Infoblox
CONTROL YOUR NETWORK

Data Connector 3.0 SIEM Support

By Thomas Lee, Technical Marketing Engineer

Date: October, 2018

Summary

In late August 2018, Infoblox released Data Connector 3.0. Infoblox Data Connector is a purpose-built, highly efficient, virtual appliance that collects DDI (DNS, DHCP, and IPAM) data from Infoblox Grid for Infoblox Active Trust Cloud, Splunk Enterprise, and Infoblox Reporting Server. Data Connector 3.0 converts the data to formats that are easily consumable by those systems and, in the case of Splunk Enterprise and Infoblox Reporting Server, it also filters the data. In doing so, it saves customers' time and resources by automating the collection, transfer, and converting of DDI data to reporting/analytics systems. It also minimizes the burden on the Infoblox Grid members by offloading the data processing functions. In addition, Data Connector 3.0 supports sending this DDI to MicroFocus Arcsight, McAfee ESM, and IBM QRadar SIEMs.

Note: These instructions only apply to the SIEM integrations. Please refer to the Data Connector 3.0 Deployment Guide or the Data Connector 3.0 User Guide for further instructions.

SIEM Integration Instructions

Data Connector 3.0 tested the forwarding of DNS query data to:

- Microfocus ArcSight 7.0.0.2410.0
- McAfee ESM 10.1.0.
- IBM QRadar 7.2.8.

ArcSight Integration Instructions

Here are the instructions for configuring the Data Connector to ArcSight:

1. Type 'data destination siem' to go to the SIEM configuration section.

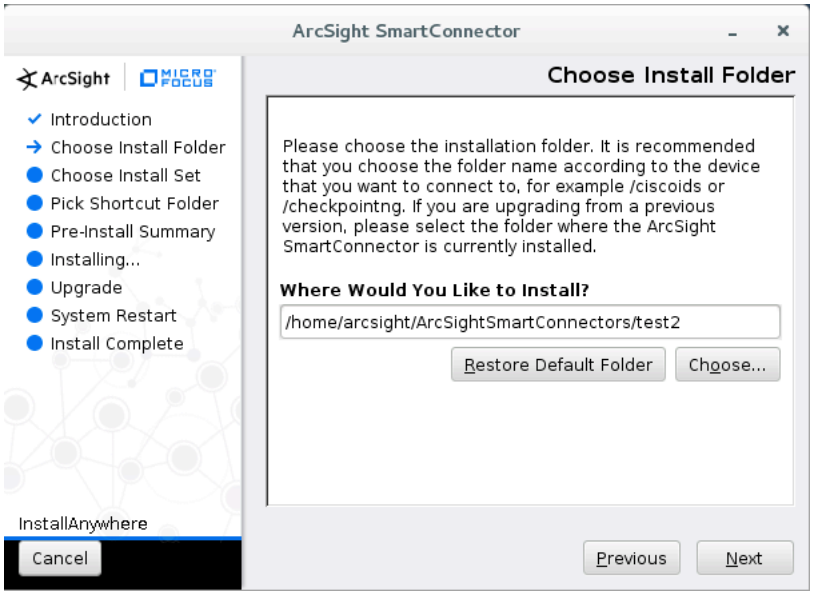
```
[ > data destination siem
data.destination.siem >
```

2. Type 'ArcSight'.

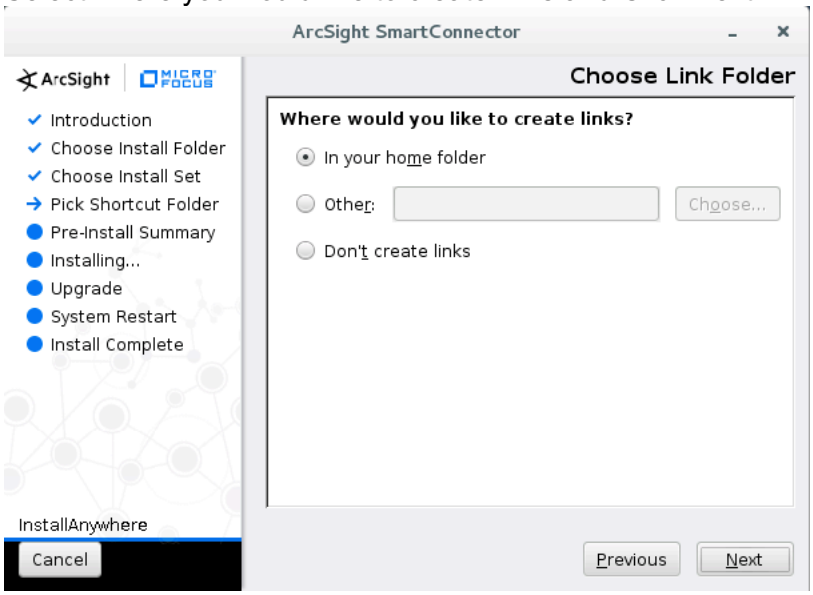
```
data.destination.siem > ArcSight
data.destination.siem.ArcSight >
```

3. To add the IP address of your ArcSight SIEM, type 'add address <IP address>'.
4. By default, the forwarding mode is set to hold. The possible settings are: hold, forward, or disabled. The hold setting allows the data connector to accumulate data gathered from the Infoblox Grid Members. The disabled setting disables any accumulation and forward of DNS data. To configure the output mode to forward, type 'set mode forward' to start forwarding data to the SIEM.
5. To set the port number to communicate with the ArcSight SIEM, type 'set port <number>'.
6. To import the certificate from the ArcSight SIEM, type certificate import <scp|ftp>://loginname@serverIP:[port:]path
7. On the ArcSight side, execute the program called 'ArcSight-<version string>-connector' to add a SmartConnector.

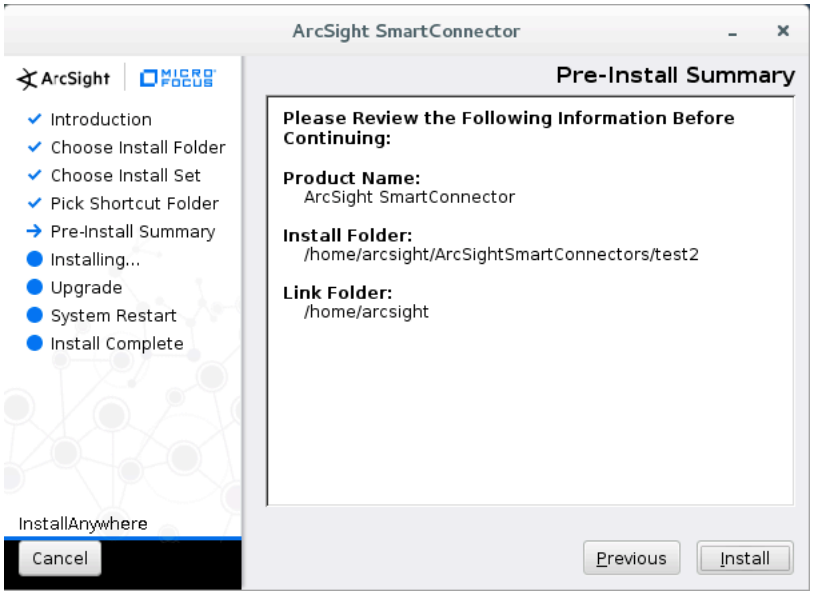
8. Select the installation folder and Click Next.



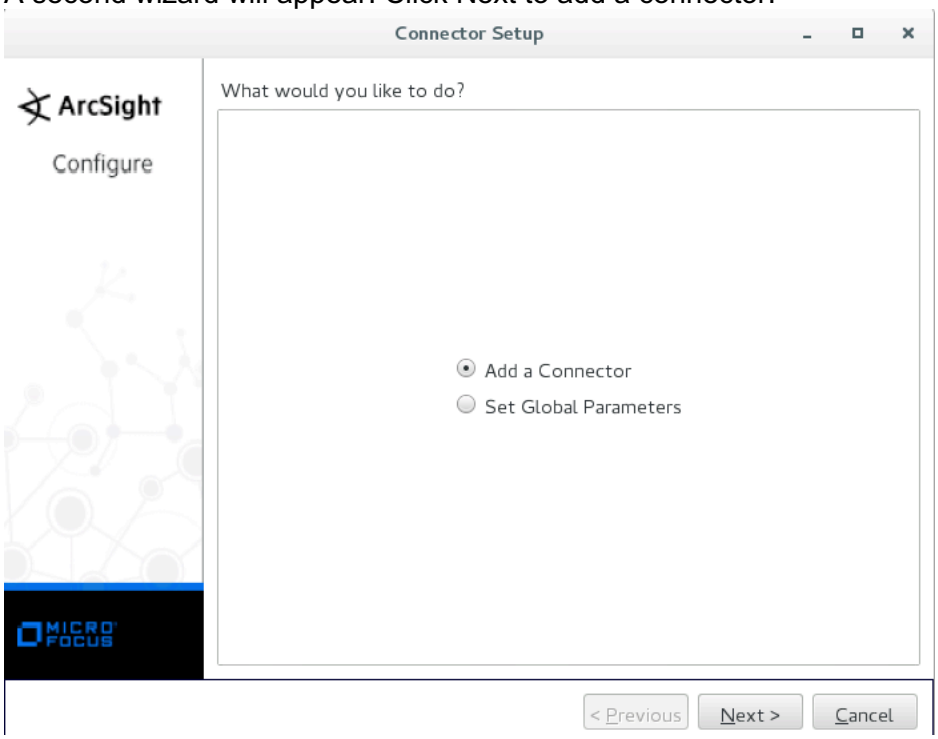
9. Select where you would like to create links and Click Next.



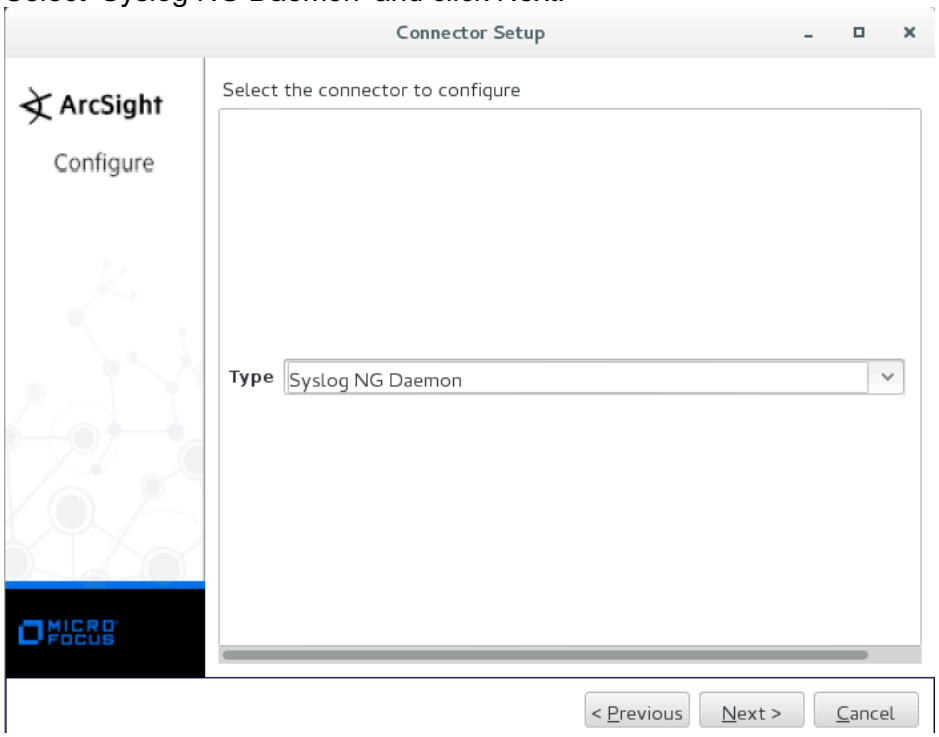
10. Review the information and click Next to confirm or click Previous to go back.



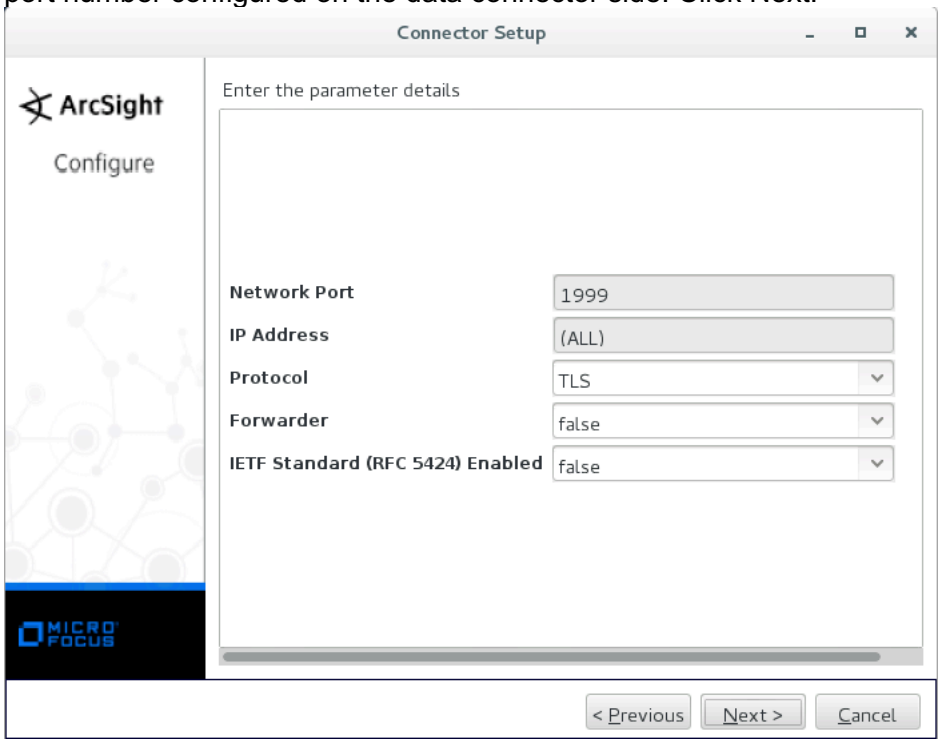
11. A second wizard will appear. Click Next to add a connector.



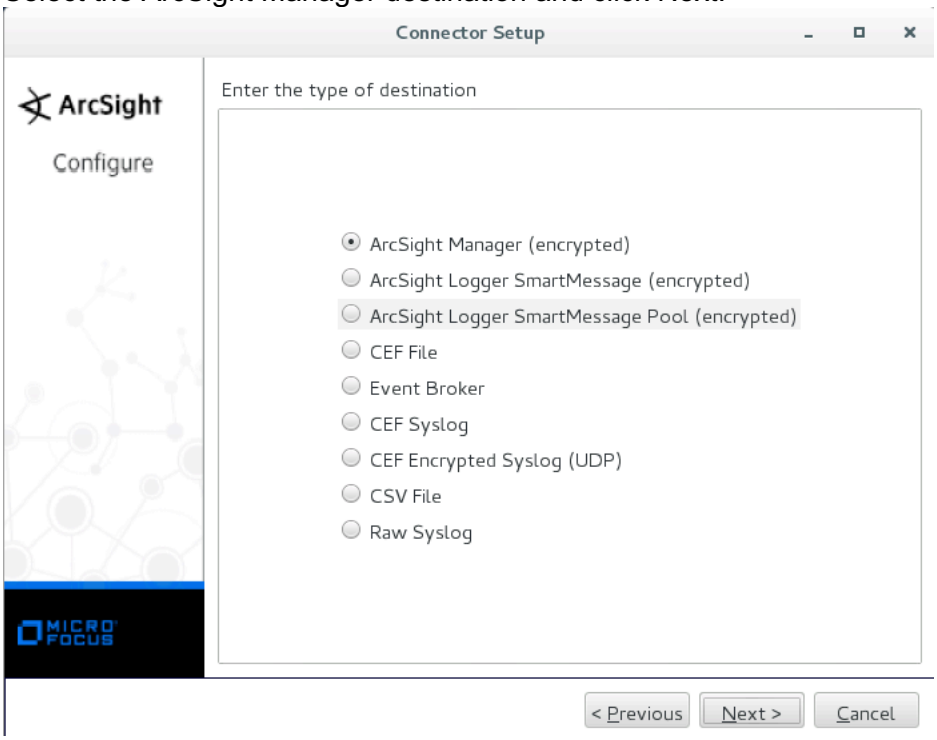
12. Select ‘Syslog NG Daemon’ and click Next.



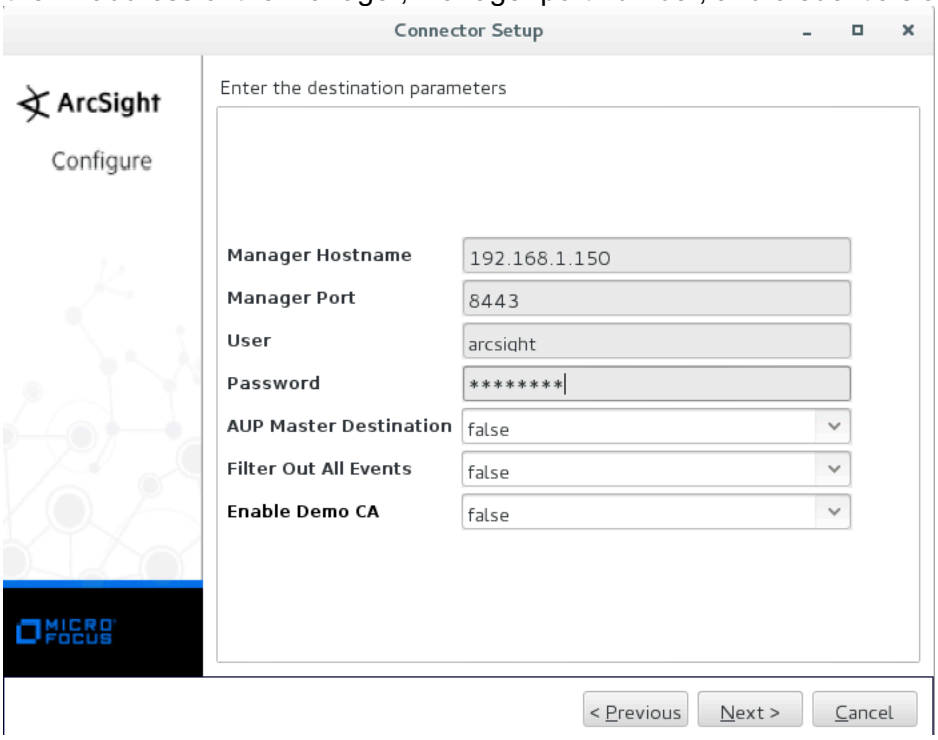
13. Enter the port number and IP address of data connector. The port number must match the port number configured on the data connector side. Click Next.



14. Select the ArcSight Manager destination and click Next.



15. Enter the IP address of the manager, manager port number, and credentials and click Next.



16. Complete the rest of the installation per the installation wizard.

McAfee Integration Instructions

Here are the instructions for configuring the Data Connector to McAfee ESM:

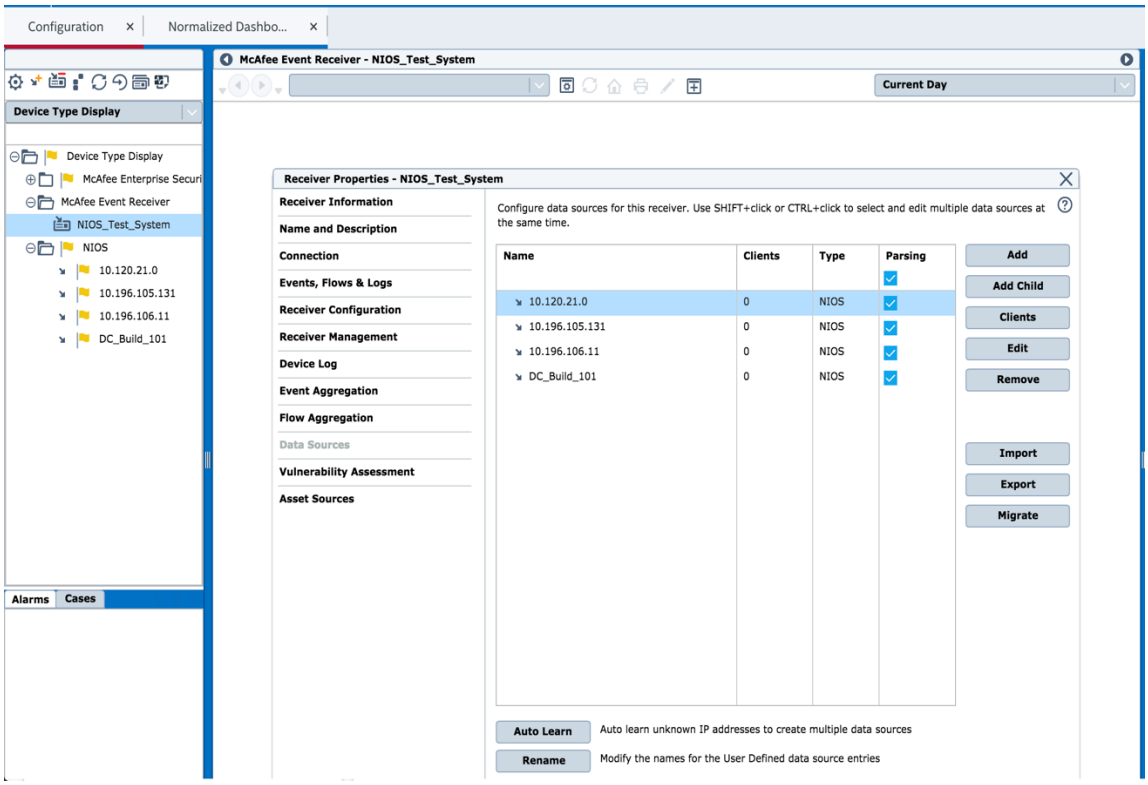
1. Type ‘data destination siem’ to go to the SIEM configuration section.

```
[ > data destination siem
data.destination.siem >
```

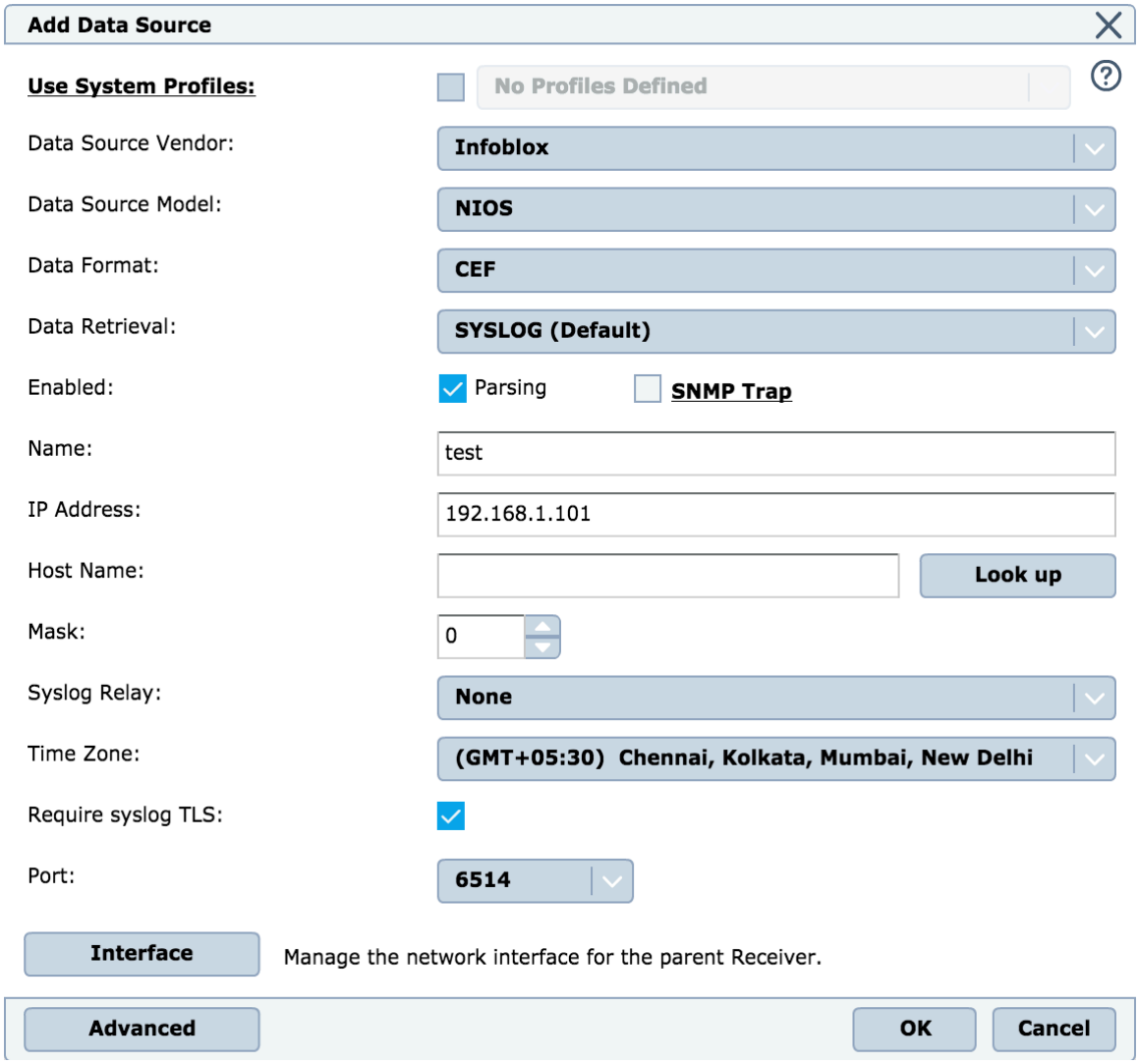
2. Type ‘McAfee’.

```
data.destination.siem > McAfee
data.destination.siem.McAfee >
```

3. To add the IP address of your McAfee SIEM, type ‘add address <IP address>’.
4. By default, the forwarding mode is set to hold. The possible settings are: hold, forward, or disabled. The hold setting allows the data connector to accumulate data gathered from the Infoblox Grid Members. The disabled setting disables any accumulation and forward of DNS data. To configure the output mode to forward, type ‘set mode forward’ to start forwarding data to the SIEM.
5. To set the port number to communicate with the McAfee SIEM, type ‘set port <number>’.
6. To import the certificate from the McAfee SIEM, type certificate import <scp|ftp>://loginname@serverIP:[port:]path
7. Log into McAfee ESM.
8. Navigate to System Navigation Tree → Configuration → McAfee Event Receiver → Selected Event Receiver.



9. Click on the ‘Add’ button.



10. Fill out the following fields:
    a. Data Source Vendor: Infoblox
    b. Data Source Model: NIOS. This will be filled in automatically when Infoblox is selected in Data Source Vendor pull-down menu.
    c. Data Format: CEF.
    d. Data Retrieval: Syslog
    e. Name of Data Source.
    f. IP Address: IP address of data connector.
    g. Require syslog TLS: Enabled.
    h. Port number: Use the default if that is acceptable.
11. Click OK.

IBM QRadar Integration Instructions

Here are the instructions for configuring the Data Connector to QRadar:

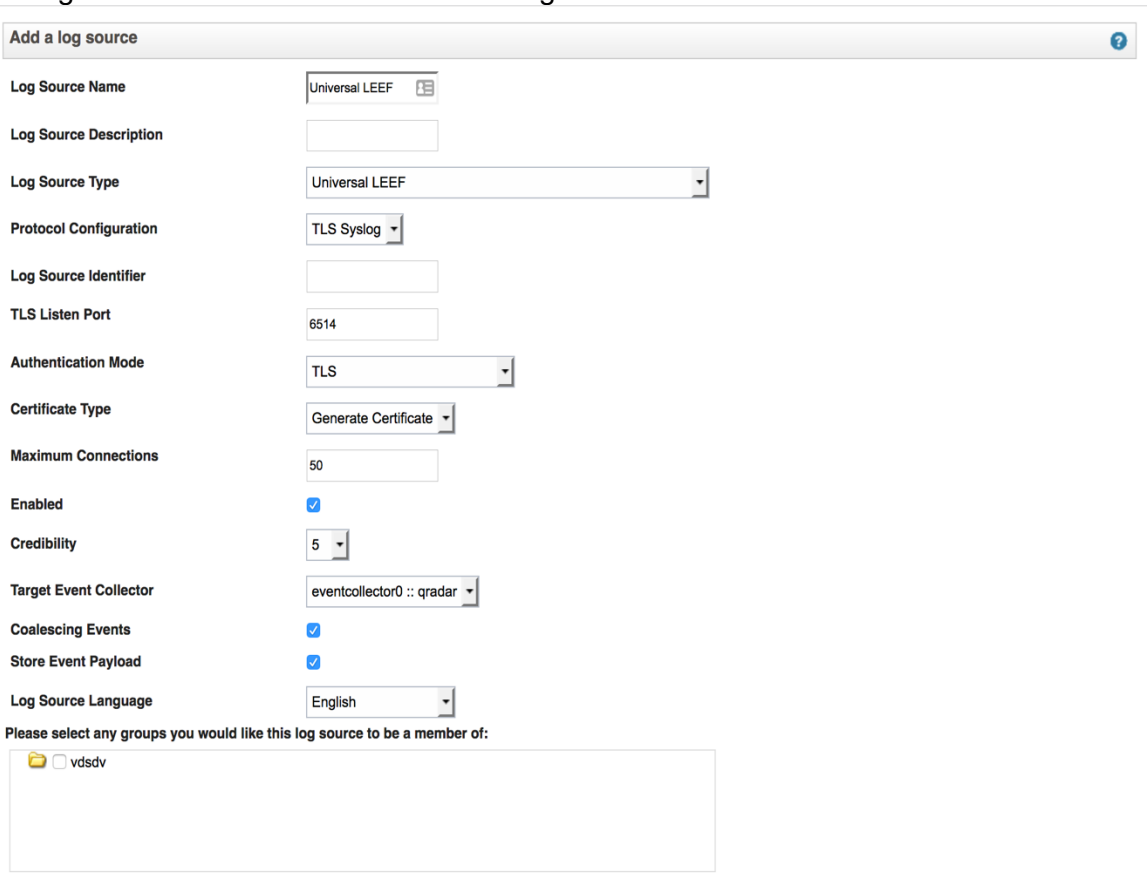
1. Type ‘data destination siem’ to go to the SIEM configuration section.

```
[ > data destination siem
data.destination.siem > 
```

2. Type ‘QRadar’.

```
[data.destination.siem > QRadar
 data.destination.siem.QRadar > 
```

3. To add the IP address of your QRadar SIEM, type ‘add address <IP address>’.
4. By default, the forwarding mode is set to hold. The possible settings are: hold, forward, or disabled. The hold setting allows the data connector to accumulate data gathered from the Infoblox Grid Members. The disabled setting disables any accumulation and forward of DNS data. To configure the output mode to forward, type ‘set mode forward’ to start forwarding data to the SIEM.
5. To set the port number to communicate with the QRadar SIEM, type ‘set port <number>’.
6. To import the certificate from the QRadar SIEM, type certificate import <scp|ftp>://loginname@serverIP:[port:]path
7. Log into IBM QRadar.
8. Navigate to Admin → Data Sources → Log Sources.



9. Click on the ‘Add’ button.
10. Fill out the following fields:
    a. Log Source Name.
    b. Log Source Description (optional).
    c. Log Source Type: Universal LEEF.
    d. Protocol Configuration: TLS Syslog
    e. Log Source Identifier; this is the IP address of the data connector.

f. TLS Listen Port; ensure the port numbers match between IBM QRadar and Infoblox Data Connector.
g. Authentication Mode: TLS
h. Certificate Type.

11. Enable the log source when ready.
12. Add the log source to the groups.

Click Save.