

DEPLOYMENT GUIDE

# Infoblox Integration with Checkpoint NGFW



# Table of Contents

<b>Introduction</b>	<b>2</b>
<b>Prerequisites</b>	<b>2</b>
<b>Known Limitations</b>	<b>2</b>
<b>Best Practices</b>	<b>3</b>
<b>Workflow</b>	<b>3</b>
<b>Infoblox Community Website Templates</b>	<b>3</b>
<b>Extensible Attributes</b>	<b>3</b>
<b>Session Variables</b>	<b>4</b>
<b>Supported Notifications</b>	<b>4</b>
List of Supported Notifications	4
<b>Check Point Configuration</b>	<b>6</b>
Enabling WAPI	6
Creating API Only User	8
Creating Network Groups	15
<b>Infoblox NIOS Configuration</b>	<b>17</b>
Verify Security Ecosystem is Installed	17
Add/Upload Templates	17
Modify Templates	20
Add a Rest API Endpoint	20
Add Notifications	22
Test the Integration	25
<b>Additional Resources</b>	<b>26</b>

## Introduction

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 Check Point's Next Generation Firewall (NGFW) enable security and incident response teams to leverage the integration of vulnerability scanners 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 is a list of prerequisites required for Outbound API notifications:

Infoblox:

1. NIOS 8.3 or higher
2. Security Ecosystem License
3. Outbound API integration templates
4. Prerequisites for the templates (e.g. configured and set extensible attributes)
5. Pre-configured required services: ADP, DHCP, Discovery, DNS, RPZ, and Threat Analytics
6. 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

Check Point Next Generation Firewall (NGFW):

1. Installed and configured Check Point NGFW
2. Access to the Check Point GAIA interface of the Check Point NGFW
3. Access to Check Point SmartConsole of the Check Point NGFW
4. User Credentials to the Check Point NGFW (User must be able to create and modify all Check Point Objects via the web interface.)

## Known Limitations

Check Point's API will prevent updates to its database if another session is editing the same object elsewhere. Due to this, the Outbound API template publishes any and all changes to Check Point after a MODIFY, INSERT, or DELETE event occurs within the Infoblox device. Note that if CP\_SecurityGroup or CP\_AssetGroup are left open for editing or are modified without publishing in a different session, Check Point's API will not accept any changes or additions to those groups or objects.

Security events are statically assigned to the network group CP\_SecurityGroup by the template. An administrator may need to flush devices that were placed in the aforementioned network group depending on the associated firewall rules and company policies.

## Best Practices

As with most infrastructure changes to a production environment, it is recommended that a lab environment is utilized to test the functionalities and impact of any changes being made. Additionally, it is highly suggested to set the end point log level to Inform or higher (Warning, Error). Please refer to the NIOS Administration guide about other best practices, limitations, and any details on how to develop or modify notification templates.

## Workflow

Use the following workflow to deploy this integration:

1. Properly configure Check Point to accept WAPI calls
2. Create an account for Check Point WAPI calls
3. Create the required Network Groups within Check Point's SmartConsole
4. Check that necessary services DHCP, DNS, RPZ and Threat Analytics are configured
5. Create Extensible Attributes
6. Create or download the appropriate templates from the Infoblox community Website (<https://community.infoblox.com>): Check Point Assets, Check Point Security, Check Point Session, Check Point Login, Check Point Logout
7. Add/Upload Templates to Infoblox Grid
8. Add a REST API Endpoint
9. Add Notifications
10. Emulate an event, then check the debug log to verify changes on the REST API Endpoint

## Infoblox Community Website Templates

Outbound API notification templates are an essential part of this integration. Templates enable Infoblox's Outbound API to automatically transfer data to Outbound endpoints based on notification configuration. Detailed information on how to develop templates is found within the NIOS Administrator guide. Infoblox does not distribute any templates with NIOS releases.

Templates are available on the Infoblox community Website. Templates may require additional extensible attributes, parameters, or WAPI credentials. Guidance on the required configurations are included with templates in the form of Deployment guides.

## Extensible Attributes

Below is a table consisting of all extensible attributes utilized in this integration.

Name	Description	Type
CP_AddByHostName	Defines if Host records are to be added to Check Point by name.	List (true, false)
CP_AssetSync	Defines if syncing asset events with Check Point is desired or not.	List (true, false)

CP_AssetTimestamp	Timestamp that records when the asset was last synced with Check Point.	String
CP_SecuritySync	Defines if syncing security events with Check Point is desired or not.	List (true, false)
CP_SecurityTimestamp	Timestamp that is updated whenever a security event occurs.	String

## Session Variables

Below is a table consisting of all necessary Session Variables required for this integration.

Name	Description
CP_AssetGroup	The Asset Group is a Network Group located on the Check Point NGFW. All supported network objects that are populated from Infoblox are members of this group.
CP_SecurityGroup	The Security Group is a Network Group located on the Check Point NGFW. When a security event is triggered by a device, the device is added to this group.

## Supported Notifications

A notification can be considered as a link between a template, an endpoint and an event. In the notification properties, you can define which events trigger the notification, the template to be executed, and the external endpoint. The Check Point Asset and Security templates support a variety of notifications. In order to simplify the integration, create the notifications listed in the table below and utilize relevant filters. It is highly recommended to configure deduplication for RPZ events and exclude a feed that is automatically populated by Threat Analytics. Modify events that occur in real time will update the CP\_AssetTimestamp on the associated object.

### List of Supported Notifications

Notification	Description
DHCP Leases	DHCP Lease event

DNS RPZ	DNS query that is malicious or unwanted
DNS Tunneling	Data exfiltration that occurs on the network
Object Change Discovery Data	Device that is discovered on the network by Infoblox
Object Change Fixed Address IPv4	Fixed IPv4 address that is inserted, modified, or deleted
Object Change Fixed Address IPv6	Fixed IPv6 address that is inserted, modified, or deleted
Object Change Host Address IPv4	IPv4 host address that is inserted, modified, or deleted
Object Change Host Address IPv6	IPv6 host address that is inserted, modified, or deleted
Object Change Network IPv4	IPv4 Network that is inserted, or deleted
Object Change Network IPv6	IPv6 Network that is inserted, or deleted
Object Change Range IPv4	IPv4 Range that is inserted, modified, or deleted
Object Change Range IPv6	IPv6 Range that is inserted, modified, or deleted
Security ADP	ADP events that occur on the network

# Check Point Configuration

## Enabling WAPI

To Enable Check Point to accept inbound WAPI calls from Infoblox follow these steps:

1. (Optional) If you have not acquired the Check Point SmartConsole, please do so and install the program. On Gaia 2.6.18's network interface a light blue banner at the top contains a link to download the Check Point SmartConsole.

Manage Software Blades using SmartConsole

[Download Now!](#)

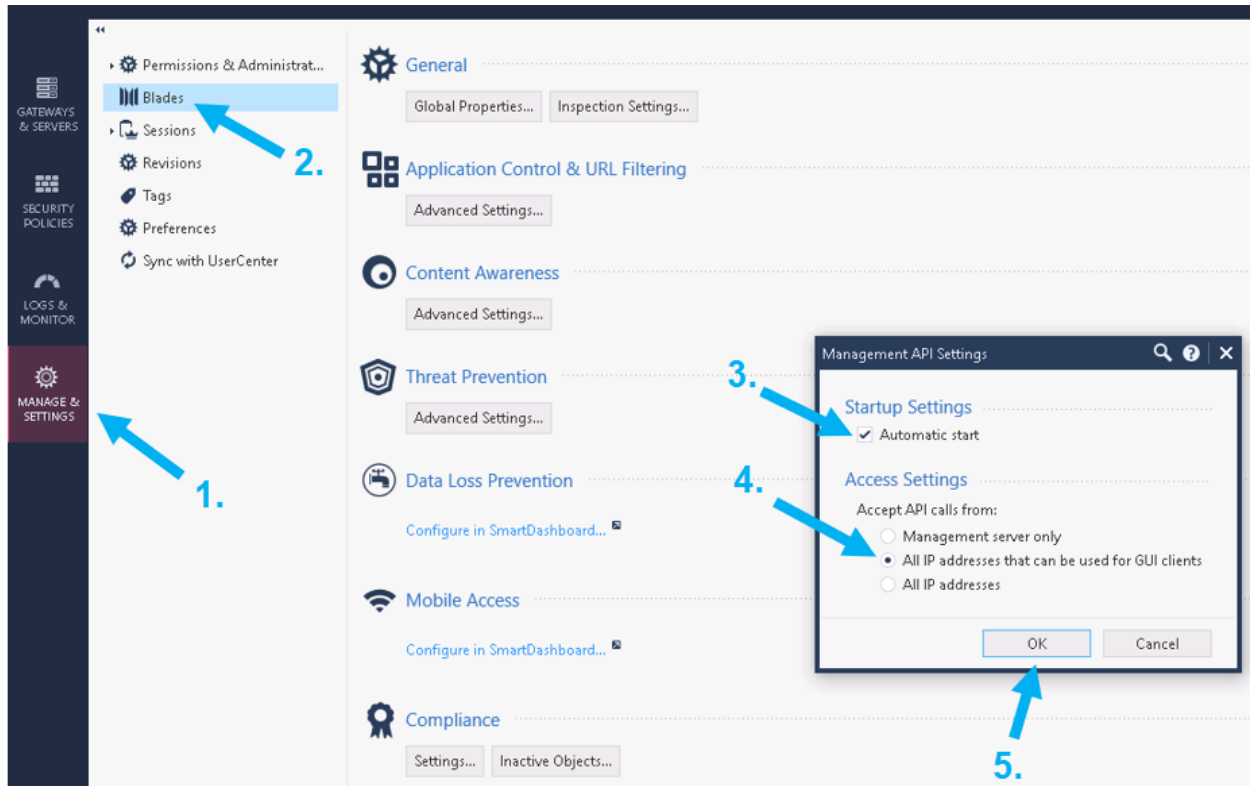
Alternatively, you can download the SmartConsole from Check Point's website at <https://supportcenter.checkpoint.com> All SmartConsole screenshots will be from version R80.30. Please verify that you have the correct version that corresponds to your Check Point appliance.

2. Access the GAIA interface of the Check Point appliance. Once inside, browse the left side panel and navigate to **User Management** **GUI Clients**. Ensure that the Infoblox Grid Master's IP is added to the **Security Management GUI Clients** list. Additionally, you may want to add your current device to this list for testing purposes.

The screenshot shows the GAIA interface with the left navigation pane expanded to 'User Management' > 'GUI Clients'. The main content area is titled 'Security Management GUI Clients' and contains an 'Add' button, a 'Delete' button, and a table with the following data:

Type	Hostname / IP Address	Mask
Host	172.0.0.3	-
Host	172.0.0.1	-

- Log into the Check Point SmartConsole and click **MANAGE & SETTINGS** on the left side bar. Once inside, click on **Blades**, then **Advanced Settings...** under the **Management API** header. Inside the **Management API Settings** window, Click the bubble next to **All IP addresses that can be used for GUI clients** under the header **Accept API calls from:**. Before closing the dialog box, ensure that the **Automatic Start** setting under the header **Startup Settings** is checked and click **OK** to confirm all changes.



- Within the Check Point SmartConsole, Publish all changes by clicking **Publish** located on the banner.



- Navigate back to the Gaia web interface and click the **Terminal** link on the top left of the banner.



- Once inside the terminal, Log In, and input the command: **API restart**. This will finalize the changes made within the SmartConsole.

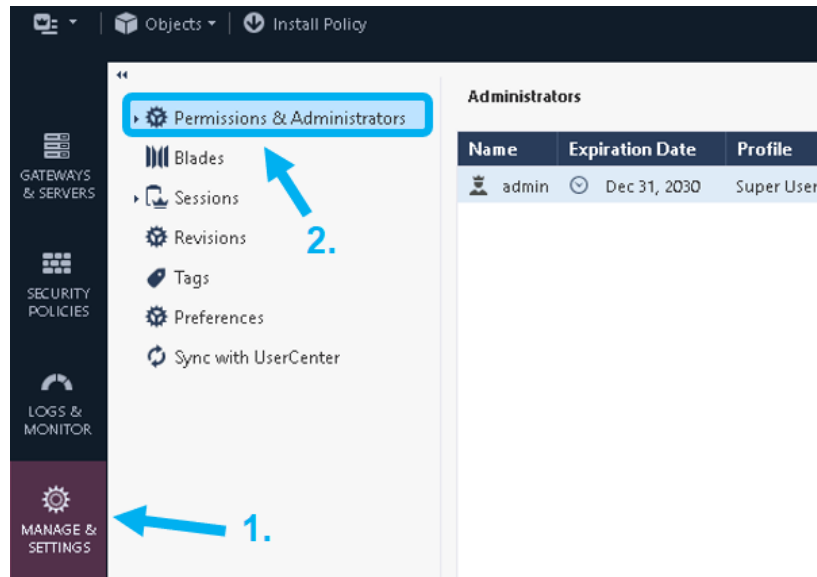
```
Terminal
login: admin
Password:
NGFW> api restart
```



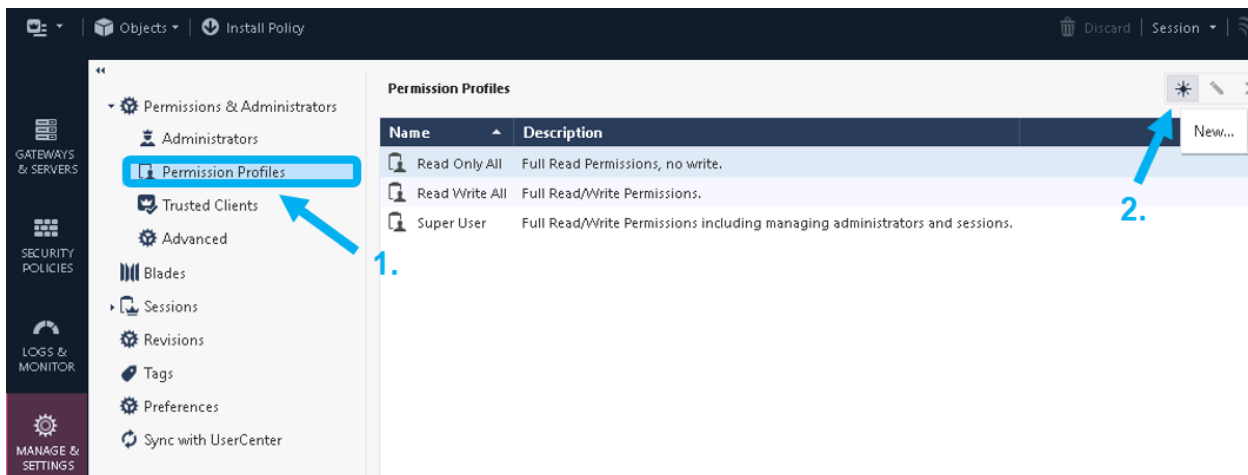
## Creating API Only User

To add a user to Check Point that only has the ability to perform necessary API calls for this integration, follow these steps:

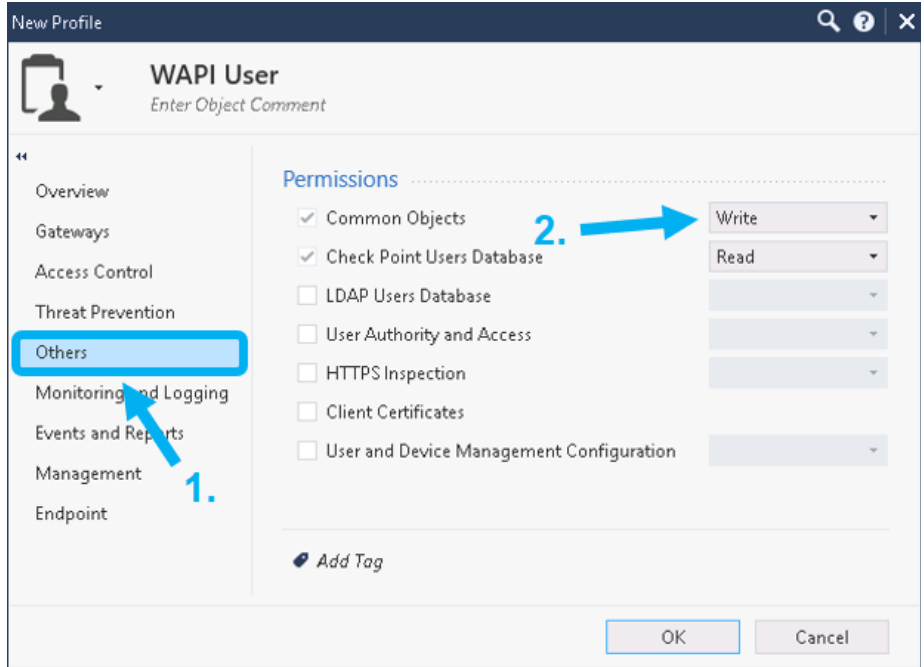
1. First create a Check Point **Permission Profile**. Within the Check Point SmartConsole, click on **MANAGE & SETTINGS** in the left side bar. Then, click on **Permissions & Administrators**.



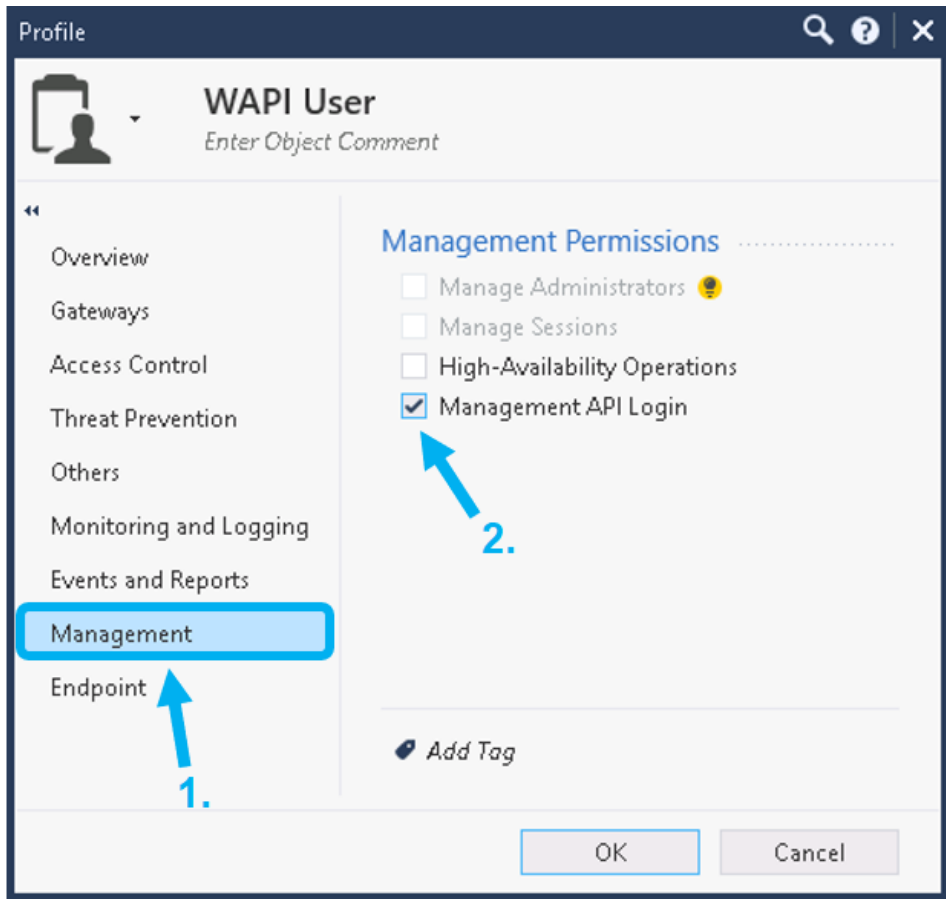
2. Then click on **Permission Profiles** under the **Permissions & Administrators** header. Then, click the **New...** button within the **Permission Profiles** window.



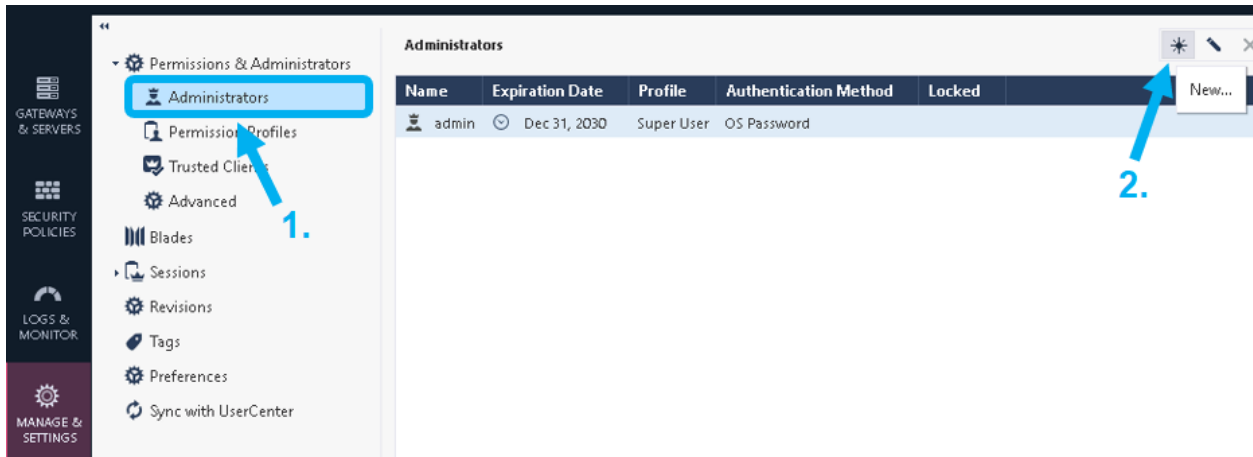
3. A **New Profile** dialog box will be revealed. Define a new name for the **Permission Profile** and customize the **Permission Profile**. Ensure all options are either deselected or are set to **Write** only. Only enable the following settings:
  - Write **Common Objects**. In the sidebar, click the **Others** option and ensure the **Permission Profile** has **Write** permissions for **Common Objects**.



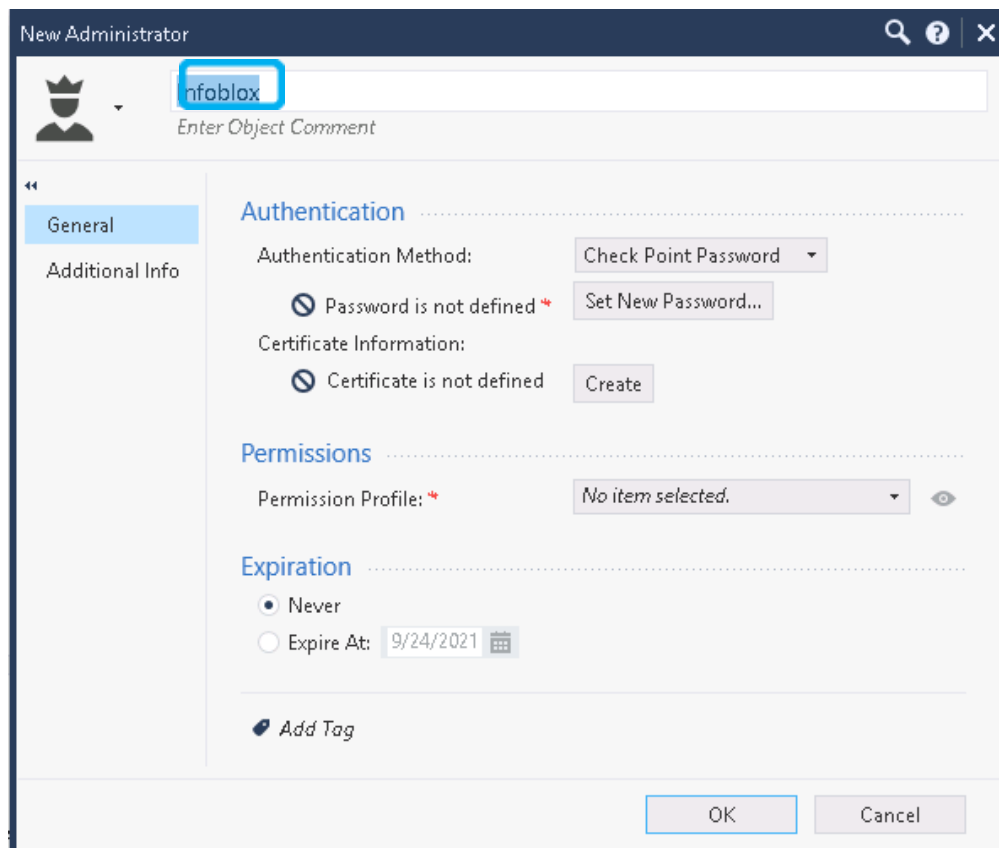
- o **Management API Login.** In the sidebar, click the **Management** option and ensure that the checkbox next to **Management API Login** is checked. Once completed click **OK**.



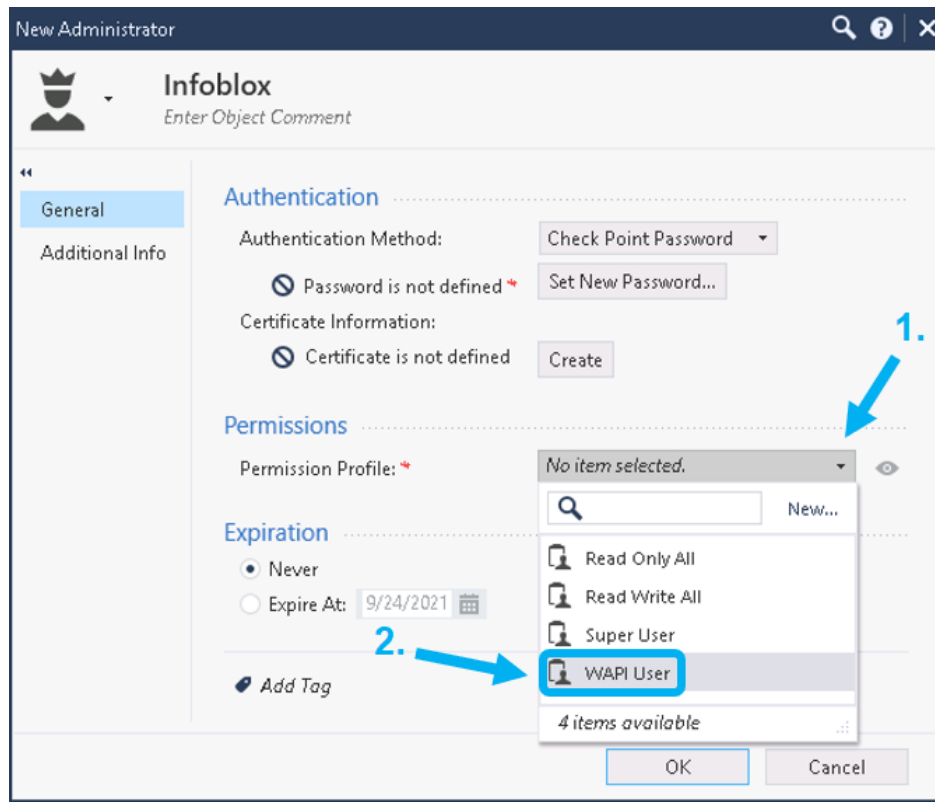
- Now create an **Administrator** account for the integration. Click on the **Administrators** option under the **Permissions & Administrators** header. Then within the **Administrators** window, click **New....** A **New Administrator** dialog box will be revealed.



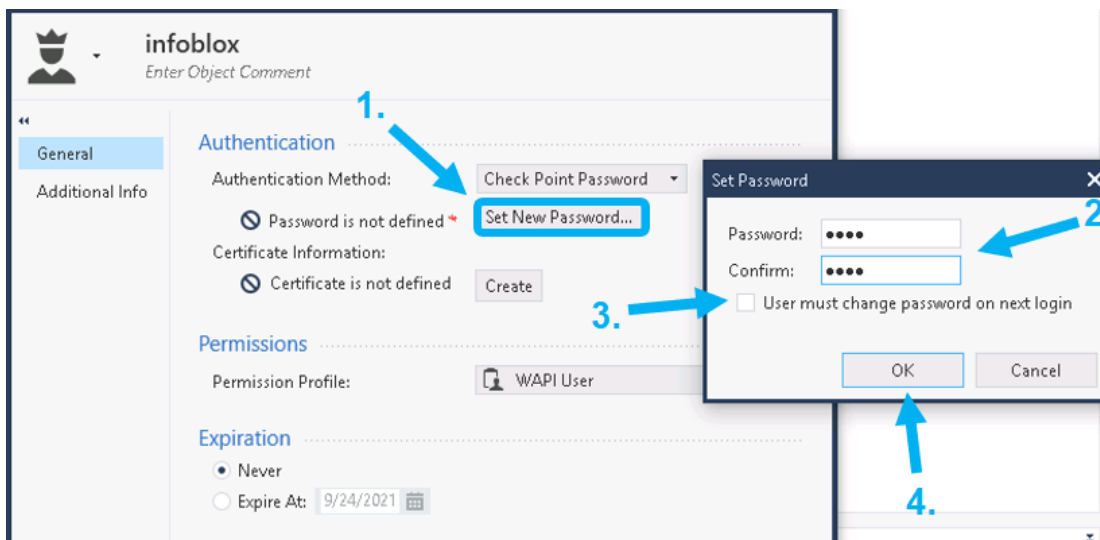
- Give the **New Administrator** a name. *note, this is the user account that will be used for the outbound endpoint later demonstrated later in this guide.*



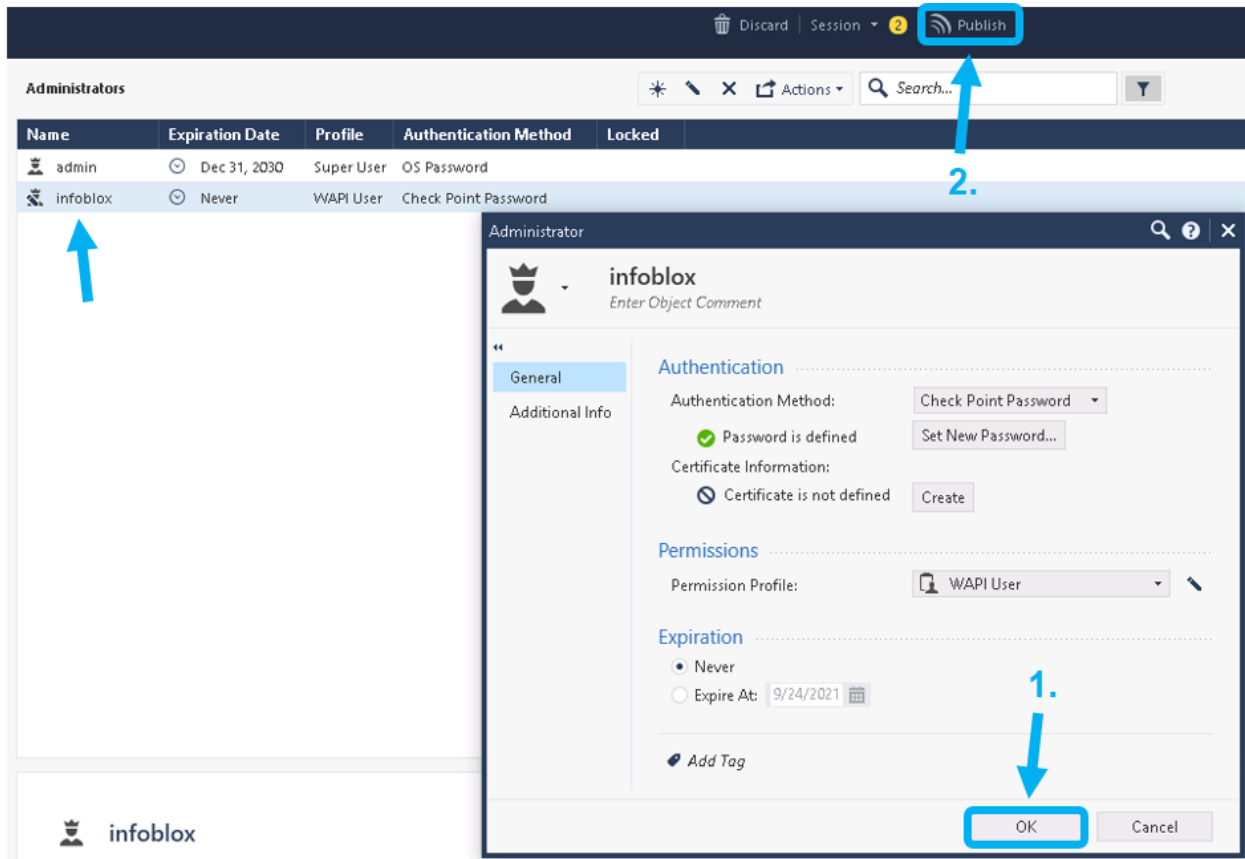
6. Select the **Permission Profile** that was created in steps 1 through 3 by clicking the dropdown menu next to **Permission Profile:** and selecting a profile.



7. Define a new password for the **New Administrator** by clicking on **Set New Password...**. Ensure that checkbox next to **“User must change password on next login”** is not checked. Click **Okay** on the **Set Password** dialog box when complete.



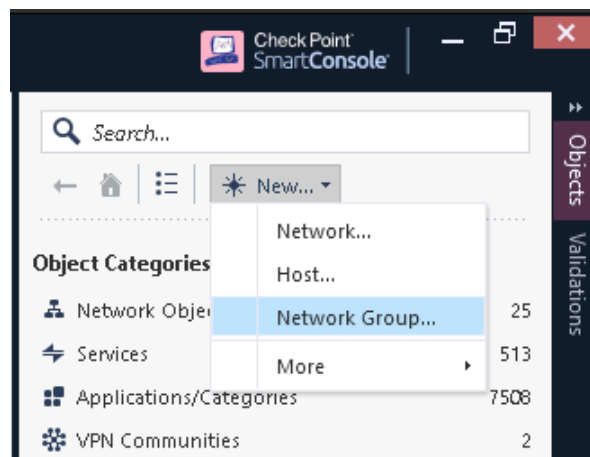
- Click **Ok** to complete the **New Administrator** creation. A new **Administrator** account should be visible in the **Administrator** window. To finalize the creation of the **Administrator**, click **Publish** located on the top center of the SmartConsole screen, and **Publish** all changes.



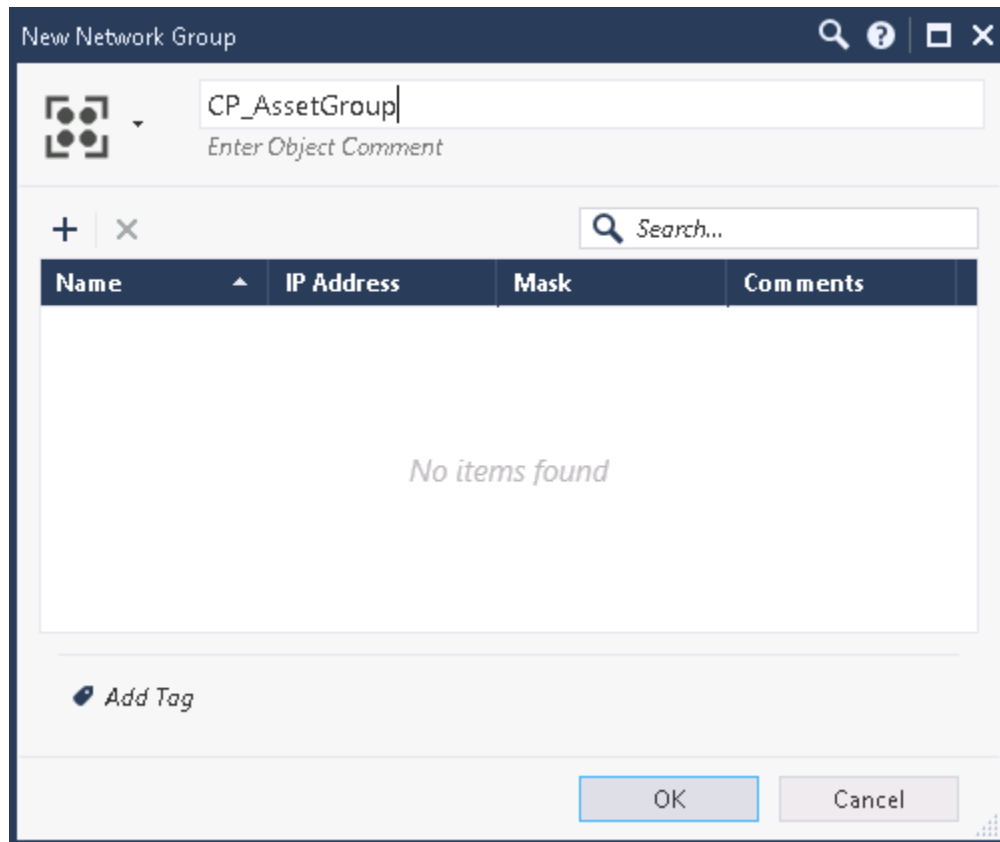
## Creating Network Groups

To add the necessary Network Groups to Check Point, follow these steps:

- Once logged into the Check Point SmartConsole, expand the tab labeled **Objects** in the top right of the window. Inside the **Objects** pane click **New...**, and select **Network Group...**



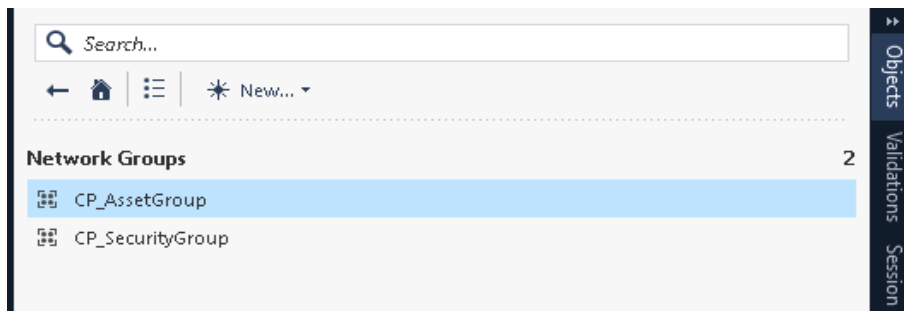
2. Name the new **Network Group CP\_AssetGroup**. Click **Ok** to finish making the Network Group. *Please note that Network Groups are case-sensitive.*



3. Repeat step 2 to create the Network Group: **CP\_SecurityGroup**. Once added, click **Publish** on the top banner to finalize the making of both **Network Groups**.



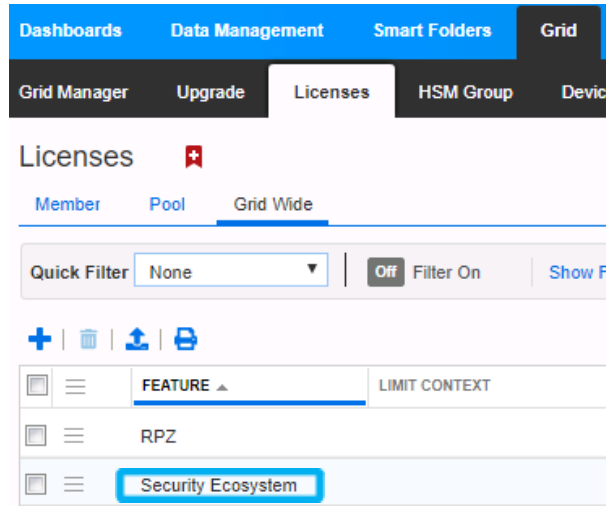
4. To verify that both **Network Groups** were created navigate to **Network Objects** **Groups** in the **Objects** pane. If done properly, you will see **CP\_AssetGroup** and **CP\_SecurityGroup** under the **Network Groups** header.



## Infoblox NIOS Configuration

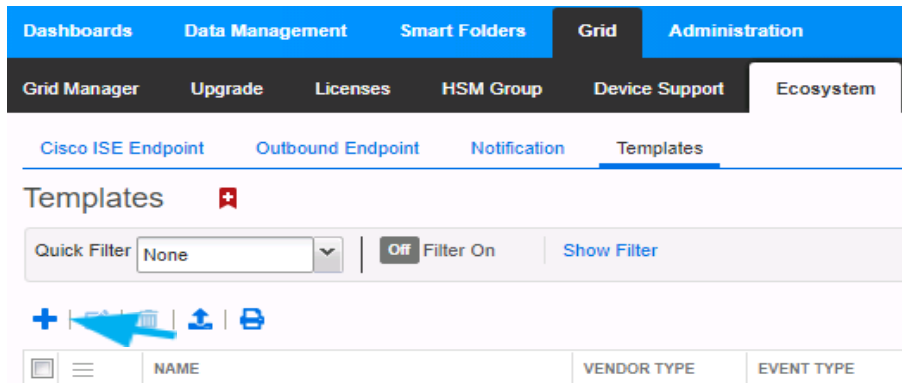
### Verify Security Ecosystem is Installed

The **Security Ecosystem** license is a Grid Wide license. Grid wide licenses activate services on all appliances in the associated Grid. To check if the license is installed navigate to **Grid Licenses Grid Wide**.

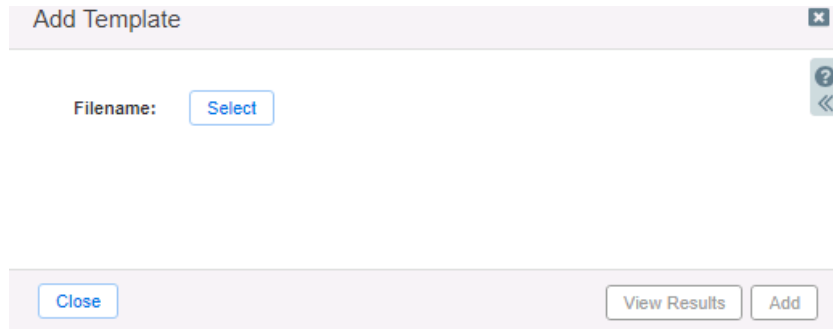


### Add/Upload Templates

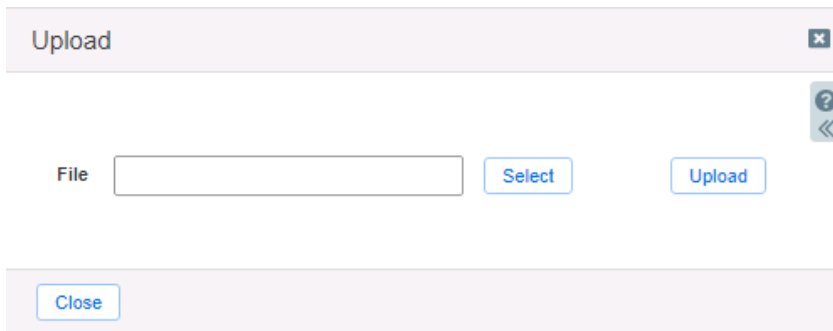
1. In order to add or upload templates, navigate to **Grid Ecosystem Templates** and click on the **+** or **+ Add Template** button in the right-side Toolbar.



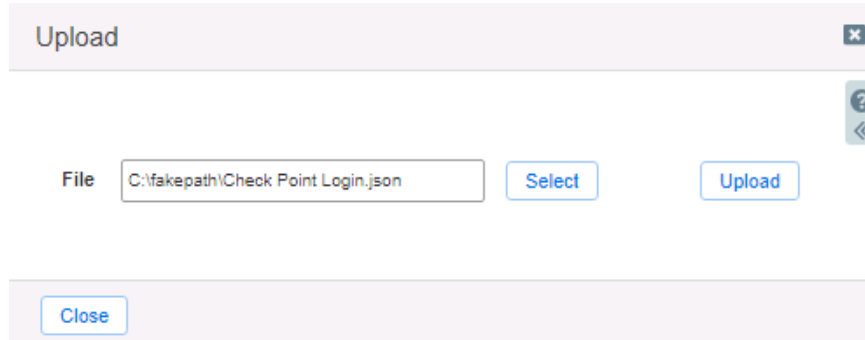
2. In the **Add Template** window click the **Select** button next to **Filename:**.



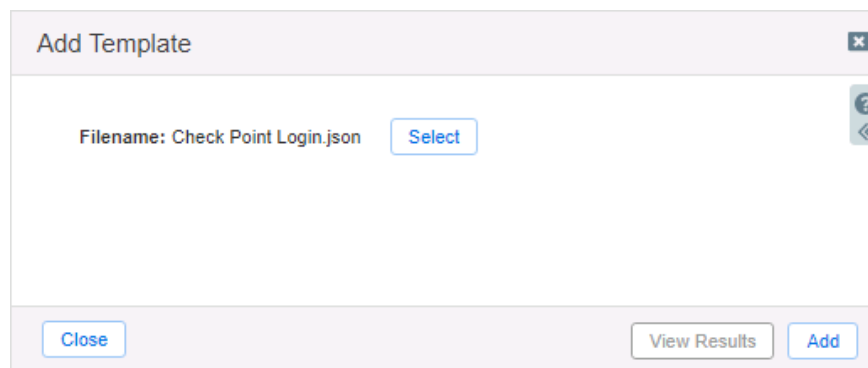
3. In the **Upload** window click **Select** and locate the **Check Point Login.json** template.



4. Once the path of the **Check Point Login.json** file is populated in the **File** text field, click the **Upload** button.



5. Click **Add** to complete the operation.






6. Verify that the **Check Point Login.json** template has been added within **Grid Ecosystem Templates**.

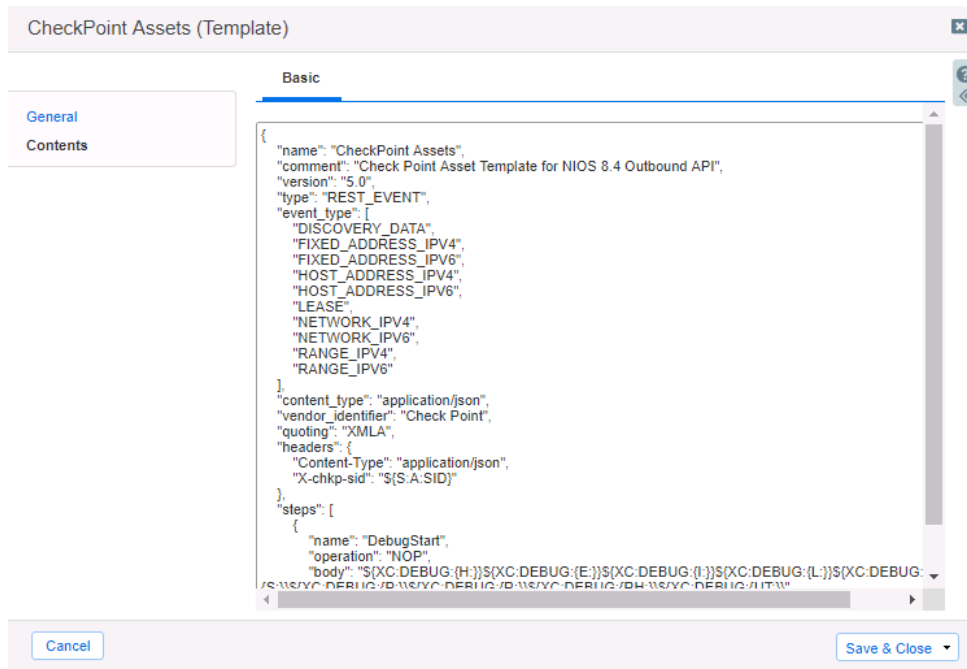


- Repeat steps 1 through 5 with all required templates. The following templates are required: **Check Point Assets**, **Check Point Security**, **Check Point Session**, **Check Point Login**, and **Check Point Logout**.

## Modify Templates

NIOS provides the ability to modify templates via the web interface.

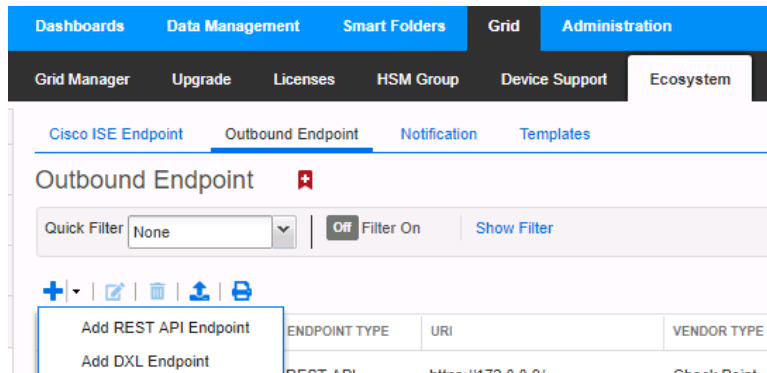
- Navigate to **Grid Ecosystem Templates** and click on the  hamburger icon next to the template you want to modify. Click the **Edit** button to open the Template window.
- The template editor is a simple interface for making changes to templates. It is recommended to only use the template editor to make minor changes. You can also edit, cut, and paste template snippets from a text editor. *Please note that you cannot delete a template if it is used by an endpoint or by a notification.*



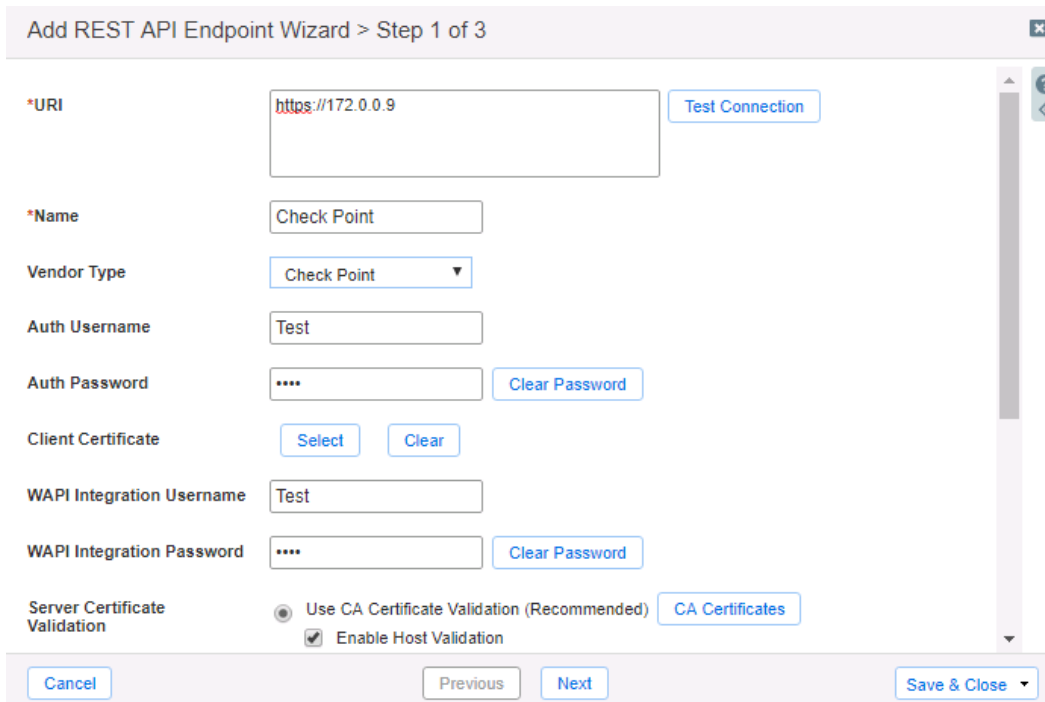
## Add a Rest API Endpoint

REST API Endpoints are remote systems that receive changes based upon notifications and configured templates. A Grid, for example, can not only send notifications, it can also receive the notification from itself for varying purposes.

1. To add a REST API Endpoint, navigate to **Grid Ecosystem Outbound Endpoint** and click the + icon, then click the **Add REST API Endpoint** button.



2. The **Add Rest API Endpoint Wizard** will open. **URI** and **Name** are requirements when configuring an endpoint. Input the following information:
  - o Enter a name you will recognize and the complete URI of the device (Example: <https://172.0.0.9>)
  - o Specify **Auth Username**, **Auth Password** (Check Point credentials. Creation of user account demonstrated on pg. 9)
  - o **WAPI Integration Username** and **WAPI Integration Password** (NIOS credentials). Once complete, Click **Next**



The screenshot shows the 'Add REST API Endpoint Wizard - Step 1 of 3'. The form contains the following fields and options:

- \*URI**:
- \*Name**:
- Vendor Type**:
- Auth Username**:
- Auth Password**:
- Client Certificate**:
- WAPI Integration Username**:
- WAPI Integration Password**:
- Server Certificate Validation**:  Use CA Certificate Validation (Recommended)  Enable Host Validation

At the bottom, there are buttons for 'Cancel', 'Previous', 'Next', and 'Save & Close'.

3. Be aware that the **Test Connection** function only checks communication (establishes TCP connection with a remote system) with the URI. It does not check the authentication credentials.
4. It is recommended to send notifications from a **Grid Master Candidate** if there is one available as an alternative to the Grid's **Grid Master**.
5. Under **Step 2** of the **Add REST API Endpoint Wizard**, set the Log Level to **Debug** for debug purposes during initial configuration. Additionally, click the **Select Template** button to populate the correct Session Template. When complete, click **Save & Close**.

Add REST API Endpoint Wizard > Step 2 of 3

Timeout: 30 Seconds

Log Level: Debug

Template: Check Point Session [Select Template] [Clear]

Vendor Type: Check Point

Template Type: Session Management

NAME	VALUE	TYPE
CP_AssetGroup	AssetGroup	String

[Cancel] [Previous] [Next] [Save & Close]

## Add Notifications

A notification is a link between a template, an endpoint, and an event. In the notification you define the event which triggers the notification, executed template, and the API endpoint of which the Grid will establish a connection. The Check Point templates on the Infoblox community Website support all available notifications.

To simplify the deployment of this integration, create only desired notifications and use relevant filters. It is highly recommended to configure deduplication for RPZ events and exclude a feed automatically populated by Threat Analytics. *Note: when testing notifications using Test Rule, rules for that notification apply.*

In order to add a Notification a Template must be added. To add a Notification, follow these steps:

1. Navigate to **Grid Ecosystem Notification** and click the **+** above the list of notifications or **+ Add Notification Rule** button on the right-side **Toolbar**. This will reveal the **Add Notification Wizard**.

Dashboards | Data Management | Smart Folders | Grid | Administration

Grid Manager | Upgrade | Licenses | HSM Group | Device Support | Ecosystem

Cisco ISE Endpoint | Outbound Endpoint | Notification | Templates

Notification

Quick Filter: None | Filter On | Show Filter

[+] [Edit] [Delete] [IDN Converter]

NAME	TARGET	ACTION	DISABLED
------	--------	--------	----------

- Once inside the **Add Notification Wizard**, enter a Name in the **Name** text box to identify the notification type. Next, click **Select Endpoint**. Then, Put a relevant comment in the **Comment** text box if desired. Finally, click the **Next** button.

Add Notification Wizard > Step 1 of 4

\*Name

\*Target Check Point

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

Target Type REST API

Vendor Type Check Point

Comment

Disable

- Click **Next**, select an **Event** type, by using the **Event** dropdown. Define one or many rules via the **Filter** and **Operator** dropdowns under the **Match the following rule:** header. Rules act as filters that decide if a template should be executed or not. To add additional rules, click the **+** button next to an existing rule. When more than one rule is present, a dropdown will populate allowing for the choice of **All** or **Any** defining the logic required before the associated action is executed. *Note: for optimal performance, it is best practice to make the rule filter as specific as possible.*

Add Notification Wizard > Step 2 of 4

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

\*Event

Match the following rule:

- Click Next until Step 4 of the **Add Notification Wizard** is reached. Then, click the **Select Template** button to populate a relevant template that will be executed if the notification is triggered. Finally, click **Save & Close** to complete the creation of the notification.

**Add Notification Wizard > Step 4 of 4**

\*Template: CheckPoint Assets [Select Template](#) [Clear](#)

Vendor Type: Check Point

Template Type: Event

Parameters

NAME	VALUE	TYPE
No data		

[Cancel](#) [Previous](#) [Next](#) [Save & Close](#)

- Complete steps 1-4 to add additional rules depending on your needs.

## Test the Integration

You can now test any notifications that you have made by emulating events via the **Test Rule** function. Testing a rule will show you if the implementation of a template is correct, and what steps the Outbound Endpoint takes when performing an Outbound API call.

- (Optional) Clear the **Debug Log** by navigating to **Grid Ecosystem Outbound Endpoint**. Select the icon next to the relevant **Outbound Endpoint** and click **Clear Debug Log**.
- Test a notification, by navigating to **Grid Ecosystem Notifications**. Once there, click on the icon next to a notification and click **Test Rule**. This will reveal a **Test Rule** window.

Navigation: Dashboards | Data Management | Smart Folders | **Grid** | Administration

Grid Manager | Upgrade | Licenses | HSM Group | Device Support | **Ecosystem**

Cisco ISE Endpoint | Outbound Endpoint | **Notification** | Templates

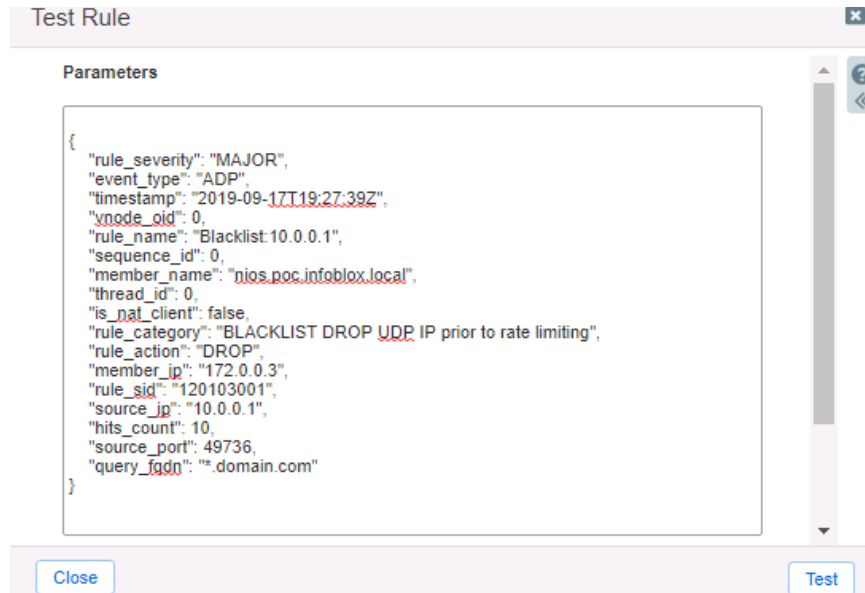
**Notification**

Quick Filter: None [Off](#) Filter On [Show Filter](#)

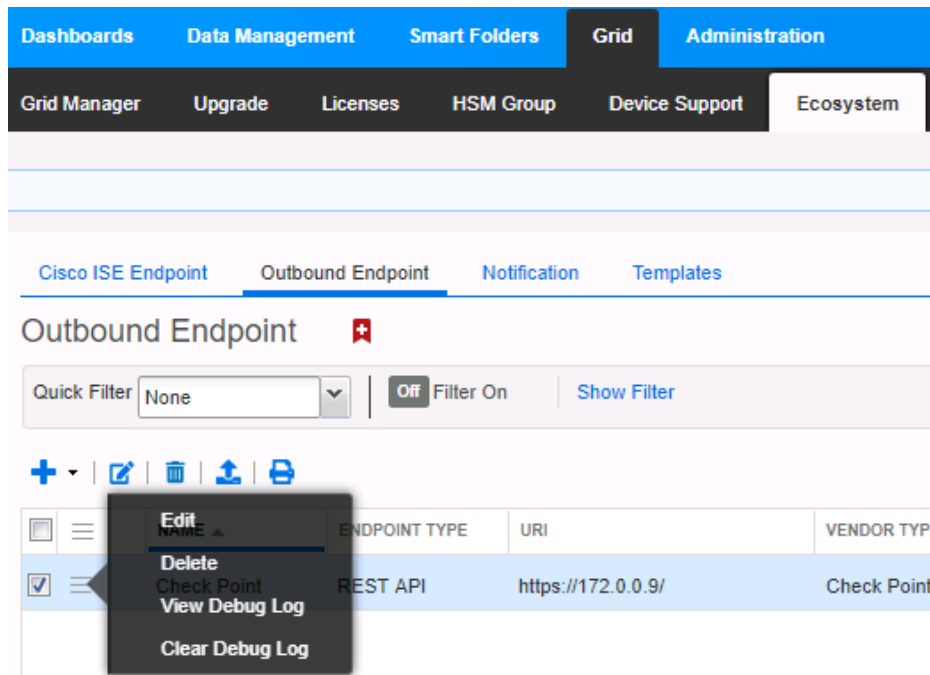
	TARGET	ACTION	DISABLED
<input checked="" type="checkbox"/>	Check Point	Outbound Template	No
<input type="checkbox"/>	Check Point	Outbound Template	No
<input type="checkbox"/>	CP_Fixed_IPv4	Outbound Template	No
<input type="checkbox"/>	CP_Fixed_IPv6	Outbound Template	No
<input type="checkbox"/>	CP_Host_IPv4	Outbound Template	No

Context Menu: Edit, Delete, **Test Rule**, View Debug Log

- You can modify test events within the **Test Rule** window. To perform the test function, click the **Test** button. If the test was successful you should see a **Success** message near the top of the window. *If the test has failed there is likely a syntax error, or there are incorrect parameters for the Test.*



- Once the **Test Rule** function has been executed, view the **Debug Log**. This is done by navigating to **Grid Ecosystem Notifications** and clicking on the ☰ hamburger icon next to a relevant notification and selecting **View Debug Log**. Alternatively, you can view the **Debug Log** by navigating to **Grid Ecosystem Outbound Endpoints** and clicking the ☰ hamburger icon next to the relevant **Outbound Endpoint**. *Please note that debug logs may be downloaded locally or be blocked by an ad blocker.*



## Additional Resources

**Infoblox community Website:**

<https://community.infoblox.com/>

**Infoblox NIOS Documentation:**

<https://docs.infoblox.com/display/nios84/Infoblox+NIOS+8.4>

**Check Point community Website:**

<https://community.checkpoint.com/>

**Check Point Management API Reference:**

<https://sc1.checkpoint.com/documents/latest/APIs/#introduction>





Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70% of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054  
+1.408.986.4000 | [info@infoblox.com](mailto:info@infoblox.com) | [www.infoblox.com](http://www.infoblox.com)



© 2021 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).