
Air Force Distributed Common Ground System (AF DCGS)



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

25 July 2023
OA DCGS

AFLCMC/HBGE
750 Third Street
Robins AFB, GA 31098

Controlled by: AFLCMC/HBGE
Controlled by: AFRL/RIEB
CUI Category: Controlled Technical Information
Distribution/Dissemination Controls: Distribution D
POC: AFRL.RIE.OADCGS@us.af.mil

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

UNCLASSIFIED

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

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/E S

UNCLASSIFIED

TABLE OF CONTENTS

1	INTRODUCTION	1
1.1	Location of Installation	1
1.2	Overview.....	1
2	System Environment.....	2
2.1	Minimum Hardware Requirements.....	2
2.2	Minimum Software Requirements	2
2.3	Site Requirements	2
3	Security Considerations	3
4	Prerequisites.....	4
4.1	Additional Documents Required for Installation	4
4.2	Roles Required.....	4
4.3	Puppet Modules Required.....	4
5	Installation Instructions.....	5
5.1	Estimated Implementation Time	5
5.2	Cleanup of Existing Versions and Files	5
5.3	Media Boot Procedures.....	5
5.4	Software Installation Instructions	5
5.4.1	Add certificate to the ArcSight cacert store.....	5
5.4.2	Modify the ArcSight ePO db SmartConnector parameters	7
5.4.3	Modify the ArcSight ePO db SmartConnector destination	18
5.4.4	Query for device plug events.....	31
5.5	Installation Instructions for Upgrades.....	33
5.6	List of Changes	33
6	De-Installation (Back Out) Instructions.....	34
6.1	De-Installation Instructions for Upgrades.....	34
7	Frequently Asked Questions	35
8	References.....	36
9	Test Results.....	37
10	Test Procedures	38
Appendix A	Acronyms	39
Appendix B	Known Issues	40

List of Figures

Figure 1 Services.....	7
Figure 2 ArcSight ePO Connector "bin" directory	8
Figure 3 Modify Connector	9
Figure 4 Modify Connector Parameters.....	10
Figure 5 JDBC page - no change	11
Figure 6 Export Current Parameters	12
Figure 7 Table Parameters CSV in Notepad for editing	12
Figure 8 Edited Event Types.....	13
Figure 9 Import Table Parameters	13
Figure 10 Import modified parameters CSV file	14
Figure 11 Confirmation of Parameter update from edited CSV file.....	15
Figure 12 Updating Parameters.....	16
Figure 13 Successful parameter update	17
Figure 14 Select Continue and click Next	18
Figure 15 - Connector Setup	19
Figure 16 Modify Destination.....	20
Figure 17 Add Destination.....	21
Figure 18 - CEF Syslog message type	22
Figure 19 Logstash server and port parameter entry.....	23
Figure 20 Continue	24
Figure 21 - Connector Setup	25
Figure 22 Modify Destination.....	26
Figure 23 - Select old and not to be used destinations	27
Figure 24 Final State - only the single destination, cefsyslog, should remain	29
Figure 25 Exit the setup script	30
Figure 26 Obtain a quick list of device plug events to compare with Elastic	31
Figure 27 Import Query	31
Figure 28 Query import screen	32
Figure 29 Sample query output.....	32
Figure 30 Edit query, filter tab.....	33
Figure 31 Export Table button.....	33

List of Tables

No table of figures entries found.

THIS PAGE INTENTIONALLY LEFT BLANK

1 INTRODUCTION

1.1 Location of Installation

Installation will be conducted in both NOFORN and REL

1.2 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.dcgsl.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.

2 SYSTEM ENVIRONMENT

2.1 Minimum Hardware Requirements

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

2.2 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.

2.3 Site Requirements

N/A.

DRAFT

3 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.

DRAFT

4 PREREQUISITES

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

4.1 Additional Documents Required for Installation

N/A

4.2 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.

4.3 Puppet Modules Required

N/A

DRAFT

5 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.

5.1 Estimated Implementation Time

The estimated time to complete the procedure is one hour.

5.2 Cleanup of Existing Versions and Files

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

5.3 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

5.4 Software Installation Instructions

5.4.1 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.

3. 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

UNCLASSIFIED

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\Policy
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.dcg.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?objectC
lass=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
```

UNCLASSIFIED

UNCLASSIFIED

```

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?certificate
RevocationList?base?objectClass=cRLDistributionPoint, URIName:
http://u00sm01ca01.dcgsmil/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.dcgsmil
  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".

```

5.4.2 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.

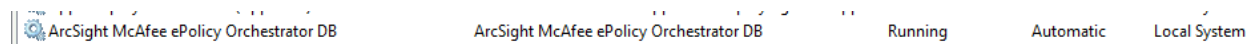


Figure 1 Services

UNCLASSIFIED

UNCLASSIFIED

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

This PC > OS (C:) > Program Files > ArcSightSmartConnectors > epo > current > bin >

Name	Date modified	Type	Size
agent	9/2/2021 5:52 PM	File folder	
installer	3/27/2023 6:28 PM	File folder	
scripts	9/2/2021 5:52 PM	File folder	
wrapper	9/2/2021 5:52 PM	File folder	
arcsight.bat	9/2/2021 5:52 PM	Windows Batch File	8 KB
checkignoreJar.bat	9/2/2021 5:52 PM	Windows Batch File	1 KB
regutil.bat	9/2/2021 5:52 PM	Windows Batch File	3 KB
runagentsetup.bat	9/2/2021 5:52 PM	Windows Batch File	1 KB

Figure 2 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**

UNCLASSIFIED

UNCLASSIFIED

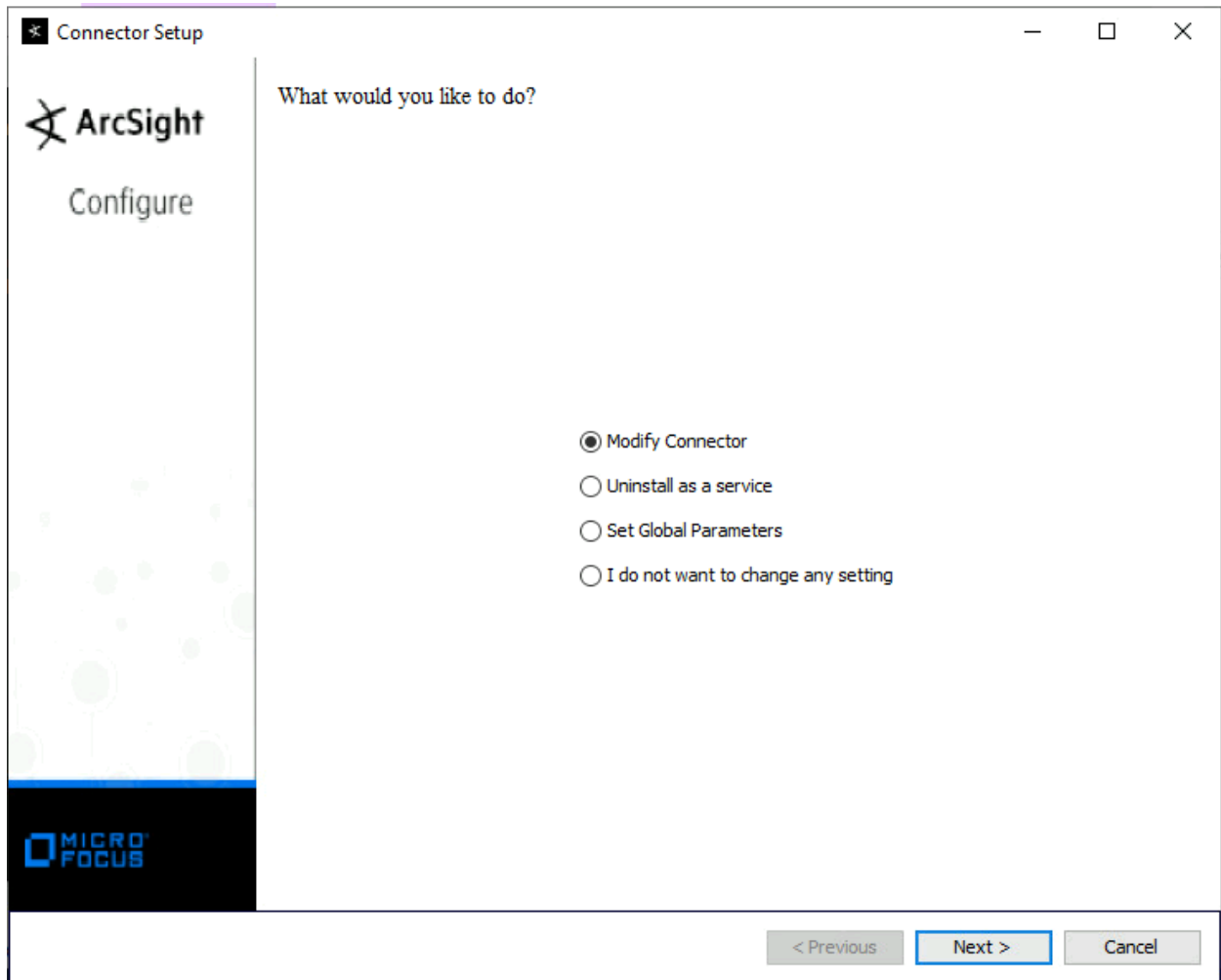


Figure 3 Modify Connector

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

UNCLASSIFIED

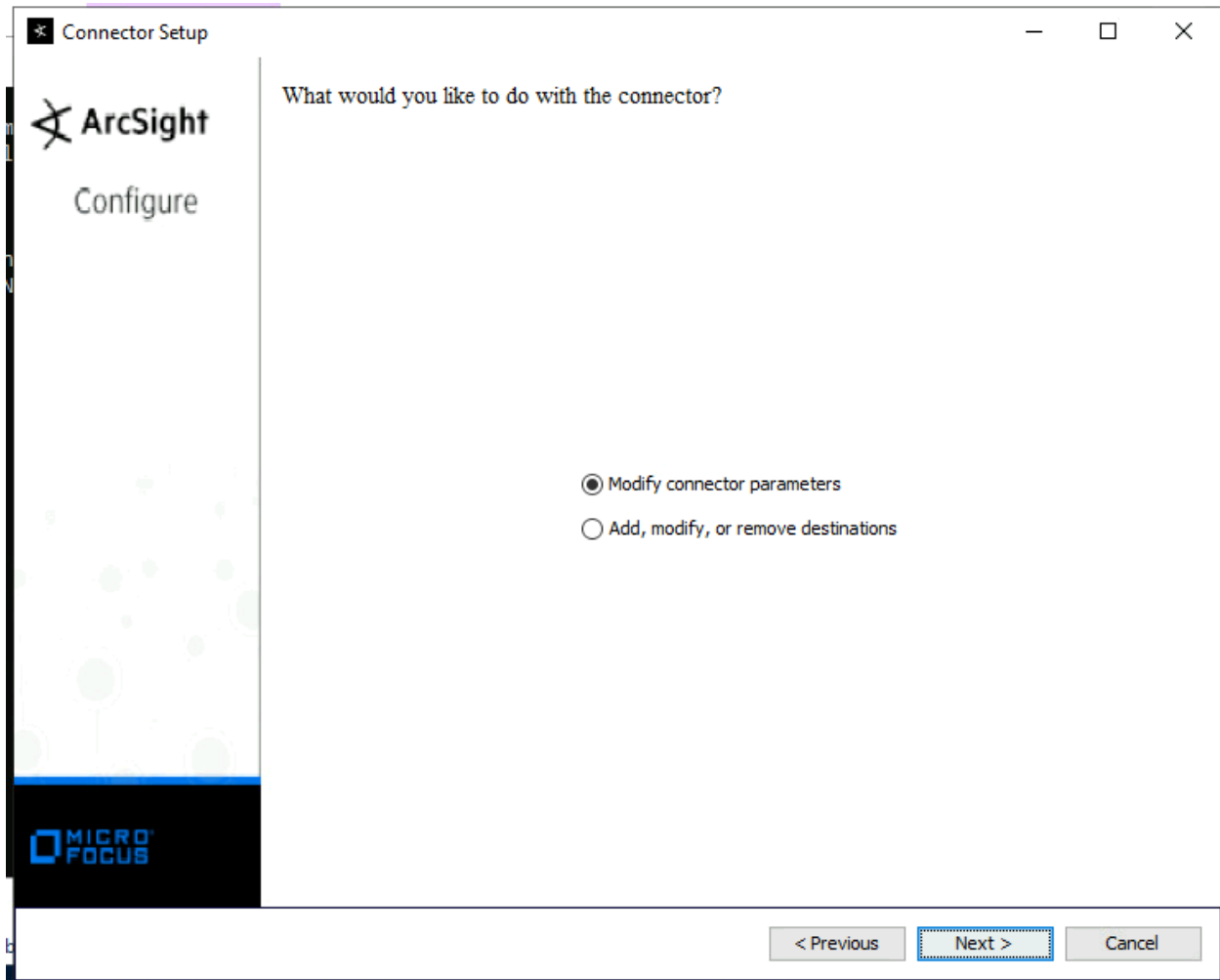


Figure 4 Modify Connector Parameters

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

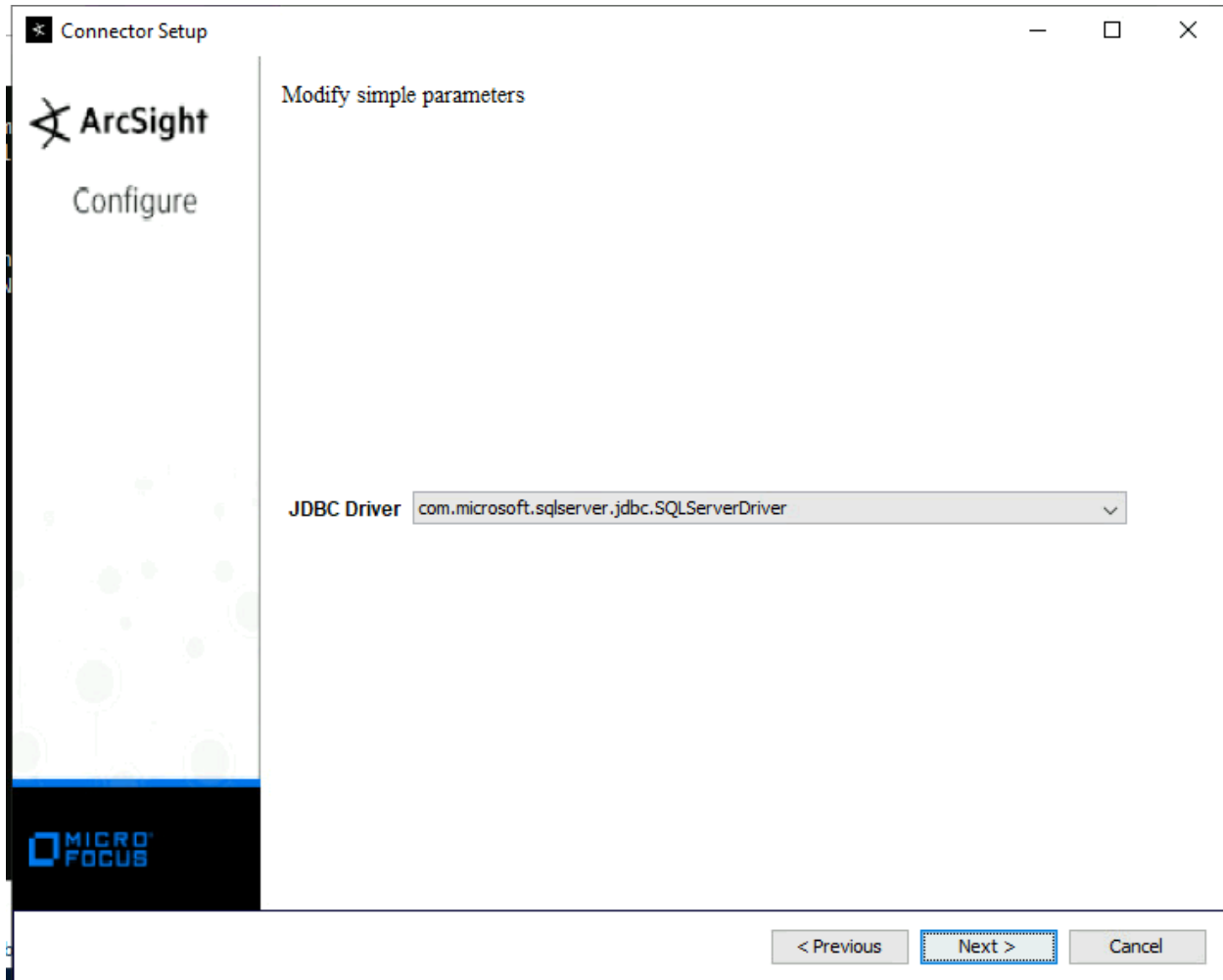


Figure 5 JDBC page - no change

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

UNCLASSIFIED

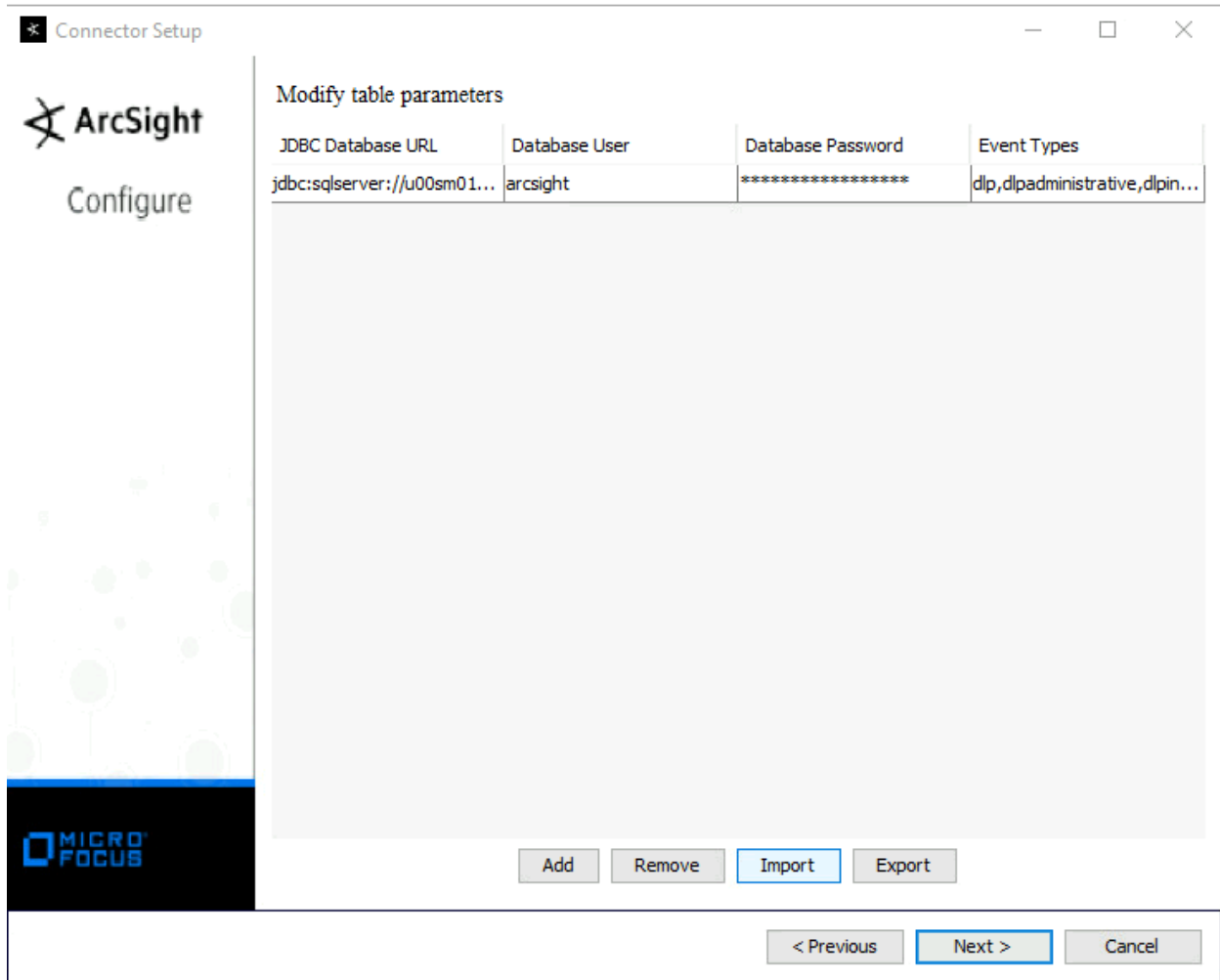


Figure 6 Export Current Parameters

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

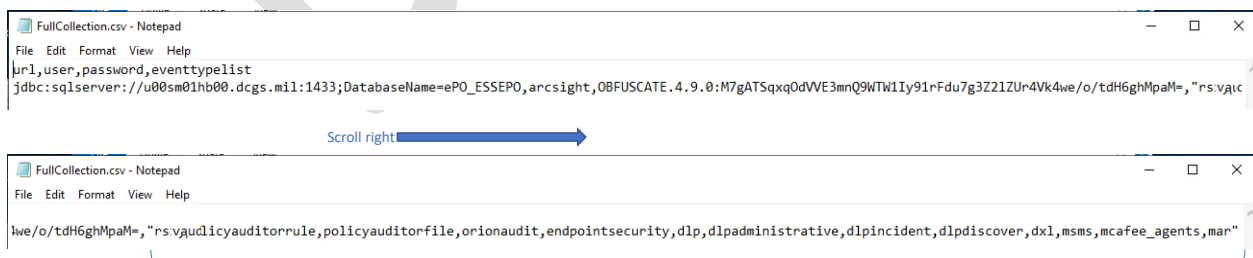
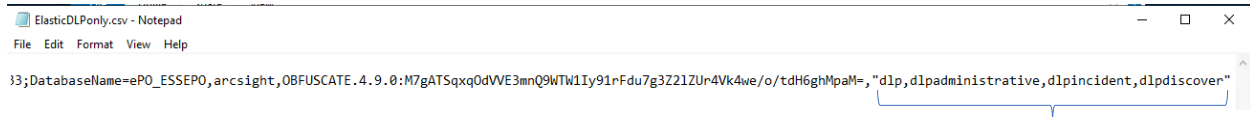


Figure 7 Table Parameters CSV in Notepad for editing

UNCLASSIFIED

UNCLASSIFIED

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



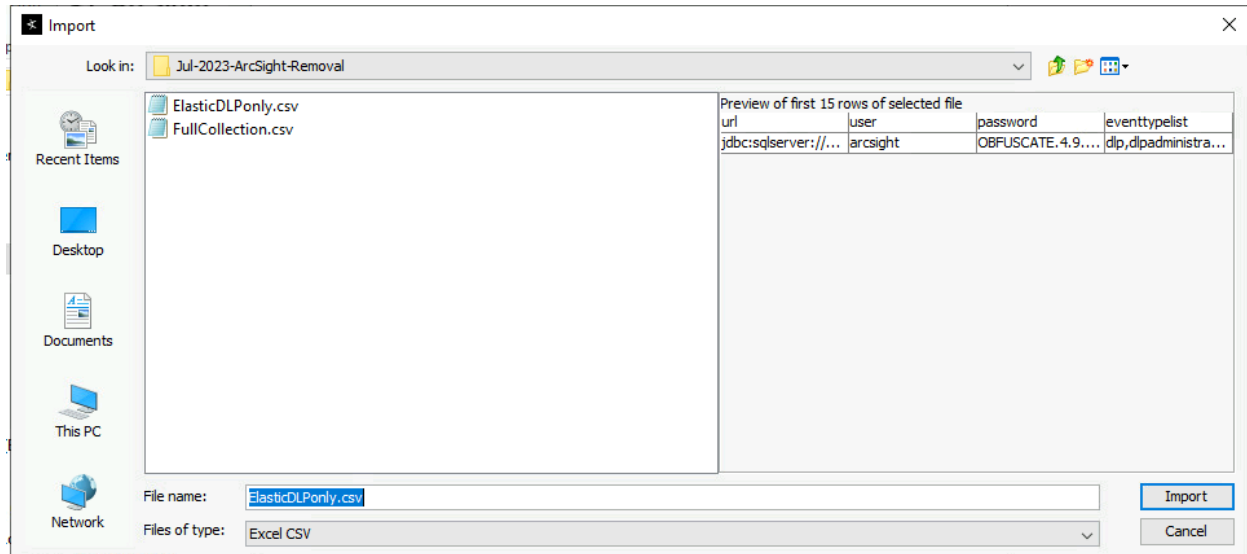


Figure 10 Import modified parameters CSV file

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

UNCLASSIFIED

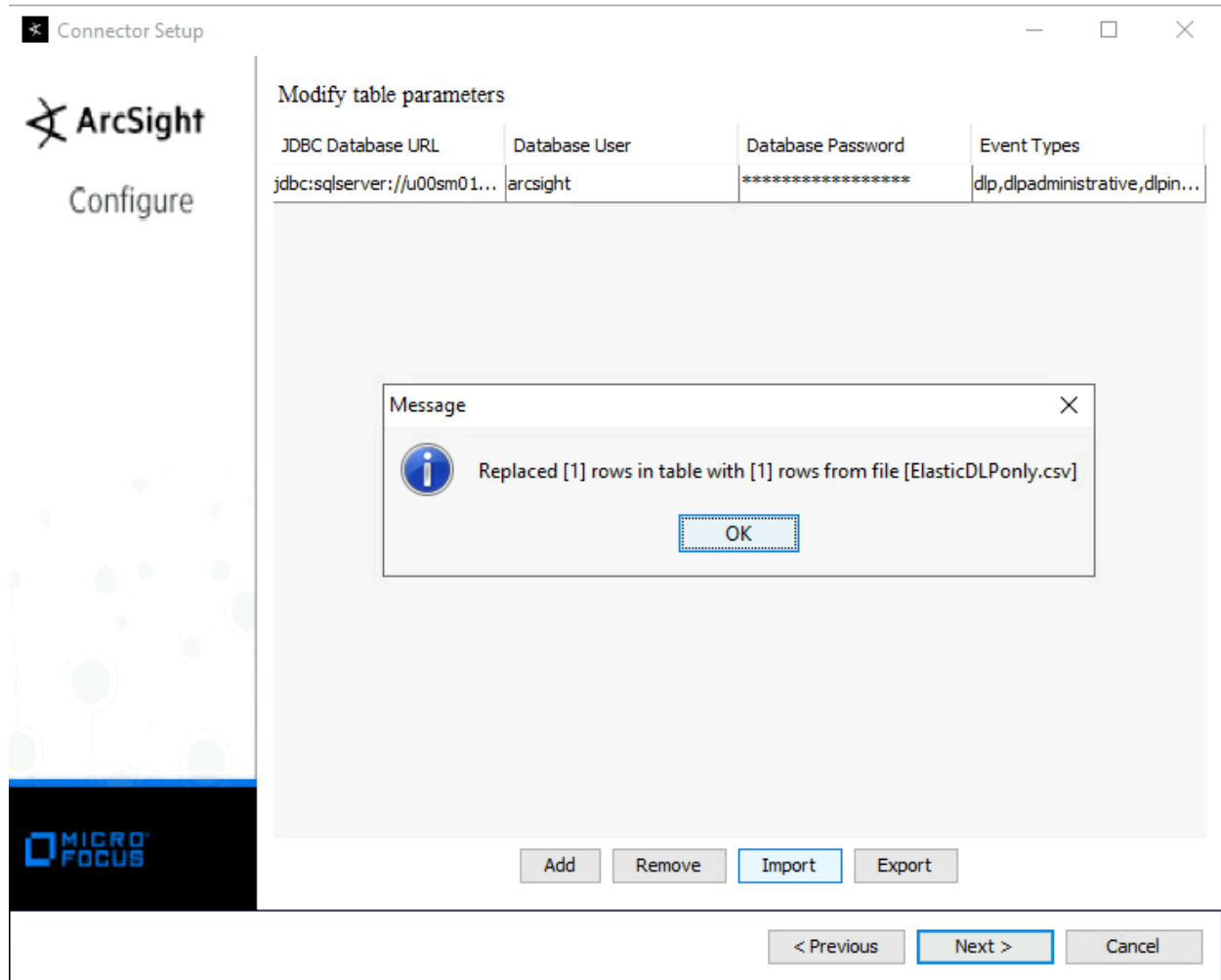


Figure 11 Confirmation of Parameter update from edited CSV file

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

UNCLASSIFIED

UNCLASSIFIED

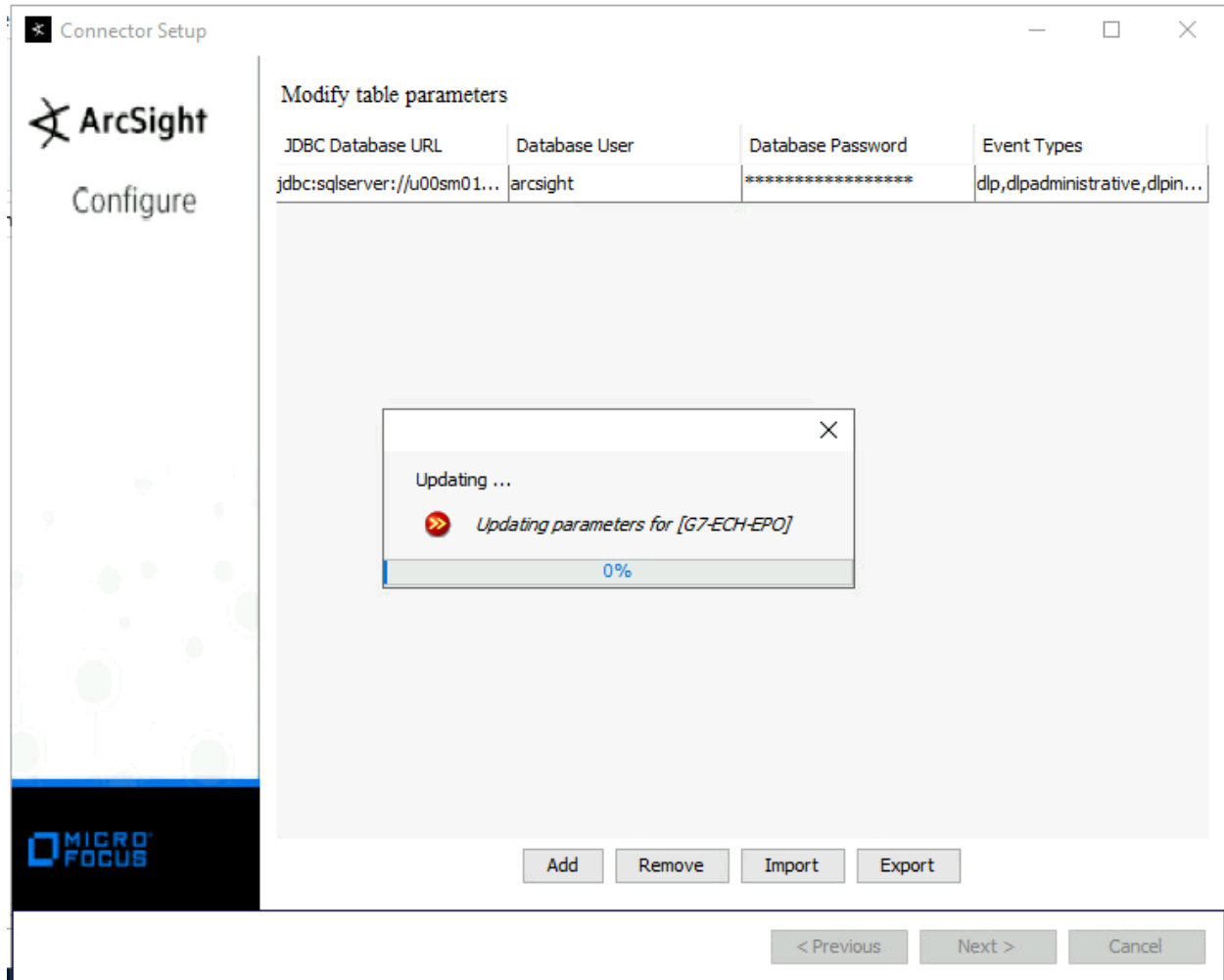


Figure 12 Updating Parameters

UNCLASSIFIED

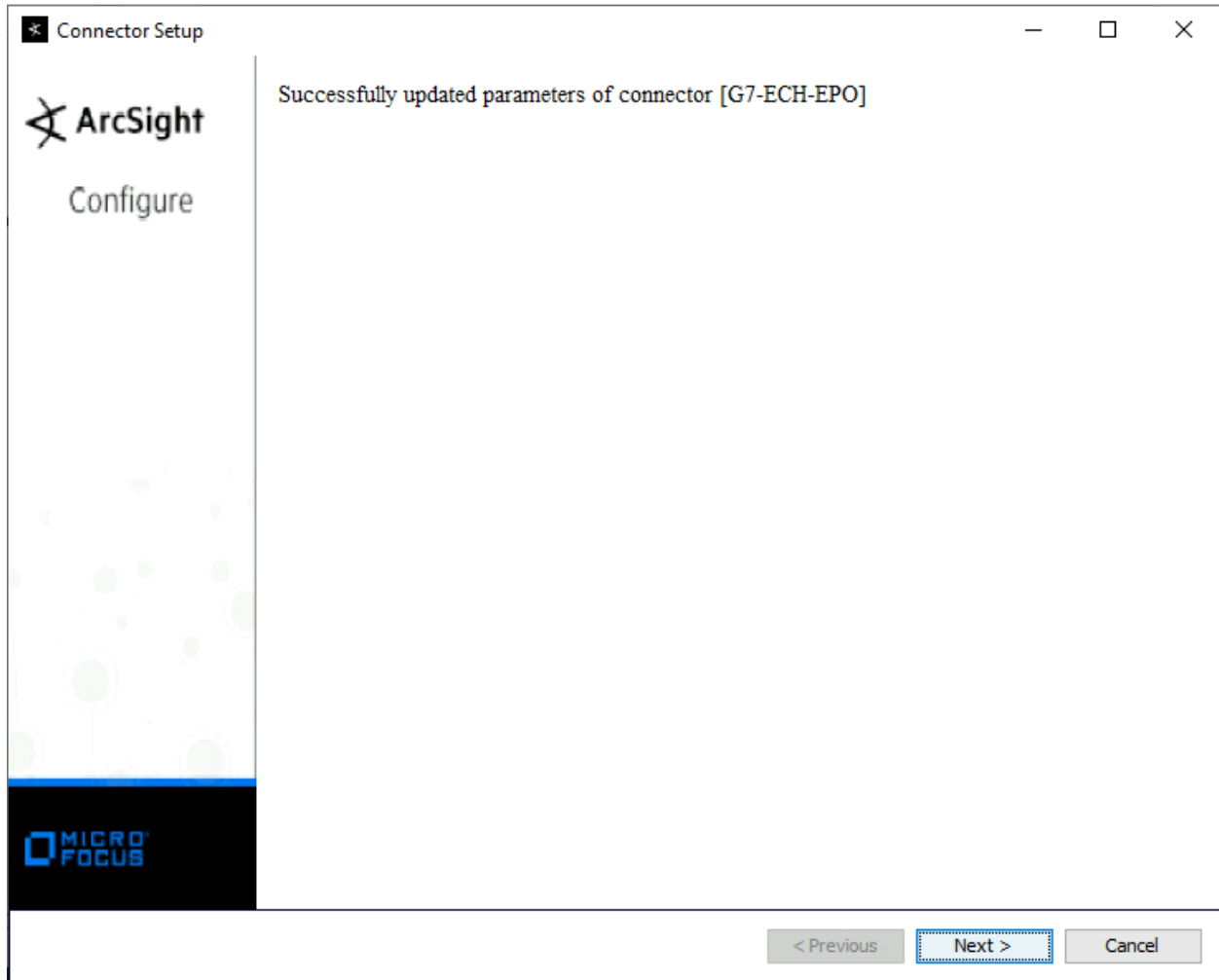


Figure 13 Successful parameter update

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

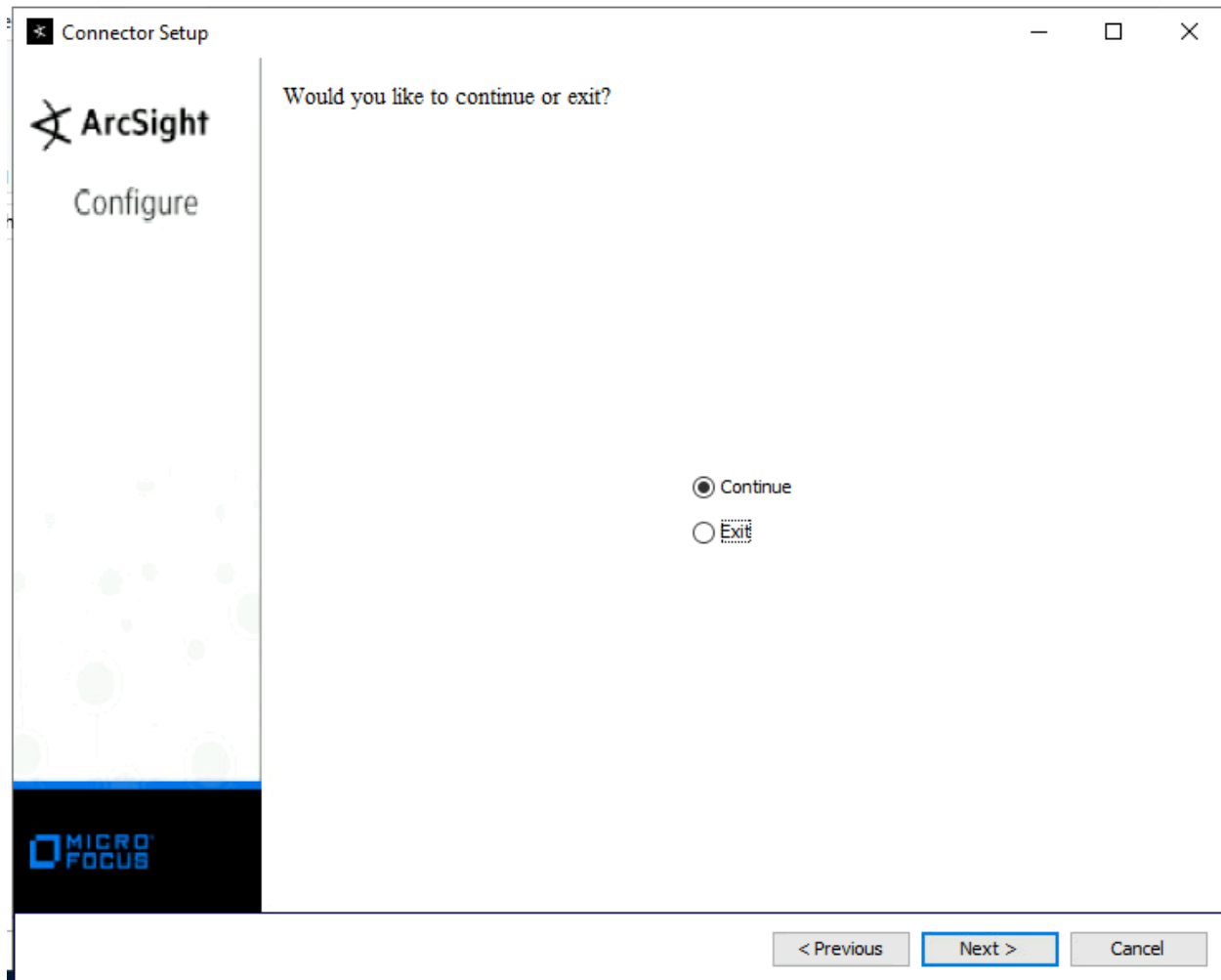


Figure 14 Select Continue and click Next

5.4.3 Modify the ArcSight ePO db SmartConnector destination

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

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

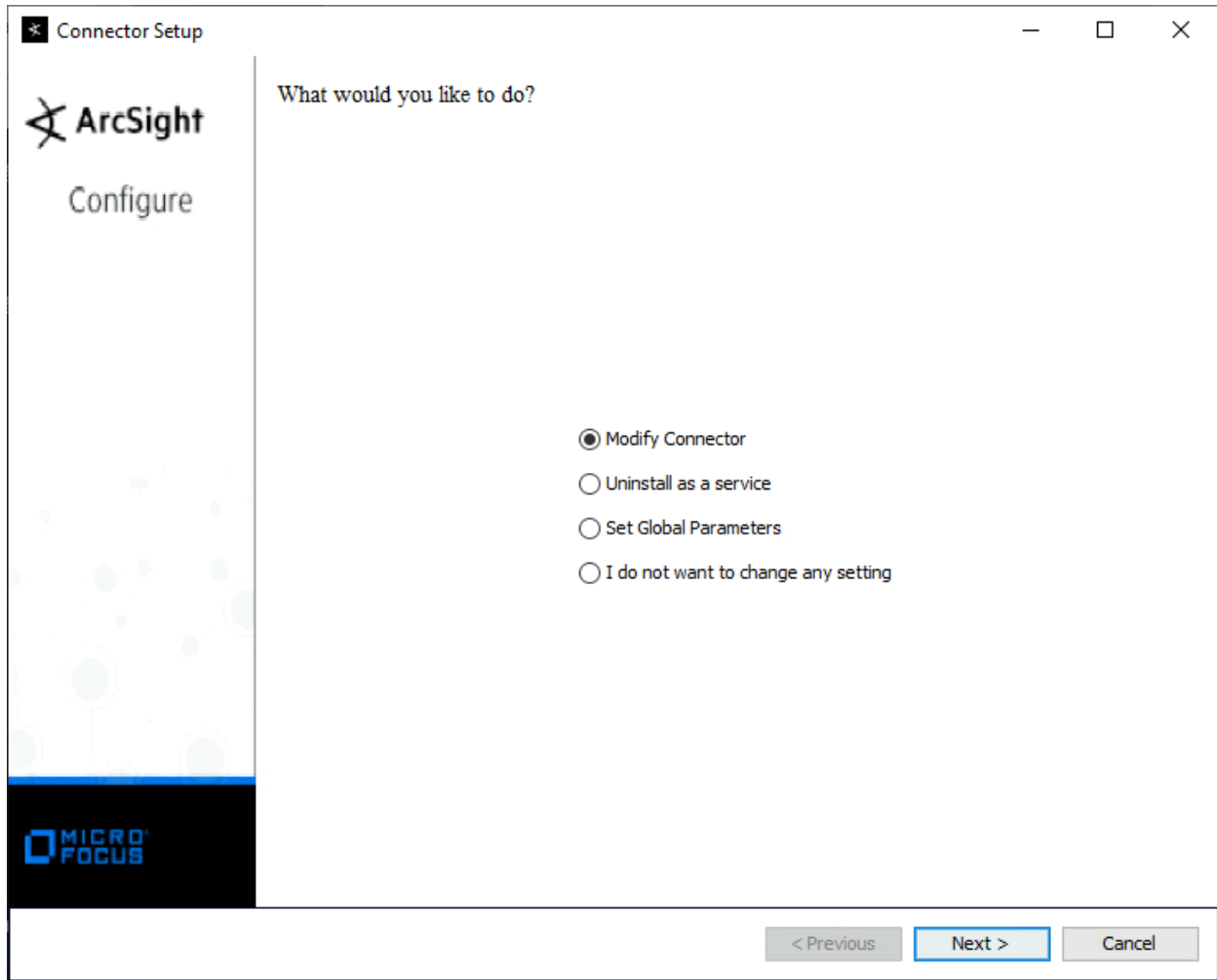


Figure 15 - Connector Setup

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

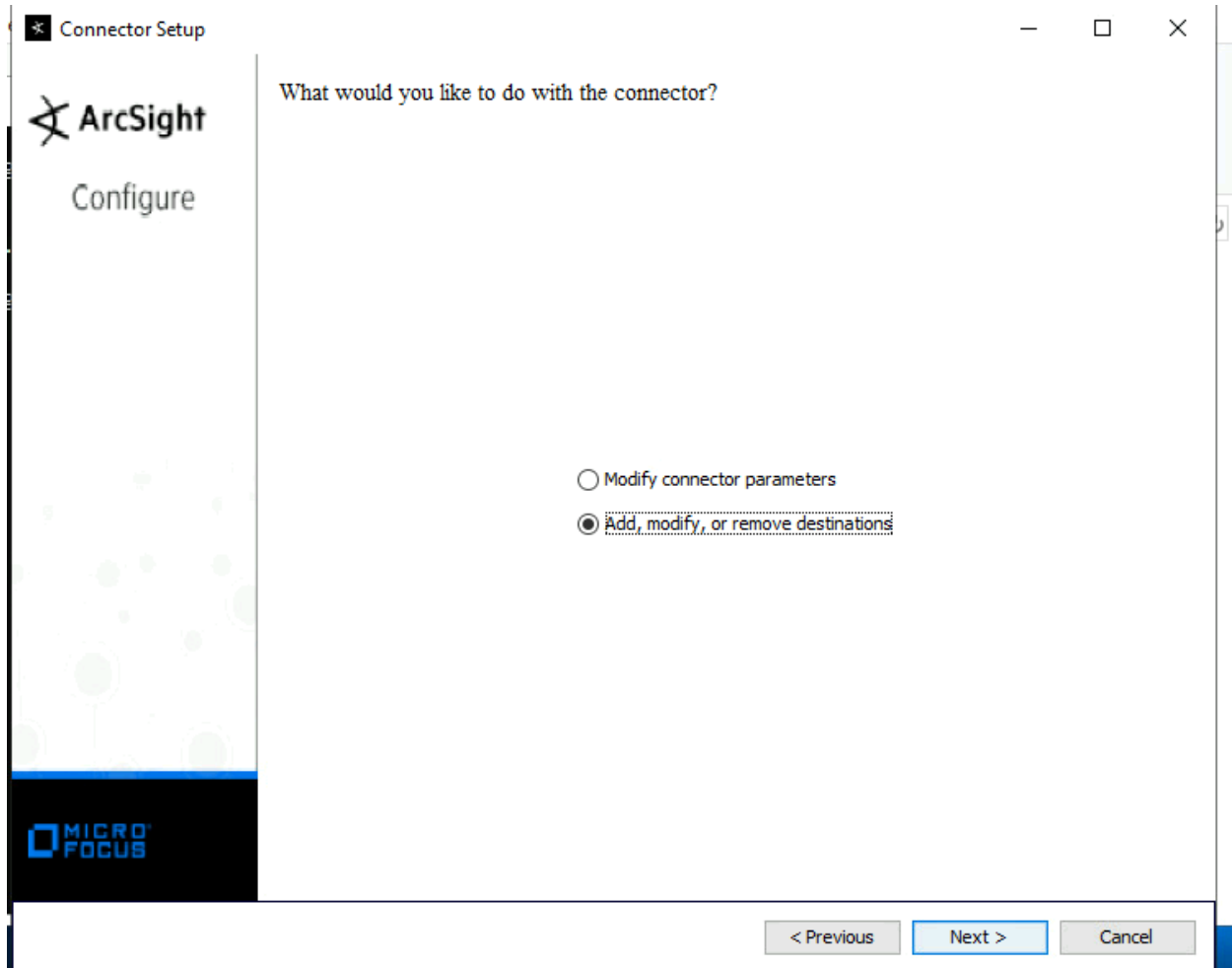


Figure 16 Modify Destination

19. 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.)

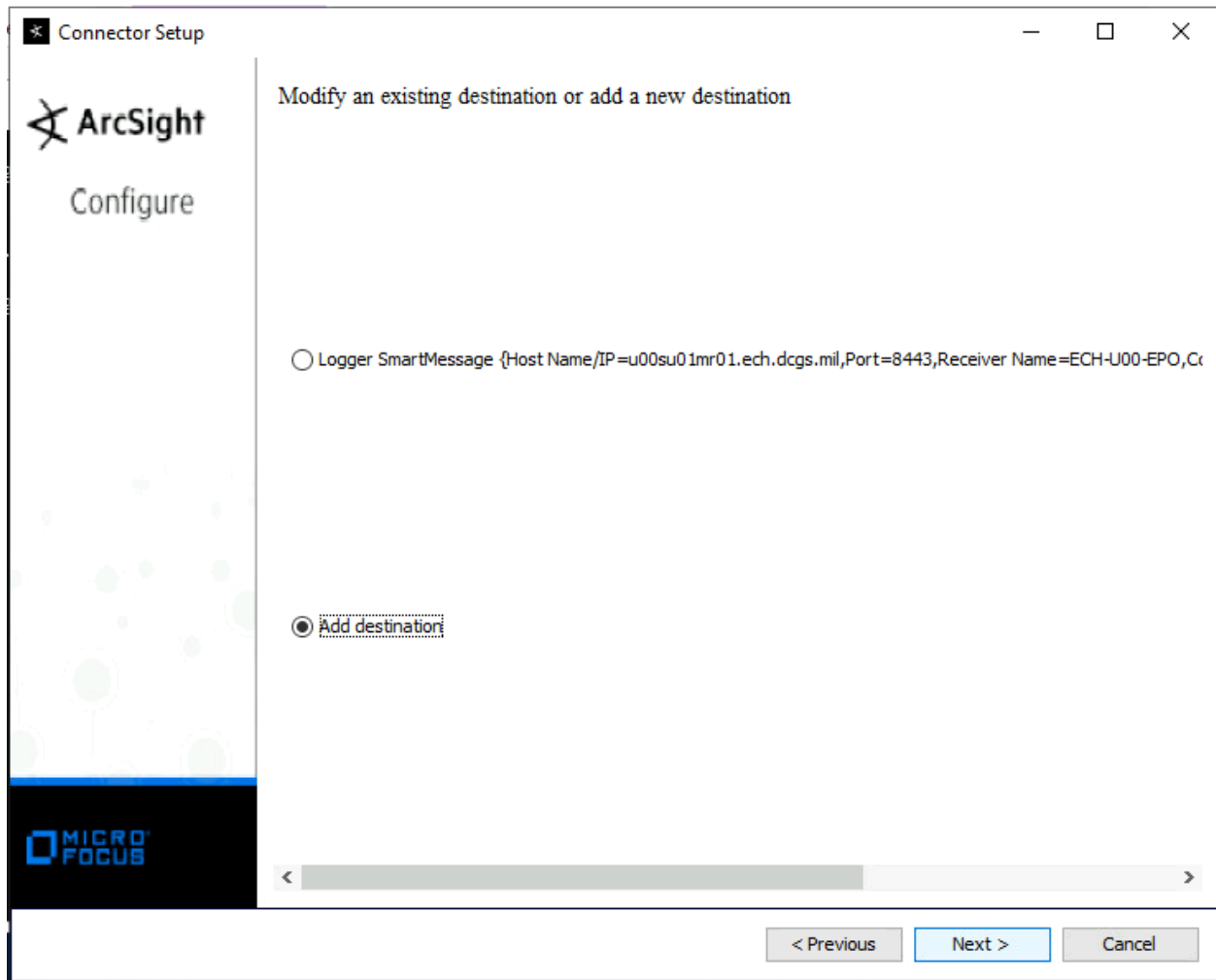


Figure 17 Add Destination

20. Select CEF Syslog, and click Next.

UNCLASSIFIED

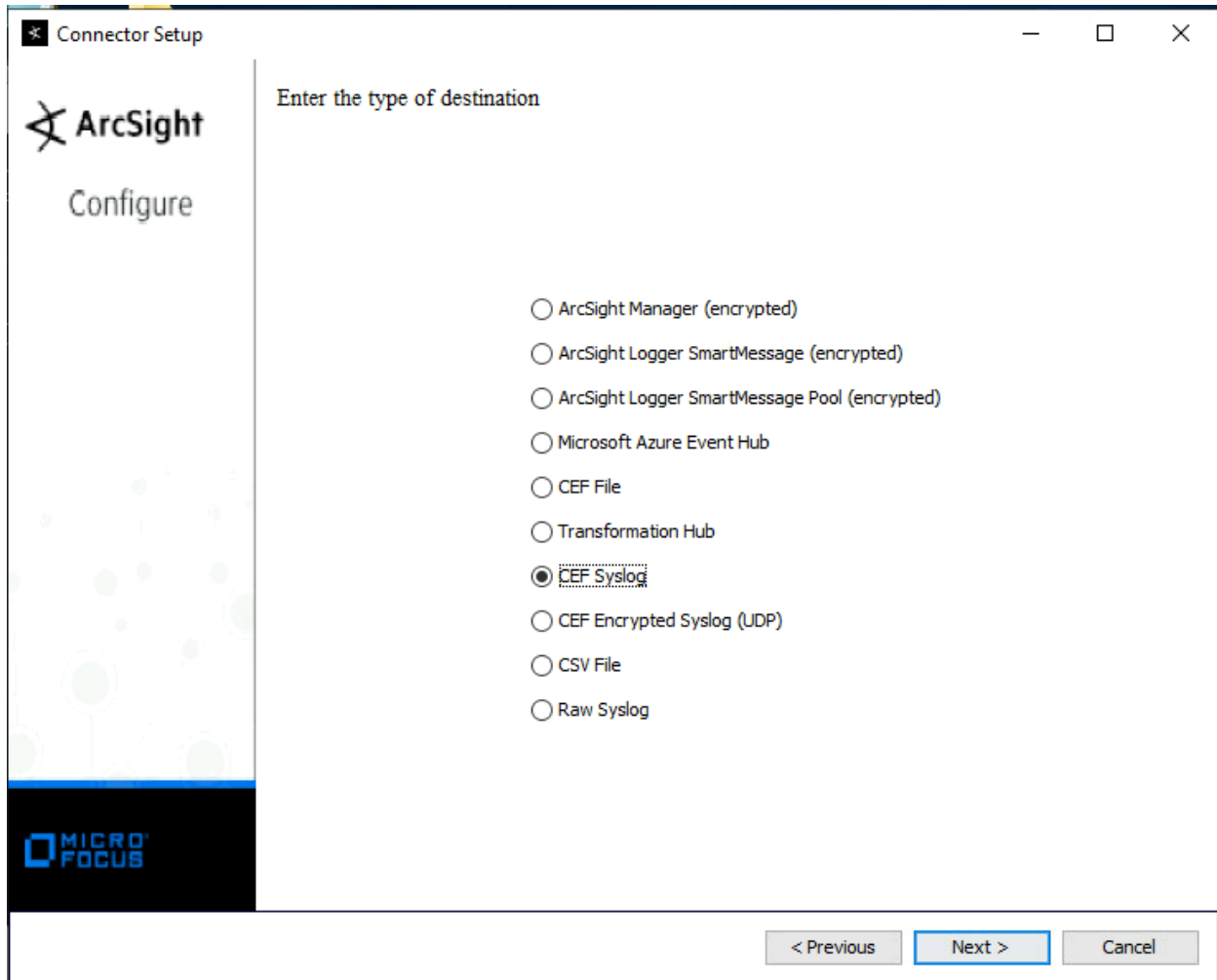
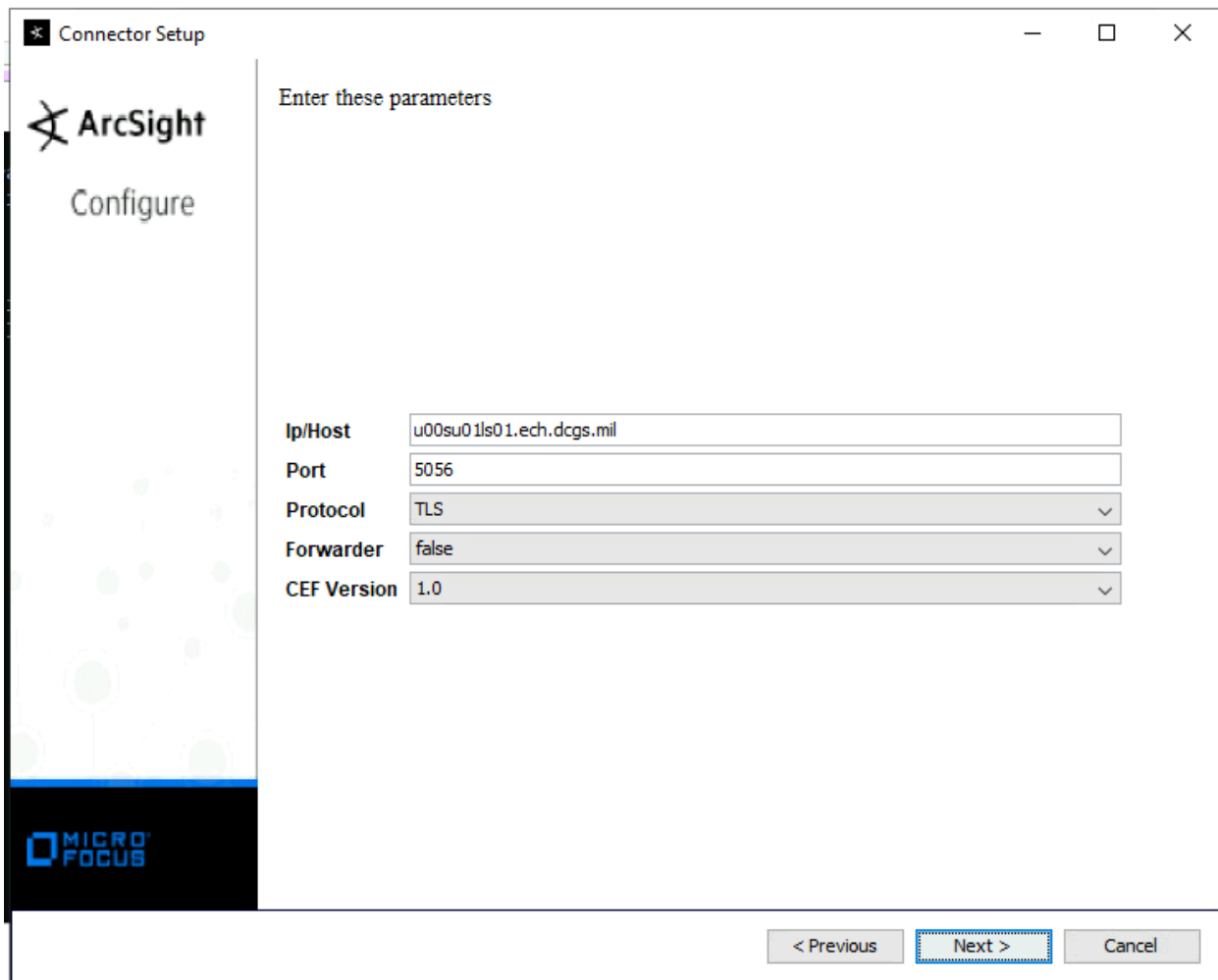


Figure 18 - CEF Syslog message type

21. 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.dcgsl.mil**. The Elastic assigned port is **5056**.

UNCLASSIFIED

UNCLASSIFIED



The screenshot shows the 'Connector Setup' window for ArcSight. The window has a title bar with standard minimize, maximize, and close buttons. On the left side, there is a sidebar with the ArcSight logo and the word 'Configure'. The main area is titled 'Enter these parameters' and contains five configuration fields:

Parameter	Value
Ip/Host	u00su01ls01.ech.dcgsl.mil
Port	5056
Protocol	TLS
Forwarder	false
CEF Version	1.0

At the bottom of the window, there are three buttons: '< Previous', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

Figure 19 Logstash server and port parameter entry

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

UNCLASSIFIED

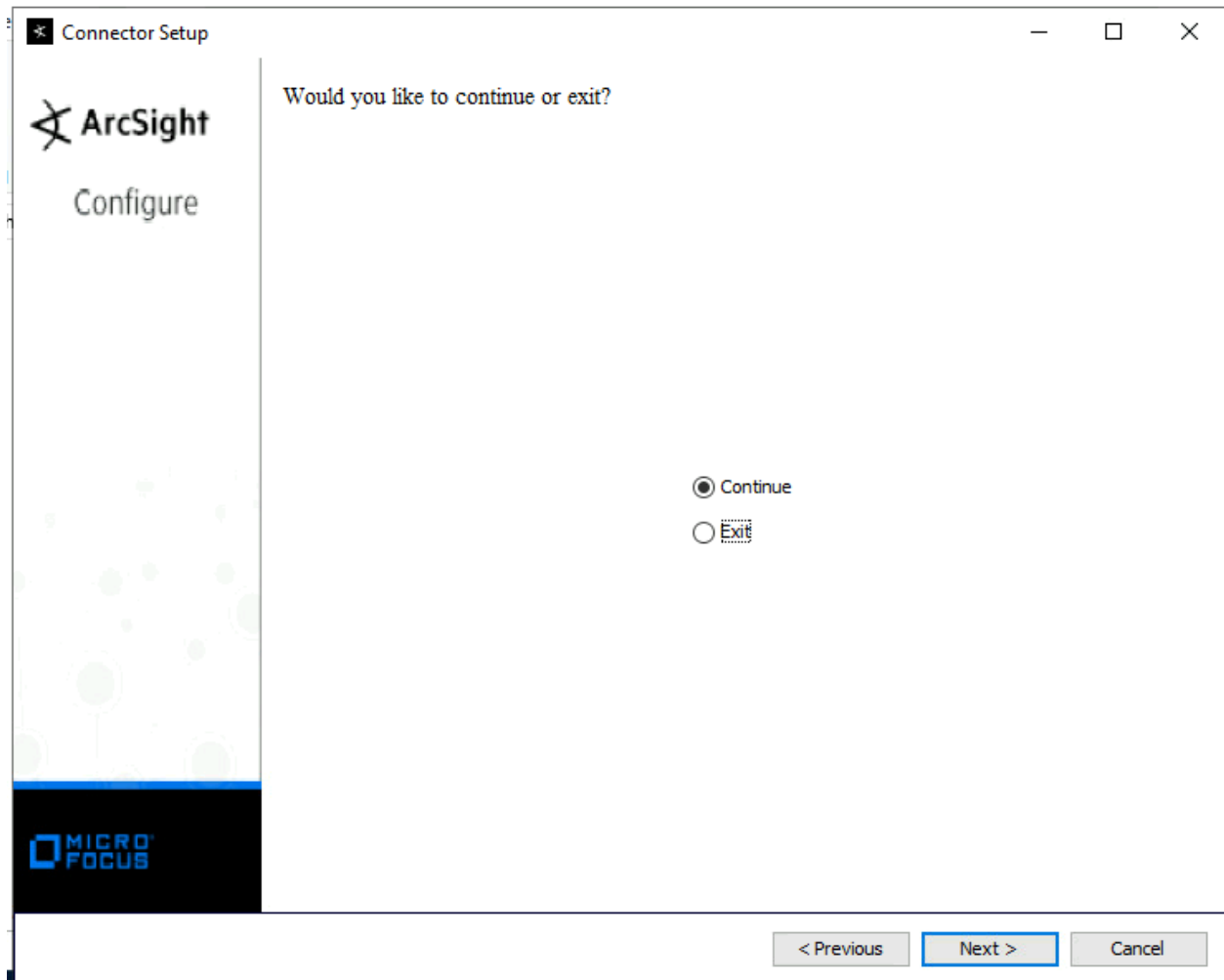


Figure 20 Continue

24. ASelect Modify a Connector and click Next

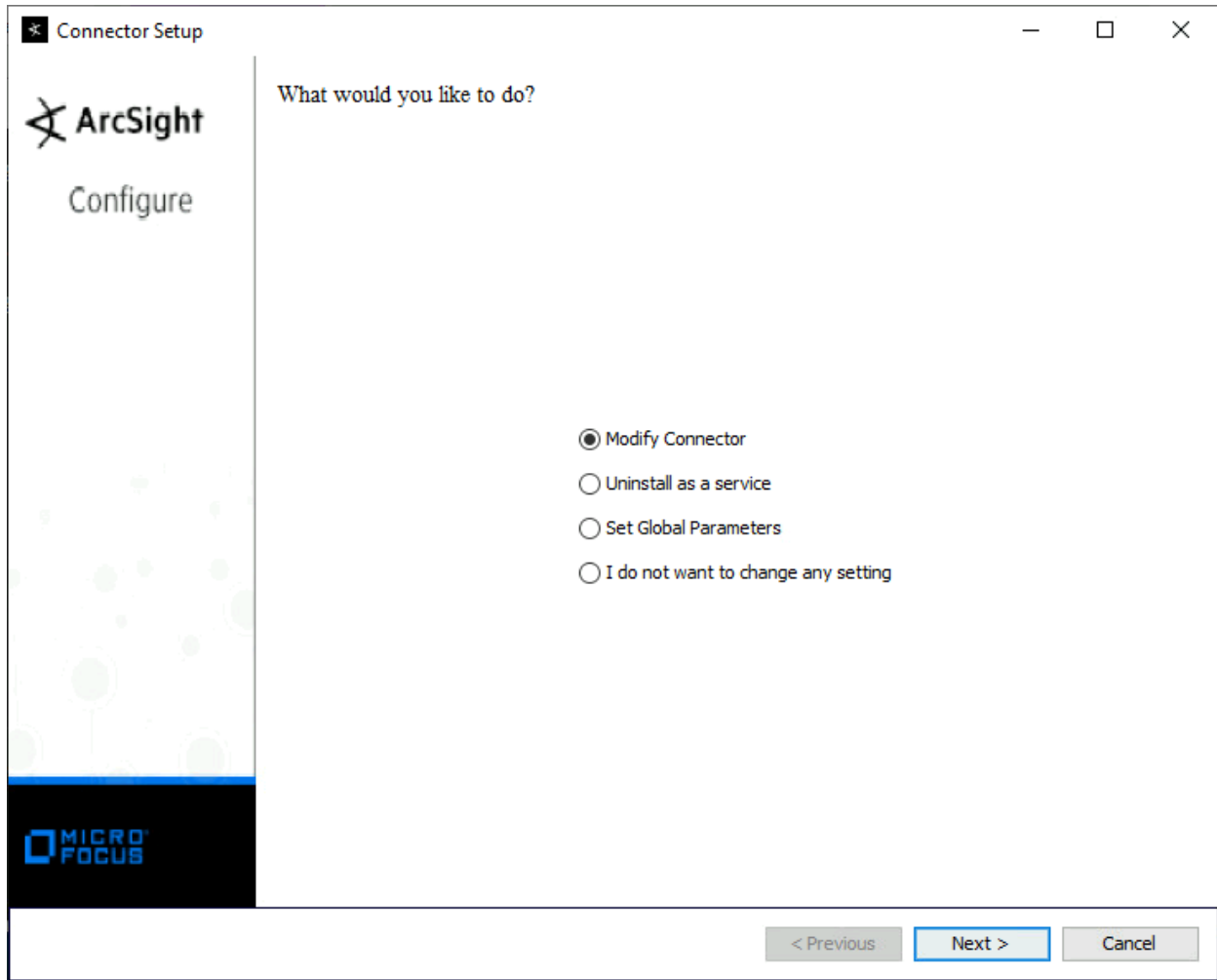


Figure 21 - Connector Setup

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

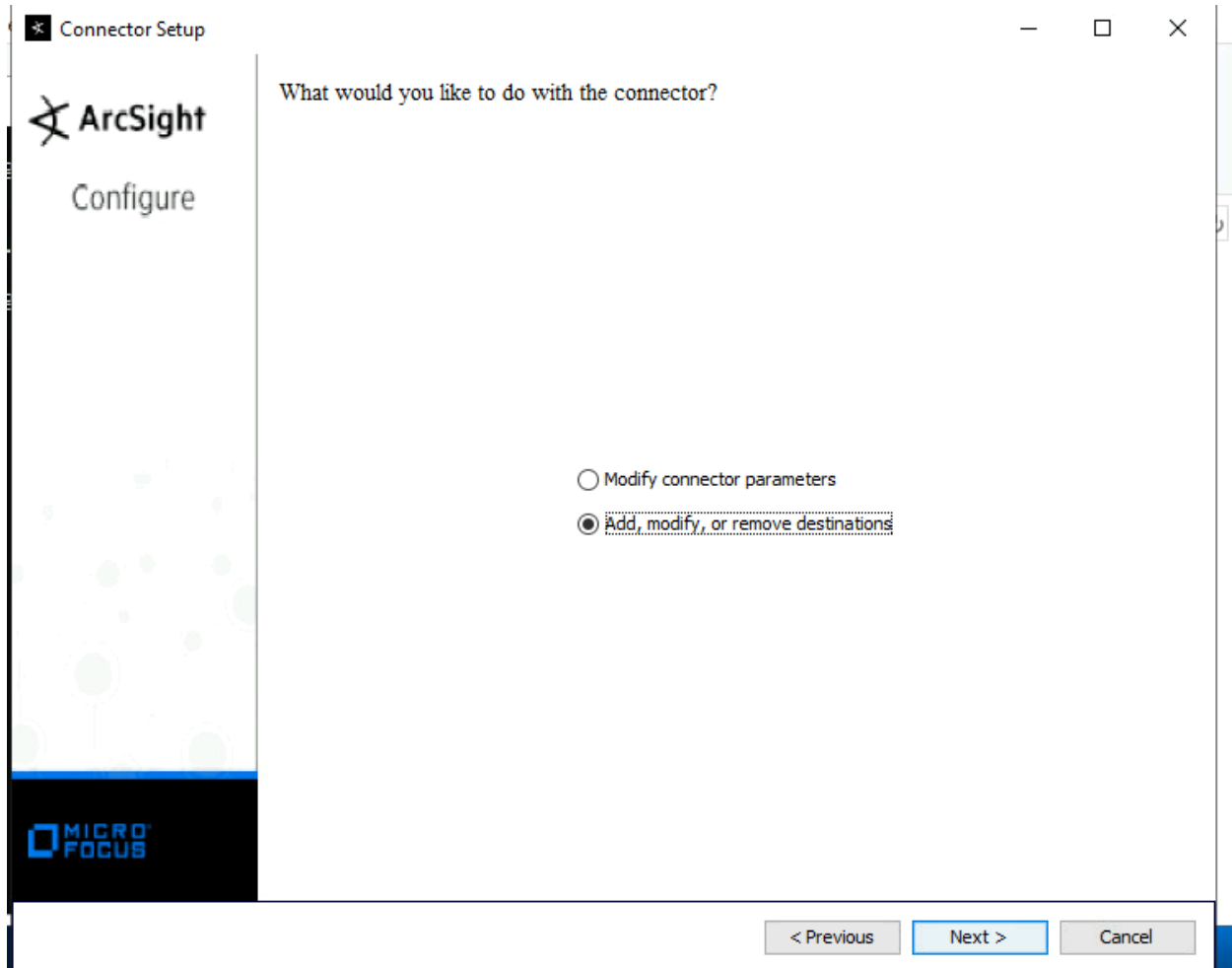


Figure 22 Modify Destination

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

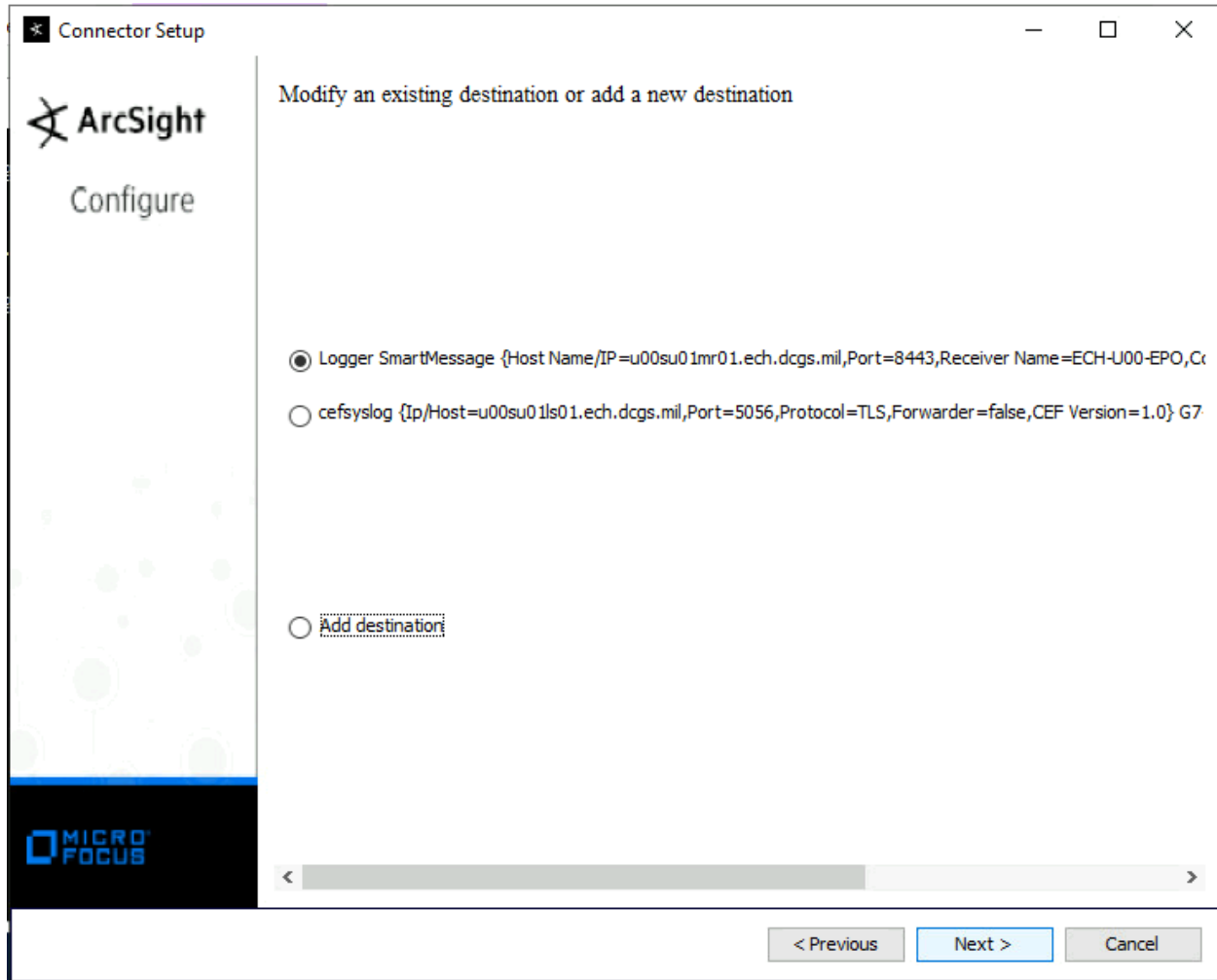
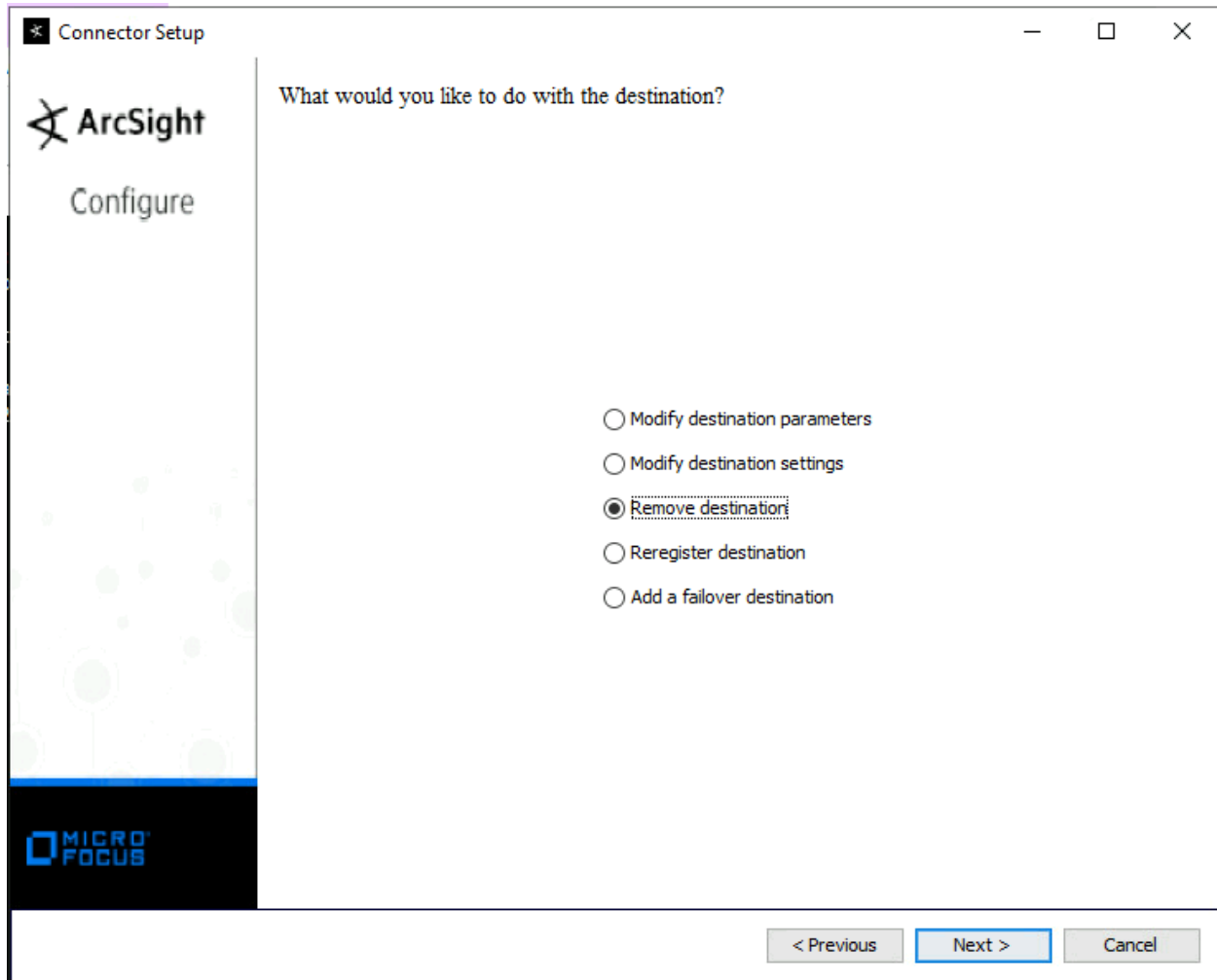


Figure 23 - Select old and not to be used destinations

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



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

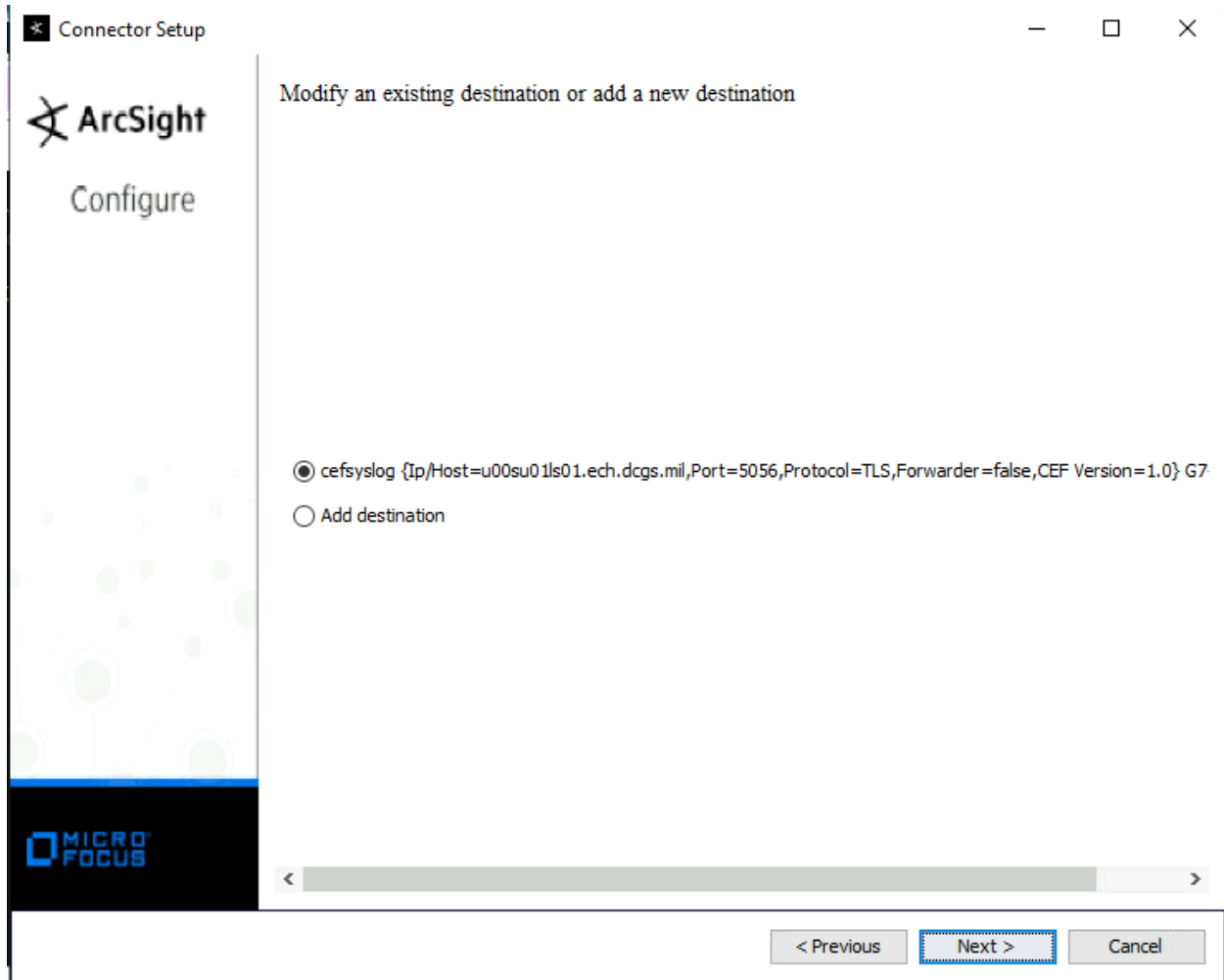


Figure 24 Final State - only the single destination, cefsyslog, should remain

29. Select exit. Click Next.

UNCLASSIFIED

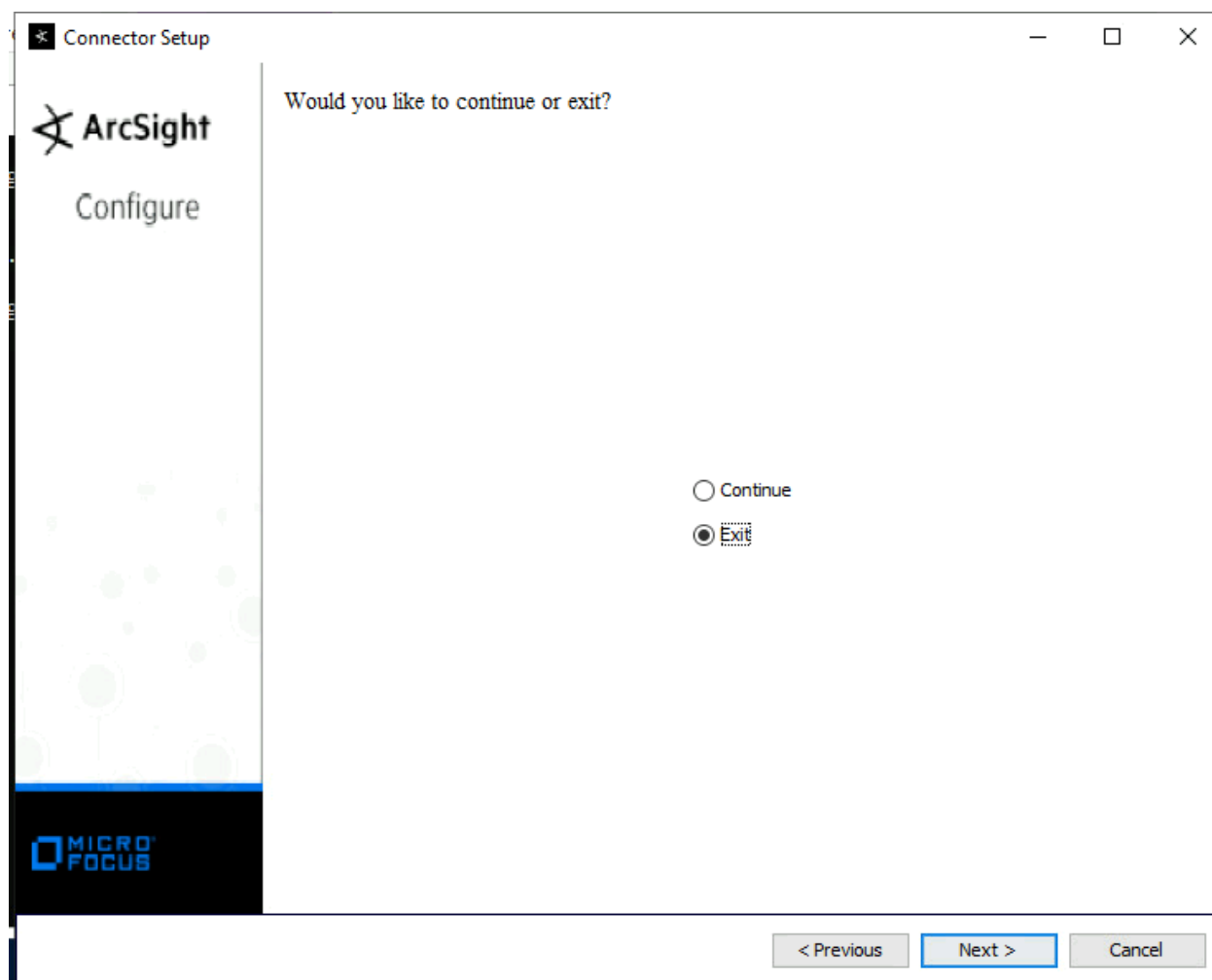


Figure 25 Exit the setup script

30. Run **Services.msc** and verify the **ArcSight McAfee ePolicy Orchestrator DB** service is present and running. **Start** the service if it is not running.
31. Generate device-plug events by plugging in an approved external USB hard disk into a physical workstation.
32. Verify reception of the event at the Elastic Server.
33. Log on to the ePO Web Console
34. 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.)

UNCLASSIFIED

UNCLASSIFIED

Reporting
Threat Event Log

Threat Event Log : Threat events received from managed systems

Preset: Last day Custom: DevicePlug Quick find: Apply Clear Show selected rows

<input type="checkbox"/>	Event Received Time	Preferred Event Time	Event ID	Event Description	Event Category	Threat Target IPv4 Ad	Action Taken	Threat Type	Th
<input type="checkbox"/>	7/19/23 6:56:56 PM UTC	7/19/23 6:44:00 PM UTC	19115	Device Plug	Policy	128.132.196.25		[DLP] Device Plugged	
<input type="checkbox"/>	7/19/23 1:56:55 PM UTC	7/19/23 1:24:00 PM UTC	19115	Device Plug	Policy	128.132.196.25		[DLP] Device Plugged	
<input type="checkbox"/>	7/19/23 1:31:51 PM UTC	7/19/23 12:46:00 PM UTC	19115	Device Plug	Policy	128.132.196.109		[DLP] Device Plugged	
<input type="checkbox"/>	7/19/23 12:56:55 AM UTC	7/19/23 12:55:00 AM UTC	19115	Device Plug	Policy	128.132.196.25		[DLP] Device Plugged	
<input type="checkbox"/>	7/19/23 12:21:52 AM UTC	7/19/23 12:16:00 AM UTC	19115	Device Plug	Policy	128.132.196.25		[DLP] Device Plugged	

Figure 26 Obtain a quick list of device plug events to compare with Elastic

5.4.4 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**

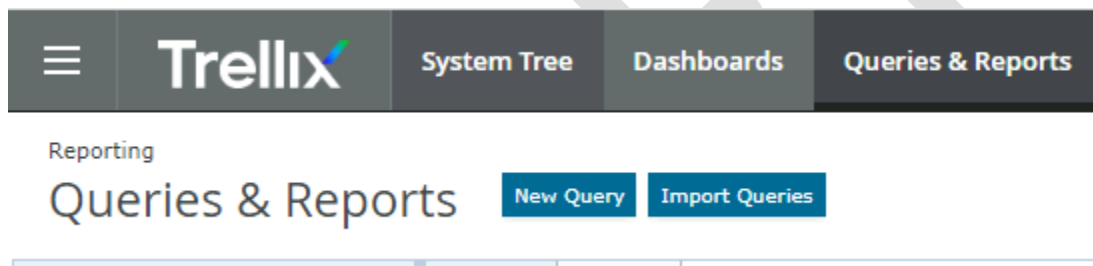


Figure 27 Import Query

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

UNCLASSIFIED

UNCLASSIFIED

Reporting
Queries & Reports

Import Queries

File to import: DevicePlugQuery.xml

Group:

☐ New group

☐ Private (Private Groups)

☐ Public (Shared Groups)

☐ Existing group

Figure 28 Query import screen

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

Reporting

Queries & Reports

DevicePlug Events

Export Table

Hide Filter

Custom:None

Show selected rows

|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

Figure 29 Sample query output

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

UNCLASSIFIED

UNCLASSIFIED

Reporting
Queries & Reports

Query Builder 1 Result Type 2 Chart 3 Columns

Which criteria do you want to use to narrow the results of the query? To return all available data, continue without selecting any properties.

Available Properties	Property	Comparison	Value
Search X	DLP Data In-use/motion Incidents History		
▼ DLP Data In-use/motion In...	Occurred (UTC)	Is within the last	2 Days

Figure 30 Edit query, filter tab

9. Export data by clicking Export Table

Reporting
Queries & Reports

DevicePlug Events

Custom: None Show selected rows

Export Table Hide Filter

Figure 31 Export Table button

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

5.5 Installation Instructions for Upgrades

N/A

5.6 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.

UNCLASSIFIED

6 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

6.1 De-Installation Instructions for Upgrades

N/A

7 FREQUENTLY ASKED QUESTIONS

N/A

DRAFT

8 REFERENCES

N/A

DRAFT

9 TEST RESULTS

LEAVE THIS BLANK BUT DO NOT DELETE.

FILL OUT THE IAAS-023 TEST REPORT TEMPLATE.

DRAFT

10 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	

UNCLASSIFIED

APPENDIX A ACRONYMS

Acronym	Definition

UNCLASSIFIED

APPENDIX B KNOWN ISSUES

You can delete this if there are no known issues.

DRAFT