Infoblox
CONTROL YOUR NETWORK

DEPLOYMENT GUIDE

Integration with McAfee DXL

Visibility into Network Changes and Faster Threat Containment Using Outbound APIs

Contents

Introduction

Security ecosystem tools lack easy access to network data and don't have visibility into threats detected by DNS security solutions. Being able to detect and respond in real time to network events and threats seen by the DNS protection platform greatly accelerates incident response. However, the lack of easy access to network data inhibits taking the right action based on context. Infoblox integration with McAfee DXL enables ecosystem solutions to take action on network and security events detected by Infoblox and contain threats faster.

Infoblox publishes security and networking event topics, along with context over DXL using outbound RESTful application programming interfaces (APIs). This enables DXL topic subscribers to integrate DDI network changes and identified DNS threats within their solutions and trigger response to these events as needed.

SIA DXL Task Manager which runs on top of McAfee ePO can subscribe to the Infoblox notifications and convert them into ePO threat events, apply policies and enable remediation actions.

Infoblox's Outbound API integration framework is a new automated way to update both IPAM data (networks, hosts, leases) and DNS threat data into additional ecosystem solutions.

Infoblox DDI provides device discovery and single source of truth for devices and networks. It knows when there are changes in the network, such as new devices joining the network, virtual workloads being spun up, or malicious activities detected by the DNS security solution.

Prerequisites

The following are prerequisites for the integration using Outbound API notifications:

- Infoblox:
  - NIOS 8.2 or higher.
  - Security Ecosystem License.
  - Outbound API integration templates (available via Infoblox community).
  - Prerequisites for the templates (e.g. configured and set extensible attributes).
  - Pre-configured services: DNS, RPZ, Threat Insight.
- McAfee ePO:
  - McAfee ePO 5.1.1 or later.
  - McAfee DXL 3.0 broker(s).
  - (Optional) SIA DXL Task Manager Tool.

Known Limitations

The current template supports DNS Firewall(RPZ) notifications only. IPAM change events and Threat Insight (DNS Tunneling) events will be supported by additional templates which will be posted on the community site later.

Best Practices

Outbound API templates can be found on the Infoblox community site on the partners integration page. After registering an account, you can subscribe to the relevant groups and forums.

For production systems, it is highly recommended to set the log level for an end-point to **"Info"** or higher (**"Warning", "Error"**).

Please refer to the Infoblox NIOS Administrator's Guide about other best practices, limitations and any detailed information on how to develop notification templates. The NIOS Administrator's Guide can be found through the Help panel in your Infoblox GUI, or on the Infoblox Support portal.

Configuration

Workflow

Use the following workflow to enable, configure and test outbound API notifications:

1. On the Infoblox Grid:
    a. Install the Security Ecosystem license, if not previously installed.
    b. Check that the necessary services and features are properly configured and enabled. These include DNS, RPZ and Threat Insight.
    c. Create the required Extensible Attributes.
    d. Download (or create your own) notification templates (session_dxl_tmpl.json, mcafee_dxl_rpz.json) from the Infoblox community web-site.
    e. Add the templates.
    f. Add a DXL Endpoint:
        i. Generate NIOS client certificate.
        ii. Import DXL broker certificates.
        iii. Import list of DXL brokers (or add them manually).
    g. Add Notifications.
2. McAfee:
    a. Import NIOS certificate.
    b. Export DXL broker certificates.
    c. Export DXL broker list.
    d. (Optional) Subscribe SIA DXL Task Manager Tool on topics published by NIOS and configure automated actions.
3. Emulate an event, check DXL debug log and/or verify changes on the grid.

Before you get started

Download Templates from the Infoblox Community Web-site

Outbound API templates are an essential part of the configuration. Templates fully control the integration and steps required to execute the outbound notifications. Detailed information on how to develop templates can be found in the NIOS Administrator's guide.

Infoblox does not distribute any templates out-of-the-box with the NIOS releases. Templates are available on the Infoblox community web-site. Templates for the McAfee integration will be located in the "Partner Integrations". You can find other templates posted in the **"API & Integration"** forum.

Templates may require additional extensible attributes, parameters or WAPI credentials to be created or defined. The required configuration should be provided with a template. Don't forget to apply any changes required by the template before testing a notification.

Create Extensible Attributes

McAfee templates use extensible attributes to adjust the templates' behavior. The supported extensible attribute is described in the table below and can be entered through the grid GUI at **"Administration"** → **"Extensible Attributes"**.

Extensible Attributes	Description
ePO_GUID	The ePO GUID of the object if it is known. The template generates a random GUID if the EA is not defined or contains an empty value.
DXL_LastEventSentAt	Internal attribute. Provides the last time that an object's information was sent to McAfee DXL.

DXL_Sync	“True or False” Defines if an object should be sent to McAfee DXL.

Editing Instance Variables

McAfee DXL templates use an instance variable to adjust the templates’ behavior. Instance variables can be entered through the grid GUI at **“Grid”** → **“Ecosystem”** → **“Notification”** and then selecting the notification you created at **“Edit”** → **“Templates”.**

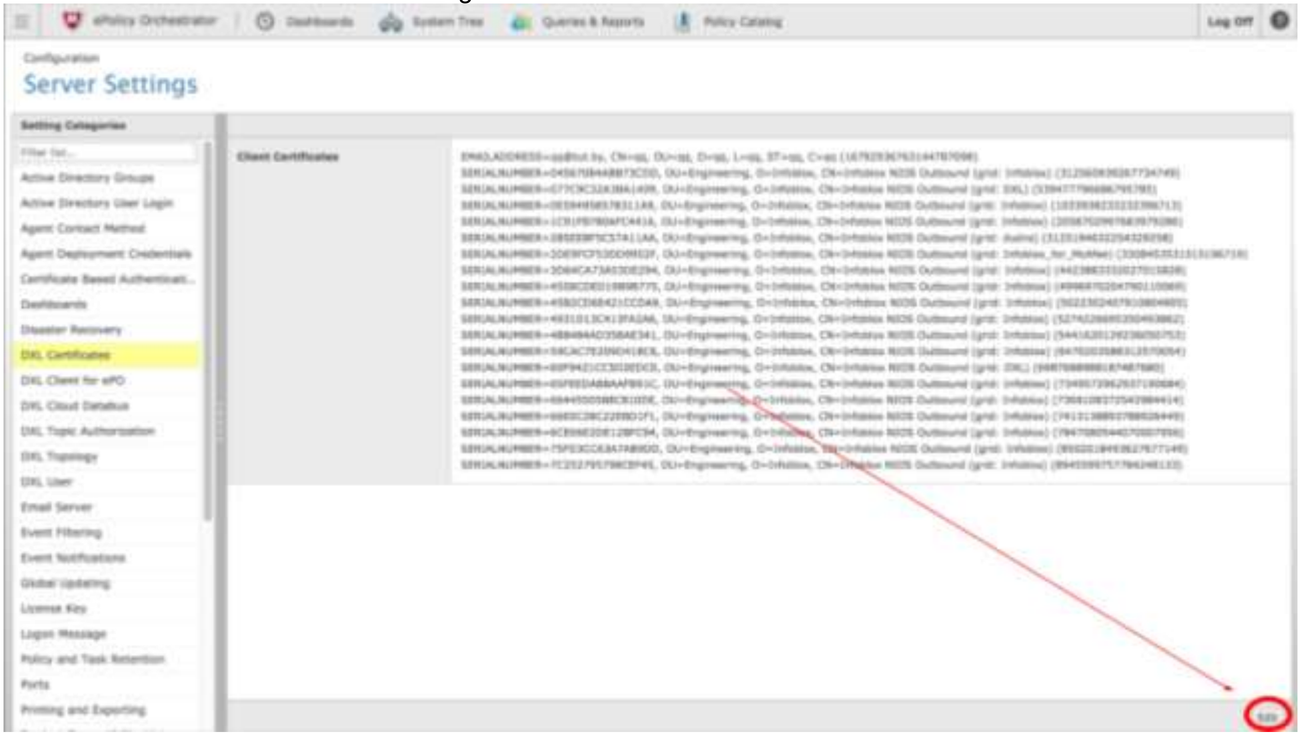
Instance Variable	Description
DXL_MessageFormat	CEF or OpenDXL Defines the format of an outbound message
OPERATION_TYPES	insert/modify/delete Defines the grid event types sent to McAfee DXL

McAfee DXL ePO Configuration

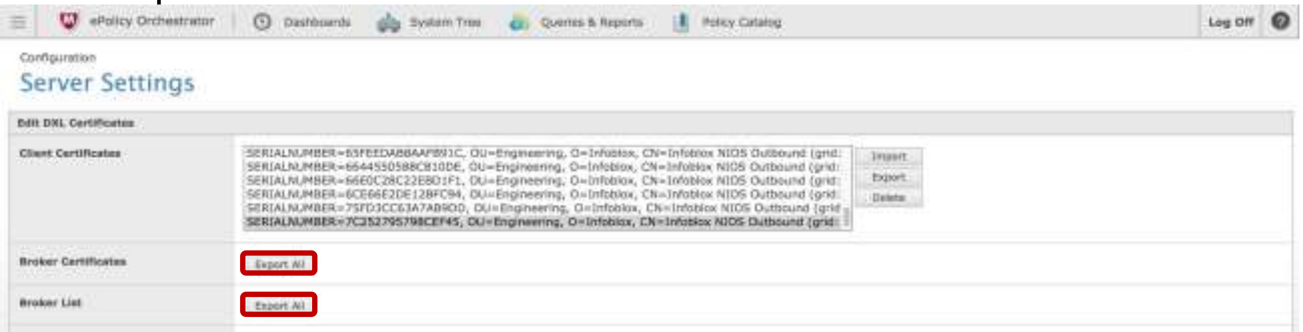
McAfee DXL Broker List, their Certificates and Infoblox Certificate

The DXL endpoint configuration requires import of DXL brokers list and their certificates on the Infoblox side as well as import of Infoblox certificate on the McAfee side. In order to export the broker list and certificates

1. Open the menu, select **“Server Settings”** under **“Configuration”**, select **“DXL Certificates”** and then click the **“Edit”** button on the bottom right of the screen.



2. Click the **“Export All”** button for the **“Broker Certificates”** and **“Broker List”** and save the files.



Configuration

Server Settings

Edit DXL Certificates

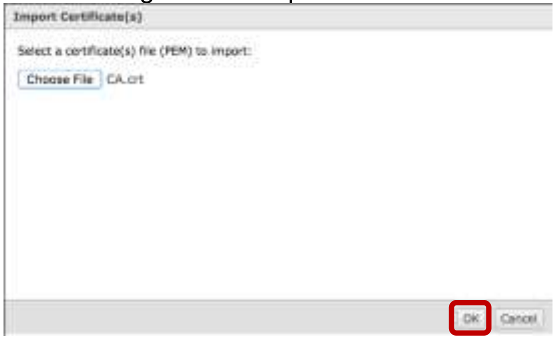
Client Certificates

SERIALNUMBER=65FEEDABBAAFB91C, OU=Engineering, O=Infoblox, CN=Infoblox NIOS Outbound (grid:
SERIALNUMBER=6644550588C810DE, OU=Engineering, O=Infoblox, CN=Infoblox NIOS Outbound (grid:
SERIALNUMBER=66E0C28C22EBD1F1, OU=Engineering, O=Infoblox, CN=Infoblox NIOS Outbound (grid:
SERIALNUMBER=6CE66E2DE128FC94, OU=Engineering, O=Infoblox, CN=Infoblox NIOS Outbound (grid:
SERIALNUMBER=75FD3CC63A7AB9DD, OU=Engineering, O=Infoblox, CN=Infoblox NIOS Outbound (grid:
SERIALNUMBER=7C252795798CEF45, OU=Engineering, O=Infoblox, CN=Infoblox NIOS Outbound (grid:

Broker Certificates

Broker List

3. Please not that this step should only be performed after you added a DXL endpoint.
   Click the **“Import”** button, then click choose File and choose the Infoblox certificate that you generated when adding a DXL endpoint in Add a DXL Endpoint. Once the file is uploaded click the **“ok”** button.



Import Certificate(s)

Select a certificate(s) file (PEM) to import:

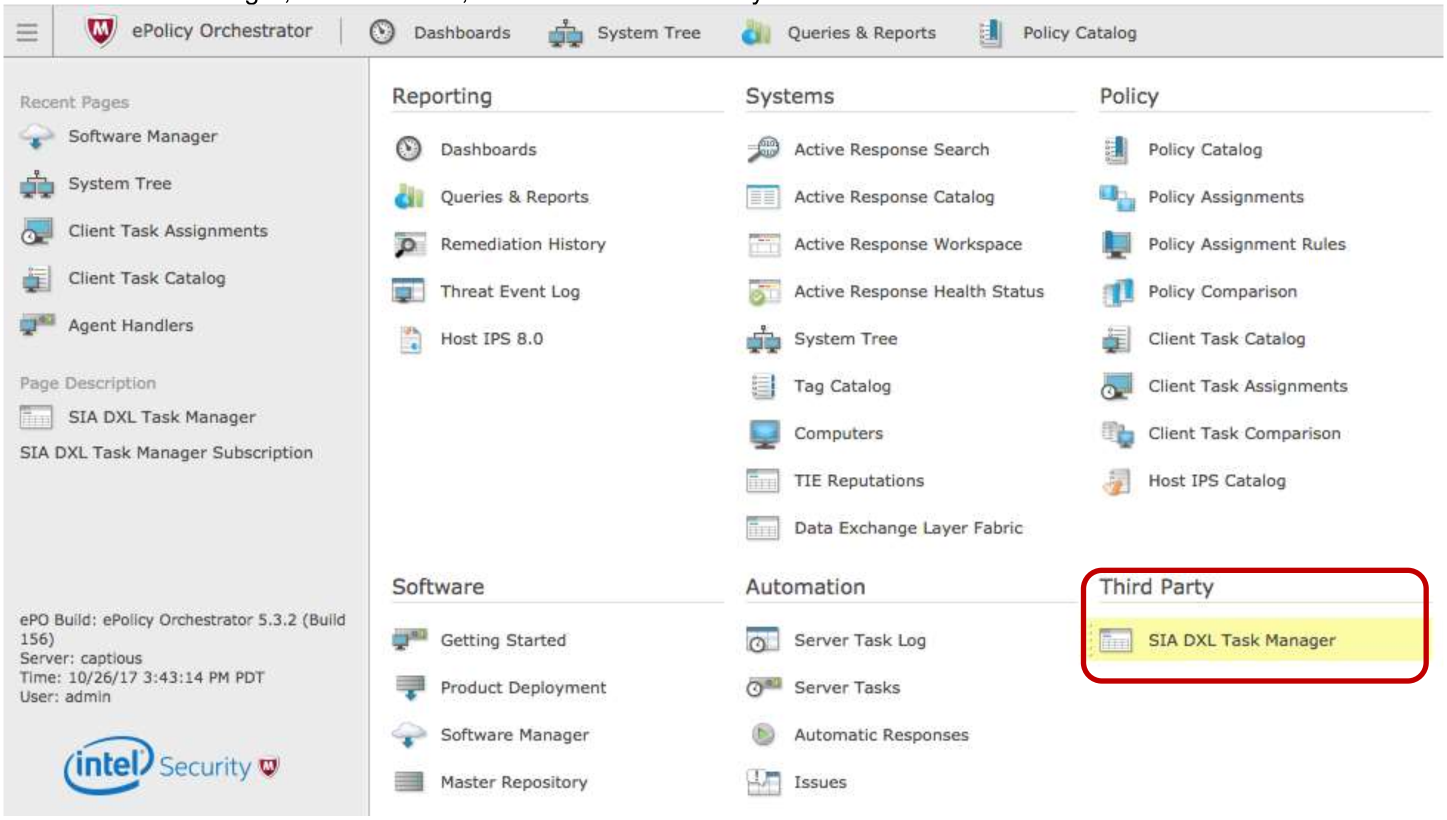
CA.crt

(optional) SIA DXL Task Manager Configuration

The purpose of the SIA DXL Task Manager Tool is to provide a centralized location for DXL fabric users to monitor and visualize DXL events within the ePO Console, and enable simple workflows within ePO to solve basic security issues.

The SIA DXL Task Manager Tool is designed as an ePO Extension that consumes DXL Topic information and enables policy reactions within ePO, based on the data received over a given topic. Reactions include, but are not limited to endpoint based policy changes (such as scanning, quarantine, etc.), McAfee Active Response (MAR) reactions (such delete files, delete registry entries, kill process) and other actions exposed by third party extensions within the ePO framework.

SIA DXL Task Manager, once installed, is located in "Third Party" menu section.



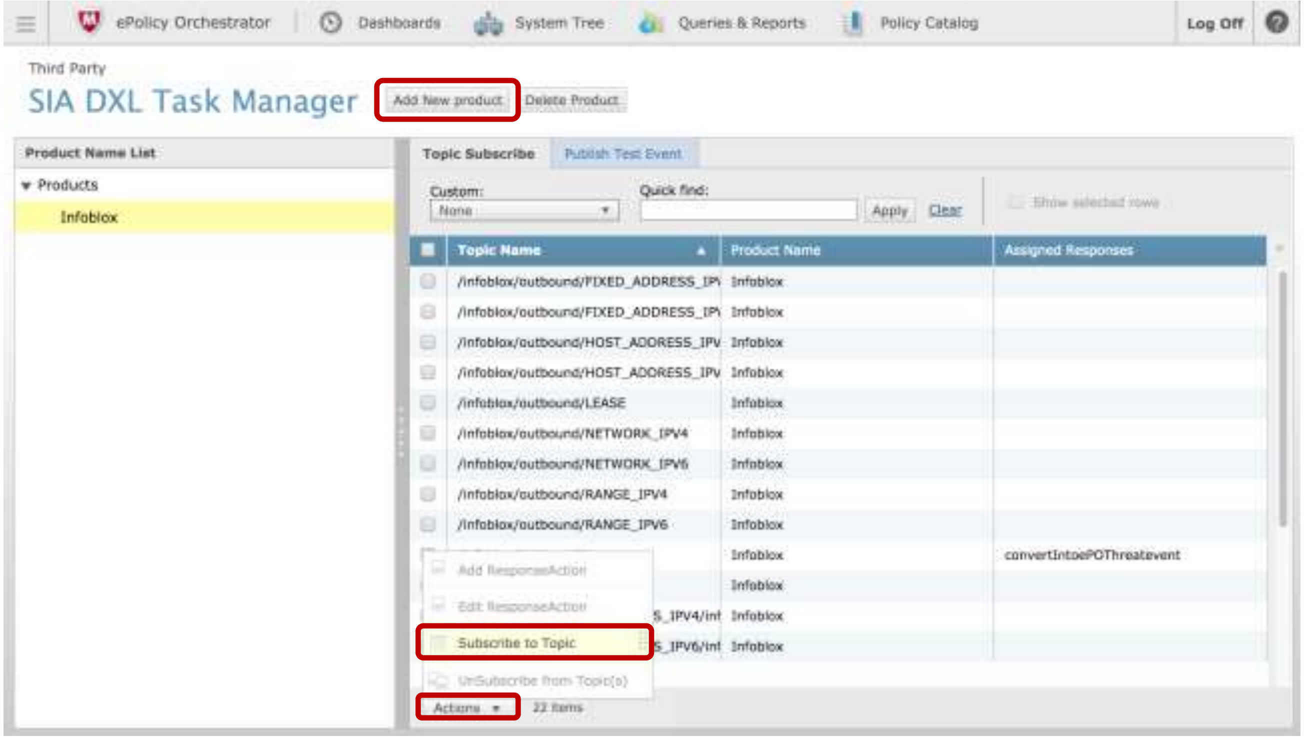
ePO Build: ePolicy Orchestrator 5.3.2 (Build 156)
Server: captious
Time: 10/26/17 3:43:14 PM PDT
User: admin

Subscribing for Infoblox Topics

To subscribe for DXL topics, it is first required to create a product.

1. Click on "**Add New product**" and enter a product name and a description. For example, "Infoblox" as the product name and "Infoblox DXL topics" as the description.

2. Select the product and click on "**Actions**" → "**Subscribe to Topic**" and enter a topic.



Topic Name	Product Name	Assigned Responses
/infoblox/outbound/FIXED_ADDRESS_IPV	Infoblox	
/infoblox/outbound/FIXED_ADDRESS_IPV	Infoblox	
/infoblox/outbound/HOST_ADDRESS_IPV	Infoblox	
/infoblox/outbound/HOST_ADDRESS_IPV	Infoblox	
/infoblox/outbound/LEASE	Infoblox	
/infoblox/outbound/NETWORK_IPV4	Infoblox	
/infoblox/outbound/NETWORK_IPV6	Infoblox	
/infoblox/outbound/RANGE_IPV4	Infoblox	
/infoblox/outbound/RANGE_IPV6	Infoblox	
	Infoblox	convertIntoePOThreatevent
	Infoblox	
S_IPV4/int	Infoblox	
S_IPV6/int	Infoblox	

The current version of DXL template supports:

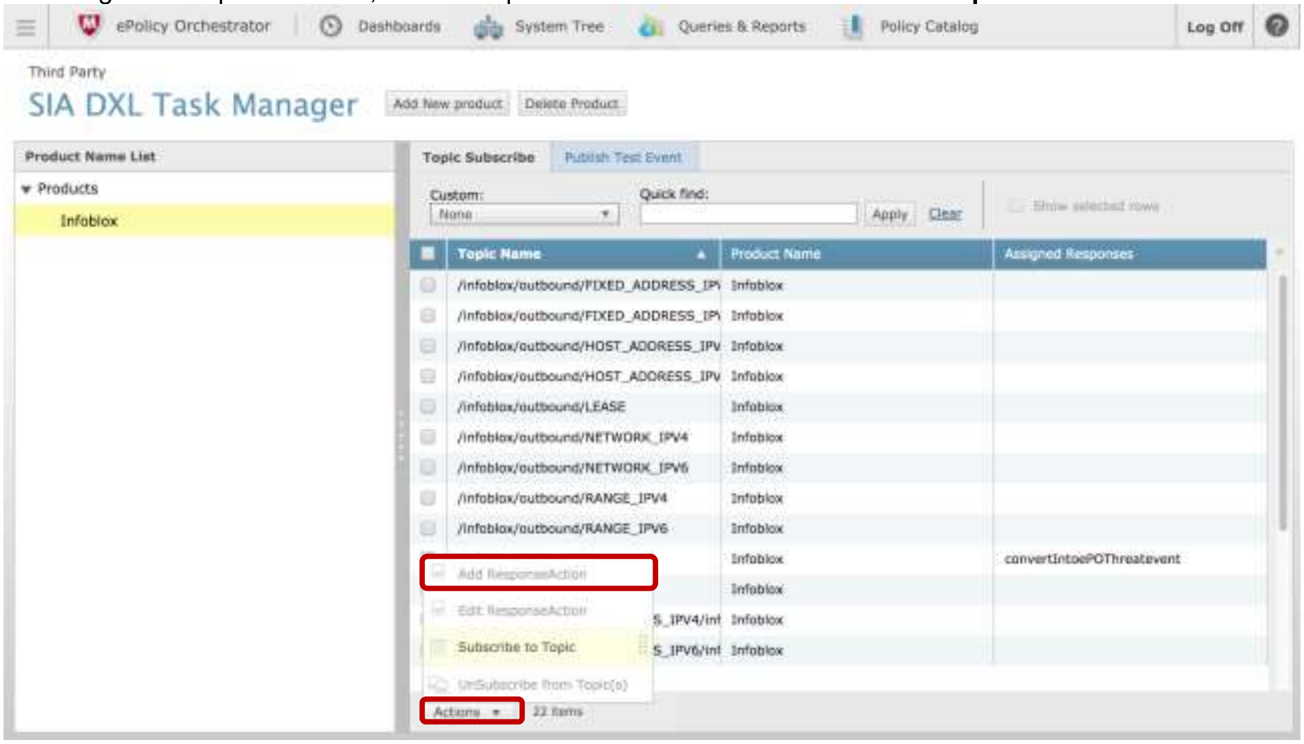
events in OpenDXL format	events in CEF format
/open/threat/v1/RPZ/infoblox	/infoblox/outbound/RPZ
/open/threat/v1/TUNNEL/infoblox	/infoblox/outbound/TUNNEL
/open/DDI/v1/FIXED_ADDRESS_IPV4/infoblox	/infoblox/outbound/FIXED_ADDRESS_IPV4
/open/DDI/v1/FIXED_ADDRESS_IPV6/infoblox	/infoblox/outbound/FIXED_ADDRESS_IPV6
/open/DDI/v1/HOST_ADDRESS_IPV4/infoblox	/infoblox/outbound/HOST_ADDRESS_IPV4
/open/DDI/v1/HOST_ADDRESS_IPV6/infoblox	/infoblox/outbound/HOST_ADDRESS_IPV4
/open/DDI/v1/LEASE/infoblox	/infoblox/outbound/LEASE
/open/DDI/v1/NETWORK_IPV4/infoblox	/infoblox/outbound/NETWORK_IPV4
/open/DDI/v1/NETWORK_IPV6/infoblox	/infoblox/outbound/NETWORK_IPV6
/open/DDI/v1/RANGE_IPV4/infoblox	/infoblox/outbound/RANGE_IPV4

/open/DDI/v1/RANGE_IPV6/infoblox	/infoblox/outbound/RANGE_IPV6

SIA DXL Task Manager version 1.0 and higher (1.x releases) can be used to automatically configure response on actions for events in the “/open/threat/v1/RPZ/infoblox” topic only.

Configuring automated response actions

To configure a response action, select a topic and click on "**Actions**" → "**Add ResponseAction**".



Topic Name	Product Name	Assigned Responses
/infoblox/outbound/FIXED_ADDRESS_IP\	Infoblox	
/infoblox/outbound/FIXED_ADDRESS_IP\	Infoblox	
/infoblox/outbound/HOST_ADDRESS_IPV	Infoblox	
/infoblox/outbound/HOST_ADDRESS_IPV	Infoblox	
/infoblox/outbound/LEASE	Infoblox	
/infoblox/outbound/NETWORK_IPV4	Infoblox	
/infoblox/outbound/NETWORK_IPV6	Infoblox	
/infoblox/outbound/RANGE_IPV4	Infoblox	
/infoblox/outbound/RANGE_IPV6	Infoblox	
	Infoblox	convertIntoePOThreatevent
	Infoblox	
S_IPV4/inf	Infoblox	
S_IPV6/inf	Infoblox	

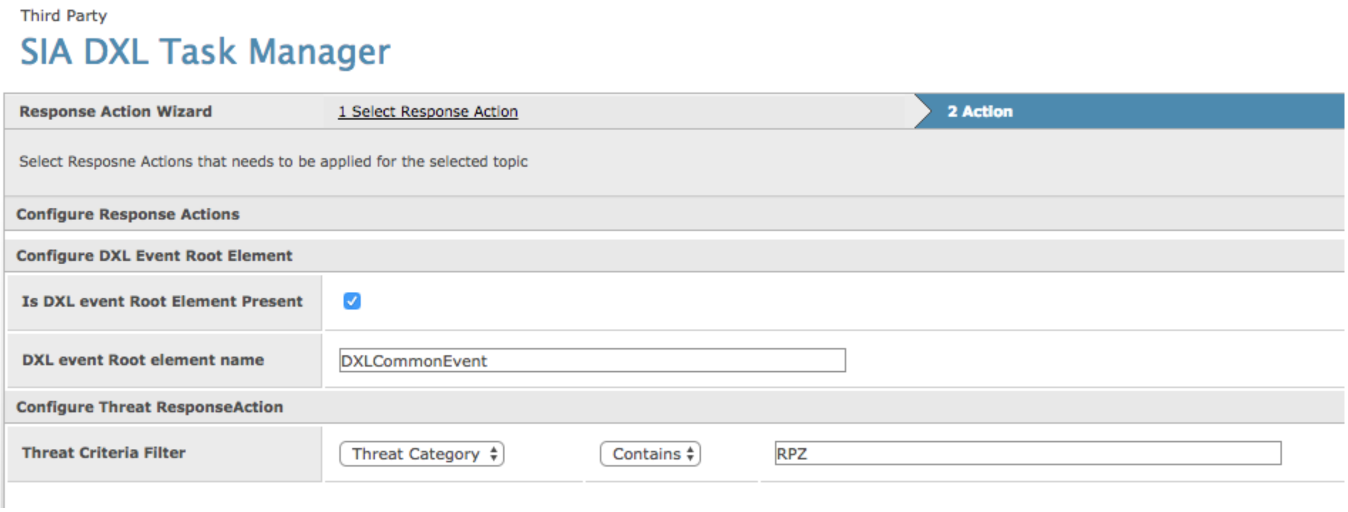
For the SIA DXL Task Manager Tool 1.1, the following Response Actions are available:

- Convert Into ePO Threat Event
- Assign ePO Client Task
- Assign ePO Policy
- Assign ePO Tag
- Assign MAR Reaction

As an example, in this document, we configure "Convert Into ePO Threat Event" action:

1. Select "**Convert Into ePO Threat Event**" and click "Next".
2. Enable "Is DXL event Root Element Present" checkbox.
3. Set "DXL event Root element name" to "DXLCommonEvent" (without quotes).

4. Specify "Threat Criteria Filter" as "Threat Category" contains "RPZ" and save the configuration.



Third Party

SIA DXL Task Manager

Response Action Wizard | 1 Select Response Action | 2 Action

Select Resposne Actions that needs to be applied for the selected topic

Configure Response Actions

Configure DXL Event Root Element

Is DXL event Root Element Present	☑
DXL event Root element name	DXLCommonEvent

Configure Threat ResponseAction

Threat Criteria Filter	Threat Category	Contains	RPZ

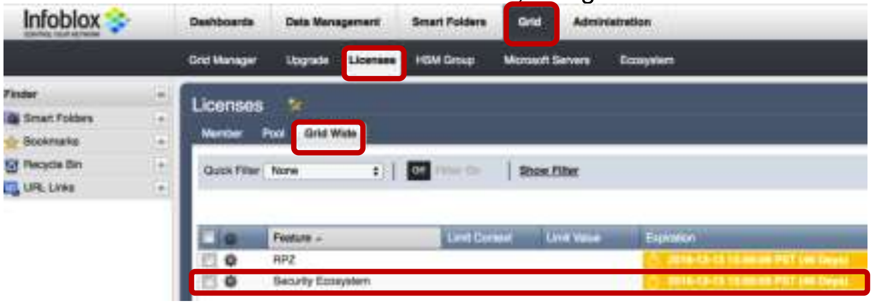
Refer "McAfee SIA DXL Task Manager Tool 1.1" reference guide for directions about configuring other automatic responses.

Infoblox NIOS Configuration

Check if the Security Ecosystem License is Installed

Security Ecosystem license is a Grid Wide license. Grid wide licenses activate services on all appliances in the same Grid.

In order to check if the license was installed, navigate to **“Grid”** → **“Licenses”** → **“Grid Wide”**.

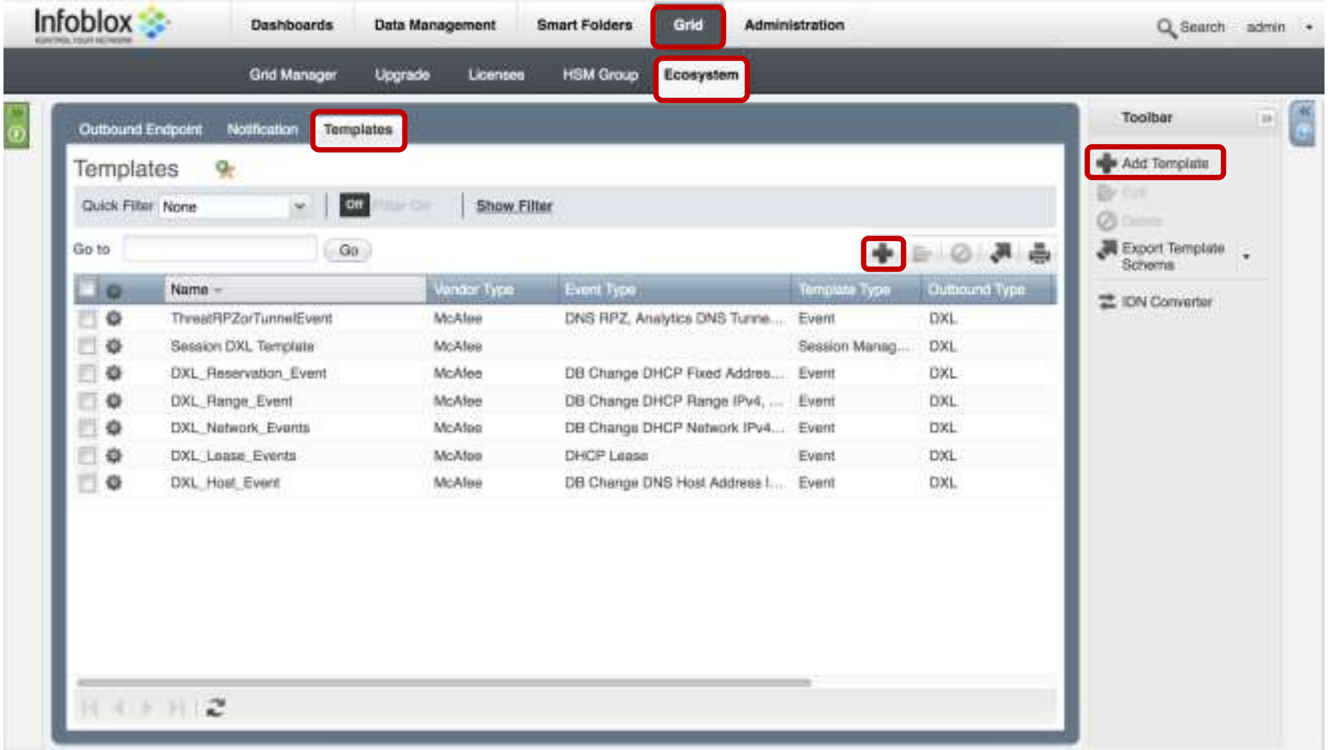


Feature	Limit Context	Limit Value	Expiration
RPZ			[illegible]
Security Ecosystem			[illegible]

Add/Upload Templates

In order to upload/add templates:

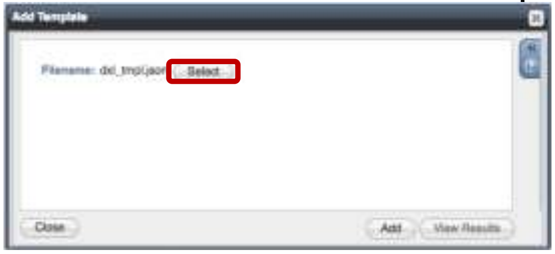
1. Navigate to **“Grid”** → **“Ecosystem”** → **“Templates”**, and press **“+”** or **“+ Add Template”** then the **“Add template”** window will open.



Templates

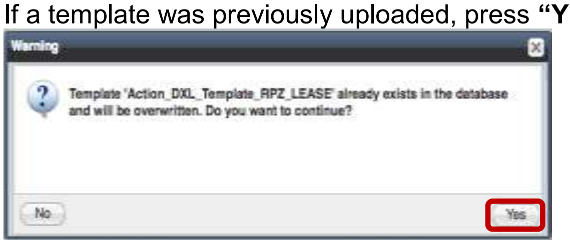
Name	Vendor Type	Event Type	Template Type	Outbound Type
ThreatRPZorTunnelEvent	McAfee	DNS RPZ, Analytics DNS Tunne...	Event	DXL
Session DXL Template	McAfee		Session Manag...	DXL
DXL_Reservation_Event	McAfee	DB Change DHCP Fixed Addres...	Event	DXL
DXL_Range_Event	McAfee	DB Change DHCP Range IPv4, ...	Event	DXL
DXL_Network_Events	McAfee	DB Change DHCP Network IPv4...	Event	DXL
DXL_Lease_Events	McAfee	DHCP Lease	Event	DXL
DXL_Host_Event	McAfee	DB Change DNS Host Address I...	Event	DXL

2. Press the **“Select”** button on the **“Add template”** window.



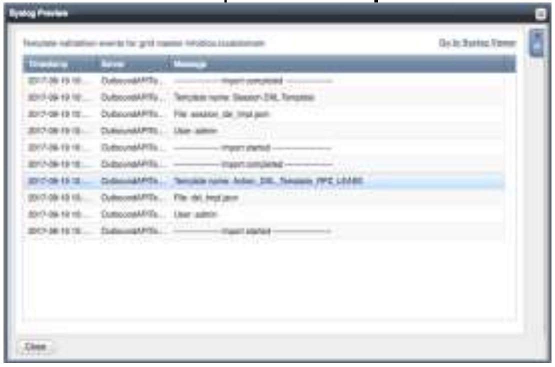
Filename: dxl_tmpl.json

3. If a template was previously uploaded, press **“Yes”** to overwrite the template.



Template 'Action_DXL_Template_RPZ_LEASE' already exists in the database and will be overwritten. Do you want to continue?

4. Press the **“Select”** button on the **“Upload”** window. The standard file selection dialog will open.
5. Select the file and press the **“Upload”** button on the **“Upload”** window.

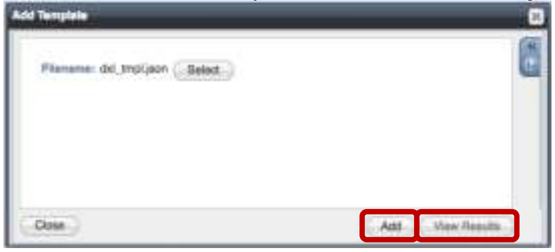


Template validation events for grid master infoblox.localdomain

```
Timestamp        Server            Message
2017-08-19 10:...  OutboundAPITe...  ------------ import completed ------------
2017-08-19 10:...  OutboundAPITe...  Template name: Session DXL Template
2017-08-19 10:...  OutboundAPITe...  File: session_dxl_tmpl.json
2017-08-19 10:...  OutboundAPITe...  User: admin
2017-08-19 10:...  OutboundAPITe...  ------------ import started ------------
2017-08-19 10:...  OutboundAPITe...  ------------ import completed ------------
2017-08-19 10:...  OutboundAPITe...  Template name: Action_DXL_Template_RPZ_LEASE
2017-08-19 10:...  OutboundAPITe...  File: dxl_tmpl.json
2017-08-19 10:...  OutboundAPITe...  User: admin
2017-08-19 10:...  OutboundAPITe...  ------------ import started ------------
```

6. Press the **“Add”** button and the template will be added/uploaded.

7. You can review the uploaded results in the syslog or by pressing the **“View Results”** button.



Add Template

Filename: dxl_tmpl.json Select

Close Add View Results

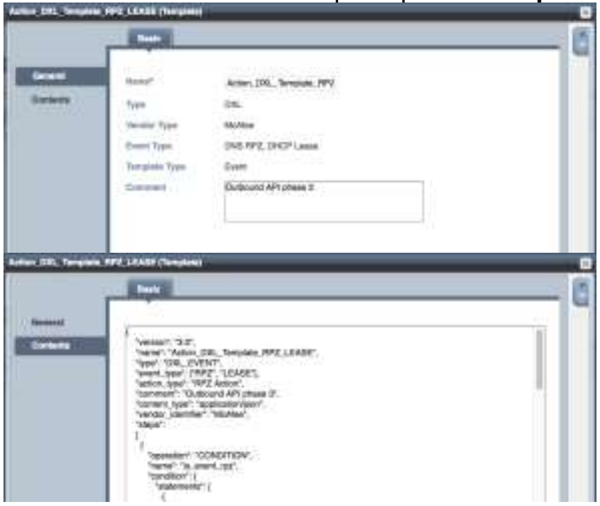
8. There is no difference between uploading session management and action templates.

Modifying Templates

NIOS provides the facility to modify the templates via the web-interface.

1. Navigate to **“Grid”** → **“Ecosystem”** → **“Templates”**, and then press the gear icon next to the template you want to modify.

2. Press the **“Edit”** button to open up the **“Template”** window.



Action_DXL_Template_RPZ_LEASE (Template)

Name*	Action_DXL_Template_RPV
Type	DXL
Vendor Type	McAfee
Event Type	DNS RPZ, DHCP Lease
Template Type	Event
Comment	Outbound API phase 3

Action_DXL_Template_RPZ_LEASE (Template)

```
{
 "version": "3.0",
 "name": "Action_DXL_Template_RPZ_LEASE",
 "type": "DXL_EVENT",
 "event_type": ["RPZ", "LEASE"],
 "action_type": "RPZ Action",
 "comment": "Outbound API phase 3",
 "content_type": "application/json",
 "vendor_identifier": "McAfee",
 "steps":
 [
  {
   "operation": "CONDITION",
   "name": "is_event_rpz",
   "condition": {
    "statements": [
     {
```

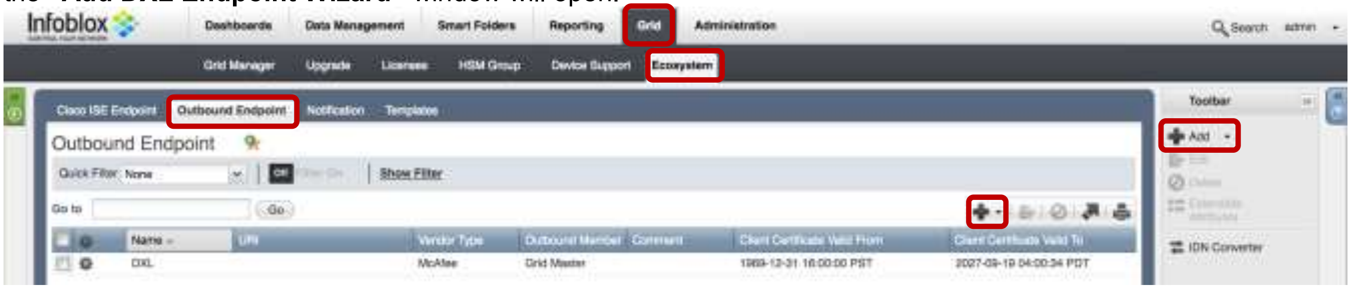
The template editor is a simple interface for making changes to templates. It is recommended to only use the template editor to make minor changes. You can also edit, cut and paste template snippets from a text editor of your choice.
Note: You cannot delete a template if it is used by an endpoint or by a notification.

Add a DXL Endpoint

A **“DXL Endpoint”** is basically a remote DXL broker(s) which should receive changes based on a notification and configured template.

In order to add a DXL Endpoint:

1. Navigate to **“Grid”** → **“Ecosystem”** → **“Outbound Endpoint”** and press **“+ Add DXL Endpoint”** then the **“Add DXL Endpoint Wizard”** window will open.



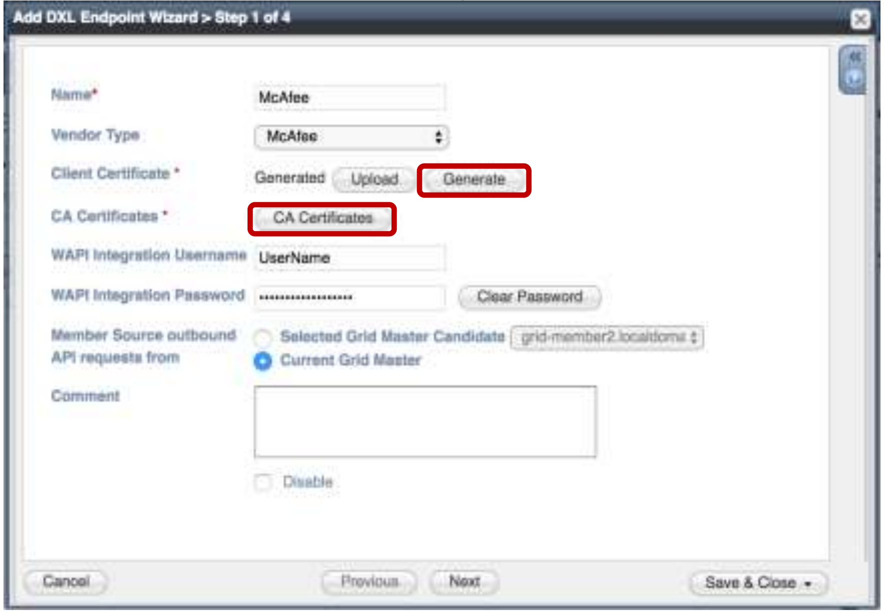
Outbound Endpoint

Quick Filter: None Off Show Filter

Go to Go

Name	URI	Vendor Type	Outbound Member	Comment	Client Certificate Valid From	Client Certificate Valid To
DXL		McAfee	Grid Master		1969-12-31 16:00:00 PST	2027-09-19 04:00:34 PDT

2. The **Name, Client Certificate,** and **CA Certificate** fields are required.
   a. Press the **“Generate”** button and save a certificate which should be imported into DXL client certificates.
   b. Press the **“CA Certificate”** button to open a **“CA Certificates”** window.



Add DXL Endpoint Wizard > Step 1 of 4

Name*: McAfee

Vendor Type: McAfee

Client Certificate *: Generated

CA Certificates *

WAPI Integration Username: UserName

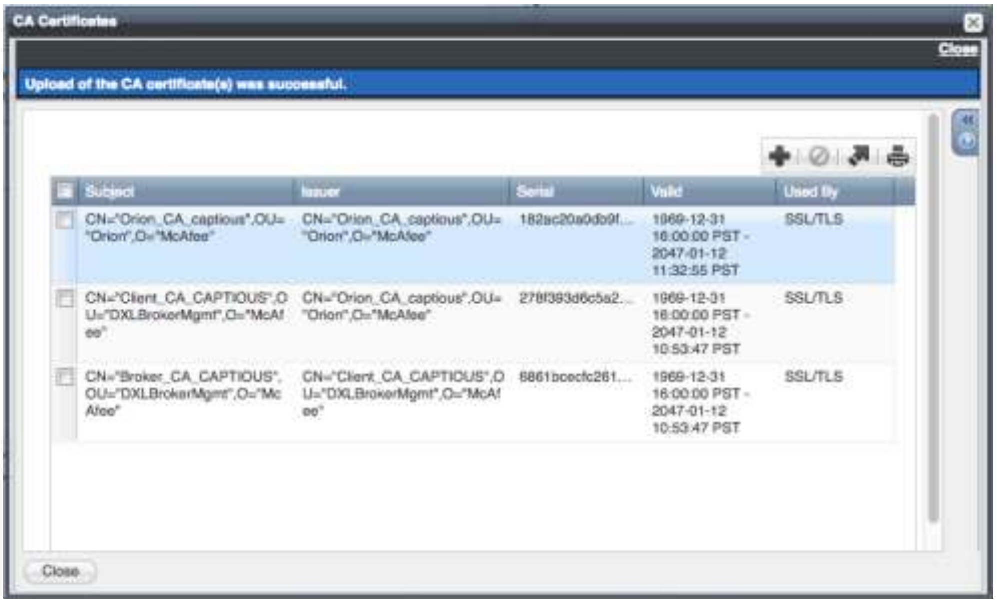
WAPI Integration Password: ••••••••••••••••••

Member Source outbound API requests from: ○ Selected Grid Master Candidate (grid-member2.localdoma) ● Current Grid Master

Comment:

□ Disable

   c. Press the **“+”** and select the Broker Certificates from the McAfee ePO DXL then click the Upload button.

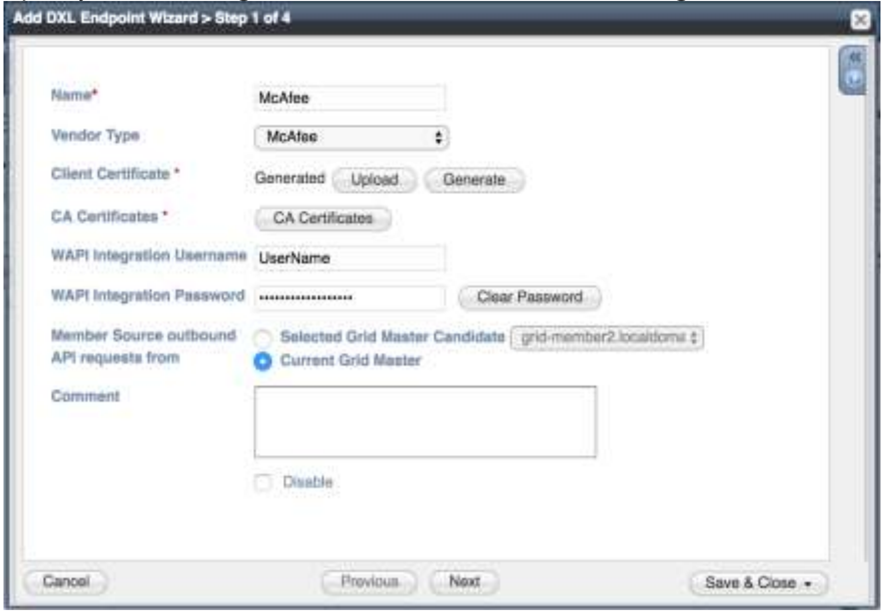


CA Certificates

Upload of the CA certificate(s) was successful.

□	Subject	Issuer	Serial	Valid	Used By
□	CN="Orion_CA_captious",OU="Orion",O="McAfee"	CN="Orion_CA_captious",OU="Orion",O="McAfee"	182ac20a0db9f...	1969-12-31 16:00:00 PST - 2047-01-12 11:32:55 PST	SSL/TLS
□	CN="Client_CA_CAPTIOUS",OU="DXLBrokerMgmt",O="McAfee"	CN="Orion_CA_captious",OU="Orion",O="McAfee"	278f393d6c5a2...	1969-12-31 16:00:00 PST - 2047-01-12 10:53:47 PST	SSL/TLS
□	CN="Broker_CA_CAPTIOUS",OU="DXLBrokerMgmt",O="McAfee"	CN="Client_CA_CAPTIOUS",OU="DXLBrokerMgmt",O="McAfee"	6861bcecfc261...	1969-12-31 16:00:00 PST - 2047-01-12 10:53:47 PST	SSL/TLS

3. Specify **“WAPI Integration Username”** and **“WAPI Integration Password”** (NIOS credentials).



Name* McAfee

Vendor Type McAfee

Client Certificate * Generated

CA Certificates *

WAPI Integration Username UserName

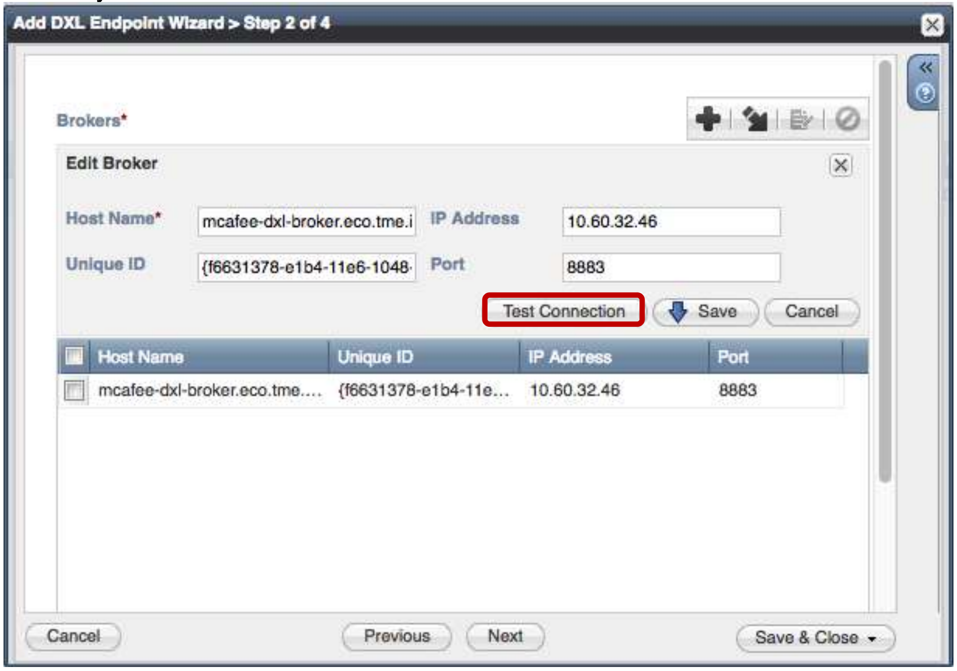
WAPI Integration Password ••••••••••••••••••

Member Source outbound API requests from ○ Selected Grid Master Candidate grid-member2.localdoma ● Current Grid Master

Comment

□ Disable

4. Press **“Next”** to continue with brokers configuration:
    a. Press the import button and select the broker list properties that you exported from the McAfee **“**Server Settings**”.**
    b. Select the checkbox next to the broker you want to test a connection with and press the edit button.
    c. Press the **“Test Connection”** to make sure that everything is working.
    You may need to wait a minute before the connection will work.



Host Name* mcafee-dxl-broker.eco.tme.i

IP Address 10.60.32.46

Unique ID {f6631378-e1b4-11e6-1048

Port 8883

□	Host Name	Unique ID	IP Address	Port
□	mcafee-dxl-broker.eco.tme....	{f6631378-e1b4-11e...	10.60.32.46	8883

5. (Optional) **For debug purposes only:** Press **“next”** and Under **“Session Management”,** set **“Log Level”** to **“Debug”.**
6. Press **“Save & Close”** button.

When possible, it is recommended to send notifications from a Grid Master Candidate instead of from the Grid Master.

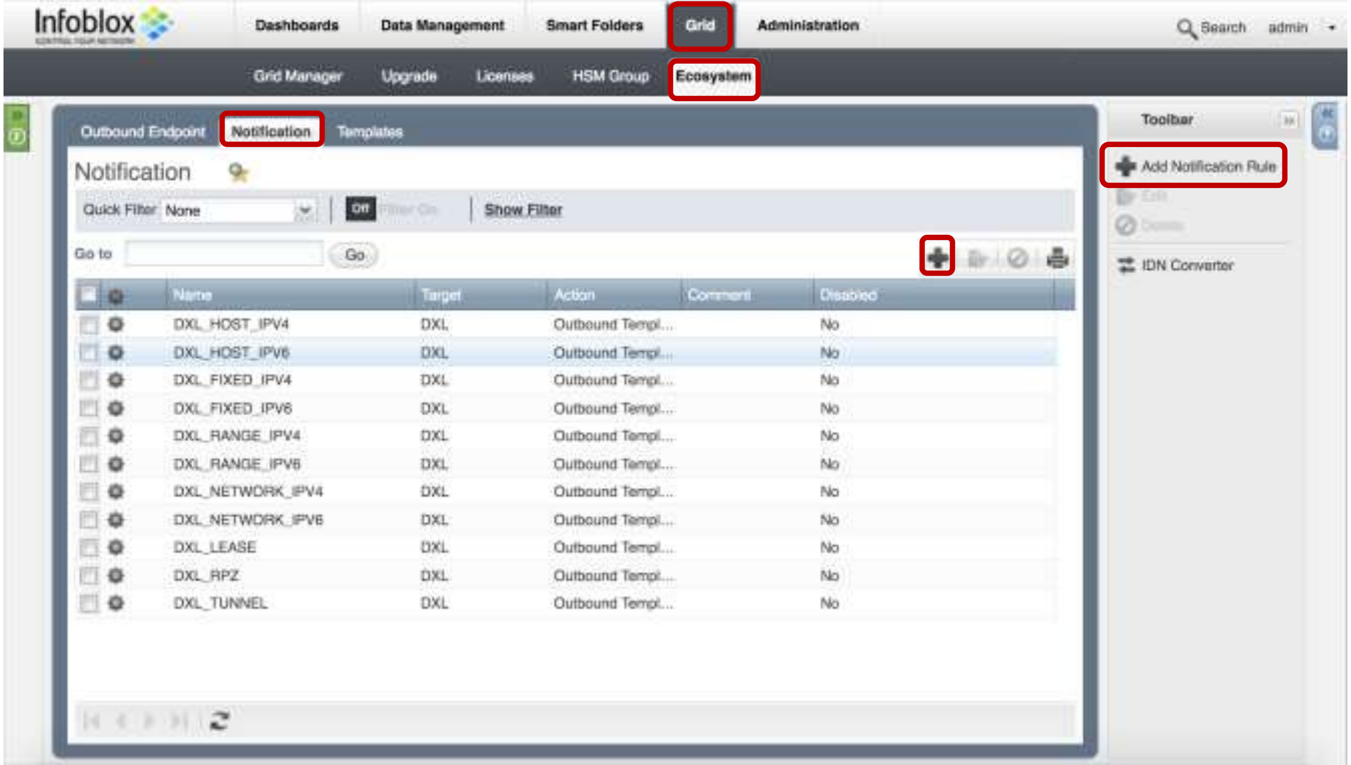
Add a Notification

A notification can be considered as a **“link”** between a template, an endpoint, and an event. In the notification properties, you define which event triggers the notification, which template is executed and with which API/DXL endpoint NIOS will establish the connection to. The DXL templates support a subset of available notifications (refer to Known Limitations in this guide for more details). In order to simplify the deployment, this guide only creates required notifications and use the relevant filters. It is highly recommended to configure deduplication for RPZ events and exclude a feed that is automatically populated by Threat Analytics.

An endpoint and a template must be added before you can add a notification.

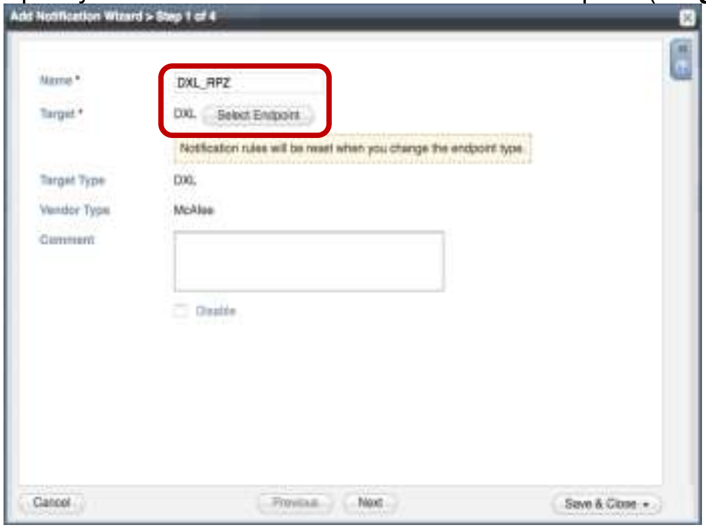
In order to add notifications:

1. Navigate to **“Grid”** → **“Ecosystem”** → **“Notification”** and press **“+”** or **“+ Add Notification Rule”** then the **“Add Notification Wizard”** window will open.



Name	Target	Action	Comment	Disabled
DXL_HOST_IPV4	DXL	Outbound Templ...		No
DXL_HOST_IPV6	DXL	Outbound Templ...		No
DXL_FIXED_IPV4	DXL	Outbound Templ...		No
DXL_FIXED_IPV6	DXL	Outbound Templ...		No
DXL_RANGE_IPV4	DXL	Outbound Templ...		No
DXL_RANGE_IPV6	DXL	Outbound Templ...		No
DXL_NETWORK_IPV4	DXL	Outbound Templ...		No
DXL_NETWORK_IPV6	DXL	Outbound Templ...		No
DXL_LEASE	DXL	Outbound Templ...		No
DXL_RPZ	DXL	Outbound Templ...		No
DXL_TUNNEL	DXL	Outbound Templ...		No

2. Specify the notification’s name and select an endpoint (**Target**), click **“Next”**.



Name * DXL_RPZ

Target * DXL

Notification rules will be reset when you change the endpoint type

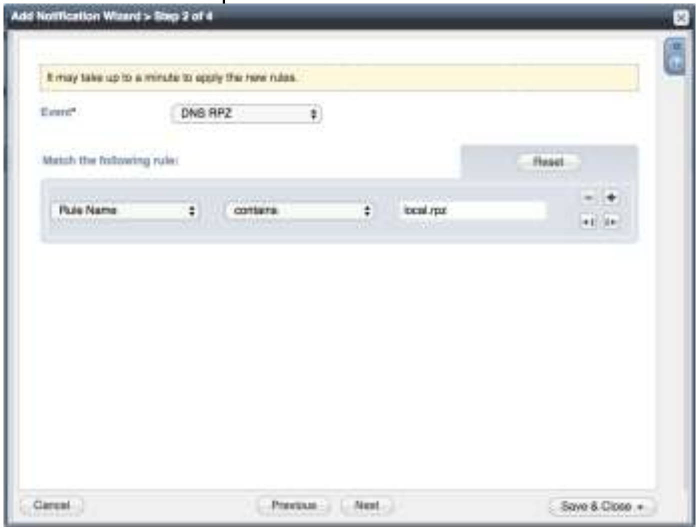
Target Type DXL

Vendor Type McAfee

Comment

□ Disable

3. Select an event type and define a filter. Note: For optimal performance, it is best practice to make the filter as narrow as possible. Click **“Next”**.



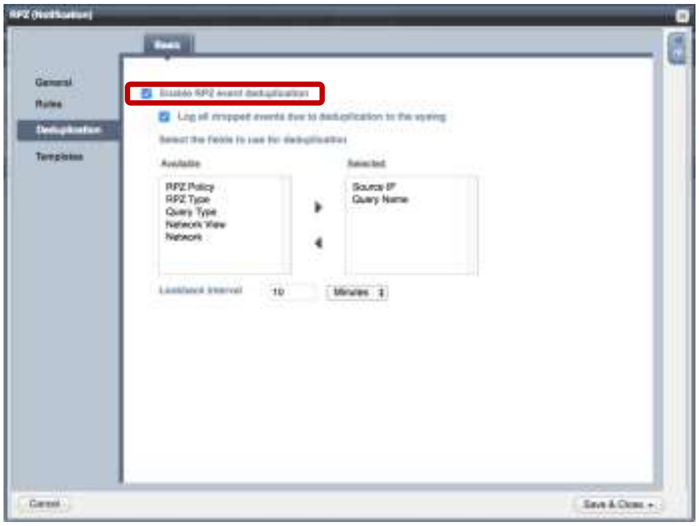
It may take up to a minute to apply the new rules.

Event*: DNS RPZ

Match the following rule:

Rule Name | contains | local.rpz

4. (For RPZ notifications only) Check **“Enable RPZ event deduplication”** and specify relevant parameters. Click **“Next”**.



☑ Enable RPZ event deduplication

☑ Log all dropped events due to deduplication to the syslog

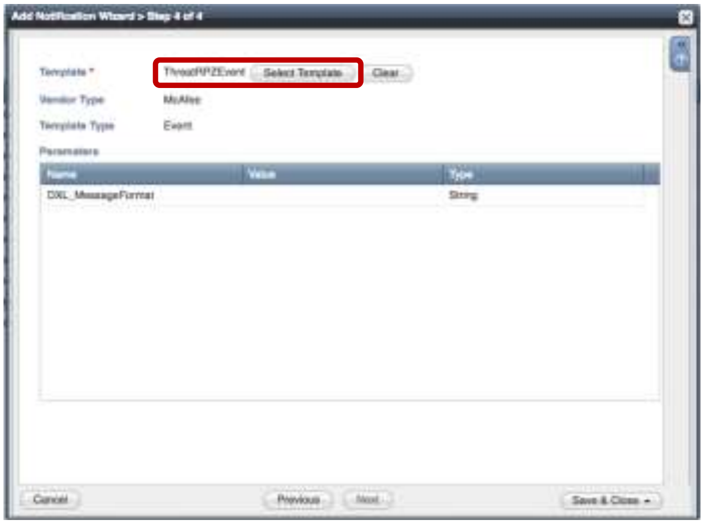
Select the fields to use for deduplication

Available: RPZ Policy, RPZ Type, Query Type, Network View, Network

Selected: Source IP, Query Name

Lookback interval: 10 Minutes

5. Select a relevant template and specify the template's parameters if any are required. Click **“Save & Close”**.



Template *: ThreatRPZEvent

Vendor Type: McAfee

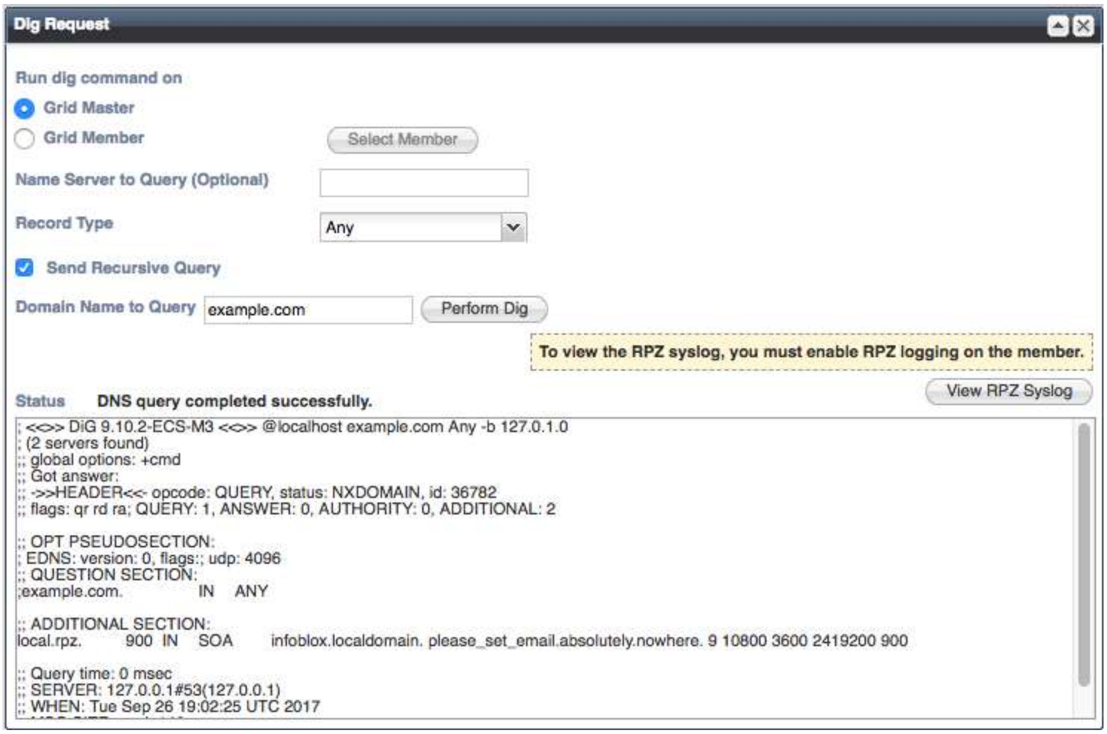
Template Type: Event

Parameters

Name	Value	Type
DXL_MessageFormat		String

Check the Configuration

You can emulate an event for which a notification was added by going to **“DashBoards”** → **“Status”** → **“Security”** then on the **“Dig Request”** panel, fill in the **“Domain Name to Query”** text box and click the **“Perform Dig”** button.



Dig Request

Run dig command on

● Grid Master

○ Grid Member

Name Server to Query (Optional)

Record Type: Any

☑ Send Recursive Query

Domain Name to Query: example.com

To view the RPZ syslog, you must enable RPZ logging on the member.

Status **DNS query completed successfully.**

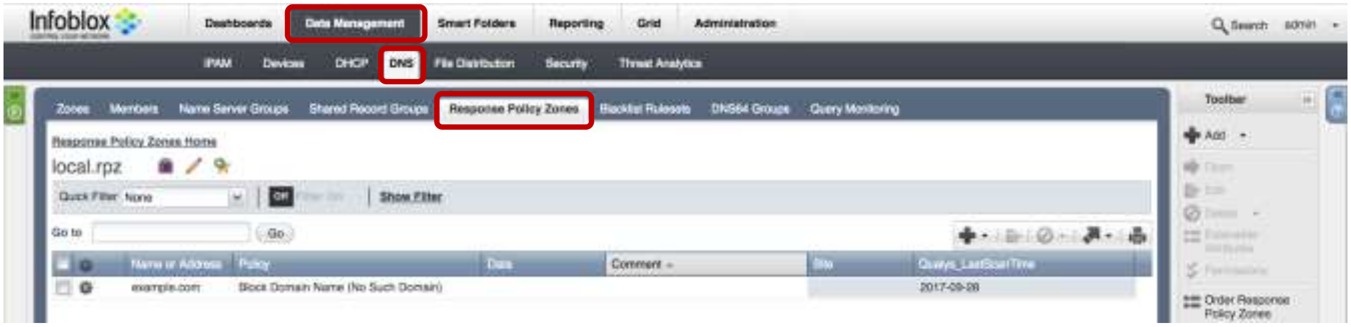
```
; <<>> DiG 9.10.2-ECS-M3 <<>> @localhost example.com Any -b 127.0.1.0
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 36782
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.com.              IN    ANY

;; ADDITIONAL SECTION:
local.rpz.        900  IN    SOA      infoblox.localdomain. please_set_email.absolutely.nowhere. 9 10800 3600 2419200 900

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Sep 26 19:02:25 UTC 2017
```

When performing the dig request above, make sure that the **“Domain Name to Query”** is blocked by your RPZ. To check this, navigate to **“Data Management”** → **“DNS”** → **“Response Policy Zone”**. You can export a RPZ feed or check the content of a local RPZ.



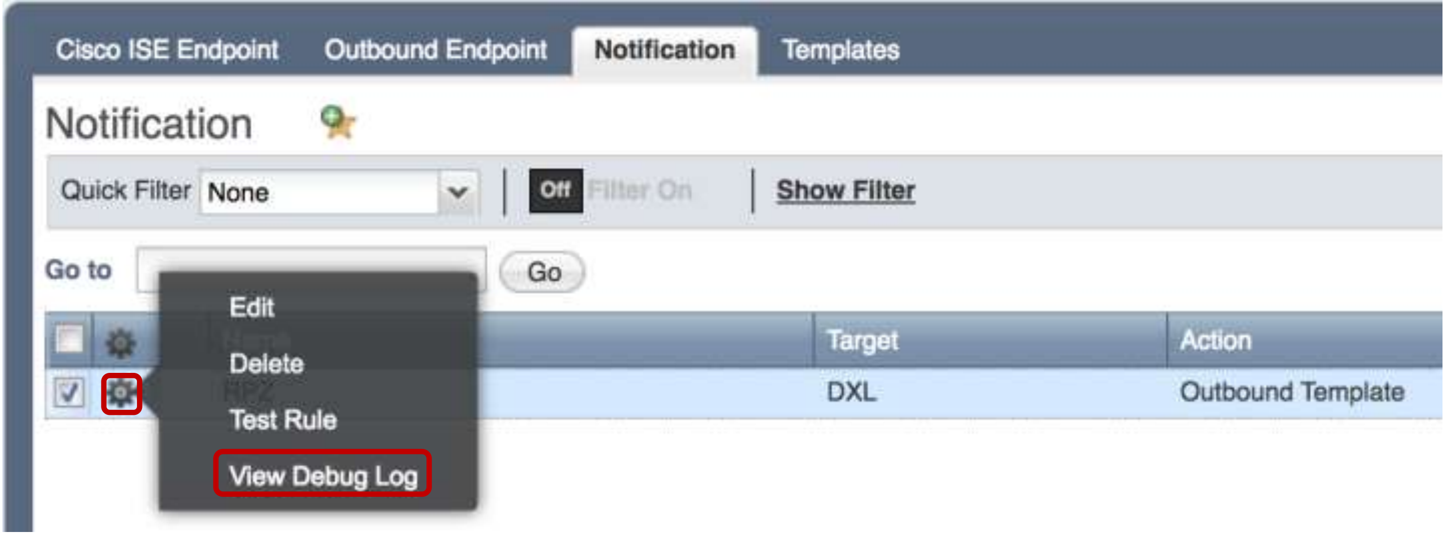
local.rpz

Quick Filter: None

Go to

Name or Address	Policy	Data	Comment	Site	Quays_LastScanTime
example.com	Block Domain Name (No Such Domain)				2017-09-28

To check a debug log for an endpoint, go to **“Grid”** → **“Ecosystem”** → **“Outbound Endpoint”**, click on the gear wheel and select **“View Debug Log”**.



Depending on a browser, the debug log will be downloaded or opened in a new tab. You may need to check your popup blocker or download settings.

Summary

The integrated solution from Infoblox and McAfee provides visibility into network events, plugs the DNS security gap in organizations, and automates data sharing between Infoblox DNS, DHCP, IPAM (DDI), and McAfee product suites for faster response to threats.