DEPLOYMENT GUIDE

Integration with ForeScout

Outbound API

2018-02-28

Contents

Introduction

Infoblox's Outbound REST API integration framework is a new way to update both IPAM data (networks, hosts, leases) and DNS threat data into additional ecosystem solutions. Infoblox and ForeScout CounterACT together enable security and incident response teams to leverage the integration of NAC, DDI and DNS security to enhance visibility, manage assets, ease compliance and automate remediation. Thus, improving your security posture while maximizing your ROI in both products.

Prerequisites

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

- Infoblox:
  1. NIOS 8.1 or higher
  2. Security Ecosystem License
  3. Outbound API integration templates
  4. Prerequisites for the templates (e.g. configured and set extensible attributes)
- ForeScout:
  1. ForeScout CounterACT 7.0
  2. Open Integration Module license and installed Data Exchange Plugin
  3. A web service account which will be used to send events to ForeScout
  4. Data Exchange Web Service Properties, which will be populated by Infoblox
  5. Policies which will handle: device removal, grouping, response on security events
  6. Managed networks should be pre-configured on CounterACT

Limitations

Known limitations:

1. Supported notifications: RPZ, TUNNEL, HOST_ADDRESS_IPV4, LEASE and FIXED_ADDRESS_IPV4
2. Assets created/updated via Data Exchange plugin can contain only web service properties defined for a specific account. ForeScout will discover the asset and populate standard properties.
3. ForeScout CounterACT REST API does not support delete asset API. The assets are deleted by a policy which monitors a specific Web Service property.

Best Practices

Outbound API templates can be found on the Infoblox community site: https://community.infoblox.com. 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 for other best practices, limitations and detailed information on how to develop notification templates. The NIOS Administrator's Guide can be found through the Help panel in the Infoblox Grid Manager GUI, or on the Infoblox Support portal (https://support.infoblox.com).

Configuration

Workflow

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

- ForeScout:
  1. Install Open Integration Module and a license
  2. Create a Web Service Account
  3. Create Web Service Properties
  4. Create Policies
- Infoblox:
  1. Install the Security Ecosystem license if it was not installed
  2. Check that the necessary services and features are properly configured and enabled, including DHCP, DNS, RPZ and Threat Analytics.
  3. Create the required Extensible Attributes (refer to the list provided below)
  4. Download (or create your own) notification templates (FS_Assets.json, FS_SecEvent.json) from the Infoblox community web-site
  5. Add/upload the notification templates
  6. Add a REST API Endpoint "ForeScout CounterACT"
  7. Add Notifications
- Emulate an event, check REST API debug log and/or verify changes on ForeScout side.

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 with the NIOS releases (out-of-box). Templates are available on the Infoblox community web-site. Templates for integration with ForeScout are in the ForeScout group (https://community.infoblox.com/t5/ForeScout/gp-p/FORESCOUT). Other templates are posted in the “API & Integration” forum (https://community.infoblox.com/t5/API-Integration/bd-p/API_Integration).

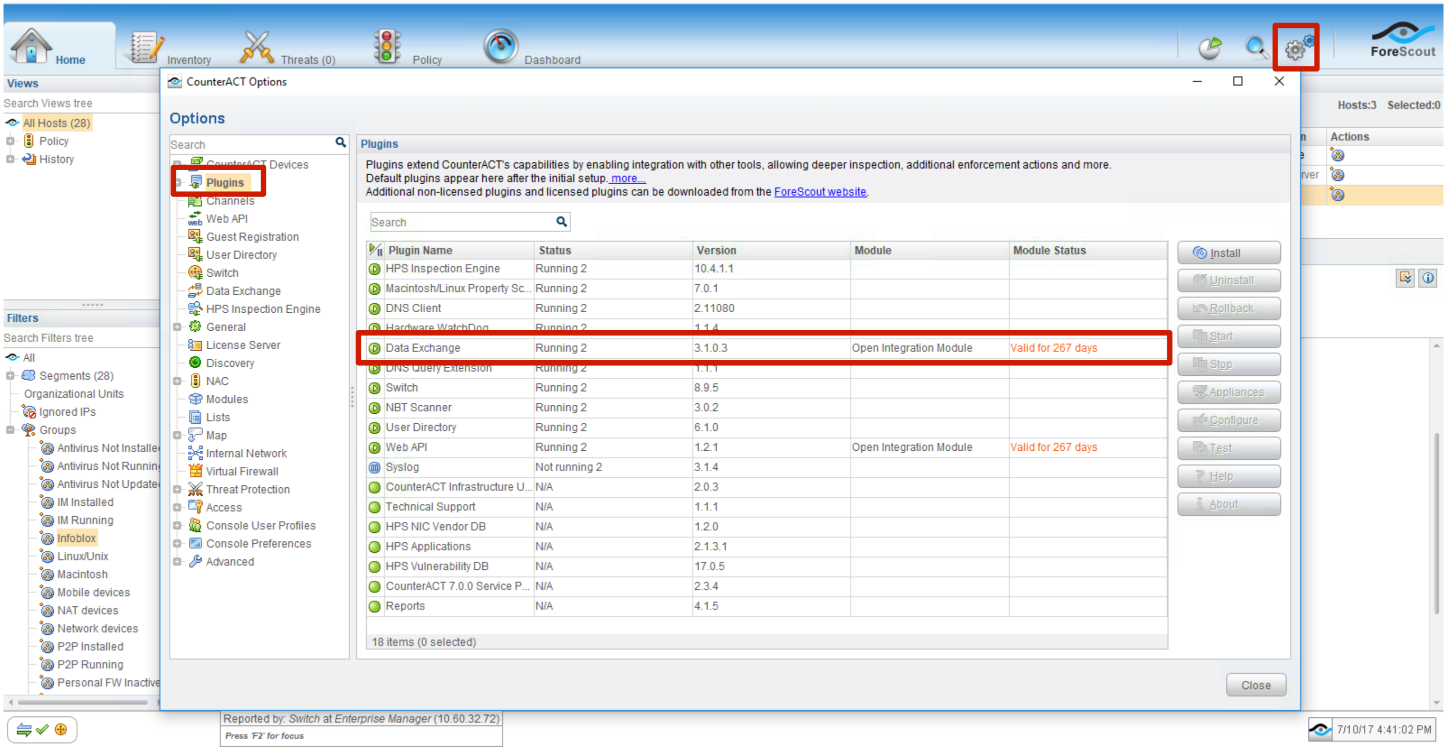
Templates may require additional extensible attributes, parameters or WAPI credentials to be created or defined. The required configuration should be provided with a template. Remember to apply changes, required by the template, before testing a notification.

ForeScout CounterACT configuration

Check if the Open Integration Module is installed and licensed

The **Data Exchange** plugin included with **Open Integration Module** is required for the integration. To verify if the plugin is installed and has a valid license:

1. Open CounterACT configuration (click on gears icon nearby the ForeScout logo).
2. Navigate to the "Plugins" page and verify that the "Data Exchange" plugin is installed and the module status.



Plugins

Plugins extend CounterACT's capabilities by enabling integration with other tools, allowing deeper inspection, additional enforcement actions and more.
Default plugins appear here after the initial setup. more...
Additional non-licensed plugins and licensed plugins can be downloaded from the ForeScout website.

Plugin Name	Status	Version	Module	Module Status
HPS Inspection Engine	Running 2	10.4.1.1		
Macintosh/Linux Property Sc...	Running 2	7.0.1		
DNS Client	Running 2	2.11080		
Hardware WatchDog	Running 2	1.1.4		
Data Exchange	Running 2	3.1.0.3	Open Integration Module	Valid for 267 days
DNS Query Extension	Running 2	1.1.1		
Switch	Running 2	8.9.5		
NBT Scanner	Running 2	3.0.2		
User Directory	Running 2	6.1.0		
Web API	Running 2	1.2.1	Open Integration Module	Valid for 267 days
Syslog	Not running 2	3.1.4		
CounterACT Infrastructure U...	N/A	2.0.3		
Technical Support	N/A	1.1.1		
HPS NIC Vendor DB	N/A	1.2.0		
HPS Applications	N/A	2.1.3.1		
HPS Vulnerability DB	N/A	17.0.5		
CounterACT 7.0.0 Service P...	N/A	2.3.4		
Reports	N/A	4.1.5		

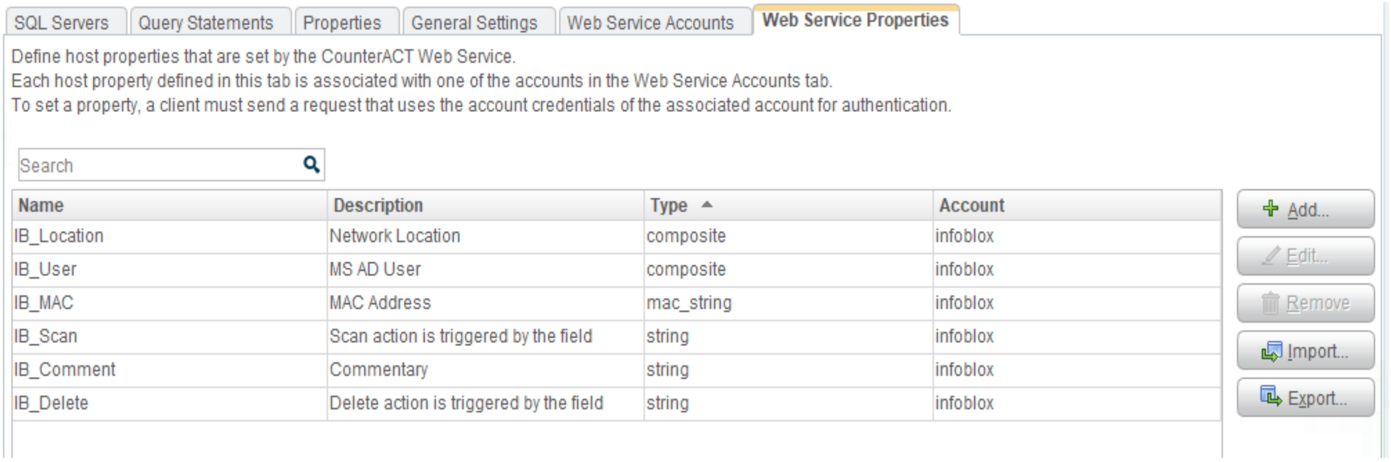
18 items (0 selected)

Reported by: *Switch* at *Enterprise Manager* (10.60.32.72)

Create a Web Service account and properties

The **Data Exchange** plugin uses its own accounts and properties. To create a "Web Service Account" and a "Web Service Properties":

1. Open CounterACT configuration (click on the gears icon near the ForeScout logo).
2. Navigate to the "Data Exchange" page.
3. On the "Web Service Accounts" tab click the "Add..." button. The "Add Account" window will appear.
4. Specify "Name", "Username", "Password" and click "Save". In NIOS, you should specify "Auth Username" using the format "Username@Name".
5. Navigate to the "Web Service Properties" tab and add properties according with the table below. Please note that IB_Location and IB_User are composite properties.



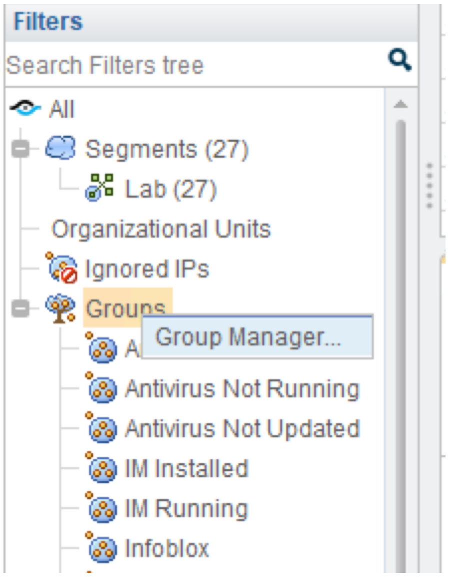
Define host properties that are set by the CounterACT Web Service.
Each host property defined in this tab is associated with one of the accounts in the Web Service Accounts tab.
To set a property, a client must send a request that uses the account credentials of the associated account for authentication.

Name	Description	Type ▲	Account
IB_Location	Network Location	composite	infoblox
IB_User	MS AD User	composite	infoblox
IB_MAC	MAC Address	mac_string	infoblox
IB_Scan	Scan action is triggered by the field	string	infoblox
IB_Comment	Commentary	string	infoblox
IB_Delete	Delete action is triggered by the field	string	infoblox

Property	Type	Field	Field Type	Description
IB_Location	composite			Location device in the network
		Site	string	Extensible attribute FS_Site
		Discoverer	string	IPAM property: discoverer
		Discovered name	string	IPAM property:discovered_name
		Virtual Machine Name	string	IPAM property:v_entity_name
		Device Vendor	string	IPAM property:device_vendor
		Device Model	string	IPAM property:device_model
		Device Type	string	IPAM properties: device_type, v_entity_type
		Attached Device Name	string	IPAM properties: v_switch, network_component
		Attached Device Port	string	IPAM properties: network_component_port_name, v_adapter
		Attached Device Address	string	IPAM property: network_component_ip
		Virtual Datacenter	string	IPAM property: v_datacenter
		Virtual Host	string	IPAM property: v_host
IB_User	composite			MS AD and Cisco ISE username and domains
		Username	string	Username (MS AD and Cisco ISE)
		Domain	string	Domain (MS AD only)
IB_MAC	mac_string			MAC Address
IB_Comment	string			Synchronize date and time
IB_Scan	string			Internal field used to initiate policy by a security event
IB_Delete	string			Internal field used to requests asset removal

(Optional) Configure segments and a group

ForeScout CounterACT accept new assets only if they are in the defined segments. You can add new segments using segments manager in filters (right click on "Segments" and select "Segments Manager") or in the configuration select "Internal Network" options.

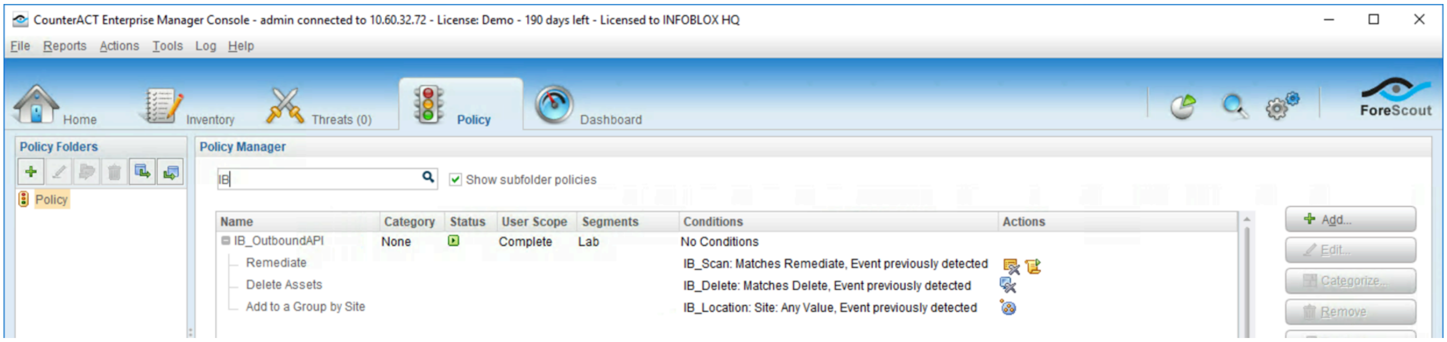


All assets created using Outbound API from Infoblox NIOS can be simply managed by grouping them in a group. Policy groups should be created prior to creating the policy. To add a group on the "Filters" panel, right-click on "Groups" and select "Group Manager".

(Optional) Create policies

To implement responses on security issues, asset groupings and deletions, you should create:

1. Policy which will add assets to a group with parameters:
    - Criteria: any value in IB_Comment property;
    - Action: Add to Group.
2. Policy which will delete assets with parameters:
    - Criteria: "Delete" value in IB_Delete property;
    - Action: "Delete Host".
3. Policy which will be executed as a response on a DNS Security event with parameters:
    - Criteria: any value in IB_Scan property;
    - Actions:
        - Delete properties, which will delete "IB_Scan";
        - Any other possible action. E.g. "Execute Script on Linux".



IB

☑ Show subfolder policies

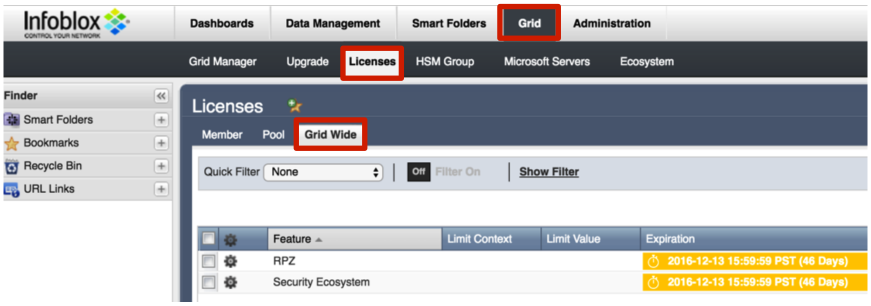
Name	Category	Status	User Scope	Segments	Conditions	Actions
IB_OutboundAPI	None	▶	Complete	Lab	No Conditions	
Remediate					IB_Scan: Matches Remediate, Event previously detected	
Delete Assets					IB_Delete: Matches Delete, Event previously detected	
Add to a Group by Site					IB_Location: Site: Any Value, Event previously detected	

Infoblox NIOS configuration

Check if the Security Ecosystem license is installed

The **Security Ecosystem** license is a Grid Wide license. Grid wide licenses activate services on all compatible appliances within the same Grid.

To check if the license was installed, navigate to **Grid** → **Licenses** → **Grid Wide**.



Quick Filter: None

Feature	Limit Context	Limit Value	Expiration
RPZ			2016-12-13 15:59:59 PST (46 Days)
Security Ecosystem			2016-12-13 15:59:59 PST (46 Days)

Create Extensible Attributes

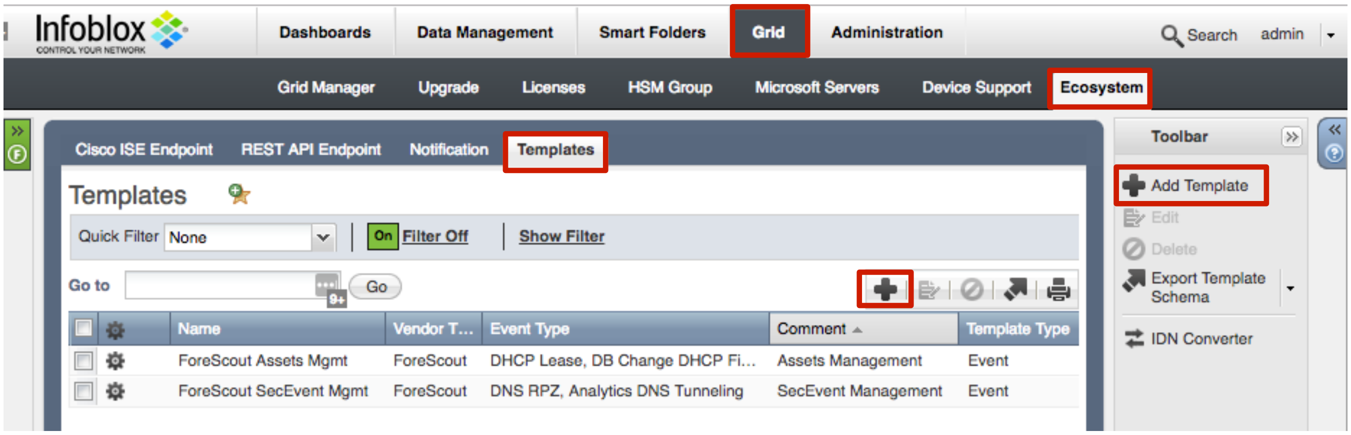
ForeScout Outbound API notifications templates use several extensible attributes to adjust the templates behavior. You can download and use the provided php-script or create them manually. The supported extensible attributes are described in the table below.

Extensible Attribute	Description
FS_Sync	Defines if an object should be synced with ForeScout. Possible values: true, false
FS_SyncedAt	Contains date/time when the object was synchronized, updated by the assets management template
FS_RemediateOnEvent	Defines if a remediation task/policy should be executed for RPZ or DNS Tunneling events that are triggered
FS_RemediatedAt	Contains a date when a remediation task was last executed by a request from Infoblox
FS_Site	Contains a site name

Add/upload templates

To add/upload templates:

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

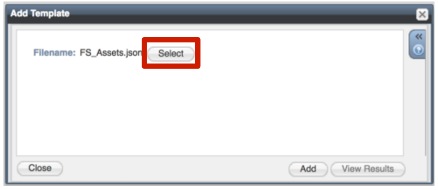


Templates

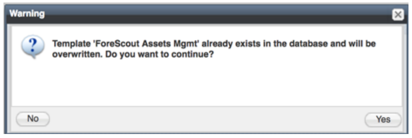
Quick Filter: None

Name	Vendor T...	Event Type	Comment	Template Type
ForeScout Assets Mgmt	ForeScout	DHCP Lease, DB Change DHCP Fi...	Assets Management	Event
ForeScout SecEvent Mgmt	ForeScout	DNS RPZ, Analytics DNS Tunneling	SecEvent Management	Event

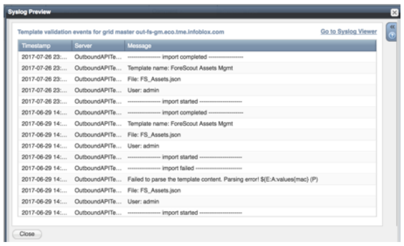
2. Press the “**Select**” button on the “**Add template**” window.
3. If the template was previously uploaded, press "**Yes**" to overwrite the template.
4. Press the “**Select**” button on the “**Upload**” window.
5. The standard file selection dialog will be opened. Select the file and press the “**Upload**” button.



Filename: FS_Assets.json



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



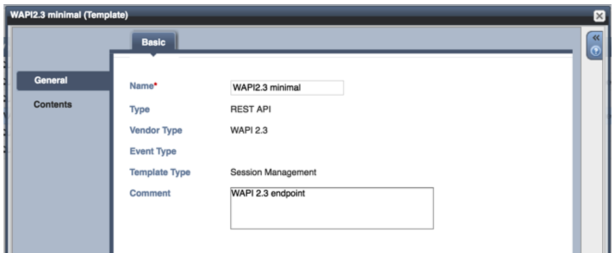
Template validation events for grid master out-fs-gm.eco.tme.infoblox.com

Timestamp	Server	Message
2017-07-26 23:...	OutboundAPITe...	---------------- import completed ----------------
2017-07-26 23:...	OutboundAPITe...	Template name: ForeScout Assets Mgmt
2017-07-26 23:...	OutboundAPITe...	File: FS_Assets.json
2017-07-26 23:...	OutboundAPITe...	User: admin
2017-07-26 23:...	OutboundAPITe...	---------------- import started ----------------
2017-06-29 14:...	OutboundAPITe...	---------------- import completed ----------------
2017-06-29 14:...	OutboundAPITe...	Template name: ForeScout Assets Mgmt
2017-06-29 14:...	OutboundAPITe...	File: FS_Assets.json
2017-06-29 14:...	OutboundAPITe...	User: admin
2017-06-29 14:...	OutboundAPITe...	---------------- import started ----------------
2017-06-29 14:...	OutboundAPITe...	---------------- import failed ----------------
2017-06-29 14:...	OutboundAPITe...	Failed to parse the template content. Parsing error! $(E:A:values{mac} (P)
2017-06-29 14:...	OutboundAPITe...	File: FS_Assets.json
2017-06-29 14:...	OutboundAPITe...	User: admin
2017-06-29 14:...	OutboundAPITe...	---------------- import started ----------------

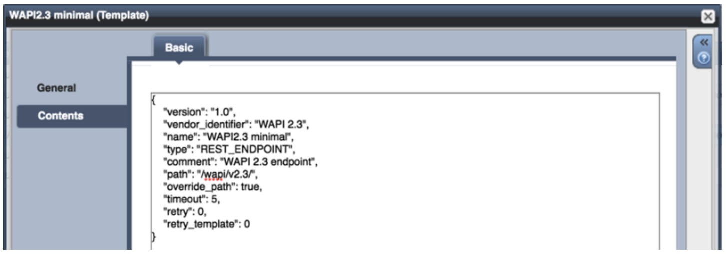
6. Press the “**Add**” button and the template will be added/uploaded.
7. You can review the uploaded results in the syslog or by pressing the “**View Results**” button.
8. There is no difference between uploading session management and action templates.

Modifying Templates

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



Name*	WAPI2.3 minimal
Type	REST API
Vendor Type	WAPI 2.3
Event Type	
Template Type	Session Management
Comment	WAPI 2.3 endpoint



```
{
  "version": "1.0",
  "vendor_identifier": "WAPI 2.3",
  "name": "WAPI2.3 minimal",
  "type": "REST_ENDPOINT",
  "comment": "WAPI 2.3 endpoint",
  "path": "/wapi/v2.3/",
  "override_path": true,
  "timeout": 5,
  "retry": 0,
  "retry_template": 0
}
```

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 the text editor of your choice.

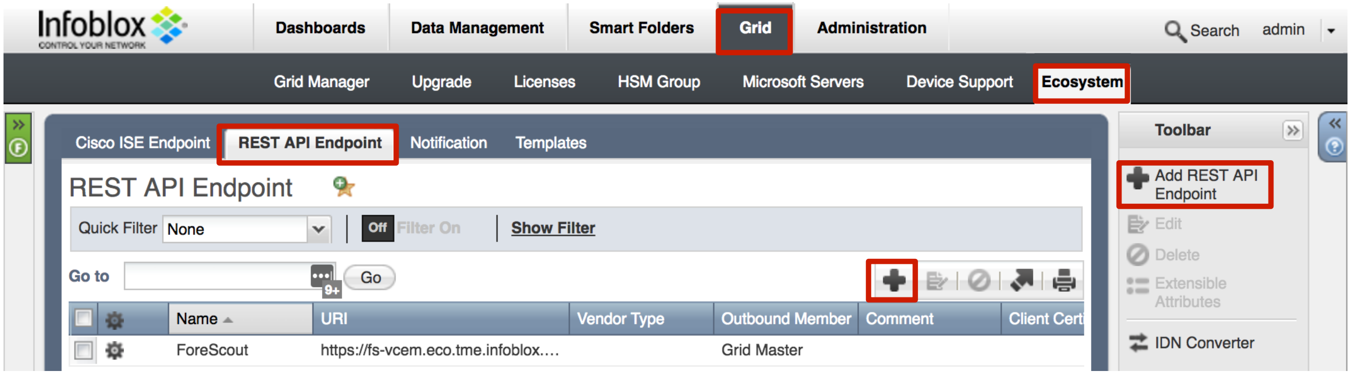
Note: You cannot delete a template if it is used by an endpoint or by a notification.

Add a REST API Endpoint

A REST API Endpoint is basically a remote system which should receive changes based on a notification and configured template. A Grid, for example, can not only send notifications, it can also receive notifications from itself (e.g. for testing purposes).

To add REST API Endpoints:

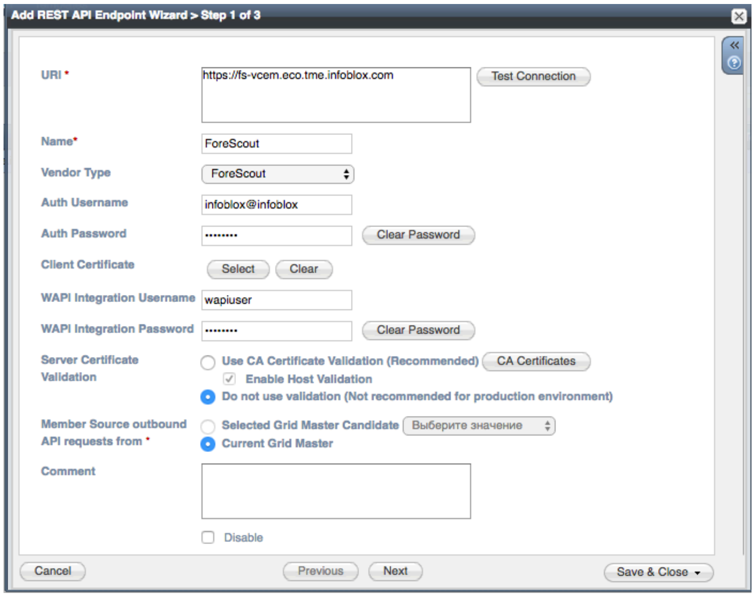
1. Navigate to **Grid** → **Ecosystem** → **REST API Endpoints** and press "**+**" or "**+ Add REST API Endpoint**". The "**Add REST API Endpoint Wizard**" window will open.



Name	URI	Vendor Type	Outbound Member	Comment	Client Cert
ForeScout	https://fs-vcem.eco.tme.infoblox.…		Grid Master		

2. The **URI** and **Name** fields are required.

3. Specify "***URI***", "***NAME***", "***Auth Username***", "***Auth Password***" (ForeScout Web Service account credentials), "***WAPI Integration Username***" and "***WAPI Integration Password***" (NIOS credentials).



URI * https://fs-vcem.eco.tme.infoblox.com

Name* ForeScout

Vendor Type ForeScout

Auth Username infoblox@infoblox

Auth Password ••••••••

Client Certificate

WAPI Integration Username wapiuser

WAPI Integration Password ••••••••

Server Certificate Validation
○ Use CA Certificate Validation (Recommended)
☑ Enable Host Validation
● Do not use validation (Not recommended for production environment)

Member Source outbound API requests from *
○ Selected Grid Master Candidate Выберите значение
● Current Grid Master

Comment

□ Disable

4. (Optional) **For debug purposes only:** Under "**Session Management**", set "**Log Level**" to "**Debug**".

It is recommended to send notifications from a Grid Master Candidate, if there is one available, instead of Grid Master.

Please be aware that the "**Test Connection**" option only checks communication (establishes a TCP connection with a remote system) with the URI. This does not validate the authentication/authorization credentials.

Note: "Test Connection" does not check if NIOS can authenticate with the provided credentials.

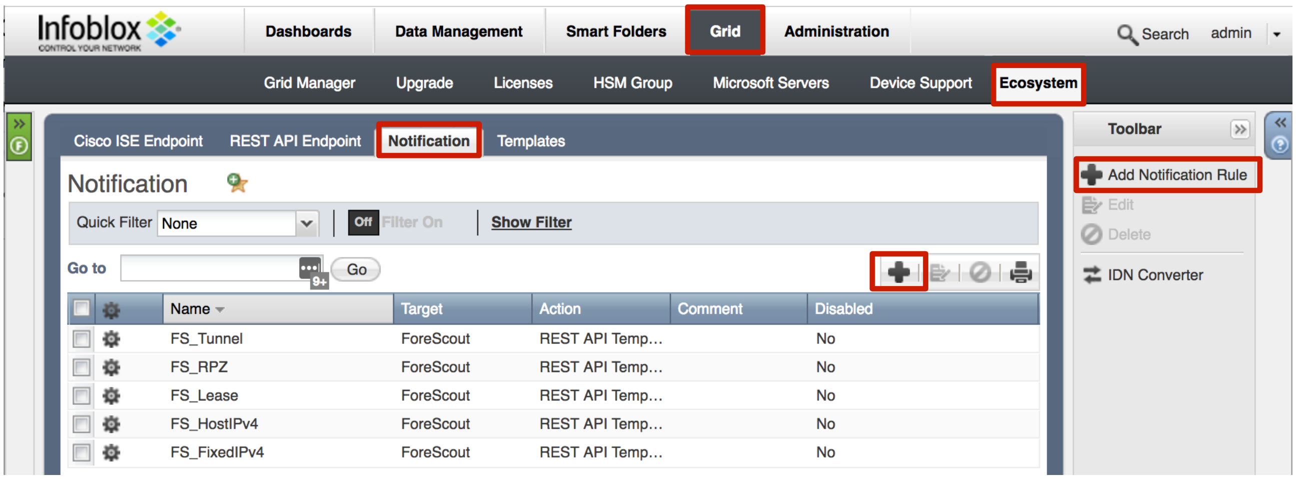
Add a Notification

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 endpoint NIOS will establish the connection to. The ForeScout templates support a subset of available notifications (refer to the Limitations in this guide for more details). To simplify the deployment, only create 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.

To add notifications:

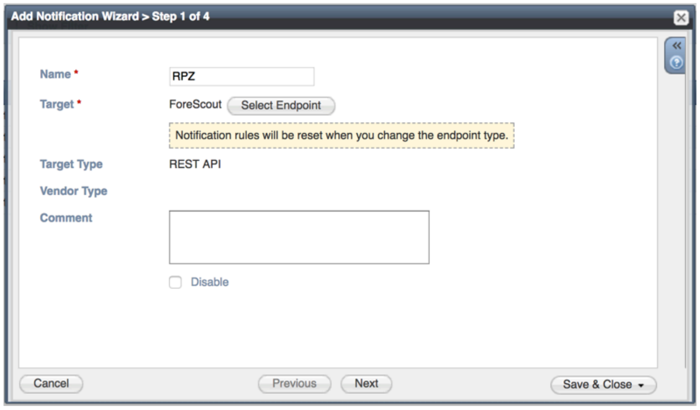
1. Navigate to **Grid** → **Ecosystem** → **Notification** and press “**+**” or “**+ Add Notification Rule**”. The “**Add Notification Wizard**” window will open.



Quick Filter: None

Name	Target	Action	Comment	Disabled
FS_Tunnel	ForeScout	REST API Temp…		No
FS_RPZ	ForeScout	REST API Temp…		No
FS_Lease	ForeScout	REST API Temp…		No
FS_HostIPv4	ForeScout	REST API Temp…		No
FS_FixedIPv4	ForeScout	REST API Temp…		No

2. Specify the notification’s name and select an endpoint (**Target**). Click "**Next**".
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**".



Name *: RPZ

Target *: ForeScout

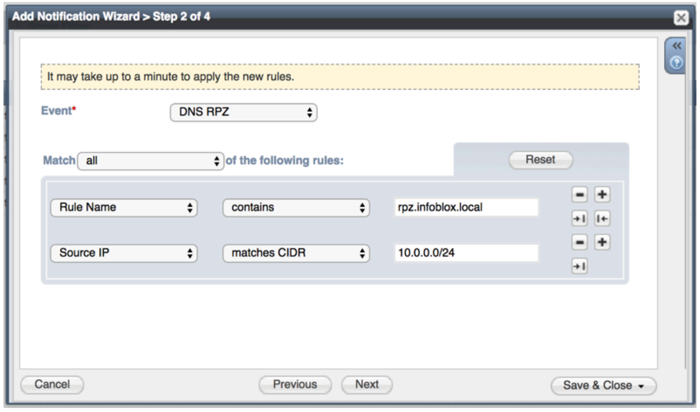
Notification rules will be reset when you change the endpoint type.

Target Type: REST API

Vendor Type

Comment

□ Disable



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

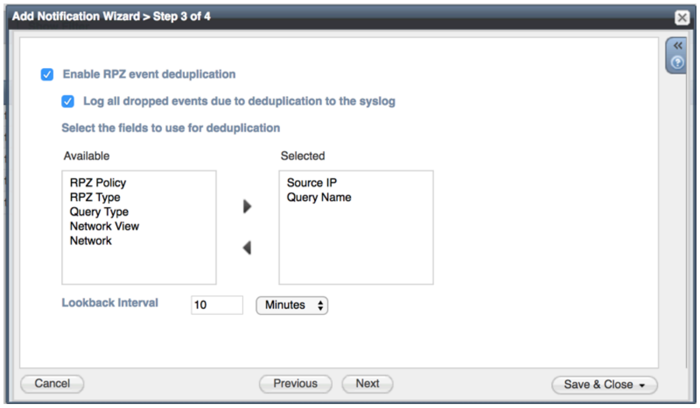
Event*: DNS RPZ

Match all of the following rules:

Rule Name contains rpz.infoblox.local

Source IP matches CIDR 10.0.0.0/24

4. (For RPZ notifications only) Check "**Enable RPZ event deduplication**" and specify relevant parameters. Click "**Next**".
5. Select a relevant template and specify the template's parameters if any are required. Click "**Save & Close**"



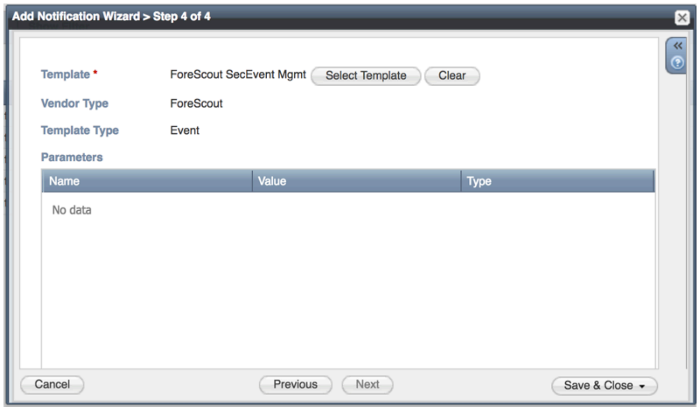
☑ Enable RPZ event deduplication

☑ Log all dropped events due to deduplication to the syslog

Select the fields to use for deduplication

Available	Selected
RPZ Policy RPZ Type Query Type Network View Network	Source IP Query Name

Lookback Interval 10 Minutes



Template * ForeScout SecEvent Mgmt

Vendor Type ForeScout

Template Type Event

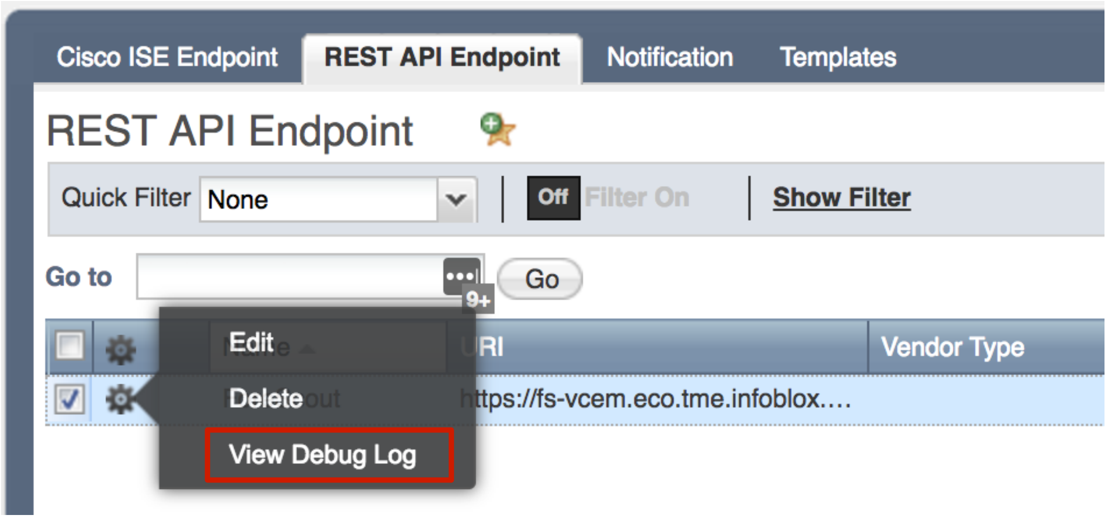
Parameters

Name	Value	Type
No data		

Check the configuration

You can emulate an event from where a notification was added by clicking on the gear wheel next to the notification and selecting “**Test Rule**”). For example, create a host record, or add a DHCP lease. If you have debug logging enabled, you can check it for any issues.

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



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

Any relevant action (e.g. a new asset) should be performed in ForeScout.