Deployment Guide

Infoblox NIOS Integration with Fortinet Fortigate

Using Outbound Notifications

TABLE OF CONTENTS

Introduction

Infoblox and Fortinet FortiGate: Securing your Network

From IoT to an always-on mobile workforce, organizations face increasingly complex IT infrastructures that are more exposed to attacks than ever before. By combining Infoblox's DNS security and protection with Fortinet's Next Generation Firewall (NGFW), users can automate the security of their network.

The Outbound REST API integration framework from Infoblox provides a mechanism to create updates for both IPAM data (networks, hosts, leases) and DNS threat data into additional ecosystem solutions.

Infoblox and FortiGate NGFW together enable security and incident response teams to leverage the integration of firewalls 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:

1. Infoblox:
    - NIOS 8.2 or higher.
    - Security Ecosystem License.
    - Outbound API integration templates.
    - Pre-configured services: DNS, DHCP, Discovery, RPZ, Threat Analytics and ADP.
    - NIOS API user with the following permissions (access via API only):
        - All Network Views – RW.
        - All Hosts – RW.
        - All IPv4 Networks – RW.
        - All IPv6 Networks – RW.
        - All IPv4 Ranges – RW.
        - All IPv6 Ranges – RW.
        - All IPv4 DHCP Fixed Addresses/Reservations – RW.
        - All IPv6 DHCP Fixed Addresses/Reservations – RW.
2. FortiGate NGFW
    - FortiGate v6.0.1 or higher.

Known Limitations

The current templates support DNS Firewall (RPZ), Threat Insight (DNS Tunneling), Advanced DNS Protection, Network IPv4, Network IPv6, Range IPv4, Range IPv6, Host IPv4, Host IPv6, Fixed address IPv4, Fixed address IPv6, lease, and discovery events only. If additional templates come out they will be found on the community site.

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. If additional templates come out, they will be found on the community site.

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

- Fortinet:
    1. Add the user and user group with the appropriate permissions.
    2. Add the required address groups.
    3. Add the Firewall 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 DNS, DHCP,Threat Insight, RPZ and Discovery.
    3. Create the required Extensible Attributes.
    4. Download (or create your own) notification templates (Fortinet_Security.json, Fortinet_Assets.json, Fortinet_Session.json) from the Infoblox community web-site.
    5. Add templates.
    6. Add a REST API Endpoint.
    7. Add Notifications.
    8. Emulate an event, check Rest API 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 Fortinet integration will be located in the **"**Partners 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.

Table 1. Extensible Attributes

Extensible Attributes	Description	Type
Fortinet_Asset_Group	Defines which address group in FortiGate NGFW to add/delete objects from.	String
Fortinet_Asset_Sync	True/False: Defines if the network object is added/deleted from FortiGate NGFW.	List (true,false)
Fortinet_Asset_SyncedAt	Provides the last time the network object was	String

	added/modified on FortiGate NGFW.	
Fortinet_Security_Group	Defines which address group in FortiGate NGFW to add objects to, at the time of a security incident.	String
Fortinet_Security_Sync	True/False: Defines if the network object is added to FortiGate NGFW, at the time of a security incident.	List (true,false)
Fortinet_Security_SyncedAt	Provides the last time the network object was added/updated after a security event in the FortiGate NGFW.	String

Editing Session Variables

The Fortinet_Session template uses a session variable to login to the FortiGate appliance. Session variables can be entered through the grid GUI at **“Grid” → “Ecosystem” → “Outbound Endpoint”** and then selecting the endpoint you created at **“Edit” → “Session Management”**.

Table 2. Session Variables

Session Variable	**Description**
Token	The token with which a user can make API calls to the FortiGate appliance

Editing Instance Variables

Fortinet_Security template uses 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”**.

Table 3. Instance Variables

Instance Variable	**Description**
Fortinet_Security_Group	Defines which address group in the FortiGate NGFW the network object needs to be added to at the time of a security event

Supported 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 Fortinet templates support a subset of available notifications (refer to the limitations chapter in this guide for more details). In order 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.

Table 4. Supported Notifications

Notification	**Description**
DNS RPZ	DNS queries that are malicious or unwanted
DNS Tunneling	Data exfiltration that occurs on the network
ADP	DNS queries that are malicious or unwanted

DHCP Leases	Lease events that occur on the network
Object Change Network IPv4	Added/Deleted IPv4 network objects.
Object Change Network IPv6	Added/Deleted network IPv6 objects.
Object Change Range IPv4	Added/Deleted Host IPv4 objects.
Object Change Range IPv6	Added/Deleted Host IPv6 objects.
Object Change Fixed Address IPv4	Added/Deleted fixed/reserved IPv4 objects.
Object Change Fixed Address IPv6	Added/Deleted fixed/reserved IPv6 objects.
Object Change Host Address IPv4	Added/Deleted Host IPv4 objects.
Object Change Host Address IPv6	Added/Deleted Host IPv6 objects.
Object Change Discovery Data	Discovery events that occur on the network.

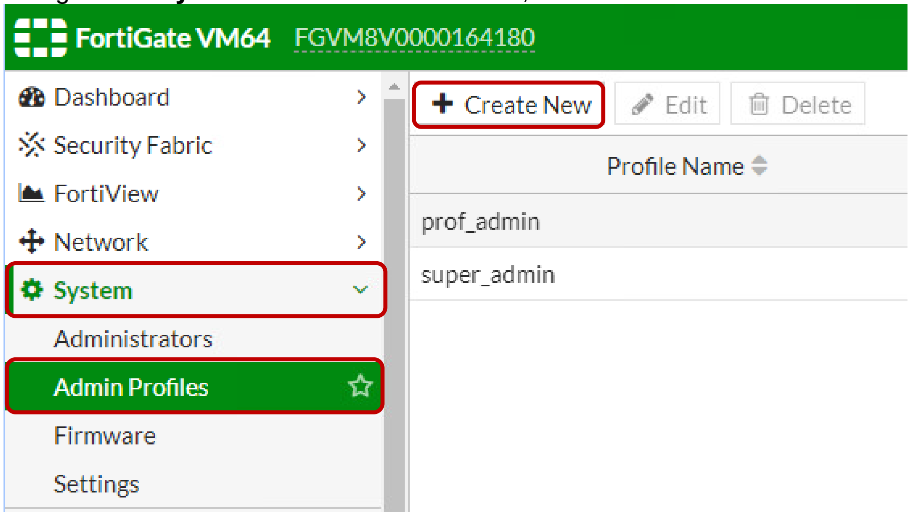
Infoblox Permissions

The Infoblox and Fortinet integration requires a few permissions for the integration to work. Navigate to **“Administration” → “Administrators”** and add a **“Roles”**, **“Permissions”**, **“Groups”** and **“Admins”** to include permissions that are required for the integrations. When creating a new group, under the **“Groups”** tab, select the **“API”** interface under the **“Allowed Interfaces”** category.

Fortinet FortiGate Configuration

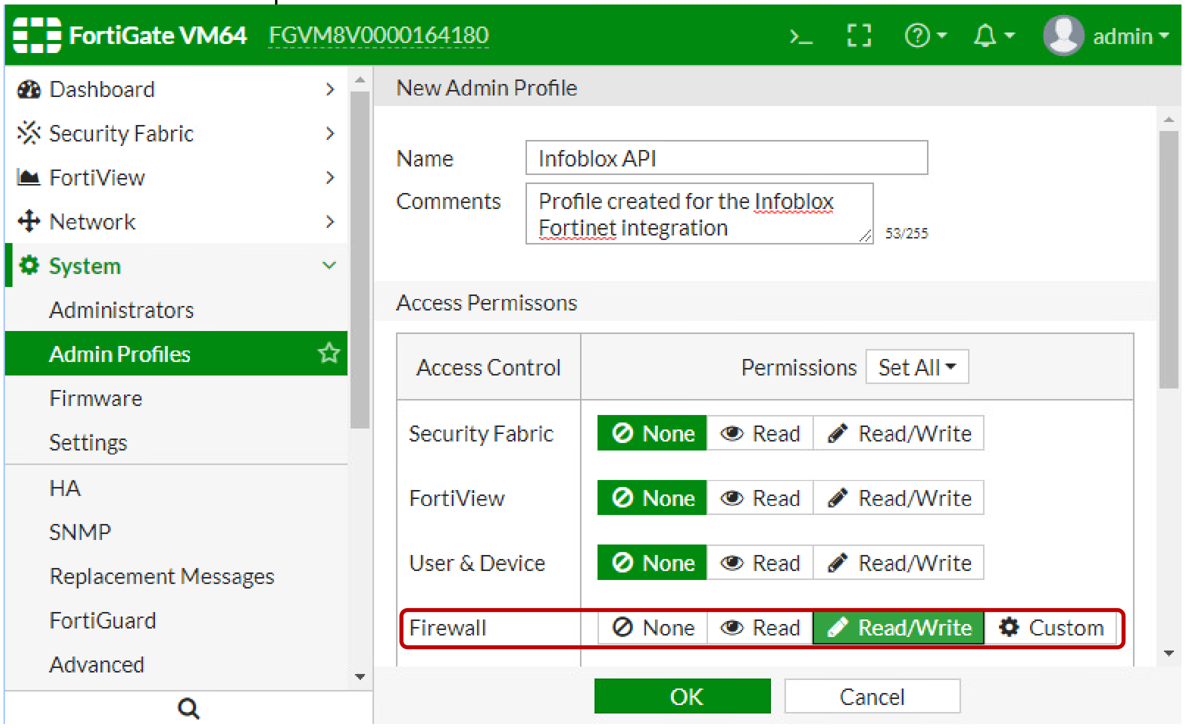
Adding API user (Permissions)

1. Navigate to **“System” → “Admin Profiles”**, the click **Create New**.



2. Enter a name for the profile.

3. Add the **“Read/Write”** permission for **“Firewall”** and click on **“OK”**.



New Admin Profile

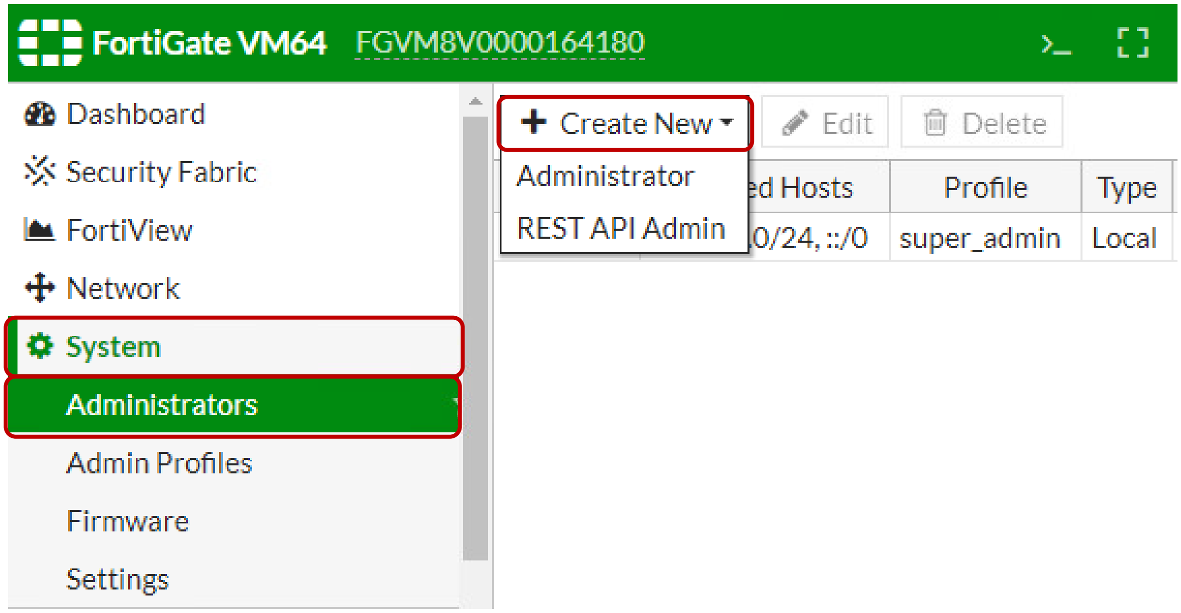
Name: Infoblox API

Comments: Profile created for the Infoblox Fortinet integration 53/255

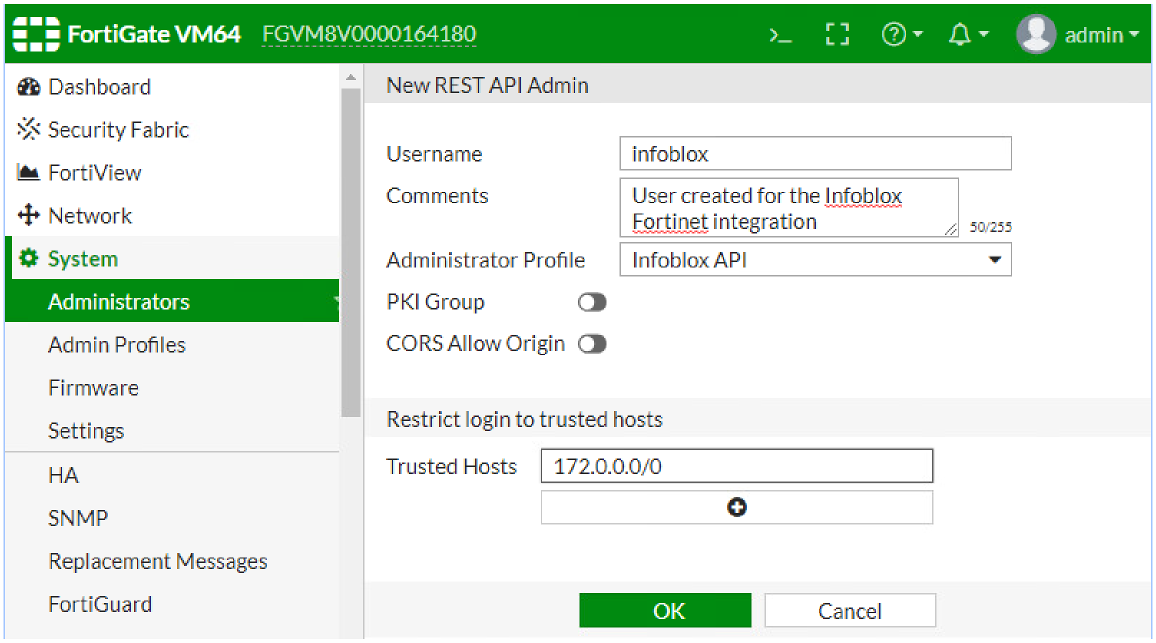
Access Permissons

Access Control	Permissions Set All
Security Fabric	[✓ None] Read Read/Write
FortiView	[✓ None] Read Read/Write
User & Device	[✓ None] Read Read/Write
Firewall	None Read [✓ Read/Write] Custom

4. Navigate to **“System”** → **“Administrators”**, then click **Create New**, and select **“REST API Admin”**.



5. Enter the details for the user, and select the previously created Admin Profile, and click on **OK**.



New REST API Admin

Username: infoblox

Comments: User created for the Infoblox Fortinet integration 50/255

Administrator Profile: Infoblox API

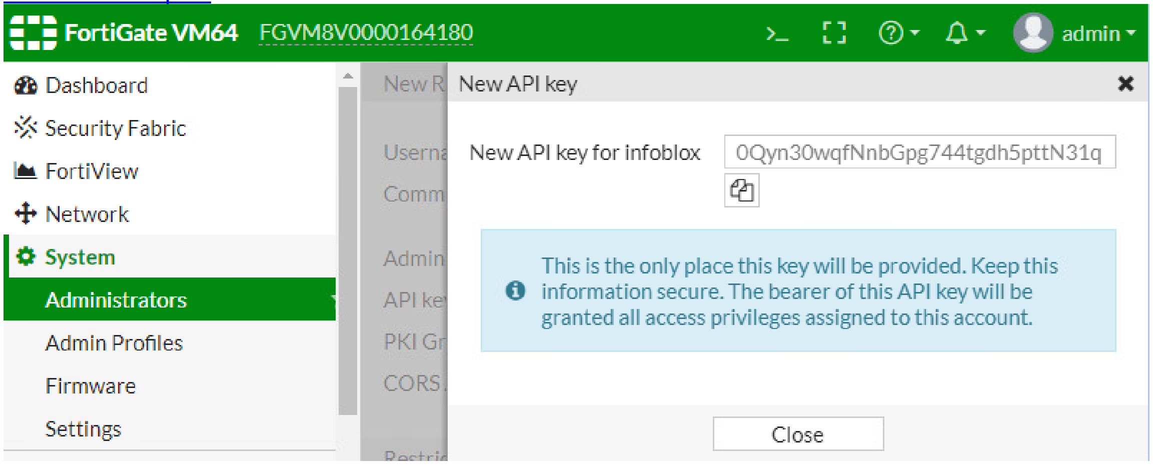
PKI Group

CORS Allow Origin

Restrict login to trusted hosts

Trusted Hosts: 172.0.0.0/0

6. A new API key is generated for this user. For the integration, this key is used as a Token for authenticating the user. The Token is fed as a session Variable, as described Editing Session Variables chapter.



New API key

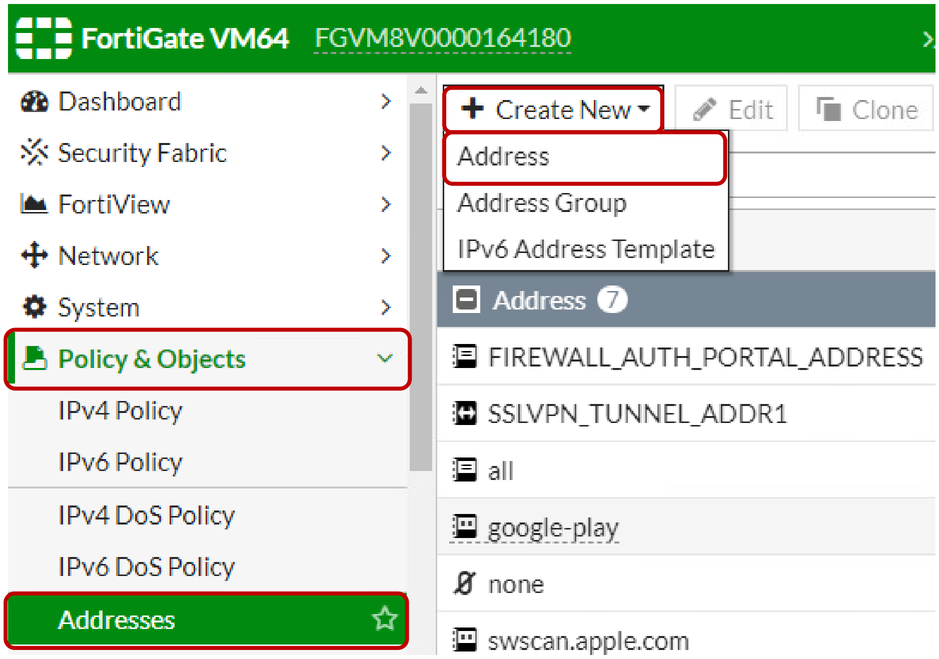
New API key for infoblox: 0Qyn30wqfNnbGpg744tgdh5pttN31q

This is the only place this key will be provided. Keep this information secure. The bearer of this API key will be granted all access privileges assigned to this account.

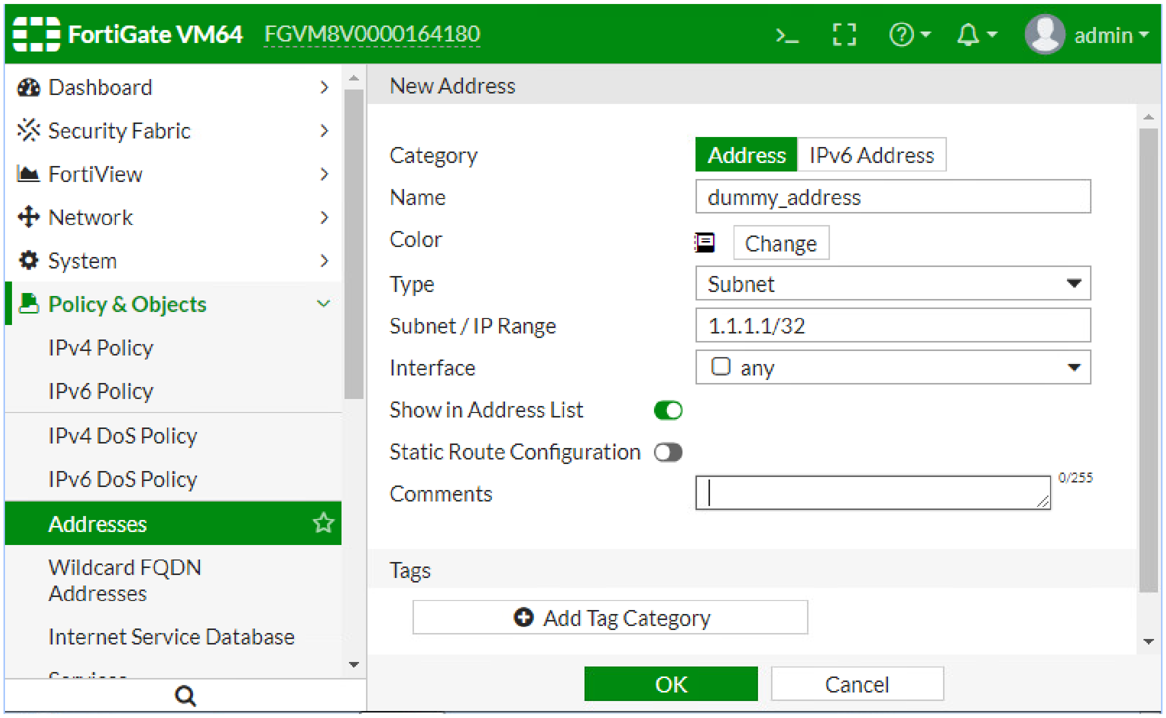
Address Groups and Policies

The Infoblox and Fortinet integration requires address groups. In order to add the address groups:

1. Navigate to **"Policy & Objects"** → **"Addresses"**, then click **"Create New"** and select **"Address"**.



2. Create a dummy address. You can use the below specified details as a reference and click on **"OK"**.

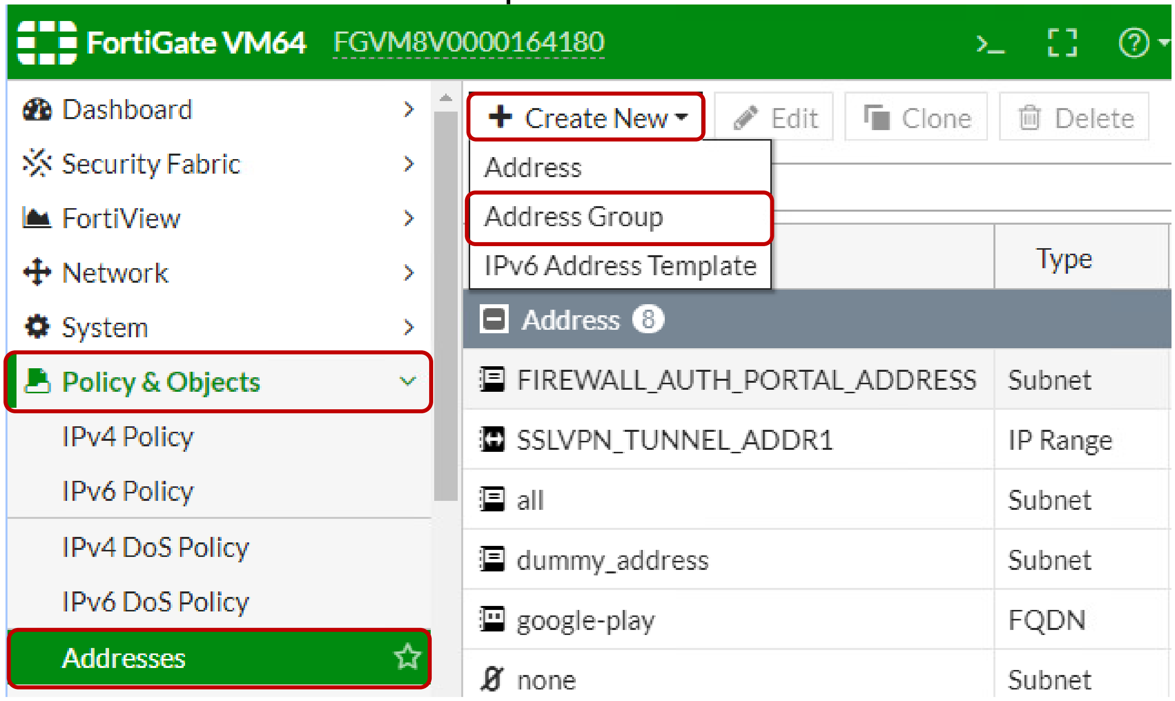


New Address

Category	Address / IPv6 Address
Name	dummy_address
Color	
Type	Subnet
Subnet / IP Range	1.1.1.1/32
Interface	□ any
Show in Address List	●
Static Route Configuration	○
Comments	0/255

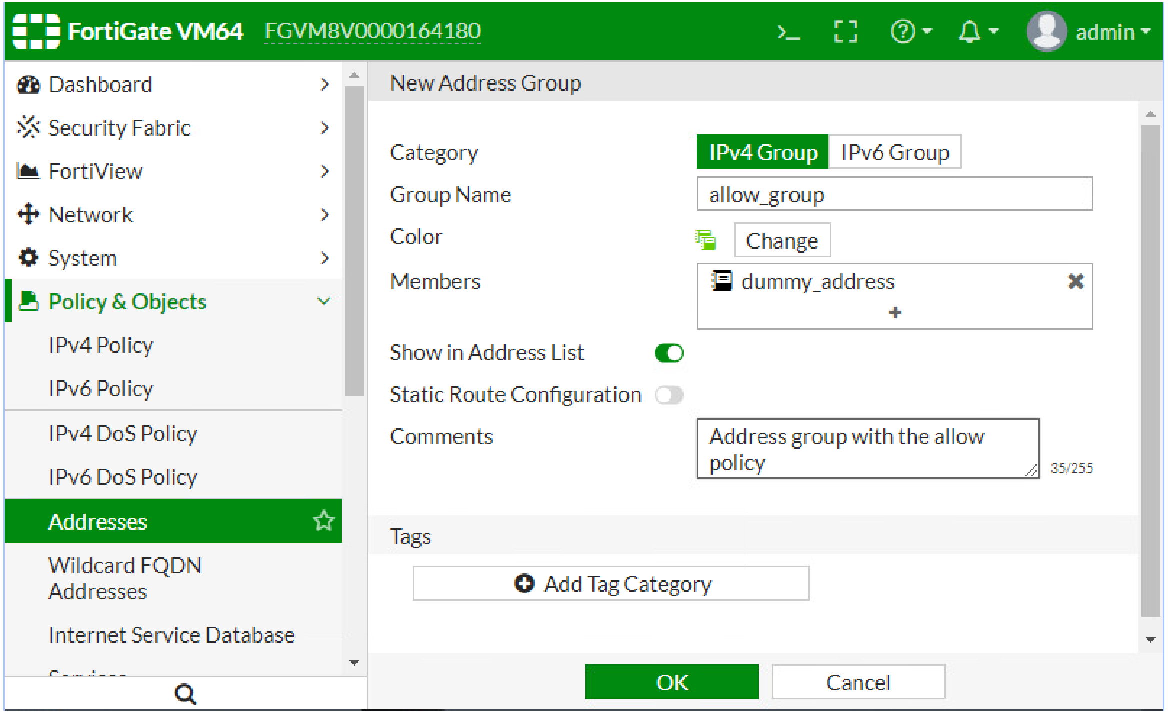
Tags

3. To create an address group, navigate to **“Policy & Objects”** → **“Addresses”,** then click **“Create New”** and select **“Address Group”**.



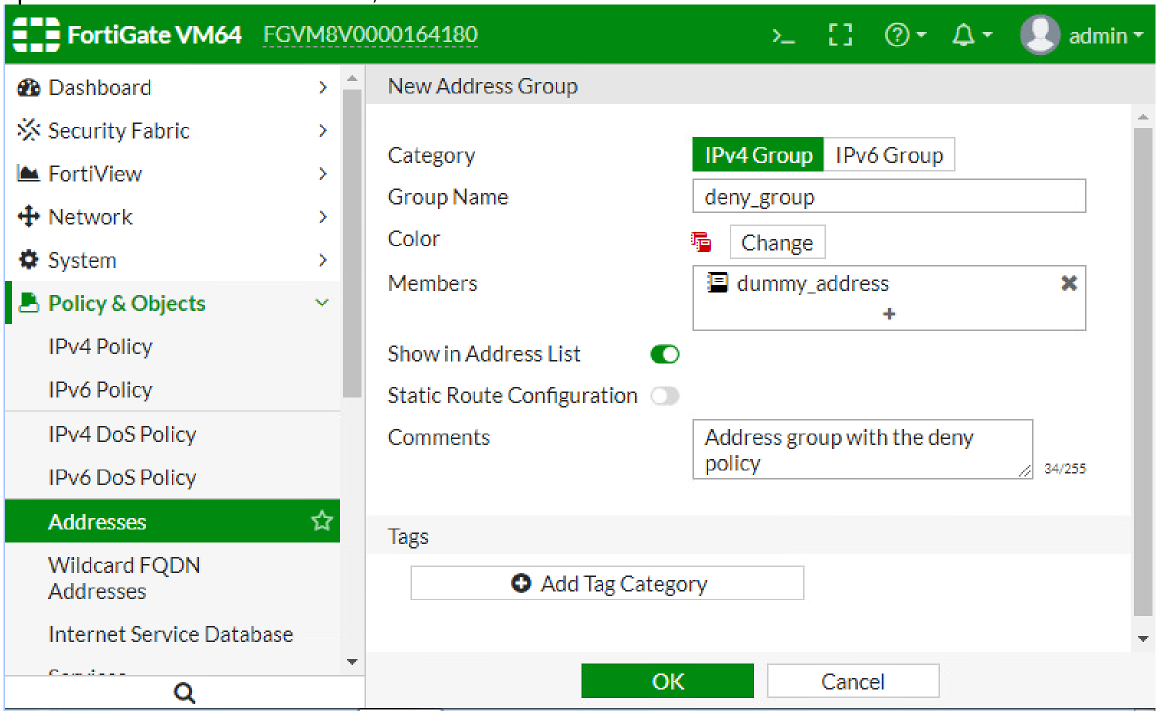
	Type
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet
SSLVPN_TUNNEL_ADDR1	IP Range
all	Subnet
dummy_address	Subnet
google-play	FQDN
none	Subnet

4. Create a group on which you can set the allow policy. You can use the below specified details as a reference, and click on **“OK”**.



Category	[✓ IPv4 Group] IPv6 Group
Group Name	allow_group
Color	
Members	dummy_address
Show in Address List	● On
Static Route Configuration	○ Off
Comments	Address group with the allow policy

5. Similarly, create a group on which you can set the deny policy. You can use the below specified details as a reference, and click on **"OK"**.

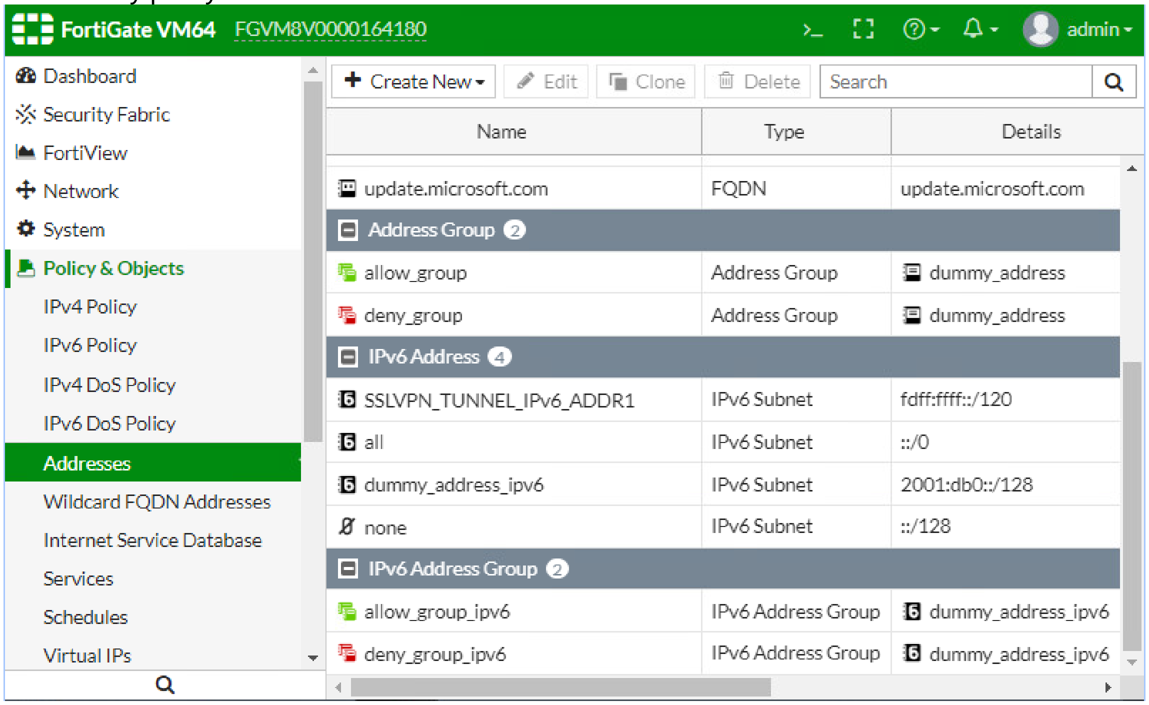


New Address Group

Category	IPv4 Group (selected) / IPv6 Group
Group Name	deny_group
Color	Change
Members	dummy_address
Show in Address List	●
Static Route Configuration	○
Comments	Address group with the deny policy (34/255)

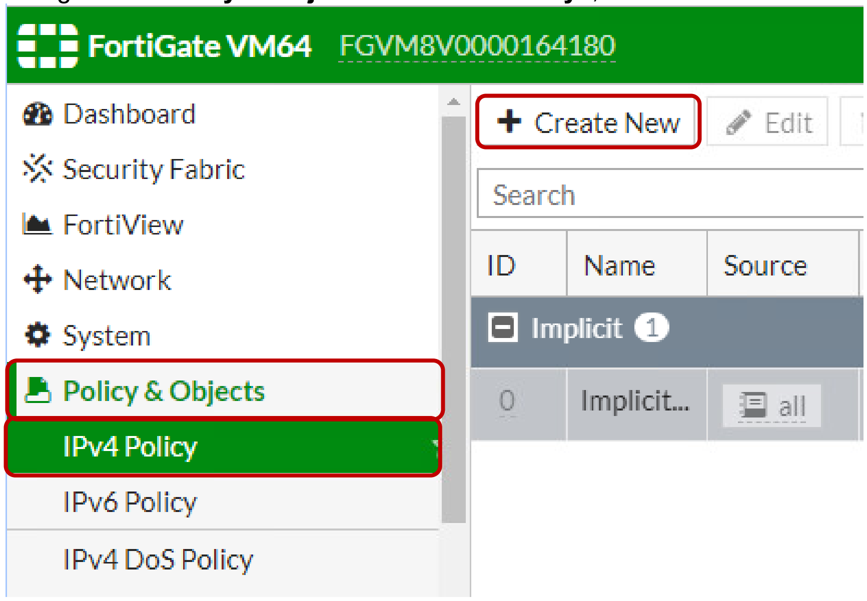
Tags

6. Similarly, create a dummy IPv6 address and 2 IPv6 groups, one for the allow policy and one for the deny policy.

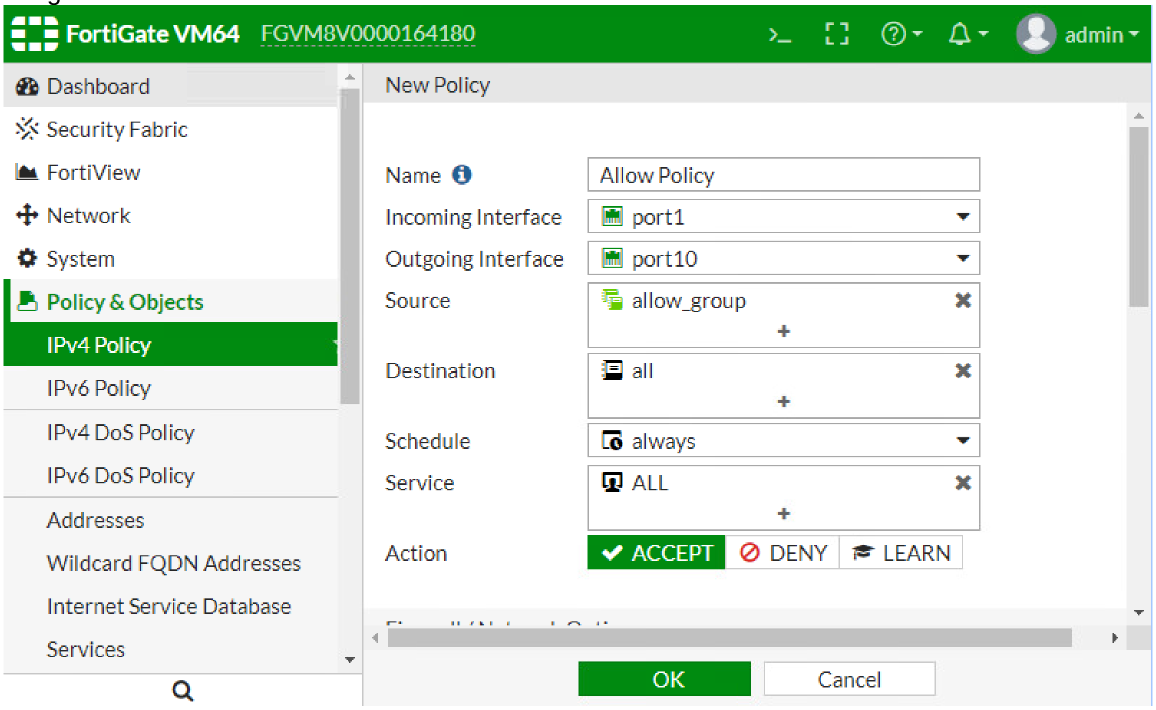


Name	Type	Details
update.microsoft.com	FQDN	update.microsoft.com
Address Group 2		
allow_group	Address Group	dummy_address
deny_group	Address Group	dummy_address
IPv6 Address 4		
SSLVPN_TUNNEL_IPv6_ADDR1	IPv6 Subnet	fdff:ffff::/120
all	IPv6 Subnet	::/0
dummy_address_ipv6	IPv6 Subnet	2001:db0::/128
none	IPv6 Subnet	::/128
IPv6 Address Group 2		
allow_group_ipv6	IPv6 Address Group	dummy_address_ipv6
deny_group_ipv6	IPv6 Address Group	dummy_address_ipv6

7. Navigate to **“Policy & Objects” → “IPv4 Policy”**, then click **“Create New”**.



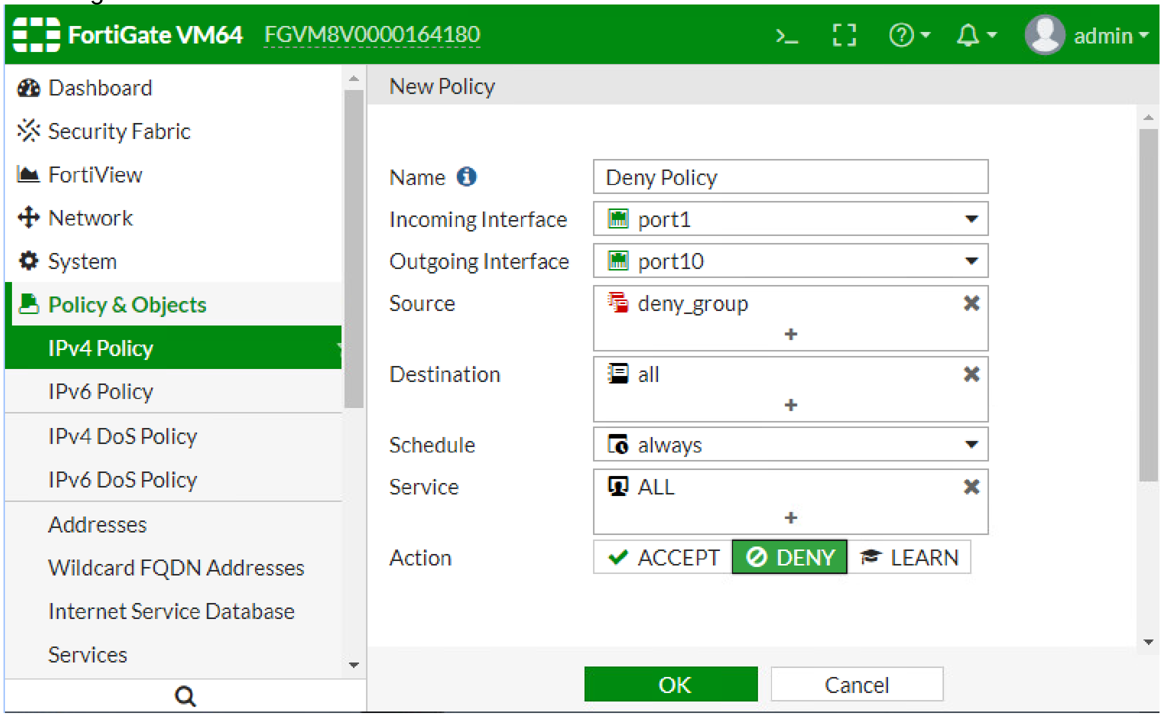
8. Create a policy for the previously created allow group to allow all traffic as shown in the image below.



New Policy

Name	Allow Policy
Incoming Interface	port1
Outgoing Interface	port10
Source	allow_group
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY LEARN

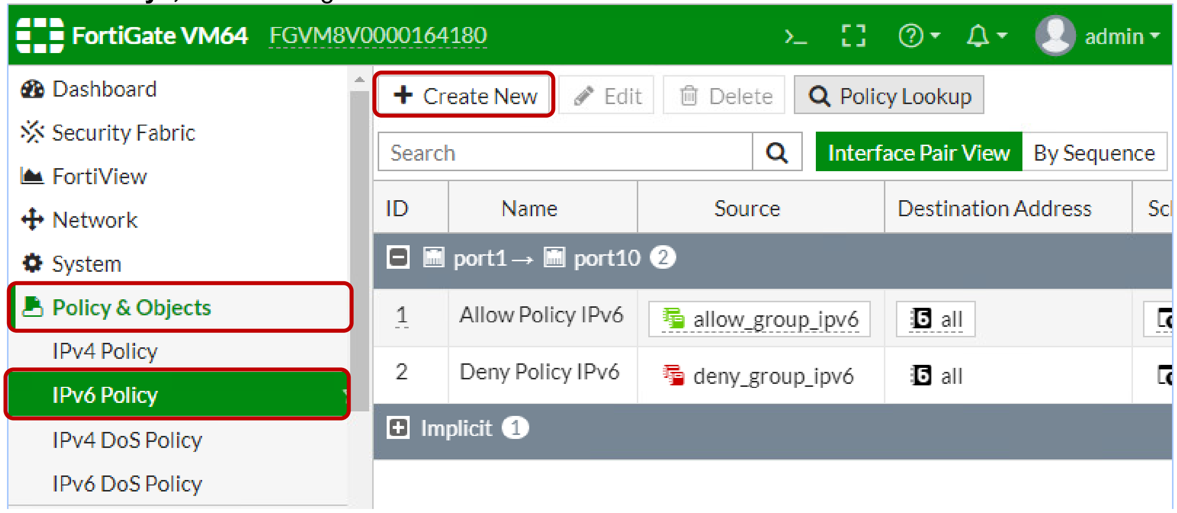
9. Similarly, create a policy for the previously created deny group to deny all traffic as shown in the image below.



New Policy

Name	Deny Policy
Incoming Interface	port1
Outgoing Interface	port10
Source	deny_group
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT [✓ DENY] LEARN

10. Similarly, create the allow and deny policies for IPv6 by navigating to **“Policy & Objects” →** **“IPv6 Policy”,** then clicking **“Create New”**.

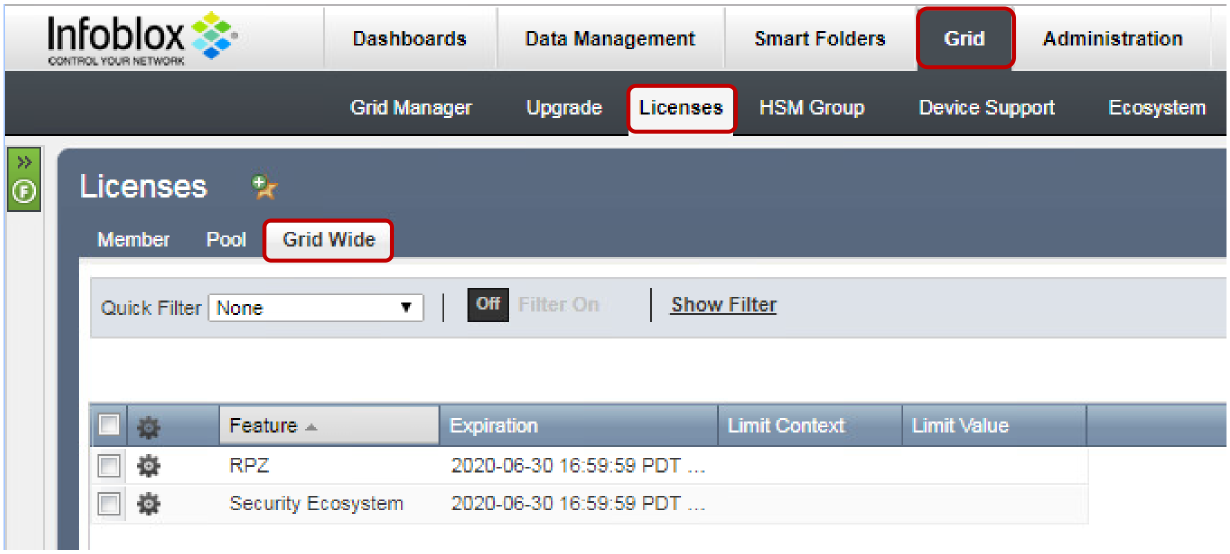


ID	Name	Source	Destination Address	Sc
port1 → port10 2				
1	Allow Policy IPv6	allow_group_ipv6	all	
2	Deny Policy IPv6	deny_group_ipv6	all	
Implicit 1				

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”**.



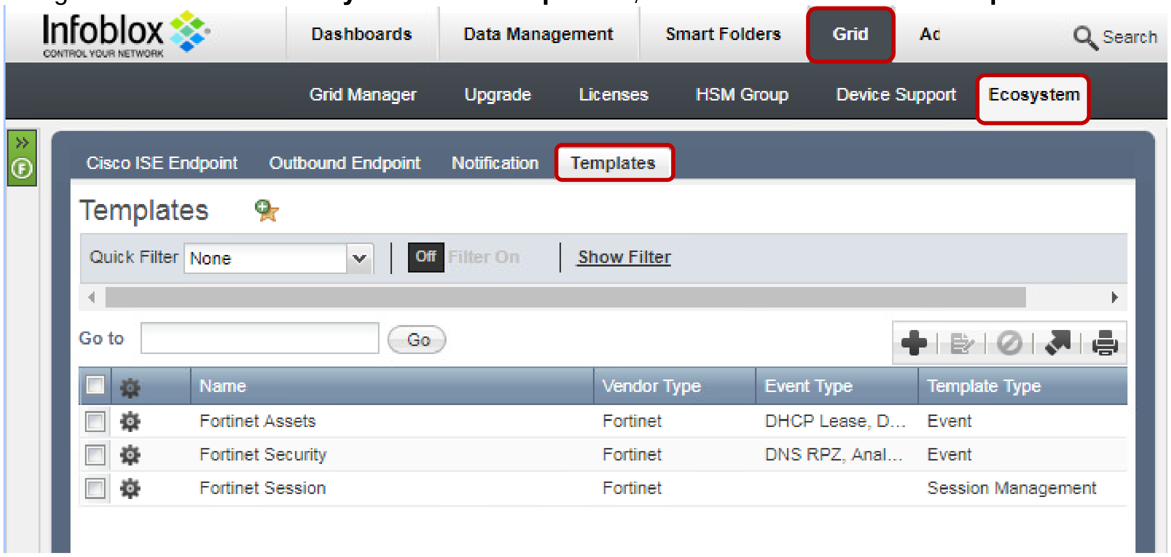
Quick Filter: None

Feature	Expiration	Limit Context	Limit Value
RPZ	2020-06-30 16:59:59 PDT ...		
Security Ecosystem	2020-06-30 16:59:59 PDT ...		

Add/Upload Templates

In order to upload/add templates:

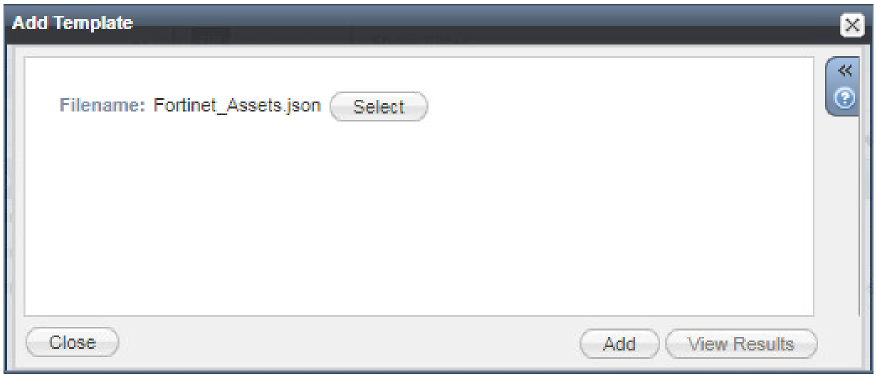
1. Navigate to **"Grid"** → **"Ecosystem"** → **"Templates"**, and click **"+"** or **"+ Add Template"**.



Quick Filter: None

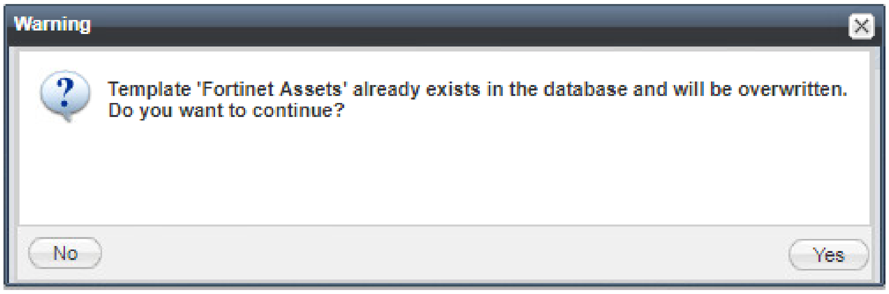
Name	Vendor Type	Event Type	Template Type
Fortinet Assets	Fortinet	DHCP Lease, D...	Event
Fortinet Security	Fortinet	DNS RPZ, Anal...	Event
Fortinet Session	Fortinet		Session Management

2. Click the **"Select"** button on the **"Add template"** window.
3. Click the **"Select"** button on the **"Upload"** window. The standard file selection dialog will open.
4. Select the file and Click the **"Upload"** button on the **"Upload"** window.
5. Click the **"Add"** button and the template will be added/uploaded.



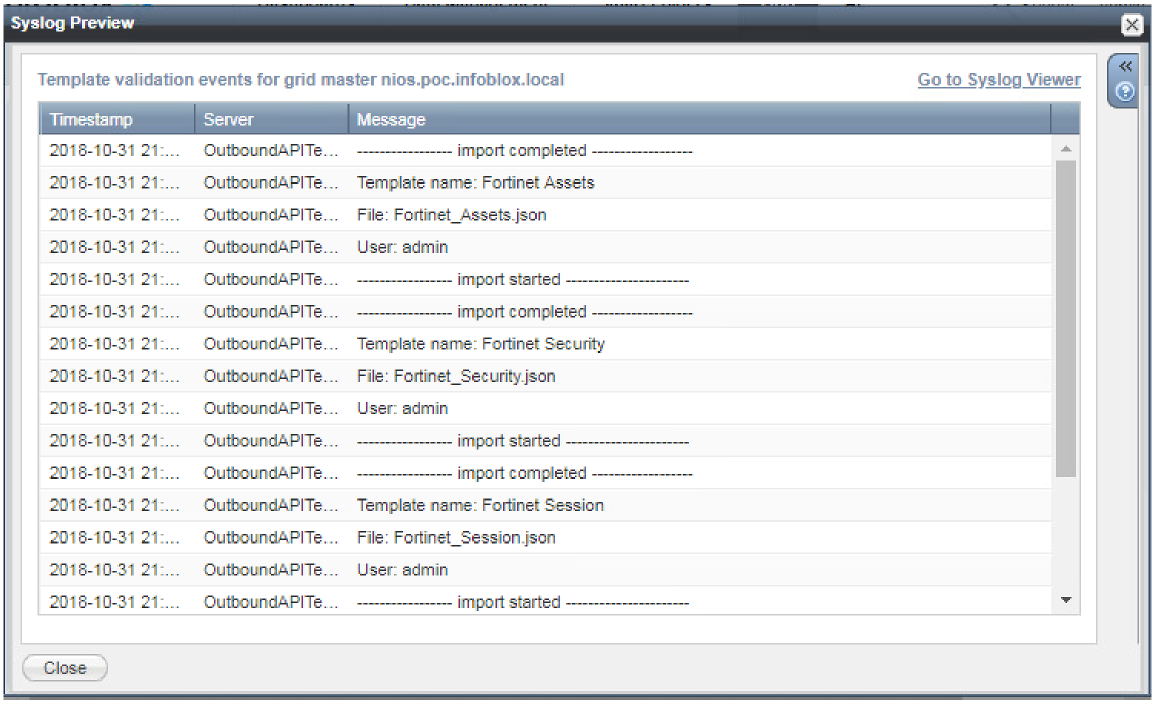
Filename: Fortinet_Assets.json

6. If a template was previously uploaded, click **“Yes”** to overwrite the template.



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

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



Template validation events for grid master nios.poc.infoblox.local

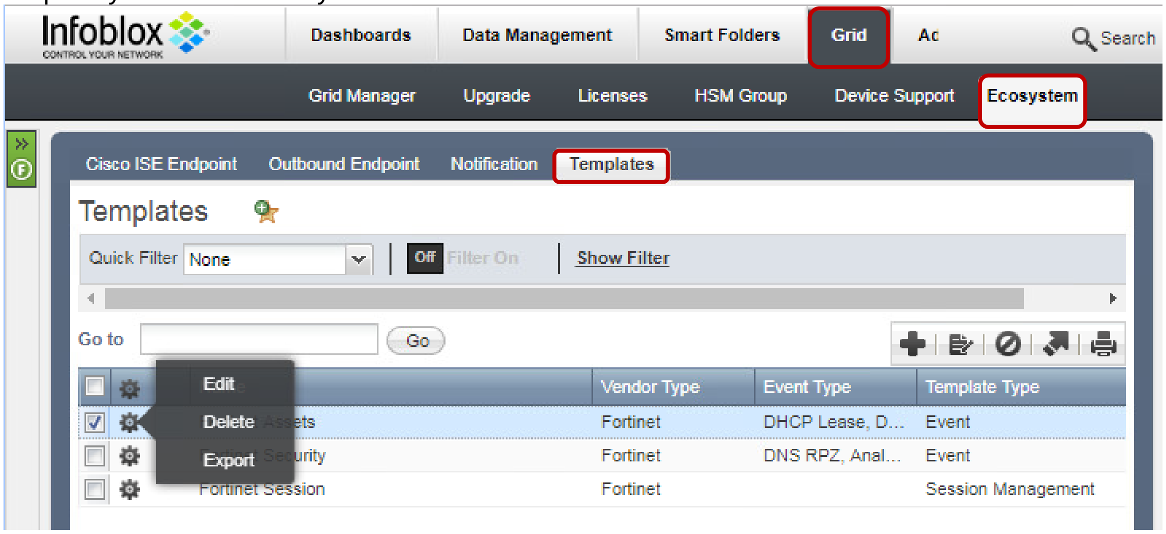
Timestamp	Server	Message
2018-10-31 21:...	OutboundAPITe...	---------------- import completed -----------------
2018-10-31 21:...	OutboundAPITe...	Template name: Fortinet Assets
2018-10-31 21:...	OutboundAPITe...	File: Fortinet_Assets.json
2018-10-31 21:...	OutboundAPITe...	User: admin
2018-10-31 21:...	OutboundAPITe...	---------------- import started ---------------------
2018-10-31 21:...	OutboundAPITe...	---------------- import completed -----------------
2018-10-31 21:...	OutboundAPITe...	Template name: Fortinet Security
2018-10-31 21:...	OutboundAPITe...	File: Fortinet_Security.json
2018-10-31 21:...	OutboundAPITe...	User: admin
2018-10-31 21:...	OutboundAPITe...	---------------- import started ---------------------
2018-10-31 21:...	OutboundAPITe...	---------------- import completed -----------------
2018-10-31 21:...	OutboundAPITe...	Template name: Fortinet Session
2018-10-31 21:...	OutboundAPITe...	File: Fortinet_Session.json
2018-10-31 21:...	OutboundAPITe...	User: admin
2018-10-31 21:...	OutboundAPITe...	---------------- import started ---------------------

Note: 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 click the gear icon next to the template you want to modify.



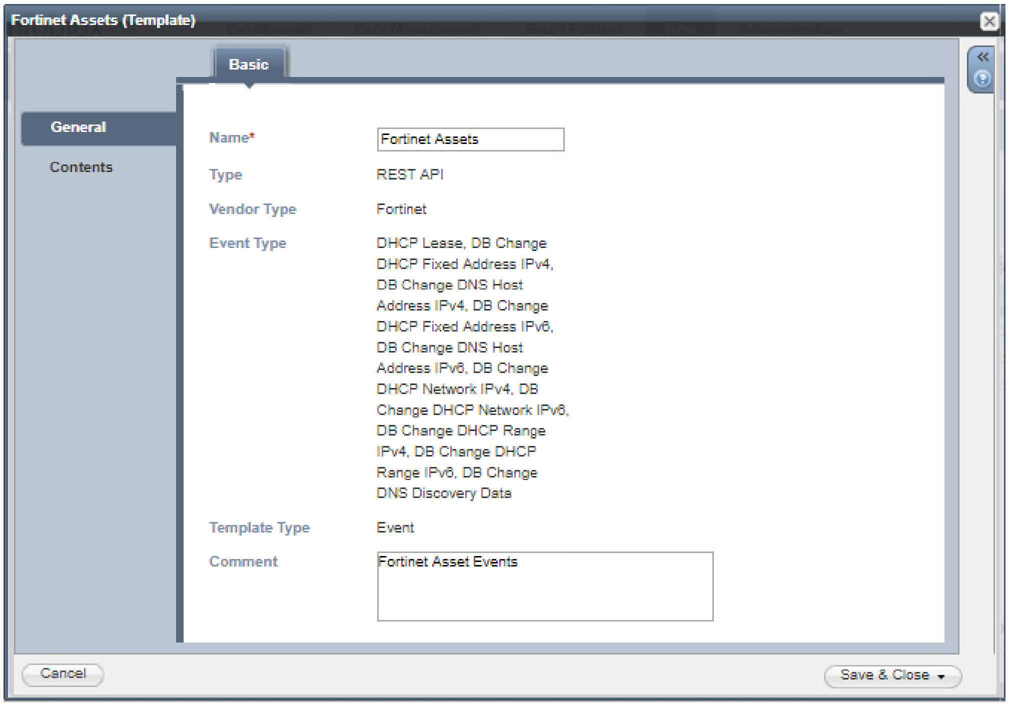
Templates

Quick Filter: None | Off Filter On | Show Filter

Go to [ ] Go

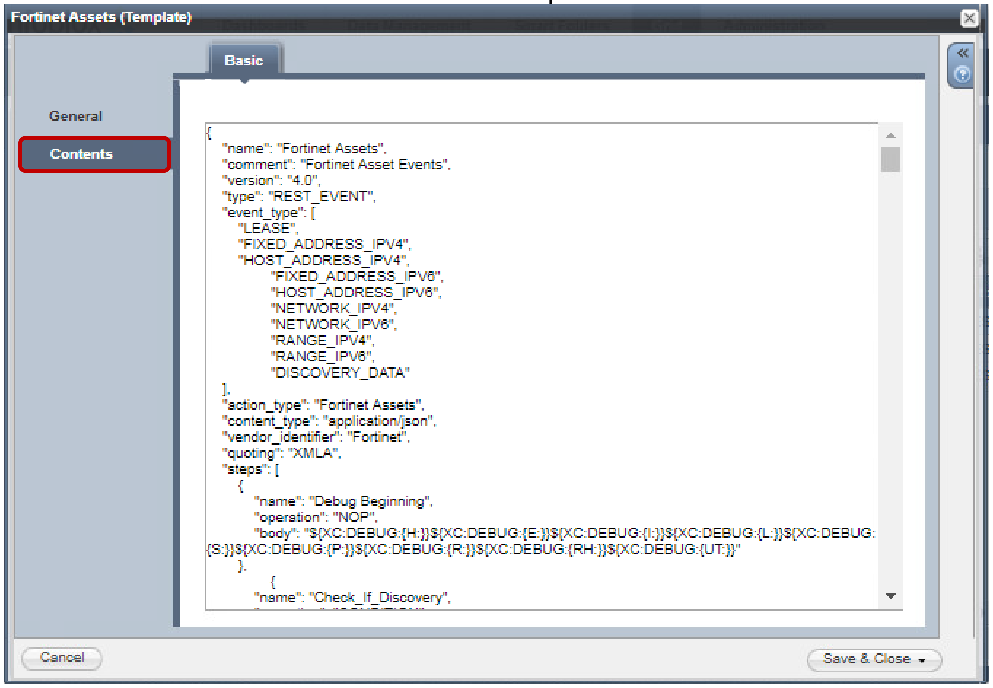
☐		Vendor Type	Event Type	Template Type
☑	Assets	Fortinet	DHCP Lease, D...	Event
☐	Security	Fortinet	DNS RPZ, Anal...	Event
☐	Fortinet Session	Fortinet		Session Management

2. Click the **"Edit"** button to open up the **"Template"** window.



Name*	Fortinet Assets
Type	REST API
Vendor Type	Fortinet
Event Type	DHCP Lease, DB Change DHCP Fixed Address IPv4, DB Change DNS Host Address IPv4, DB Change DHCP Fixed Address IPv6, DB Change DNS Host Address IPv6, DB Change DHCP Network IPv4, DB Change DHCP Network IPv6, DB Change DHCP Range IPv4, DB Change DHCP Range IPv6, DB Change DNS Discovery Data
Template Type	Event
Comment	Fortinet Asset Events

3. Click on the **Contents** tab to view/edit the template.



```
{
   "name": "Fortinet Assets",
   "comment": "Fortinet Asset Events",
   "version": "4.0",
   "type": "REST_EVENT",
   "event_type": [
      "LEASE",
      "FIXED_ADDRESS_IPV4",
      "HOST_ADDRESS_IPV4",
            "FIXED_ADDRESS_IPV6",
            "HOST_ADDRESS_IPV6",
            "NETWORK_IPV4",
            "NETWORK_IPV6",
            "RANGE_IPV4",
            "RANGE_IPV6",
            "DISCOVERY_DATA"
   ],
   "action_type": "Fortinet Assets",
   "content_type": "application/json",
   "vendor_identifier": "Fortinet",
   "quoting": "XMLA",
   "steps": [
      {
         "name": "Debug Beginning",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:
{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:{R:}}${XC:DEBUG:{RH:}}${XC:DEBUG:{UT:}}"
      },
            {
         "name": "Check_If_Discovery",
```

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.

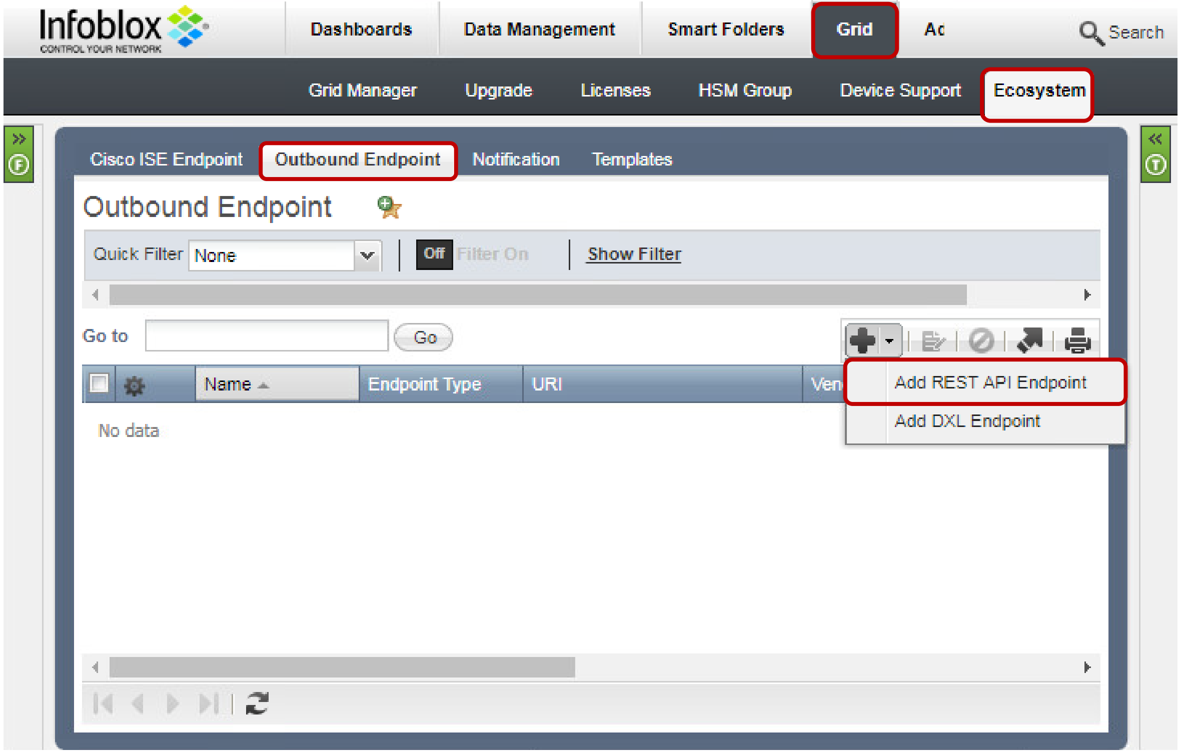
Note: You cannot delete a template if it is used by an endpoint or by a notification.

Add a Rest API Endpoint

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

In order to add REST API Endpoints:

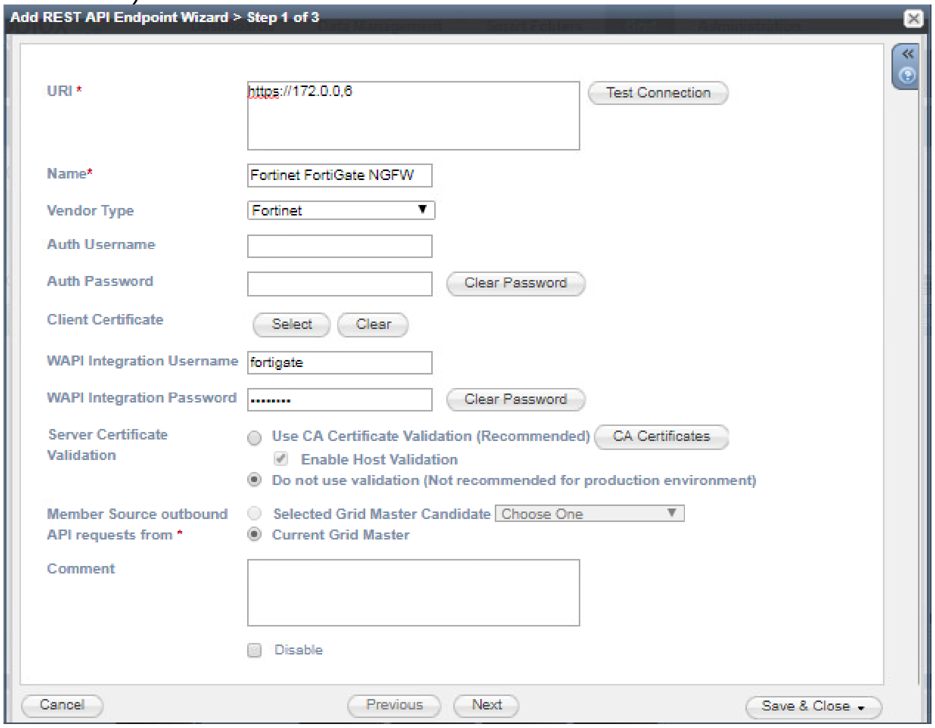
1. Navigate to **"Grid"** → **"Ecosystem"** → **"Outbound Endpoints"** and click **"+"** or **"+ Add REST API Endpoint"** buttons. The **"Add REST API Endpoint Wizard"** window will open.



2. The URI and Name for the appliance you are integrating with are required.

3. The URI should be the IP/FQDN of the appliance you are integrating with, with the correct URI scheme.

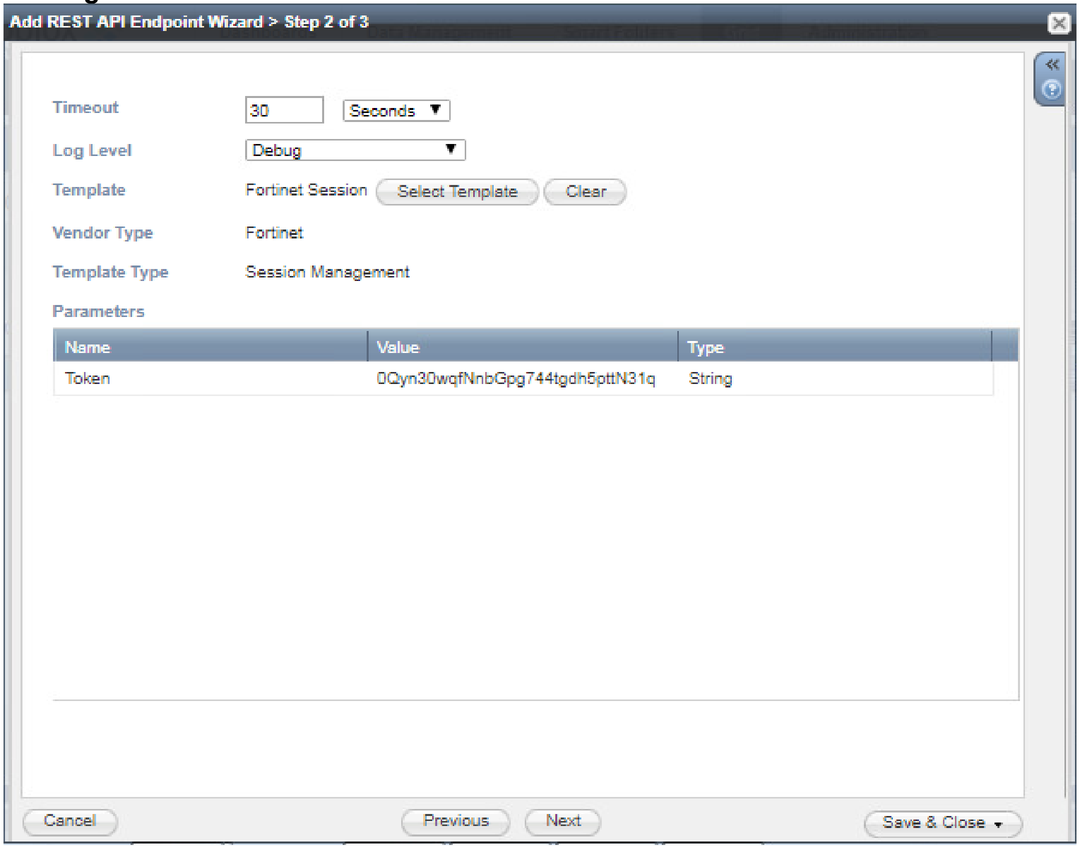
4. Specify **“WAPI Integration Username”** and **“WAPI Integration Password”** (NIOS credentials).



Add REST API Endpoint Wizard > Step 1 of 3

URI *	https://172.0.0.6
Name*	Fortinet FortiGate NGFW
Vendor Type	Fortinet
Auth Username	
Auth Password	
Client Certificate	
WAPI Integration Username	fortigate
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 Choose One ● Current Grid Master
Comment	
	□ Disable

5. (Optional) For debug purposes only: Under **“Session Management”**, set **“Log Level”** to **“Debug”**.



Add REST API Endpoint Wizard > Step 2 of 3

Timeout	30 Seconds
Log Level	Debug
Template	Fortinet Session
Vendor Type	Fortinet
Template Type	Session Management

Parameters

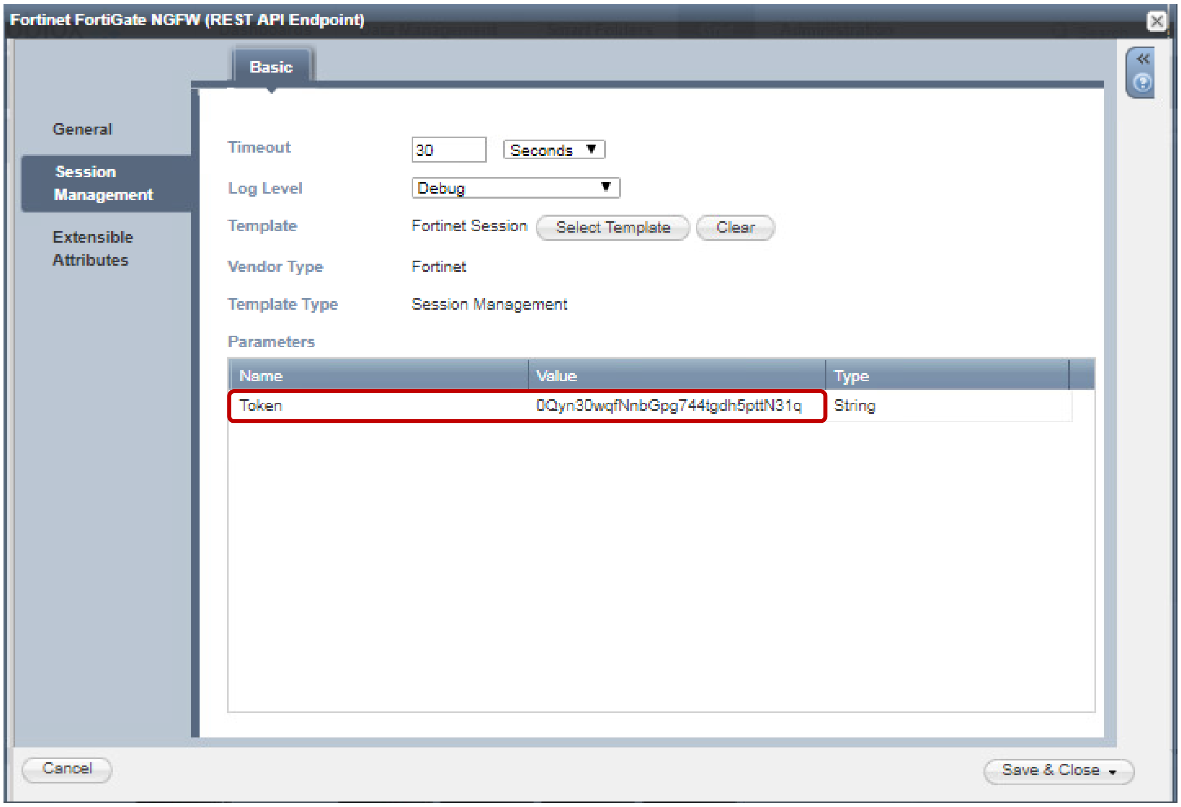
Name	Value	Type
Token	0Qyn30wqfNnbGpg744tgdh5pttN31q	String

6. The Token can be found when you create the Fortinet API user.

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

Adding Token

1. (NIOS 8.3 or later) Navigate to **"Grid"** → **"Ecosystem** → **"Outbound Endpoint"** and click on the Fortinet FortiGate NGFW endpoint and click **"Edit"**.
2. (NIOS 8.3 or later) Navigate to the **"Session Management"** tab and add the **"Token"** to the value fields.



Timeout: 30 Seconds

Log Level: Debug

Template: Fortinet Session

Vendor Type: Fortinet

Template Type: Session Management

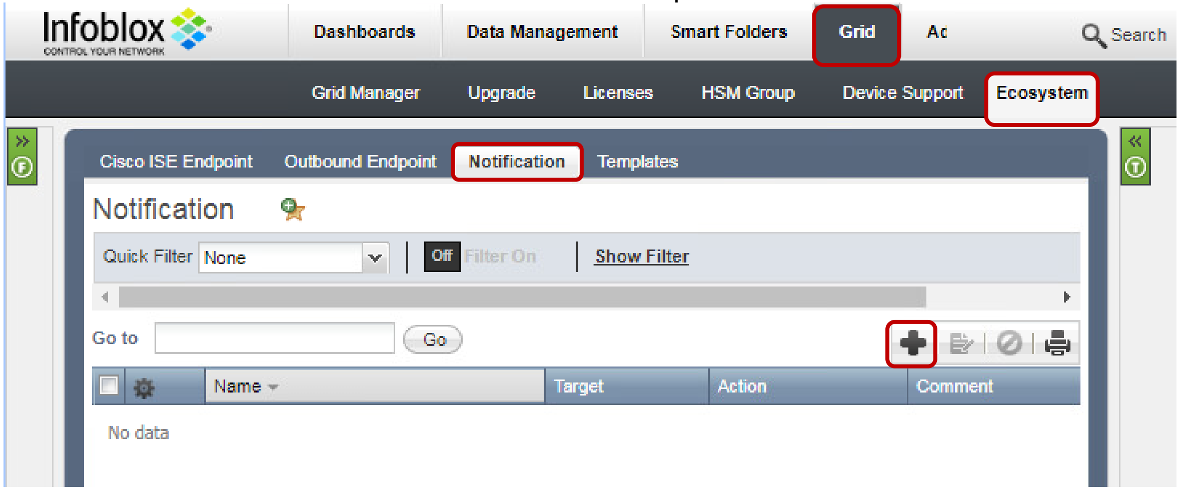
Parameters

Name	Value	Type
Token	0Qyn30wqfNnbGpg744tgdh5pttN31q	String

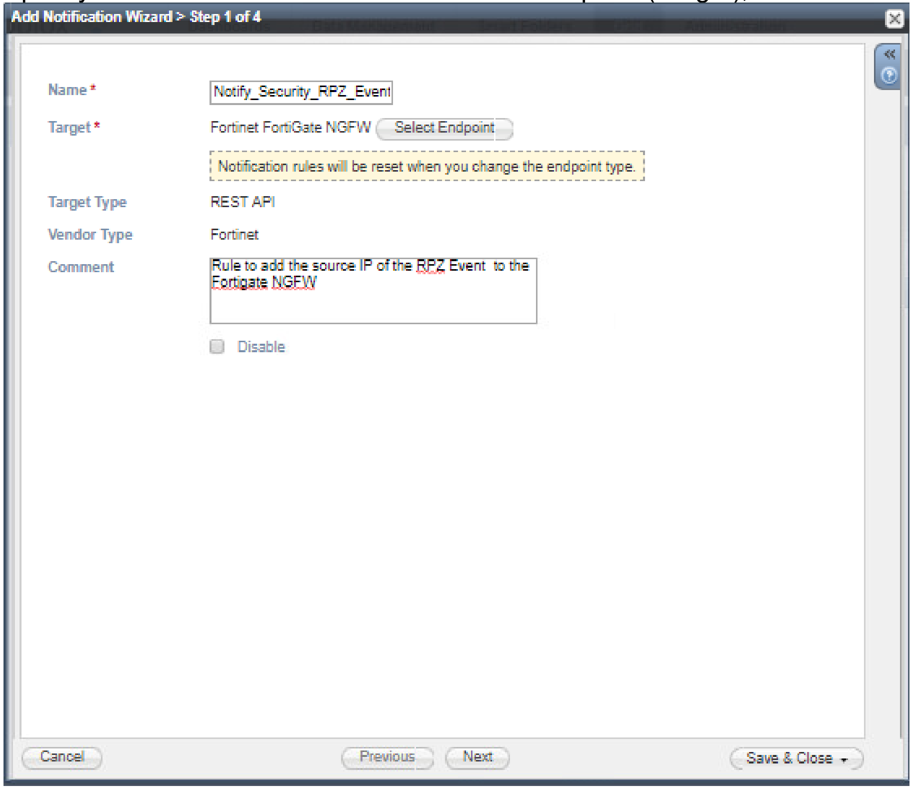
Add a Notification

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 click **"+"** or **"+ Add Notification Rule"** then the **"Add Notification Wizard"** window will open.



2. Specify the notification's name and select an endpoint (Target), click **"Next"**.


Add Notification Wizard > Step 1 of 4

Name * Notify_Security_RPZ_Event

Target * Fortinet FortiGate NGFW Select Endpoint

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

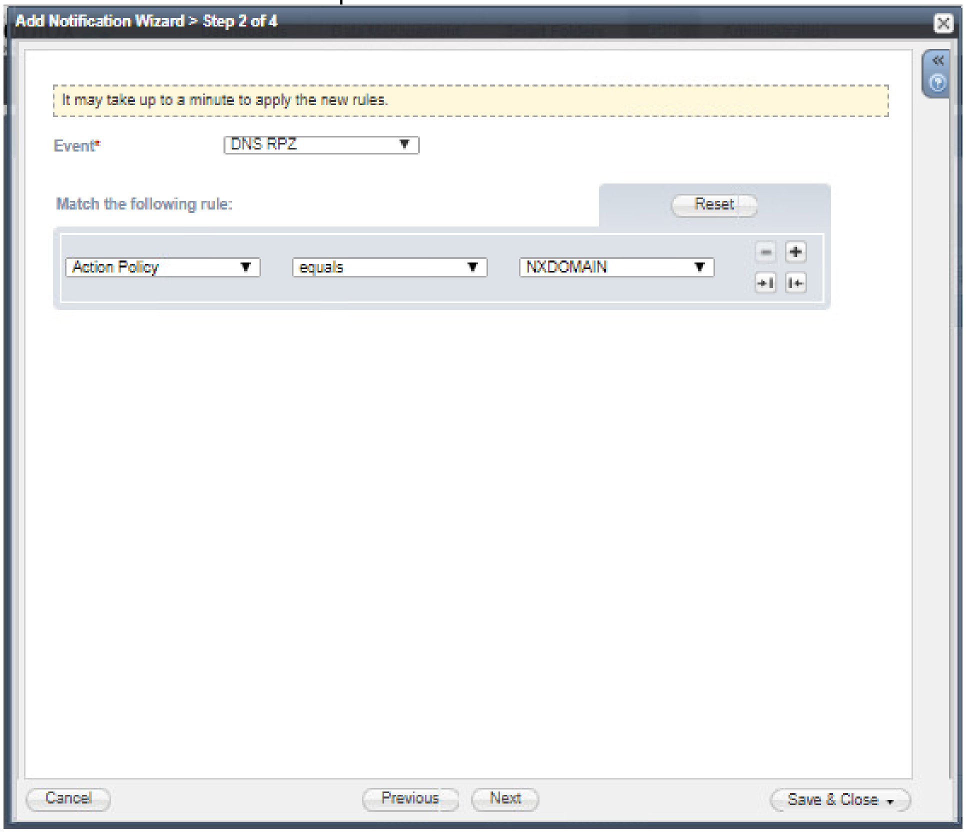
Target Type REST API

Vendor Type Fortinet

Comment Rule to add the source IP of the RPZ Event to the Fortigate NGFW

□ 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”**.



Add Notification Wizard > Step 2 of 4

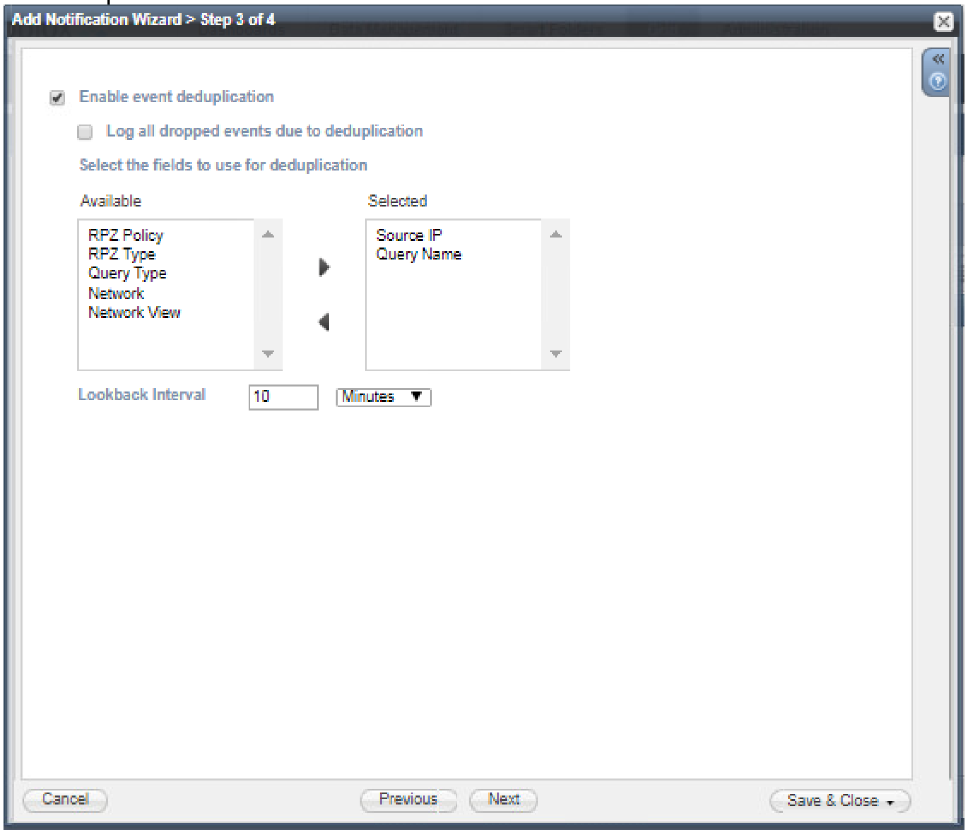
It may take up to a minute to apply the new rules.

Event* DNS RPZ

Match the following rule:

Action Policy equals NXDOMAIN

4. (For Security related notifications only) Check **"Enable event deduplication"** and specify relevant parameters. Click **"Next"**.



Add Notification Wizard > Step 3 of 4

☑ Enable event deduplication

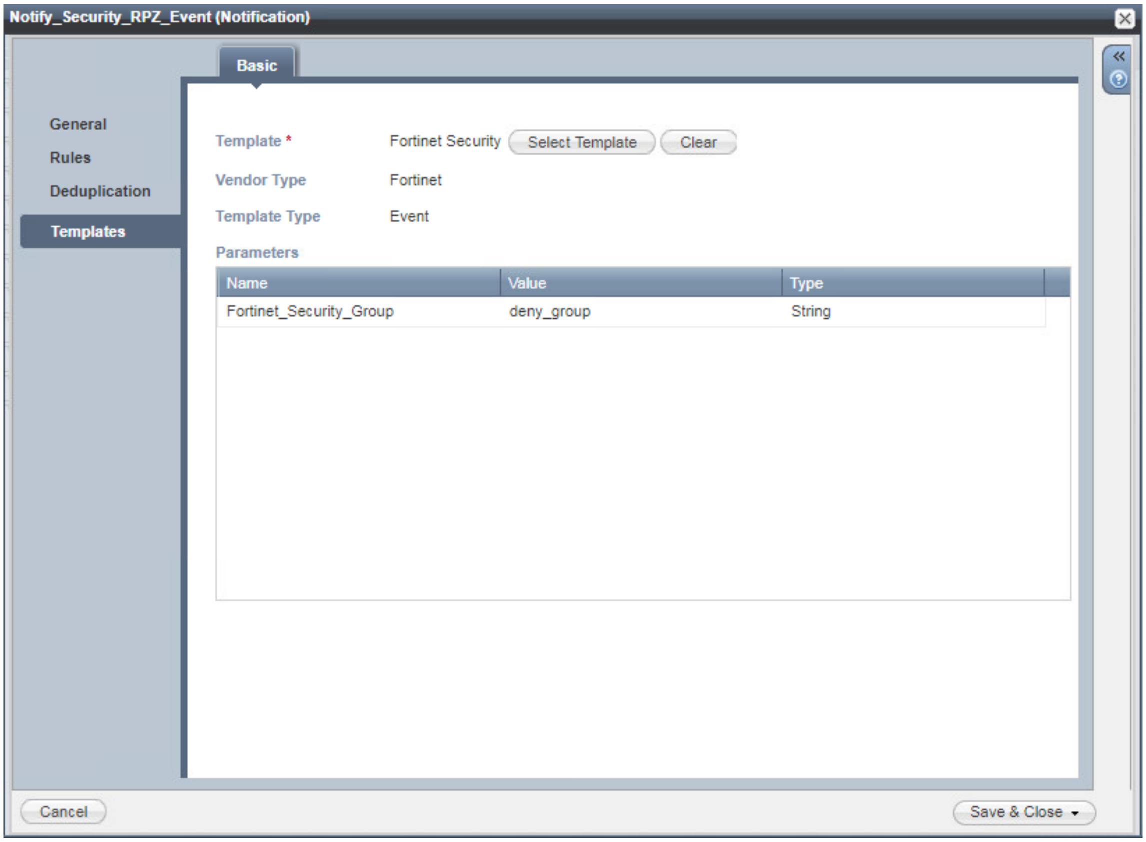
☐ Log all dropped events due to deduplication

Select the fields to use for deduplication

Available	Selected
RPZ Policy RPZ Type Query Type Network Network View	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 * Fortinet Security

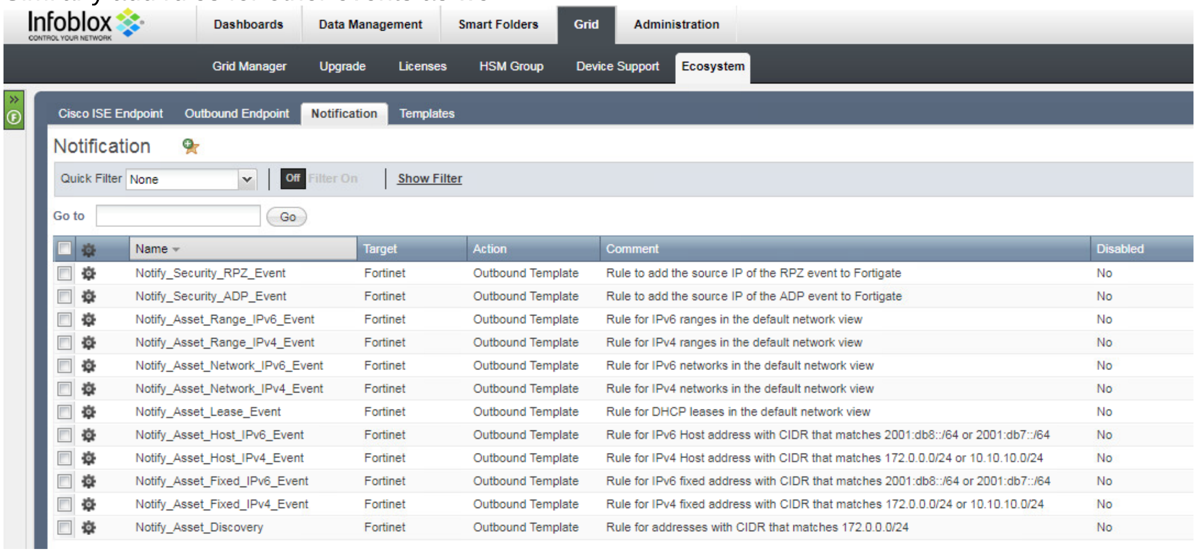
Vendor Type Fortinet

Template Type Event

Parameters

Name	Value	Type
Fortinet_Security_Group	deny_group	String

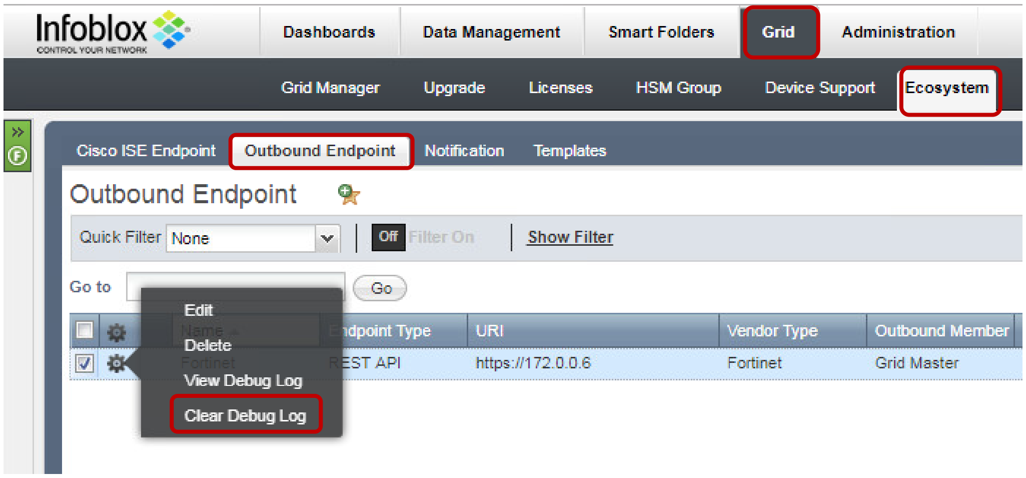
6. Similarly add rules for other events as well.



□	⚙	Name	Target	Action	Comment	Disabled
□	⚙	Notify_Security_RPZ_Event	Fortinet	Outbound Template	Rule to add the source IP of the RPZ event to Fortigate	No
□	⚙	Notify_Security_ADP_Event	Fortinet	Outbound Template	Rule to add the source IP of the ADP event to Fortigate	No
□	⚙	Notify_Asset_Range_IPv6_Event	Fortinet	Outbound Template	Rule for IPv6 ranges in the default network view	No
□	⚙	Notify_Asset_Range_IPv4_Event	Fortinet	Outbound Template	Rule for IPv4 ranges in the default network view	No
□	⚙	Notify_Asset_Network_IPv6_Event	Fortinet	Outbound Template	Rule for IPv6 networks in the default network view	No
□	⚙	Notify_Asset_Network_IPv4_Event	Fortinet	Outbound Template	Rule for IPv4 networks in the default network view	No
□	⚙	Notify_Asset_Lease_Event	Fortinet	Outbound Template	Rule for DHCP leases in the default network view	No
□	⚙	Notify_Asset_Host_IPv6_Event	Fortinet	Outbound Template	Rule for IPv6 Host address with CIDR that matches 2001:db8::/64 or 2001:db7::/64	No
□	⚙	Notify_Asset_Host_IPv4_Event	Fortinet	Outbound Template	Rule for IPv4 Host address with CIDR that matches 172.0.0.0/24 or 10.10.10.0/24	No
□	⚙	Notify_Asset_Fixed_IPv6_Event	Fortinet	Outbound Template	Rule for IPv6 fixed address with CIDR that matches 2001:db8::/64 or 2001:db7::/64	No
□	⚙	Notify_Asset_Fixed_IPv4_Event	Fortinet	Outbound Template	Rule for IPv4 fixed address with CIDR that matches 172.0.0.0/24 or 10.10.10.0/24	No
□	⚙	Notify_Asset_Discovery	Fortinet	Outbound Template	Rule for addresses with CIDR that matches 172.0.0.0/24	No

Emulate an Event

(Optional) On the Infoblox grid, navigate to **“Grid” → “Ecosystem” → “Outbound Endpoint”**, select **“Fortinet”**, click on the gear icon and select **“Clear Debug Log”.**

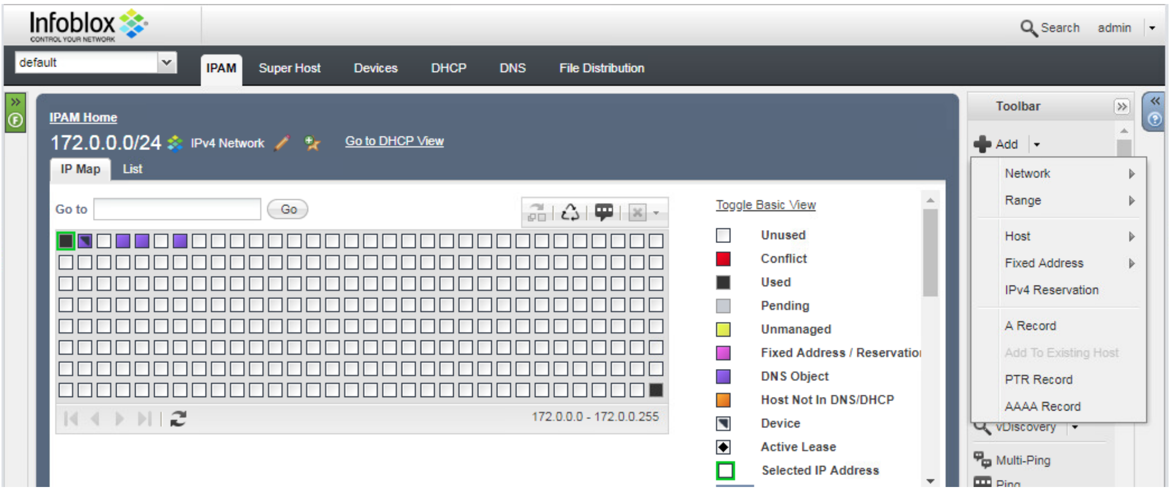


Name	Endpoint Type	URI	Vendor Type	Outbound Member
Fortinet	REST API	https://172.0.0.6	Fortinet	Grid Master

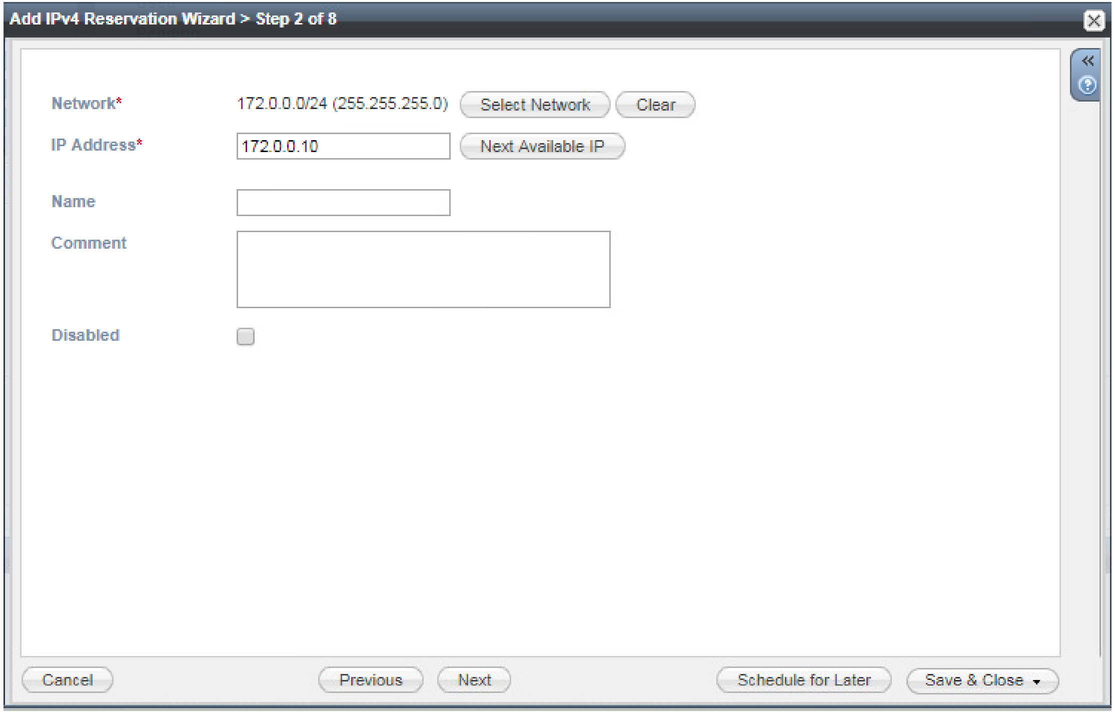
Address Object Management

The templates support IPv4/IPv6 Hosts, IPv4/IPv6 Fixed IP/Reservations, IPv4/IPv6 Networks, IPv4/IPv6 Ranges, and DHCP lease events. This use case demonstrates how to manage IP addresses on the FortiGate NGFW.

1. To create an IPv4 reservation, navigate to **"Data Management" → "IPAM"**. Select an IPv4 network here (say 172.0.0.0/24).
2. Click the drop down next to the **"+ Add"** button under the toolbar and choose **"IPv4 Reservation"**.



3. Click **"Next"**, then insert the IP **"172.0.0.10"** into the **"IP Address"** field.



Add IPv4 Reservation Wizard > Step 2 of 8

Network* 172.0.0.0/24 (255.255.255.0)

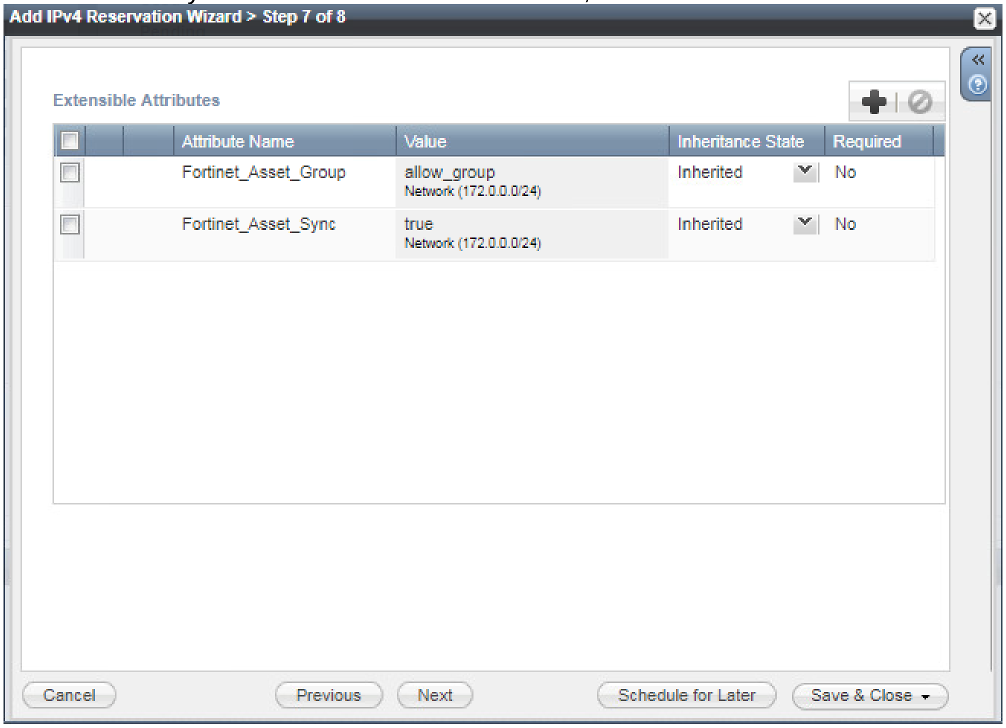
IP Address* 172.0.0.10

Name

Comment

Disabled □

4. Click on **"Next"** till you reach the Extensible Attributes window. If the Extensible Attributes have not already been inherited from the network, set them.



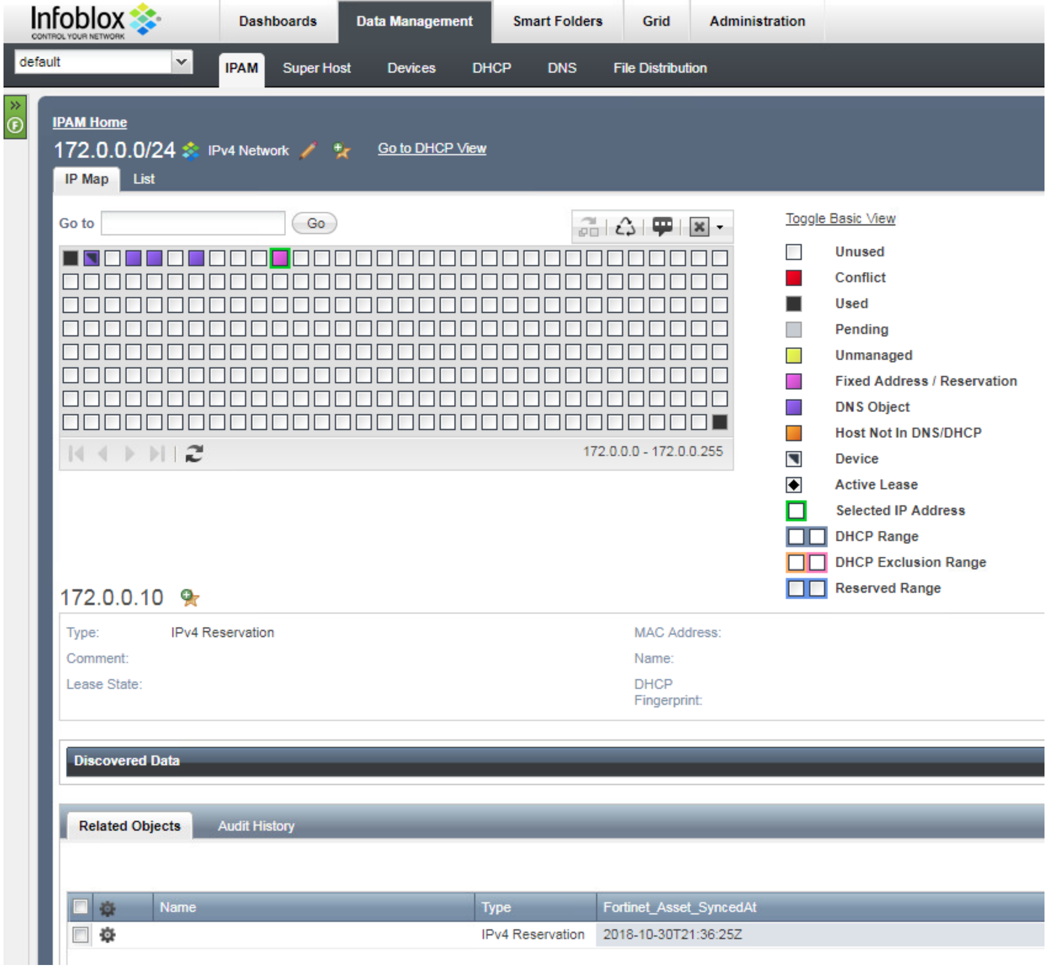
Add IPv4 Reservation Wizard > Step 7 of 8

Extensible Attributes

□	Attribute Name	Value	Inheritance State	Required
□	Fortinet_Asset_Group	allow_group Network (172.0.0.0/24)	Inherited	No
□	Fortinet_Asset_Sync	true Network (172.0.0.0/24)	Inherited	No

5. Click **"Save & Close"**.

6. Select the IP and refresh. The **“Fortinet_Asset_SyncedAt”** EA is now updated.

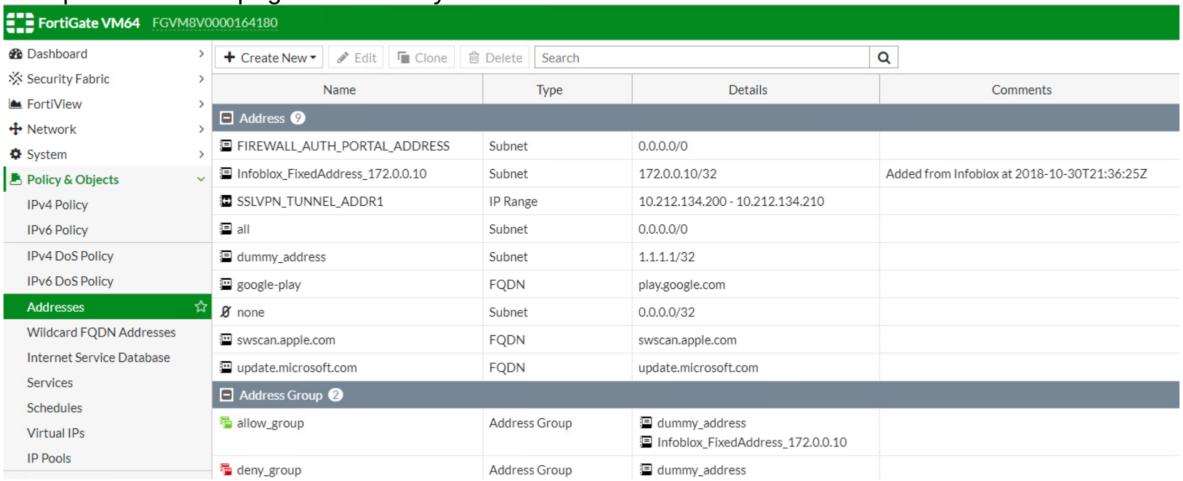


172.0.0.10

Type:	IPv4 Reservation	MAC Address:	
Comment:		Name:	
Lease State:		DHCP Fingerprint:	

Name	Type	Fortinet_Asset_SyncedAt
	IPv4 Reservation	2018-10-30T21:36:25Z

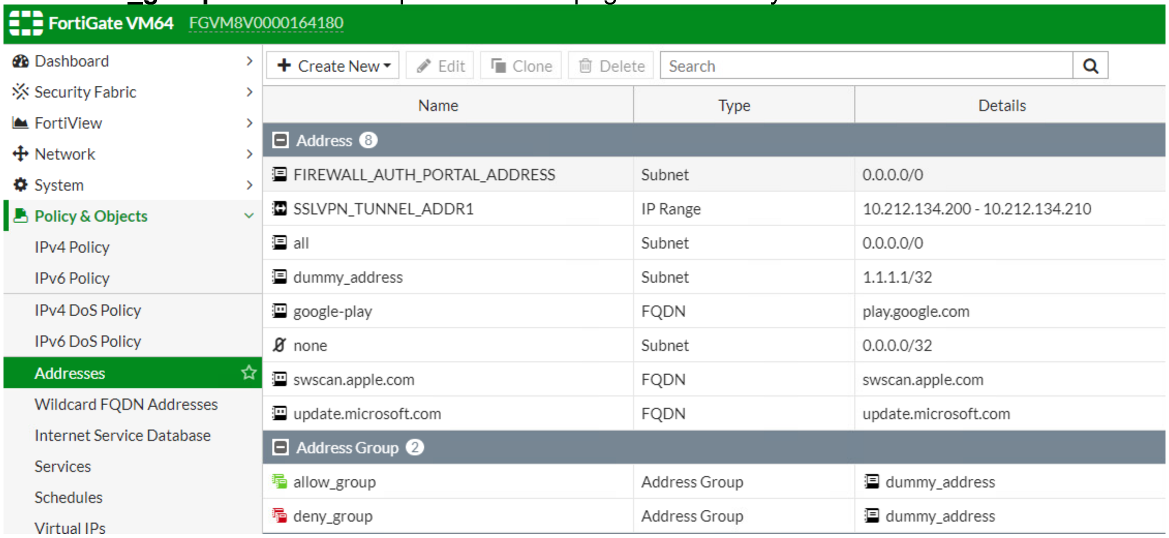
7. In the firewall, navigate to **“Policy & Objects”**. The **“Infoblox_FixedAddress_172.0.0.10”** address reservation has been added to the **“Address”** list and the **“allow_group”** Address Group. Refresh the page if necessary.



Name	Type	Details	Comments
Address 9			
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0	
Infoblox_FixedAddress_172.0.0.10	Subnet	172.0.0.10/32	Added from Infoblox at 2018-10-30T21:36:25Z
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	
all	Subnet	0.0.0.0/0	
dummy_address	Subnet	1.1.1.1/32	
google-play	FQDN	play.google.com	
none	Subnet	0.0.0.0/32	
swscan.apple.com	FQDN	swscan.apple.com	
update.microsoft.com	FQDN	update.microsoft.com	
Address Group 2			
allow_group	Address Group	dummy_address Infoblox_FixedAddress_172.0.0.10	
deny_group	Address Group	dummy_address	

8. In the Infoblox grid, delete the **“172.0.0.10”** reservation by selecting the reservation and clicking the **“reclaim**” button. Wait about 10 seconds.

9. On the Firewall, navigate to **"Policy & Objects"** and verify that the **"Infoblox_FixedAddress_172.0.0.10"** entry has been removed from the **"Address"** list and the **"allow_group"** Address Group. Refresh the page if necessary.

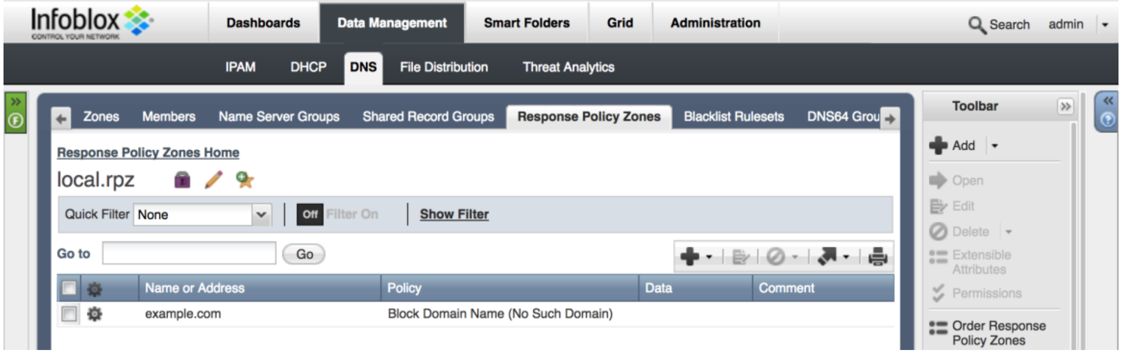


Name	Type	Details
Address 8		
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210
all	Subnet	0.0.0.0/0
dummy_address	Subnet	1.1.1.1/32
google-play	FQDN	play.google.com
none	Subnet	0.0.0.0/32
swscan.apple.com	FQDN	swscan.apple.com
update.microsoft.com	FQDN	update.microsoft.com
Address Group 2		
allow_group	Address Group	dummy_address
deny_group	Address Group	dummy_address

DNS Security Event Remediation

This use case shows Infoblox DDI possibility to respond on any DNS Security events and request FortiGate Firewall to add clients to the **"deny_group"**.

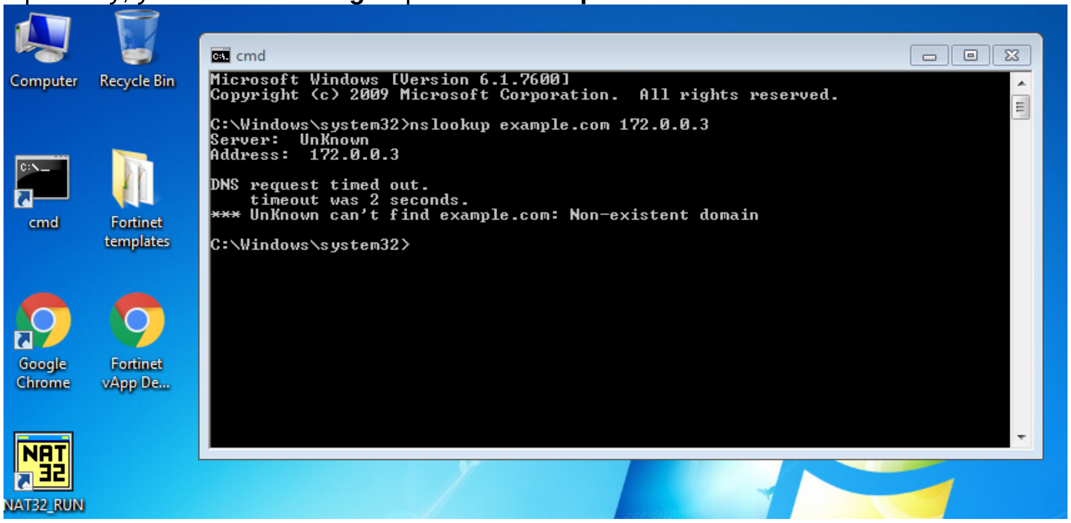
1. Simulate a security event by querying for a domain that is blocked by your RPZ.



Name or Address	Policy	Data	Comment
example.com	Block Domain Name (No Such Domain)		

a. Launch a command prompt and perform a **nslookup** request for **"example.com"**.

b. Optionally, you can send a **dig** request to **“example.com”**.



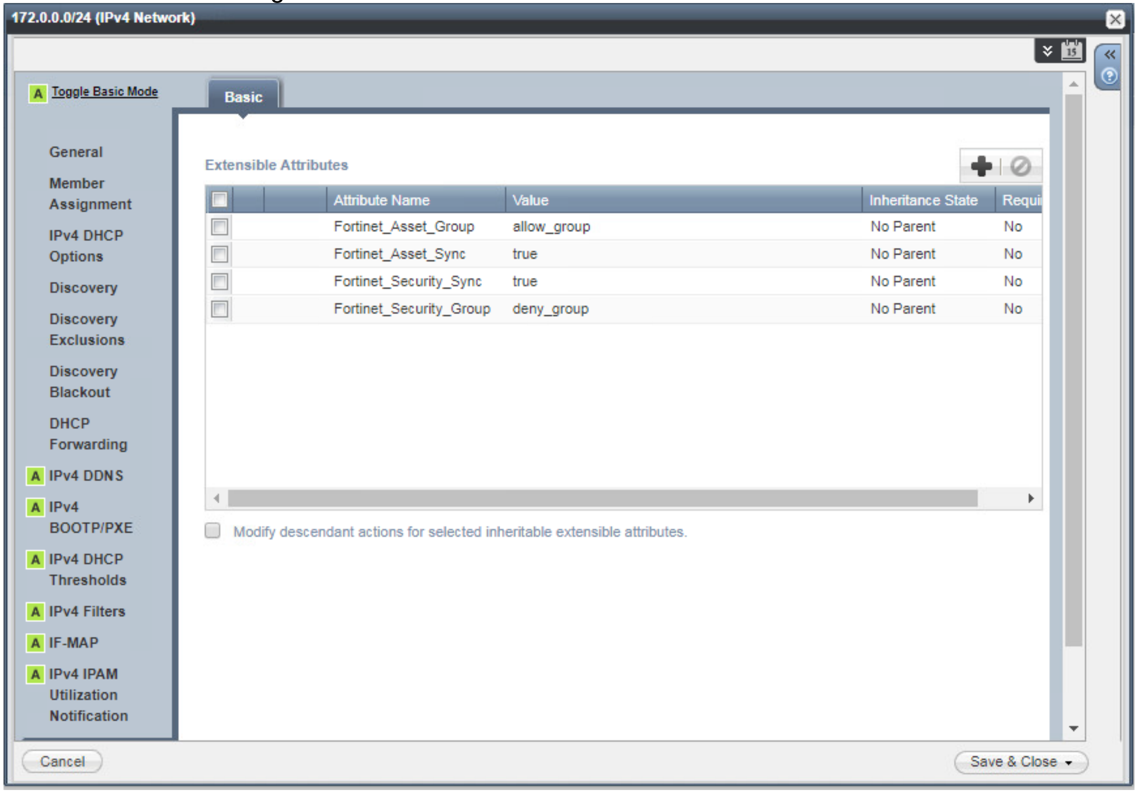
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>nslookup example.com 172.0.0.3
Server:  UnKnown
Address:  172.0.0.3

DNS request timed out.
    timeout was 2 seconds.
*** UnKnown can't find example.com: Non-existent domain

C:\Windows\system32>
```

2. Ensure the **“Fortinet_Security_Sync”** is set to **“true”** on the network or the IP address/host record. If the **“Fortinet_Security_Group”** is not set, the value specified while assigning the instance variable during the creation of notification rules is taken into account.



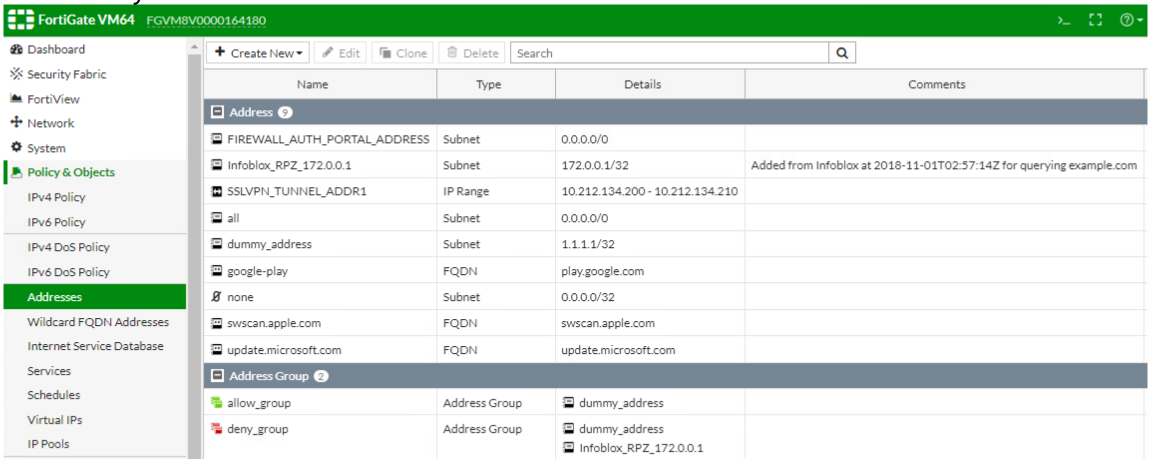
Extensible Attributes

□	Attribute Name	Value	Inheritance State	Requi
□	Fortinet_Asset_Group	allow_group	No Parent	No
□	Fortinet_Asset_Sync	true	No Parent	No
□	Fortinet_Security_Sync	true	No Parent	No
□	Fortinet_Security_Group	deny_group	No Parent	No

□ Modify descendant actions for selected inheritable extensible attributes.

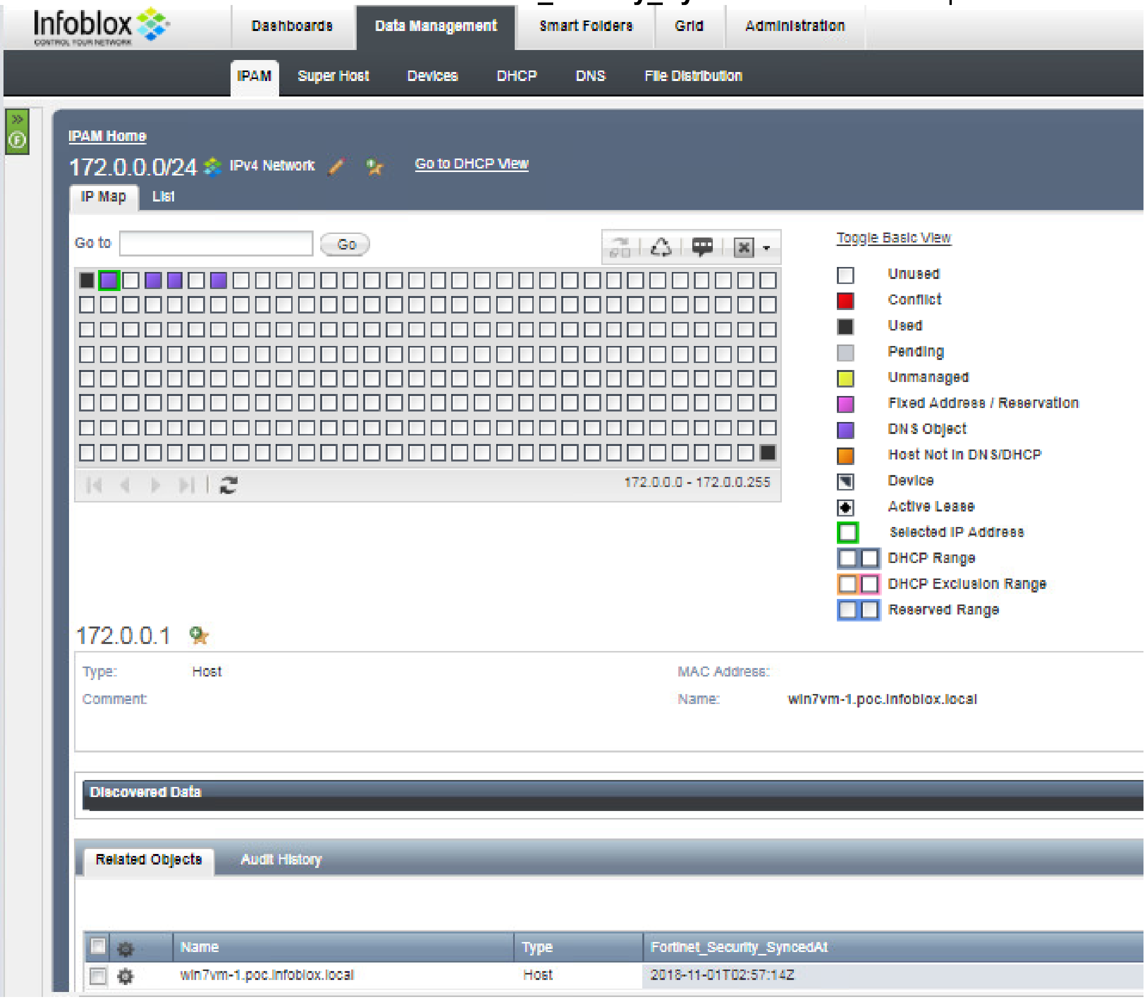
3. In the firewall, navigate to **“Policy & Objects”**. The **“Infoblox_RPZ_172.0.0.1”** host has been added to the **“Address”** list and the **“deny_group”** Address Group. Refresh the page

if necessary.



Name	Type	Details	Comments
Address 9			
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0	
Infoblox_RPZ_172.0.0.1	Subnet	172.0.0.1/32	Added from Infoblox at 2018-11-01T02:57:14Z for querying example.com
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	
all	Subnet	0.0.0.0/0	
dummy_address	Subnet	1.1.1.1/32	
google-play	FQDN	play.google.com	
none	Subnet	0.0.0.0/32	
swscan.apple.com	FQDN	swscan.apple.com	
update.microsoft.com	FQDN	update.microsoft.com	
Address Group 2			
allow_group	Address Group	dummy_address	
deny_group	Address Group	dummy_address Infoblox_RPZ_172.0.0.1	

4. In the Infoblox Grid, navigate to **"Data Management" → "IPAM" → "172.0.0.1/24"**. Select the IP **"172.0.0.1"** and refresh. The **"Fortinet_Secutiy_SyncedAt"** EA is now updated.



172.0.0.1

Type: Host

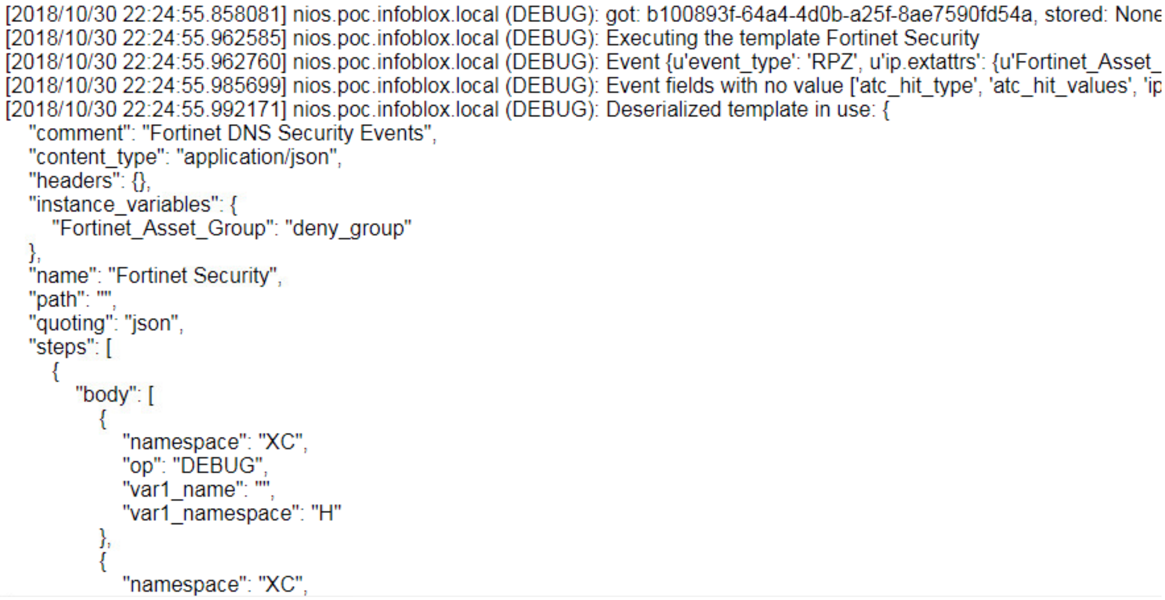
Comment:

MAC Address:

Name: win7vm-1.poc.infoblox.local

Name	Type	Fortinet_Security_SyncedAt
win7vm-1.poc.infoblox.local	Host	2018-11-01T02:57:14Z

Optionally, navigate to **"Grid" → "Ecosystem" → "Outbound Endpoint"**, select **"Fortinet"**, click on the gear icon and select **"View Debug Log"**. Here you can see the debug log's step-by-step execution flow of the template



```
[2018/10/30 22:24:55.858081] nios.poc.infoblox.local (DEBUG): got: b100893f-64a4-4d0b-a25f-8ae7590fd54a, stored: None
[2018/10/30 22:24:55.962585] nios.poc.infoblox.local (DEBUG): Executing the template Fortinet Security
[2018/10/30 22:24:55.962760] nios.poc.infoblox.local (DEBUG): Event {u'event_type': 'RPZ', u'ip.extattrs': {u'Fortinet_Asset_
[2018/10/30 22:24:55.985699] nios.poc.infoblox.local (DEBUG): Event fields with no value ['atc_hit_type', 'atc_hit_values', 'ip
[2018/10/30 22:24:55.992171] nios.poc.infoblox.local (DEBUG): Deserialized template in use: {
  "comment": "Fortinet DNS Security Events",
  "content_type": "application/json",
  "headers": {},
  "instance_variables": {
    "Fortinet_Asset_Group": "deny_group"
  },
  "name": "Fortinet Security",
  "path": "",
  "quoting": "json",
  "steps": [
    {
      "body": [
        {
          "namespace": "XC",
          "op": "DEBUG",
          "var1_name": "",
          "var1_namespace": "H"
        },
        {
          "namespace": "XC",
```

Infoblox
NEXT LEVEL NETWORKING

Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com