windows Service

- To start or stop SmartConnectors 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 SmartConnector service name and select **Start** to run the SmartConnector or **Stop** to stop the service.
- To verify that a SmartConnector service has started, view the following file:

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

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

  ```
  runagentsetup
  ```

Running Connectors as a UNIX Daemon

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

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

- To start or stop a particular SmartConnector, 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 SmartConnector service has started, view the file:

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

- To reconfigure SmartConnectors as a daemon, run the SmartConnector **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.

Additional Configurations

The following sections describe the additional configurations:

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.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.

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
```

Reloading the Connector for Data

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.

Troubleshooting

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 Intelligence SmartConnector 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.

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 Configuration Guide for CyberRes Galaxy Threat Intelligence Program SmartConnector (SmartConnector 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!