Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Box

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for Box

November 30, 2016

Warranty

Restricted Rights Legend

Revision History

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/15/2016	Added Connector Appliance/ArcSight Management considerations to this document from the Box Quick Guide for Connector Appliance.
02/16/2015	Updated mappings to reflect parser improvements.
05/15/2014	Initial release of this connector.

SmartConnector for Box

This guide provides information for installing the SmartConnector for Box and configuring the connector for event collection. When a user or an administrator performs an action, Box logs an event to account for that action. This connector collects that log data from Box concerning file access and management events (such as uploading or creating a folder or file) or for administrative events (such as adding a group or a user).

Product Overview

Box provides content management capabilities, including content access, sharing, and collaboration for individuals, businesses, and enterprise IT. Box lets users store content online, and this content can be accessed, managed and shared from anywhere. This connector cannot be installed in console mode. It must be installed using the setup wizard.

When a Box user or administrator performs an action, Box logs an event to account for that action. The SmartConnector for Box collects that log data from Box concerning file access and management events (such as uploading or creating a folder or file) or for administrative events (such as adding a group or a user).

Configuration

Connector Configuration for Event Collection

Have your Box login information on hand. During the configuration, you will enter your proxy hostname and proxy port. You are then redirected to Box's login page, where you will log into Box using your Box credentials. This will enable the connector to access Box log data. All events logged by Box are listed in the Platform Developers Documentation at http://developers.box.com/docs/, in the section *Get Events in an Enterprise*. The user who configures the connector must have the **Group Admin** privilege in Box or the connector will not collect events.

Connector Appliance/ArcSight Management Center Configuration

Run restutil to Obtain a Refresh Token

Before configuring the SmartConnector for Box on the Connector Appliance/ArcMC, you must obtain a refresh token. This token will be required when you configure the connector. The token enables the connector to access Box log data. To obtain a refresh token, use the REST FlexConnector Configuration Support Tool (restutil) to obtain a refresh token, as follows.

1. Install the SmartConnector package on a host machine where you can access a web browser.
2. After installing the SmartConnector package, navigate to `$ARCSIGHT_HOME\current\bin`.
3. To retrieve a refresh token, invoke the tool with token command:

   ```
   arcsight restutil boxtoken <-proxy >
   ```

   For example: `arcsight restutil boxtoken -proxy proxy.location.hp.com:8080`

4 A web browser launches and prompts you to log into Box. Enter your Box user name and password and click through to access Box.

5 The refresh token string displays in the command line window. You will copy this string into the Refresh Token field during connector configuration.

Install the SmartConnector

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

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.

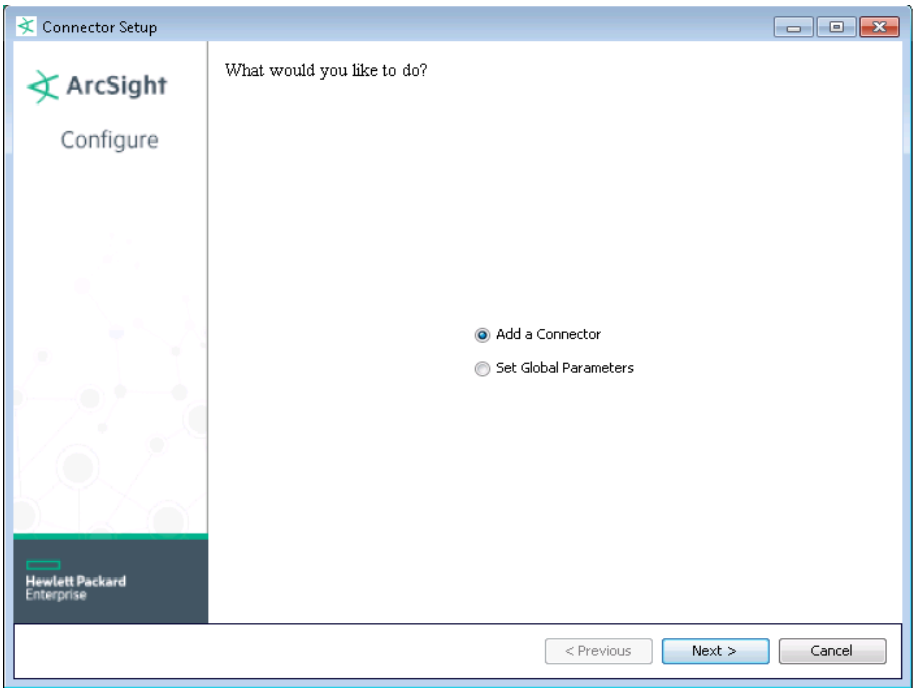
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

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'.
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'.

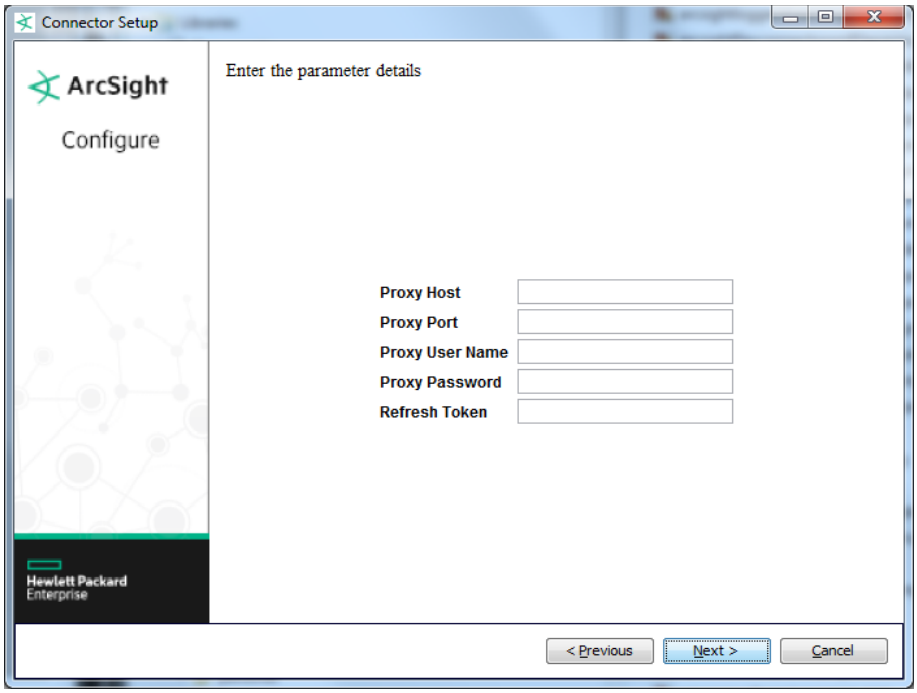
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to the "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 **Box** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Proxy Host	Enter the proxy host IP address or name. This value is required for proxy configuration in order to access Box.
Proxy Port	Enter the proxy port. This value is required for proxy configuration.
Proxy User Name	Enter the proxy user name. This value is optional for additional proxy authentication. If you specify a proxy user name, you must also specify a proxy password.
Proxy Password	Enter the password for the proxy user specified in the Proxy User Name field. This value is optional for additional proxy authentication. This field is required only if you have specified a proxy user name.
Refresh Token	Enter the refresh token; applies only to users running the SmartConnector in the Connector Appliance/ArcSight Management Center (ArcMC) environment. See the ArcSight Connector Appliance/ArcSight Management Center Administrator's Guide and "Connector Appliance/ArcSight Management Center Considerations" for more information. Other users, leave this field blank.

If you do not need a proxy to access the Internet, leave the proxy fields blank and click **Next**.

A web browser window will be launched by the connector to allow you to login to Box. You do not need to manually open the web browser to login to Box.

When the connector launches a web browser window, it attempts to use the default web browser configured for your system. If the default web browser does not launch, it will try to launch using other web browsers (Firefox, Google Chrome, Internet Explorer, Konqueror, or Mozilla). Verify that you have one of these web browsers configured on your system. Also, ensure that the proxy settings for your web browsers are configured correctly so that you can access the Internet through your web browser. The Box login opportunity expires after 10 minutes. To login, enter your Box user name and password and click through to access Box.

After you log into Box you must continue the connector configuration. The next page of the connector installation and configuration wizard displays automatically. To continue the connector configuration, be sure to return to the installation and configuration wizard window. You might have to look under the Box window to find the connector configuration window again and continue the connector configuration.

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*.

Upgrade the SmartConnector for Box (Connector Appliance/ArcMC)

To upgrade a container to the latest version of the SmartConnector for Box:

1. Upload the connector build AUP that contains the latest version of the connector.
2. In the Connector Appliance, click **Manage**.
3. Click the **Containers** tab.
4. Select the container you want to upgrade.
5. Click **Upgrade**. Click **Next** to upgrade the container.
6. Select the AUP version and click **Next**.
7. Select the container you have upgraded and then select the Action "Add New Connector".
8. Select the Box connector and click **Next**.
9. Enter the parameter values for the connector, including the Refresh Token. See the Configuration Guide for the SmartConnector for Box for details about parameters. See "Run restutil to Obtain a Refresh Token". Click **Next**.
10. Select the destination. Click **Next**.
11. Enter the destination parameters. Click **Next**.
12. Enter connector details. Click **Next**. The connector is added to the container.

Modify Advanced Parameters

You might want to modify the following advanced parameters:

- `startattime`: Enter a value for `startattime` to specify an exact timestamp from which the connector is to start processing events. The format of this timestamp should be yyyy-MM-dd'T'HH:mm:ss.SSSZ (Example: 2012-05-15T00:01:02.345-08:00). The timestamp components after yyyy-MM-dd'T'HH:mm:ss are optional. The time zone designator is Z or +hh:mm or -hh:mm. If no date is specified, all events will be processed.
- `queryfrequency`: Use to configure how frequently the connector retrieves events from Box. The default value for the `queryfrequency` parameter is 30000 ms; you can adjust this value to tune connector performance. Note that `queryfrequency` influences the number of API calls the connector makes to Box. If your Box account limits the number of API calls during a period of time, you can configure `queryfrequency` to reduce the number of API calls made by the connector. See Box administration to learn limits on API calls. The greater the `queryfrequency`, the fewer the number of API calls made by the connector over a period of time. The greater the `queryfrequency`, the fewer the number of API calls made by the connector over a period of time.
- `eventtype`: Use to specify the types of logged events retrieved can be specified. To specify the event types add `eventtype=<event type list>` to agent.properties. The <event type list> is

a comma separated list of the event types to retrieve from Box. The possible values for the <event type list> are documented at http://developers.box.com/docs in the Events section.

After SmartConnector installation, you can access the connector's parameters as follows:

1. From the `$ARCSIGHT_HOME\current\user\agent` directory open the file `agent.properties` in a pure ASCII text editor (such as Notepad++).
2. In the `agent.properties` file, locate the parameters whose values you want to modify.
3. Modify the parameters as needed.
4. Save the exited `agent.properties` file.
5. Restart the connector.

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.

Box Mappings to ArcSight Fields - JSON Parser

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	chunk_size
Device Custom String 3	next_stream_position
Device Event Class ID	eventType
Device Product	'Box.net'
Device Receipt Time	TimeStamp
Device Vendor	'Box'
External ID	eventId
File ID	One of (source_folder_id, source_item_id)
File Name	One of (source_item_name, source_folder_name)

ArcSight ESM Field	Device-Specific Field
File Type	One of (source_item_type, one of (source_folder_id, 'folder')
Name	eventType
Source Host Name	ipAddress

Mappings for Event Types NEW_USER, EDIT_USER

ArcSight ESM Field	Device-Specific Field
Destination User ID	One of (source_login, created_by_login)
Destination User Name	source_name
Device Custom Number 2	created_by_user_id
Device Custom Number 3	source_id (Created User Box ID)
Device Custom String 2	source_type
Source User ID	created_by_login
Source User Name	created_by_name

Mappings for Event Type LOGIN

ArcSight ESM Field	Device-Specific Field
Destination User ID	source_login
Destination User Name	created_by_name
Device Custom Number 2	source_id
Device Custom String 2	source type

Mappings for Event Type FAILED_LOGIN

ArcSight ESM Field	Device-Specific Field
Destination User ID	created_by_login
Destination User Name	created_by_name
Device Custom Number 2	created_by_user_id

Mappings for Event Type USER_AUTHENTICATE_OAUTH2_TOKEN

ArcSight ESM Field	Device-Specific Field
Destination User ID	source_login
Destination User Name	source_name
Device Custom Number 2	created_by_user_id
Device Custom String 1	source_id (Box User ID)
Device Custom String 2	created_by_type (Source Type)

Mappings for Event Types ADD_LOGIN_ACTIVITY_DEVICE, UPLOAD, UPLOAD_POLICY_VIOLATION, DOWNLOAD, PREVIEW, DELETE, RENAME, COMMENT_CREATE, ITEM_SYNC, SHARE, UNSHARE, SHARE_EXPIRATION

ArcSight ESM Field	Device-Specific Field
Destination User ID	created_by_login
Destination User Name	created_by_name
Device Custom Number 2	created_by_user_id

Mappings for Event Types COLLABORATION_INVITE, COLLABORATION_ACCEPT, COLLABORATION_EXPIRATION, COLLABORATION_REMOVE, COLLABORATION_ROLE_CHANGE

ArcSight ESM Field	Device-Specific Field
Destination User ID	created_by_login
Destination User Name	source_user_name
Device Custom Number 2	created_by_user_id
Device Custom Number 3	source_user_id (Collaborator User Box ID)
Source User Name	created_by_name

Troubleshooting

Box Not Accepting Credentials

If the refresh token needs to be updated, the message "Could not refresh the access token" is written to the agent.log file. In this case, update the refresh token by running `restutil`, as described in "Run restutil to Obtain a Refresh Token", and then applying the new refresh token:

1. In the Connector Appliance/ArcMC, click **Manage**.
2. Click the **Containers** tab.
3. Select the container in which the connector is running.
4. Select the connector checkbox.
5. Click **Parameters**.
6. Select **One connector at a time**.
7. On the **Update Connector Parameters** screen, delete the value for the **Refresh Token** field.
8. Copy and paste the new refresh token into the **Refresh Token** field. Obtain this token using the instructions in "Run restutil to Obtain a Refresh Token".
9. Click **Next** to apply the changes. The connector is restarted automatically.