Air Force

**Distributed Common Ground System (AF DCGS)**



IAAS-018 – ESS – ArcSight Connector to Elastic Installation Instructions

25 July 2023

OA DCGS

AFLCMC/HBGEB

750 Third Street

Robins AFB, GA 31098

Text

Description automatically generated

**DISTRIBUTION STATEMENT D –** Distribution authorized to the Department of Defense and U.S. DoD contractors only (Critical Technology) (26 October 2020). Other requests for this document shall be referred to AF DCGS Data Management Office, AFLCMC/HBGB, 750 Third Street, Robins AFB, GA 31098-1670.

THIS PAGE INTENTIONALLY LEFT BLANK

**CHANGE LOG**

This record shall be maintained throughout the life of the document. Each published update shall be recorded. Revisions are a complete re-issue of the entire document. A revision shall be made annually or when applicable. Refer questions concerning this document to: [robert.heddleson@us.af.mil](mailto:robert.heddleson@us.af.mil)

The revision numbers within the Change/Revision Record should also coincide with the AF DCGS document control number (DCN) given to this document, i.e., for DCGS DCN, DCGS-TECH-GT1-0025 REV-1, the last line in this tables should be REV-1.

**CHANGE / REVISION RECORD**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision** | **Date** | **Page/Paragraph** | **Description of Change** | **Made By** |
| Initial | 25 July 2022 | All | Initial Release;  CR-YEAR-OADCGS-XXX | C. Castellano/AFRL/ES |
|  |  |  |  |  |
|  |  |  |  |  |

TABLE OF CONTENTS

[1 INTRODUCTION 1](#_Toc141193701)

[1.1 Location of Installation 1](#_Toc141193702)

[1.2 Overview 1](#_Toc141193703)

[2 System Environment 2](#_Toc141193704)

[2.1 Minimum Hardware Requirements 2](#_Toc141193705)

[2.2 Minimum Software Requirements 2](#_Toc141193706)

[2.3 Site Requirements 2](#_Toc141193707)

[3 Security Considerations 3](#_Toc141193708)

[4 Prerequisites 4](#_Toc141193709)

[4.1 Additional Documents Required for Installation 4](#_Toc141193710)

[4.2 Roles Required 4](#_Toc141193711)

[4.3 Puppet Modules Required 4](#_Toc141193712)

[5 Installation Instructions 5](#_Toc141193713)

[5.1 Estimated Implementation Time 5](#_Toc141193714)

[5.2 Cleanup of Existing Versions and Files 5](#_Toc141193715)

[5.3 Media Boot Procedures 5](#_Toc141193716)

[5.4 Software Installation Instructions 5](#_Toc141193717)

[5.4.1 Add certificate to the ArcSight cacert store 5](#_Toc141193718)

[5.4.2 Modify the ArcSight ePO db SmartConnector parameters 7](#_Toc141193719)

[5.4.3 Modify the ArcSight ePO db SmartConnector destination 18](#_Toc141193720)

[5.4.4 Query for device plug events 31](#_Toc141193721)

[5.5 Installation Instructions for Upgrades 33](#_Toc141193722)

[5.6 List of Changes 33](#_Toc141193723)

[6 De-Installation (Back Out) Instructions 34](#_Toc141193724)

[6.1 De-Installation Instructions for Upgrades 34](#_Toc141193725)

[7 Frequently Asked Questions 35](#_Toc141193726)

[8 References 36](#_Toc141193727)

[9 Test Results 37](#_Toc141193728)

[10 Test Procedures 38](#_Toc141193729)

[Appendix A Acronyms 39](#_Toc141193730)

[Appendix B Known Issues 40](#_Toc141193731)

**List of Figures**

[Figure 1 Services 7](#_Toc141193732)

[Figure 2 ArcSight ePO Connector "bin" directory 8](#_Toc141193733)

[Figure 3 Modify Connector 9](#_Toc141193734)

[Figure 4 Modify Connector Parameters 10](#_Toc141193735)

[Figure 5 JDBC page - no change 11](#_Toc141193736)

[Figure 6 Export Current Parameters 12](#_Toc141193737)

[Figure 7 Table Parameters CSV in Notepad for editing 12](#_Toc141193738)

[Figure 8 Edited Event Types 13](#_Toc141193739)

[Figure 9 Import Table Parameters 13](#_Toc141193740)

[Figure 10 Import modified parameters CSV file 14](#_Toc141193741)

[Figure 11 Confirmation of Parameter update from edited CSV file 15](#_Toc141193742)

[Figure 12 Updating Parameters 16](#_Toc141193743)

[Figure 13 Successful parameter update 17](#_Toc141193744)

[Figure 14 Select Continue and click Next 18](#_Toc141193745)

[Figure 15 - Connector Setup 19](#_Toc141193746)

[Figure 16 Modify Destination 20](#_Toc141193747)

[Figure 17 Add Destination 21](#_Toc141193748)

[Figure 18 - CEF Syslog message type 22](#_Toc141193749)

[Figure 19 Logstash server and port parameter entry 23](#_Toc141193750)

[Figure 20 Continue 24](#_Toc141193751)

[Figure 21 - Connector Setup 25](#_Toc141193752)

[Figure 22 Modify Destination 26](#_Toc141193753)

[Figure 23 - Select old and not to be used destinations 27](#_Toc141193754)

[Figure 24 Final State - only the single destination, cefsyslog, should remain 29](#_Toc141193755)

[Figure 25 Exit the setup script 30](#_Toc141193756)

[Figure 26 Obtain a quick list of device plug events to compare with Elastic 31](#_Toc141193757)

[Figure 27 Import Query 31](#_Toc141193758)

[Figure 28 Query import screen 32](#_Toc141193759)

[Figure 29 Sample query output 32](#_Toc141193760)

[Figure 30 Edit query, filter tab 33](#_Toc141193761)

[Figure 31 Export Table button 33](#_Toc141193762)

**List of Tables**

THIS PAGE INTENTIONALLY LEFT BLANK

# INTRODUCTION

## Location of Installation

Installation will be conducted in both NOFORN and REL

## Overview

The instructions given in this document are a back-up plan to be used to assist Elastic in the event that the DLP 11.10.100 version (CR-2023-OADCGS-056) is not yet installed at the time the ArcSight system license has expired.

The objective is to use the existing ArcSight SmartConnector to the ePO Database and redirect its destination from the ArcSight Logger to the Elastic Logstash server.

The new destination is the logstash server, at an Elastic specified port. In the G7 lab where testing was performed, the destination was u00u01ls01.ech.dcgs.mil and port 5600. Data was sent TCP as CEF Syslog.

On implementation of CR-2023-OADCGS-056, DLP 11.10.100 the ArcSight connector will be removed.

# System Environment

## Minimum Hardware Requirements

The ArcSight SmartConnector is installed on the ePO Server at the Hub.

## Minimum Software Requirements

The ArcSight SmartConnector is installed on the ePO Server 5.10, and the ArcSight ePO Connector version is 8.0.0.8322.

## Site Requirements

N/A.

# Security Considerations

This installation procedure is written for ESS (HBSS) ePO administrators. An administrator account is only granted to system admins that have completed and received a certificate for the DISA HBSS 201 and 301 courses, and the ENS Essentials course.

# Prerequisites

This procedure is applied to the ePO version 5.10 with DLP, any version, and the ArcSight ePO SmartConnector installed.

## Additional Documents Required for Installation

N/A

## Roles Required

The ePO Administrators have access to the ePO Virtual Machine (VM) server. There are limited local accounts to the non-domain ePO server.

## Puppet Modules Required

**N/A**

# Installation Instructions

This procedure is not a software installation. This procedure is a configuration change of the ArcSight ePO SmartConnector.

THIS IS A TEMPORARY CHANGE AND WILL BE REMOVED WHEN RFC CR-2023-OADCGS-056 IS IMPLEMENTED.

## Estimated Implementation Time

The estimated time to complete the procedure is one hour.

## Cleanup of Existing Versions and Files

No software is installed. There are no clean up procedures required.

## Media Boot Procedures

No software is installed.

Two helper files are included.

* keytool.exe Temporary use
* DevicePlugQuery.xml.txt Optional to view and export device plug events

## Software Installation Instructions

### Add certificate to the ArcSight cacert store

This step requires:

* The logstash system certificate ( ex. u00su01ls01.cer )
* The keytool.exe program

Obtain the certificate file. The **keytool.exe** program is supplied, or may be found on the ePO in **D:\Program Files (x86)\McAfee\ePolicy  
Orchestrator\updates\LatestBuild\ePOUpdater\resources\app\release\jre\jre\bin**

1. Log on to the ePO Virtual Machine (VM)
2. Open a Command window as Administrator

Note: In this example, the logstash certificate is stored in the user’s Desktop\cert folder\u00su01ls01.cer.

1. Follow the example using the keytool.exe to import the logstash certificate to the cacert certificate store. The certificate store is located at:  
   **C:\Program Files\ArcSightSmartConnectors\epo\current\jre\lib\security\cacerts**

The command is:  
**keytool.exe -list -import -trustcacerts -file <full path cert file> -keystore <full path to keystore file>**

The password for the ArcSight keystore is: **changeit**

Enter the password when prompted.

EXAMPLE:

D:\Program Files (x86)\McAfee\ePolicy Orchestrator\updates\LatestBuild\ePOUpdater\resources\app\release\jre\jre\bin>keytool.exe -list -import -trustcacerts -file "C:\Users\cosmo.castella.adm\Desktop\cert folder\u00su01ls01.cer" -keystore "C:\Program Files\ArcSightSmartConnectors\epo\current\jre\lib\security\cacerts"

Enter keystore password:

Owner: EMAILADDRESS=DCGS@DCGS.mil, CN=u00su01ls01.ech.dcgs.mil, OU=OADCGS, O=DCGS, L=Robins AFB, ST=GA, C=US

Issuer: CN=AFRL-IBA-CA-1, DC=dcgs, DC=mil

Serial number: 7f000001779c7d5cdfdce51cea000000000177

Valid from: Tue Jul 05 12:47:56 UTC 2022 until: Fri Jul 05 12:57:56 UTC 2024

Certificate fingerprints:

SHA1: 25:6F:53:5B:2F:5F:4B:29:7C:40:B1:1E:02:BE:CB:D3:FA:DA:BC:C1

SHA256: 69:F5:80:CE:BE:26:4D:AD:55:8D:DC:78:C7:57:D0:8E:D9:FC:29:C4:44:D1:B3:0E:87:96:8C:8B:5E:8D:BC:E3

Signature algorithm name: SHA256withRSA

Subject Public Key Algorithm: 2048-bit RSA key

Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false

0000: 30 18 30 0A 06 08 2B 06 01 05 05 07 03 02 30 0A 0.0...+.......0.

0010: 06 08 2B 06 01 05 05 07 03 01 ..+.......

#2: ObjectId: 1.3.6.1.4.1.311.21.7 Criticality=false

0000: 30 2F 06 27 2B 06 01 04 01 82 37 15 08 87 FB 92 0/.'+.....7.....

0010: 3C 83 E8 BD 58 83 AD 91 1E 86 EC BC 66 82 95 EF <...X.......f...

0020: 47 81 62 86 EF DF 5D 81 A7 A2 39 02 01 64 02 01 G.b...]...9..d..

0030: 2C ,

#3: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false

AuthorityInfoAccess [

[

accessMethod: caIssuers

accessLocation: URIName: ldap:///CN=AFRL-IBA-CA-1,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=dcgs,DC=mil?cACertificate?base?objectClass=certificationAuthority

]

]

#4: ObjectId: 2.5.29.35 Criticality=false

AuthorityKeyIdentifier [

KeyIdentifier [

0000: BE 92 20 B0 BB BD D5 61 DE 74 04 BA 91 FA BB EF .. ....a.t......

0010: 69 7E 99 65 i..e

]

]

#5: ObjectId: 2.5.29.31 Criticality=false

CRLDistributionPoints [

[DistributionPoint:

[URIName: ldap:///CN=AFRL-IBA-CA-1,CN=u00sm01ca01,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=dcgs,DC=mil?certificateRevocationList?base?objectClass=cRLDistributionPoint, URIName: http://u00sm01ca01.dcgs.mil/dcgssubcrl/AFOADCGS-Sub-CA.crl]

]]

#6: ObjectId: 2.5.29.37 Criticality=false

ExtendedKeyUsages [

clientAuth

serverAuth

]

#7: ObjectId: 2.5.29.15 Criticality=true

KeyUsage [

DigitalSignature

Key\_Encipherment

]

#8: ObjectId: 2.5.29.17 Criticality=false

SubjectAlternativeName [

DNSName: u00su01ls01.ech.dcgs.mil

DNSName: u00su01ls01

DNSName: logstash-u00.ech

DNSName: u00su01ls01.ech

DNSName: logstash-u00

DNSName: logstash

DNSName: logstash-u04

]

#9: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: 78 A3 3B 8F 5C 69 F7 BA 24 8B D2 D5 03 C2 B0 1C x.;.\i..$.......

0010: FE 75 3C 73 .u<s

]

]

Trust this certificate? [no]: yes

Certificate was added to keystore

Warning:

The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore C:\Program Files\ArcSightSmartConnectors\epo\current\jre\lib\security\cacerts -destkeystore C:\Program Files\ArcSightSmartConnectors\epo\current\jre\lib\security\cacerts -deststoretype pkcs12".

### Modify the ArcSight ePO db SmartConnector parameters

1. Log on to the ePO Virtual Machine (VM)
2. Run services.msc, and click OK.
3. Verify ArcSight McAfee ePolicy Orchestrator DB service is present and running.



Figure Services

1. Close services
2. Open file explorer window to **C:\Program Files\ArcSightSmartConnectors\epo\current\bin**

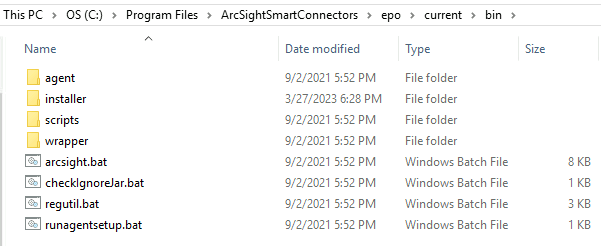


Figure ArcSight ePO Connector "bin" directory

1. Right-click **runagentsetup.bat**, and select **Run as Administrator**.
2. Click **OK** to the User Access Control
3. Select **Modify a Connector** and click **Next**

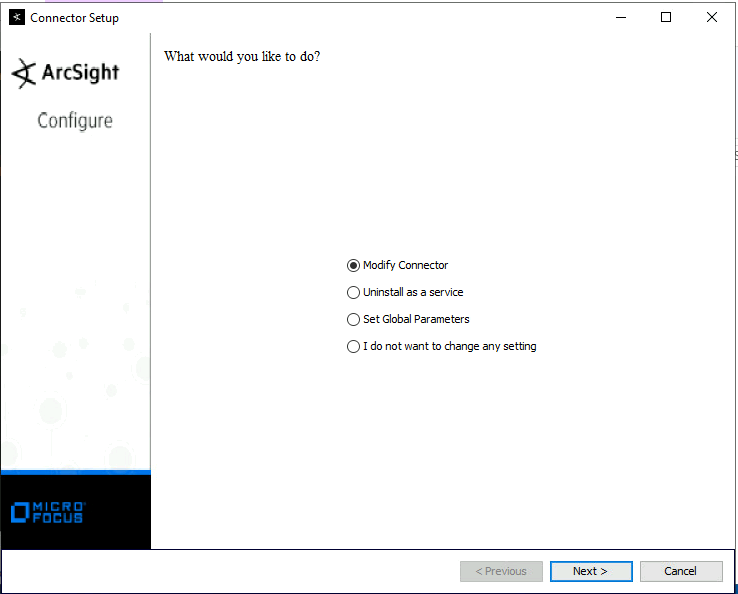


Figure Modify Connector

1. Click **Modify Connector Parameters** and click **Next**

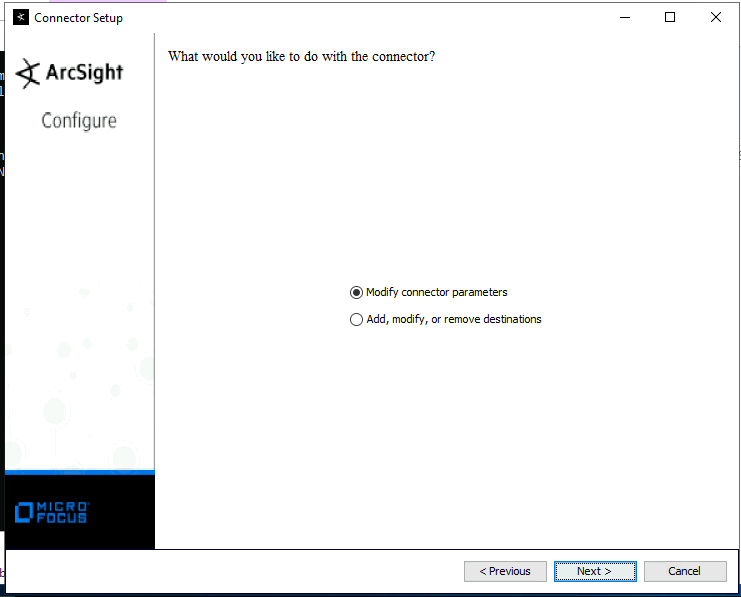


Figure Modify Connector Parameters

1. The JDBC driver setting is displayed. **Do not make any change**. Click **Next**.

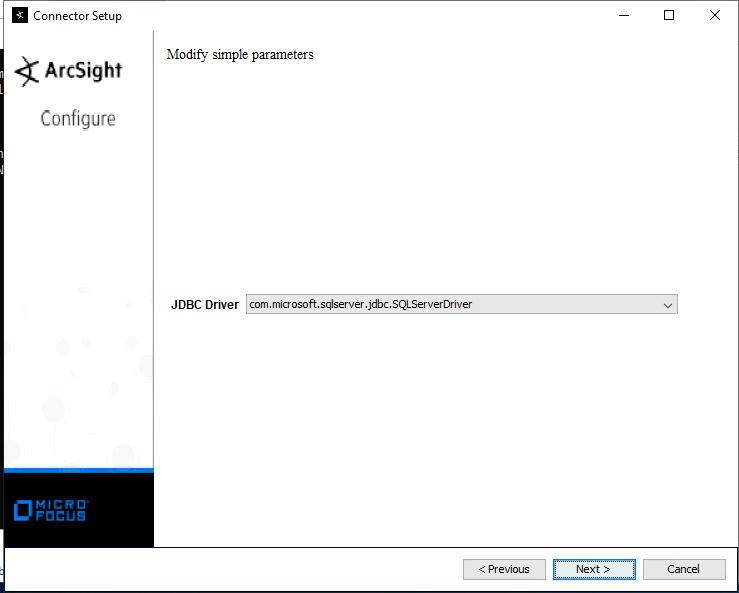


Figure JDBC page - no change

1. On the **Modify Table Parameters** Screen, click **Export**.



Figure Export Current Parameters

1. Save the exported CSV file as **FullCollection.csv** in a convenient location.
2. Open the FullCollection.csv file with Notepad.
3. Scroll to the right to find the string of Event Types



Figure Table Parameters CSV in Notepad for editing

1. Edit the Event Types, deleted all except for the DLP events. The event type string should be **“dlp,dlpadministrative,dlpincident,dlpdiscover”.**  (no spaces)



Figure Edited Event Types

1. Save the edited file as ElasticDLPonly.csv
2. Return to the **Modify Table Parameters** Screen and click **Import**



Figure Import Table Parameters

1. Select the **ElasticDLPOnly.csv** file that was just edited for **import**.

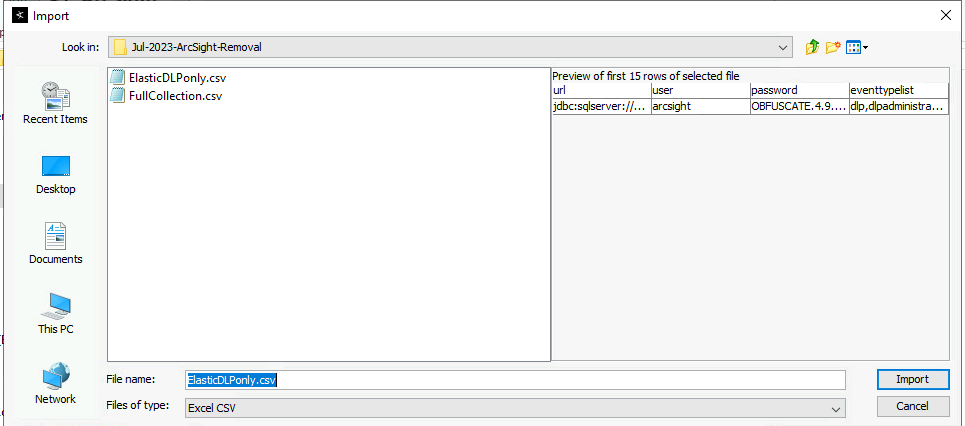


Figure Import modified parameters CSV file

1. The script should confirm that the row was replaced with the updated data. Click **Next**.

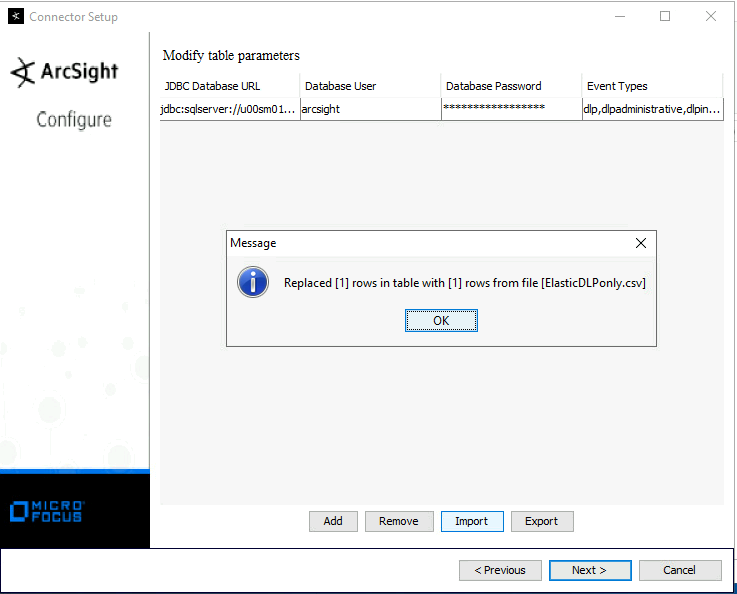


Figure Confirmation of Parameter update from edited CSV file

1. The connector parameters will be updated. Wait for completion and click **Next**.

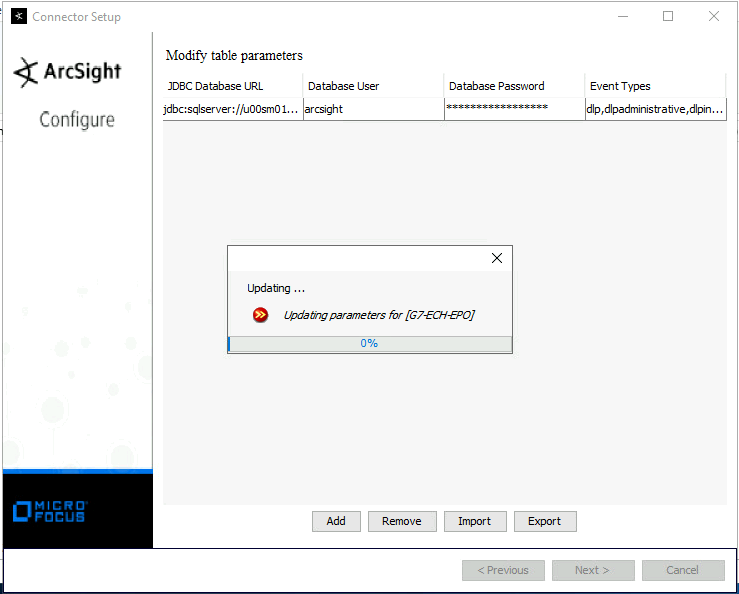


Figure Updating Parameters

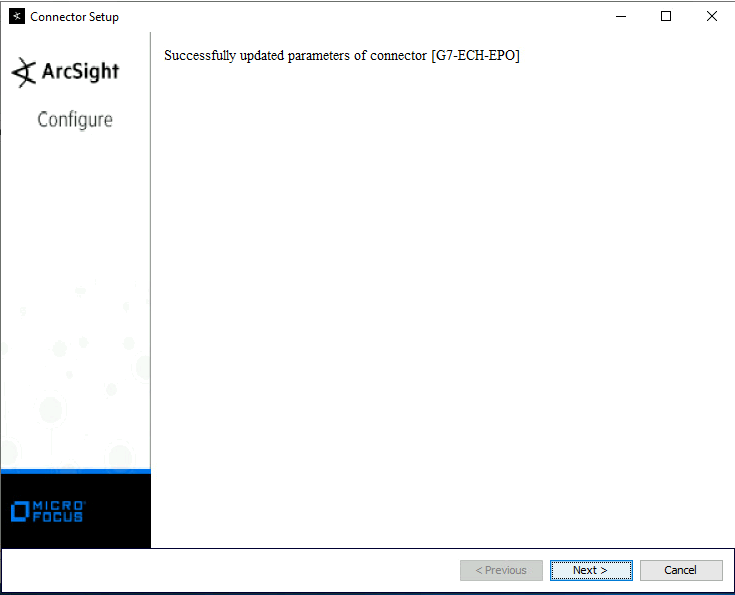


Figure Successful parameter update

1. On the final screen, select **Continue** and Click **Next**



Figure Select Continue and click Next

### Modify the ArcSight ePO db SmartConnector destination

This section describes how to modify the ArcSight ePO SmartConnect. This section continues from the previous section.

1. After selecting Continue in the previous step, Select **Modify a Connector** and click **Next**

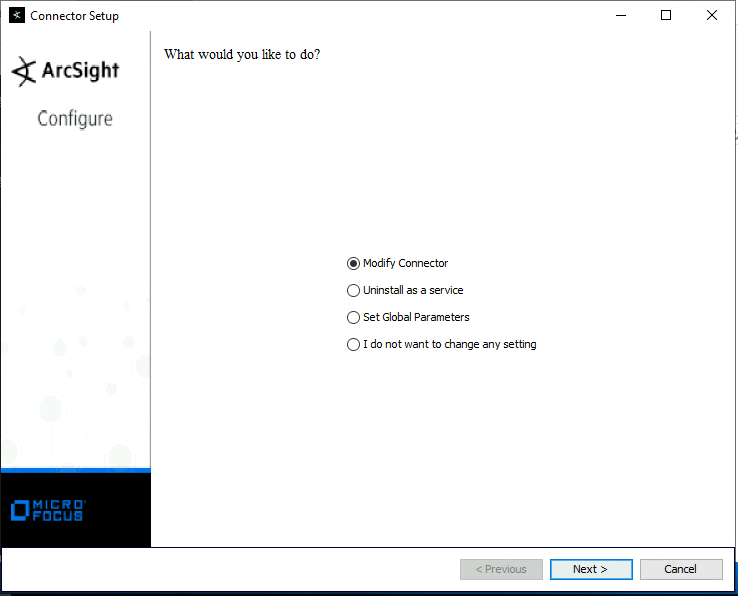


Figure - Connector Setup

1. Click Add, Modify, or Remove Destinations, and click Next.

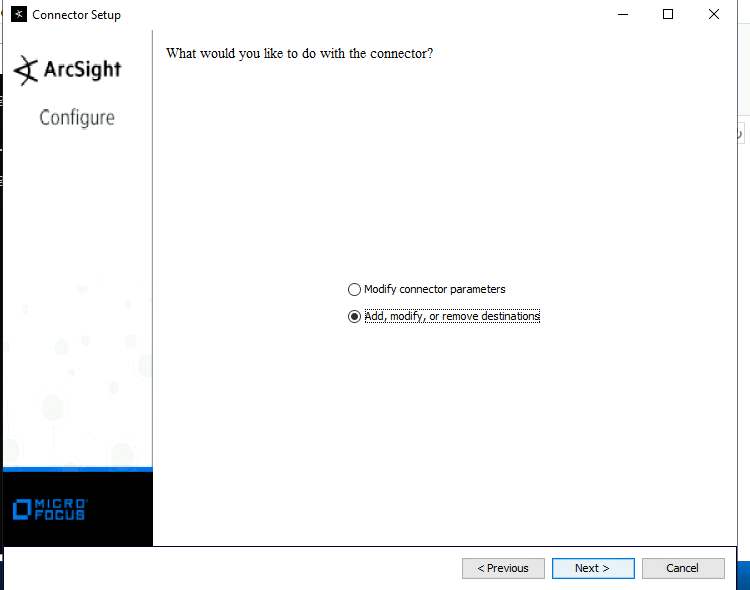


Figure Modify Destination

1. Select **Add Destination**, and click **Next**. (Note: Past destinations to the ArcSight Logger may be visible. The other connections will be removed once the new connection is completed.)



Figure Add Destination

1. Select CEF Syslog, and click Next.

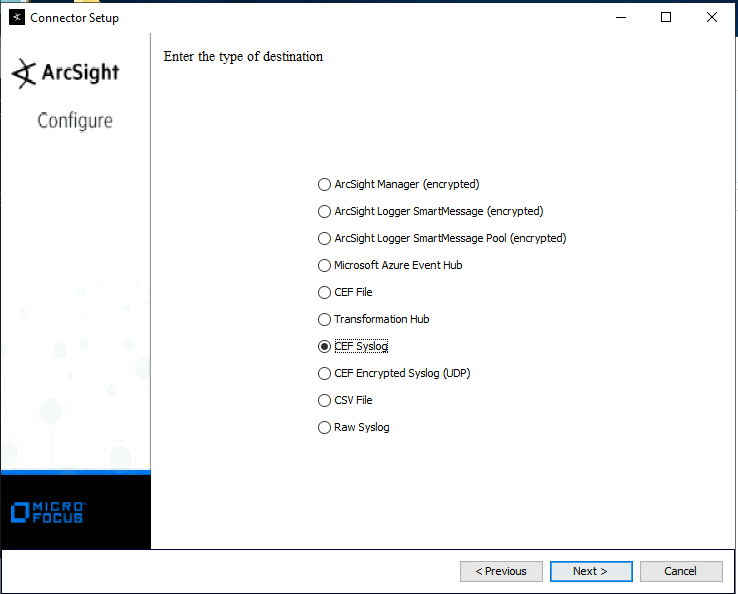


Figure - CEF Syslog message type

1. Enter the parameters to specify the logstash server and the port Elastic has provided for the temporary listener. For example, in G7 the server is **u00su01ls01.ech.dcgs.mil**. The Elastic assigned port is **5056**.

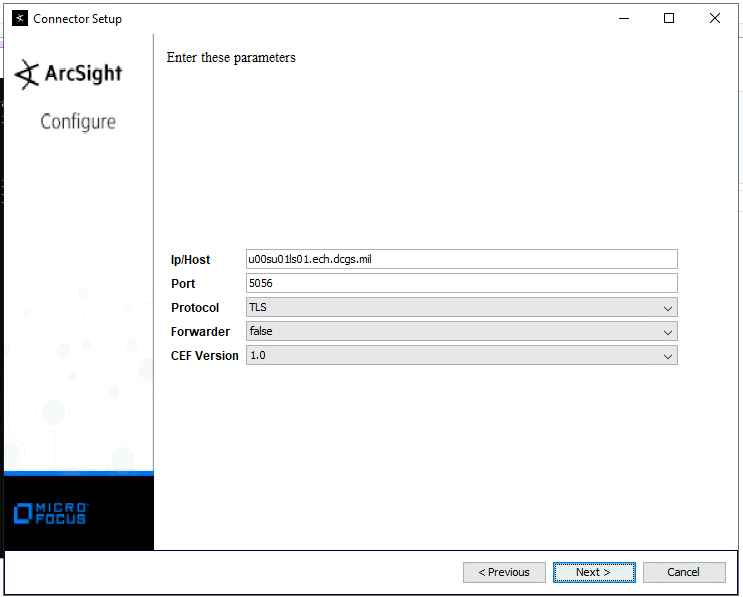


Figure Logstash server and port parameter entry

1. There may be a long delay as the changes are put into effect. Select **Exit**, and click **Next**.
2. Select **Continue** and Click **Next**.



Figure Continue

1. ASelect Modify a Connector and click Next

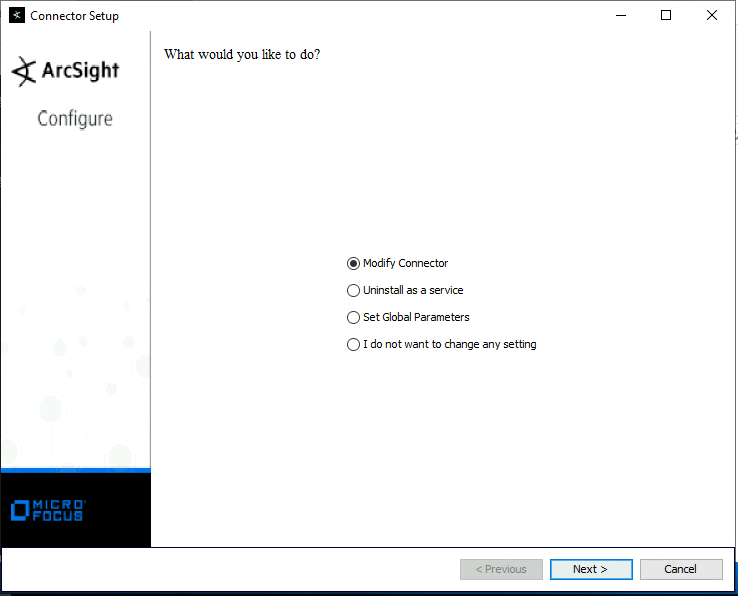


Figure - Connector Setup

1. Click Add, Modify, or Remove Destinations, and click Next.

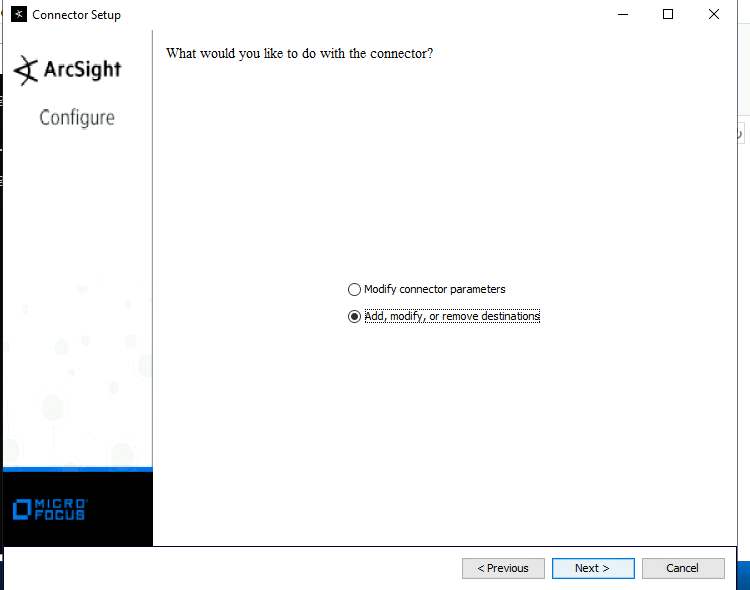


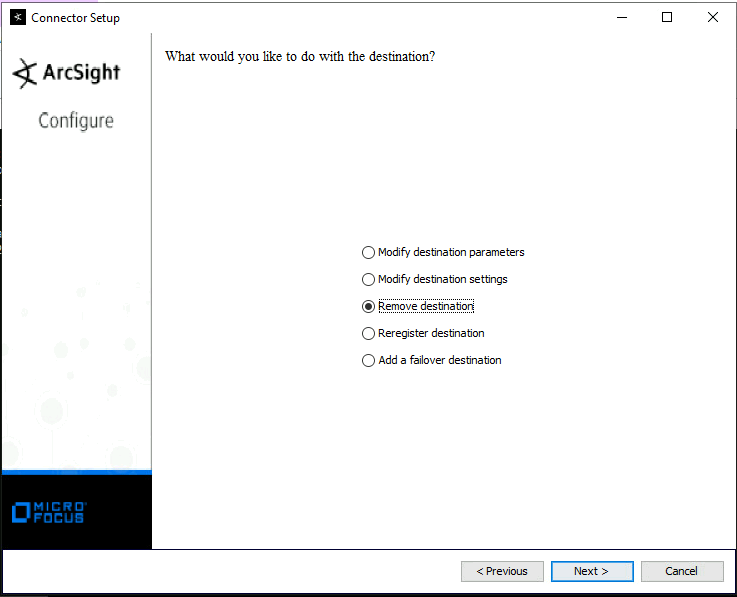
Figure Modify Destination

1. Select the old ArcSight Logger (**Logger SmartMessage**) destination and click **Next**.



Figure - Select old and not to be used destinations

1. Select **Remove Destination** and click **Next**.



1. Repeat as necessary. Only the single destination should remain.

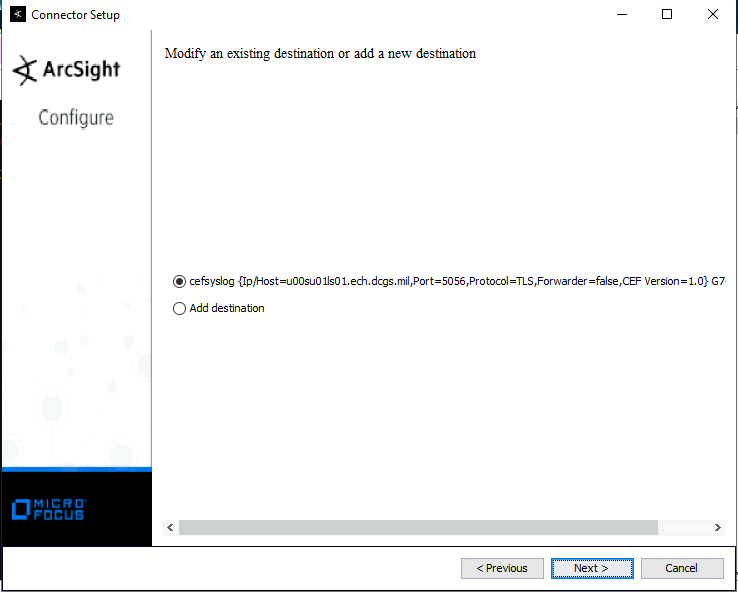


Figure Final State - only the single destination, cefsyslog, should remain

1. Select exit. Click Next.

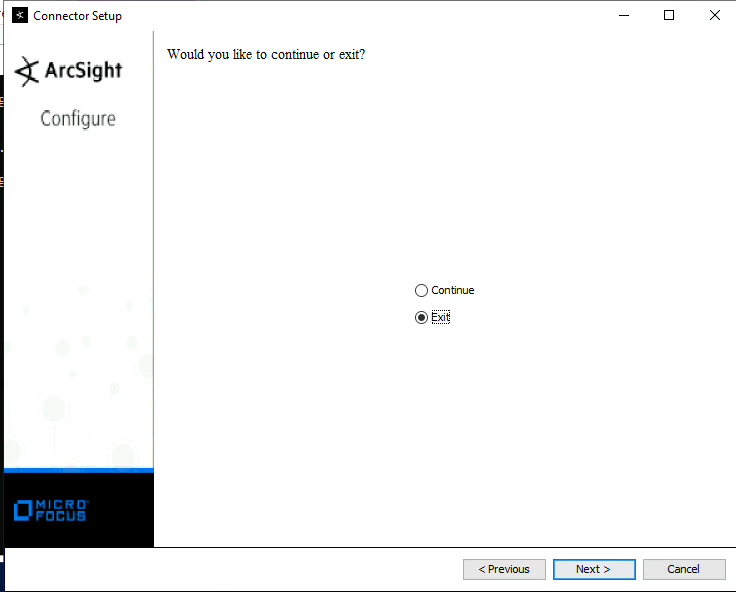


Figure Exit the setup script

1. Run **Services.msc** and verify the **ArcSight McAfee ePolicy Orchestrator DB** service is present and running. **Start** the service if it is not running.
2. Generate device-plug events by plugging in an approved external USB hard disk into a physical workstation.
3. Verify reception of the event at the Elastic Server.
4. Log on to the ePO Web Console
5. View **DLP Incidents** to obtain device-plug data, or view **Threat Events and filter for Event ID 19115**, and compare the events to the events received by Elastic. (A supplied XML Query file may be imported to view device-plug events. Modify the filter in the query for the time period desired.)

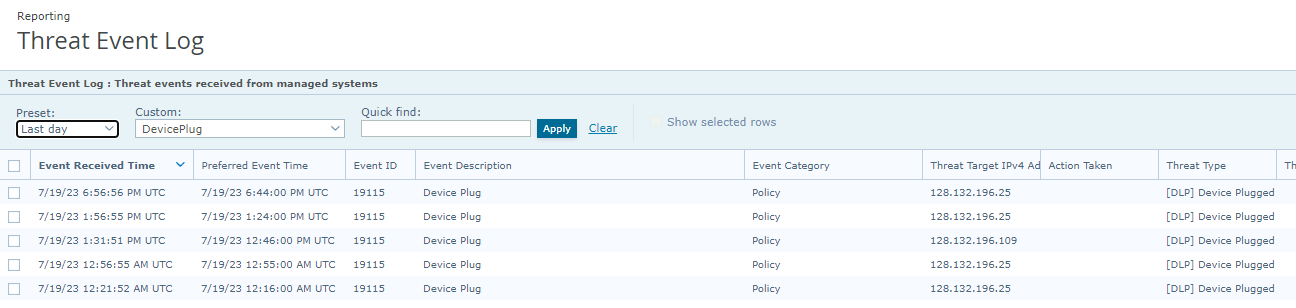


Figure Obtain a quick list of device plug events to compare with Elastic

### Query for device plug events

1. Rename the file **DevicePlugQuery.xml.txt** to **DevicePlugQuery.xml**
2. Log on to the ePO web Console
3. Go to **Menu | Reporting | Queries & Reports**
4. Click **Import Queries**

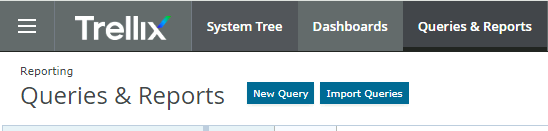


Figure Import Query

1. Click **Choose File** and select the file, **DevicePlugQuery.xml**
2. Save to a new or Existing Group

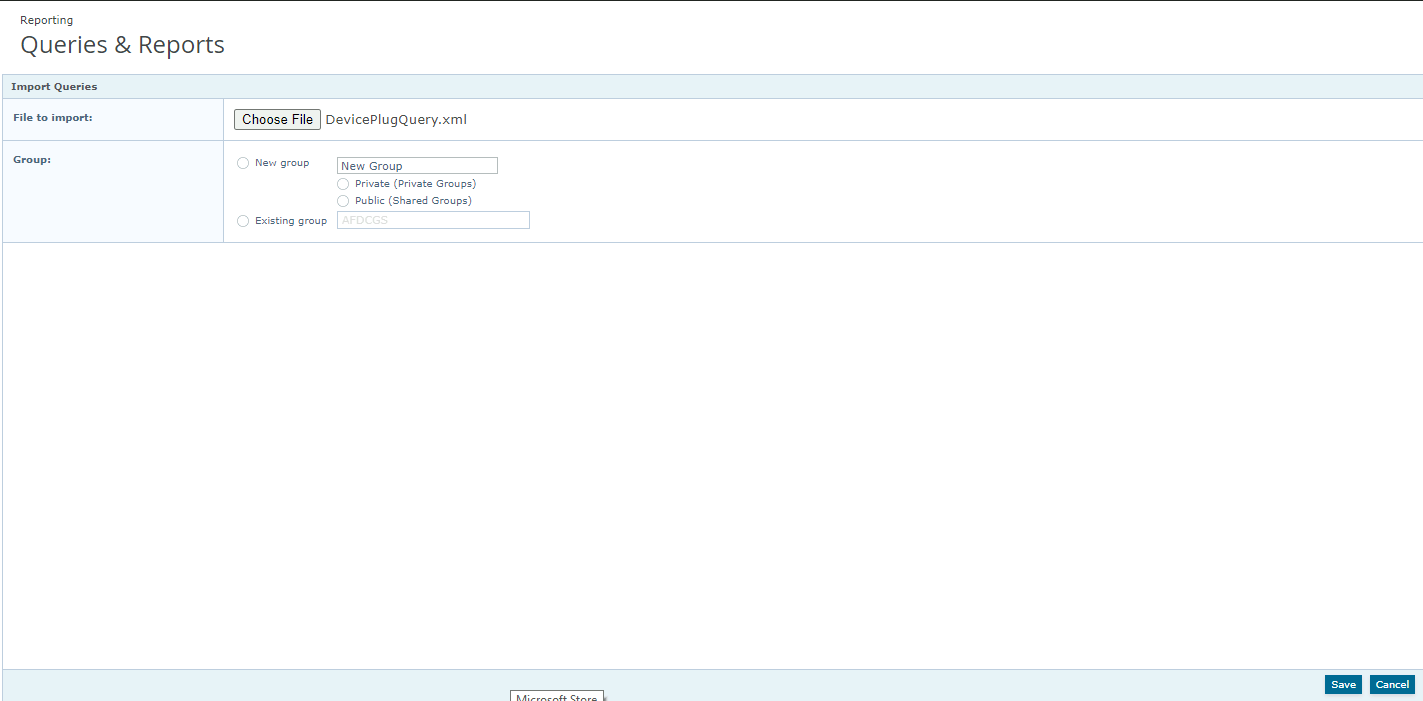


Figure Query import screen

1. Run the imported query to obtain device-plug events with user and device data

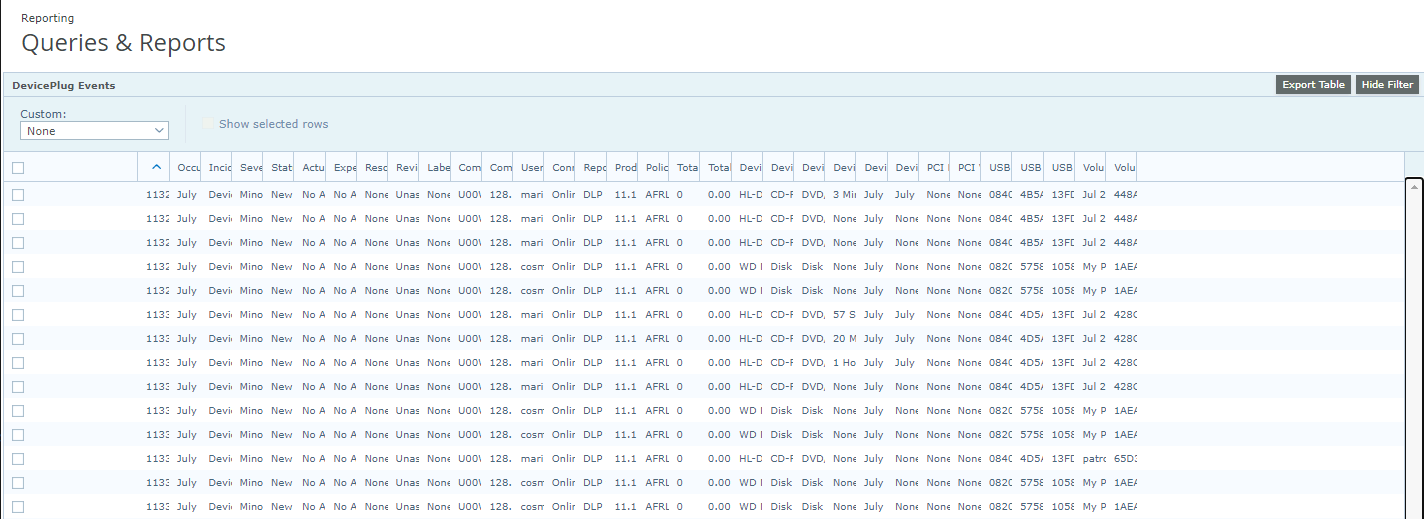


Figure Sample query output

1. Edit the query to limit the time frame. On the filter page, enter the time criteria.

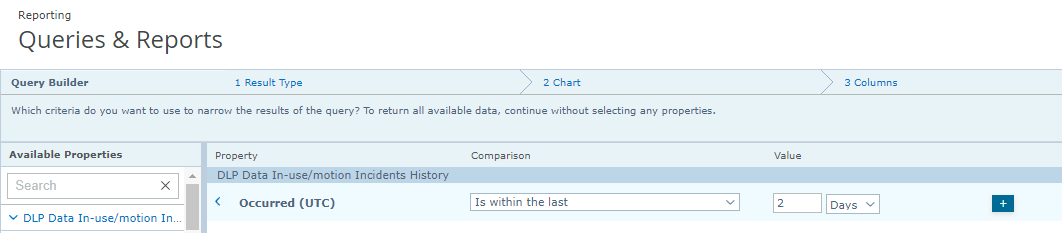


Figure Edit query, filter tab

1. Export data by clicking Export Table

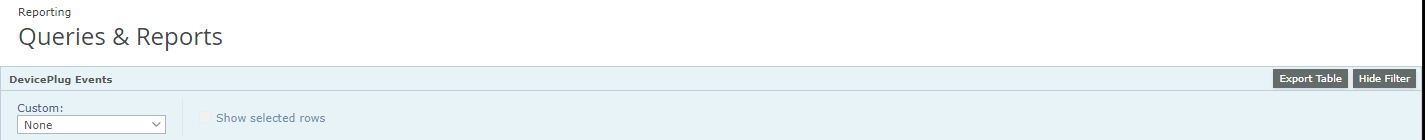


Figure Export Table button

1. Select **CSV** format and click **Next**
2. **Right Click** file link to Save As exported CSV data file.
3. Use the exported data to compare with the parsed CEF syslog data received by Elastic.

## Installation Instructions for Upgrades

N/A

## List of Changes

The change made to the configuration of the ArcSight ePO SmartConnector is to the connector destination from the ArcSight Logger, to the Elastic syslog receiver port set up for the ePO.

THIS IS A TEMPORARY CHANGE AND WILL BE REMOVED WHEN RFC CR-2023-OADCGS-056 IS IMPLEMENTED.

# De-Installation (Back Out) Instructions

THIS IS A TEMPORARY CHANGE AND WILL BE REMOVED WHEN RFC CR-2023-OADCGS-056 IS IMPLEMENTED.

When CR-2023-OADCGS-056, for DLP 11.10.100, is implemented and Elastic begins polling the DLP 11.10.100 REST API for device-plug data, uninstall the ArcSight Smart Connector.

1. Before uninstalling a connector that is running as a service or daemon, stop the service.
2. Also, be sure to remove the service files using the following command: **$ARCSIGHT\_HOME/current/bin/arcsight agentsvc -r**
3. The Uninstaller does not remove all the files and directories under the connector home folder. After completing the uninstall procedure, manually delete these folders.

To uninstall on Windows:

1. Open the Start menu.
2. Run the Uninstall SmartConnectors program found under All Programs > ArcSightSmartConnectors (or the name you used for the folder during connector installation).
3. If connectors were not installed on the Start menu, locate the $ARCSIGHT\_HOME/current/UninstallerData folder and run the following command: Uninstall\_ArcSightAgents.exe

## De-Installation Instructions for Upgrades

N/A

# Frequently Asked Questions

N/A

# References

N/A

# Test Results

LEAVE THIS BLANK BUT DO NOT DELETE.

FILL OUT THE IAAS-023 TEST REPORT TEMPLATE.

# Test Procedures

**DO NOT FILL THIS OUT. DO NOT DELETE.  
FILL OUT THE IAAS-023 TEST REPORT TEMPLATE.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sprint:** | Sprint it is tested in | **Epic:** | Epic as found on JIRA dev task |
| **User Story:** | Main task # (link) | **Test Procedure Name:** |  |
| **Test Procedure #:** | Test Task Jira Ticket # (link) | **Release:** | 1 |
| **System / Component:** | System/Component as found on JIRA dev task | **Test Purpose:** | DT |
| **Test Engineer:** | Engineer Name | **Execution Date:** | dd-month-yy |
| **Test Environment:** |  | **Test Description:** |  |
| **Prerequisites:** |  | | |
| **Estimated Implementation Time:** |  | | |
| **Test Location:** | Indicate if the test/install will be conducted in NOFORN, REL, or both NOFORN and REL. | | |
| **Notes:** |  | | |

|  |  |
| --- | --- |
| **Acceptance Criteria:** |  |
| **Overall Comments:** | N/A |
| **Overall Test Result:** | P |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step** | **Action** | **Expected Result** | **Pass/Fail** | **Comments** |
| 1 | I click X | Y Displays | P |  |
| 2 |  |  | PWE |  |
| 3 |  |  | F |  |

Acronyms

|  |  |
| --- | --- |
| **Acronym** | **Definition** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Known Issues

You can delete this if there are no known issues.