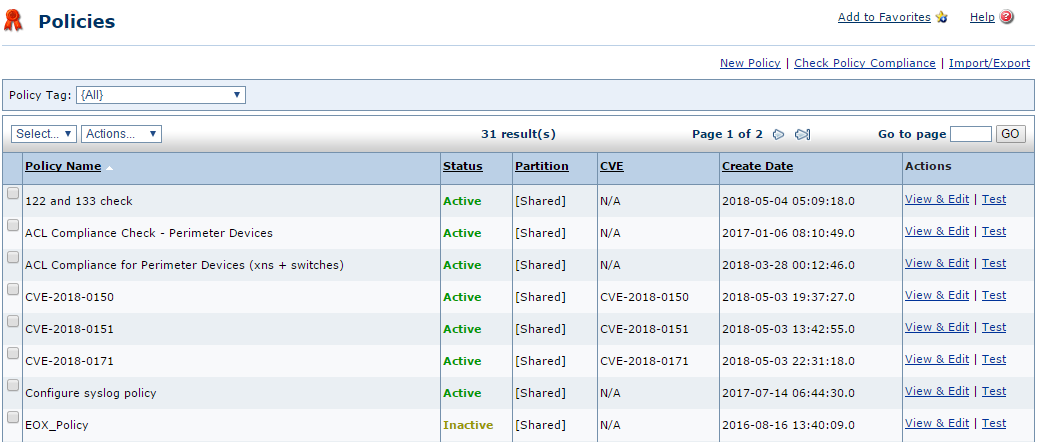
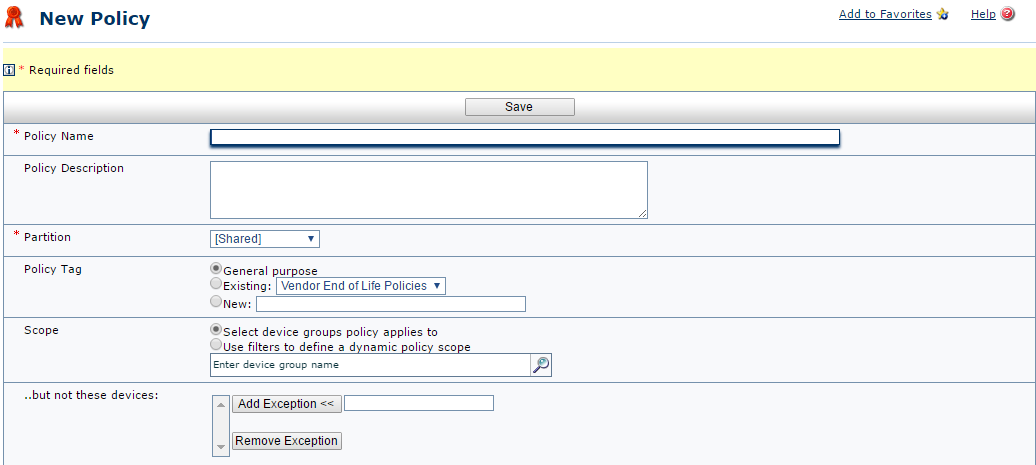
## Creating Policy in HPNA:

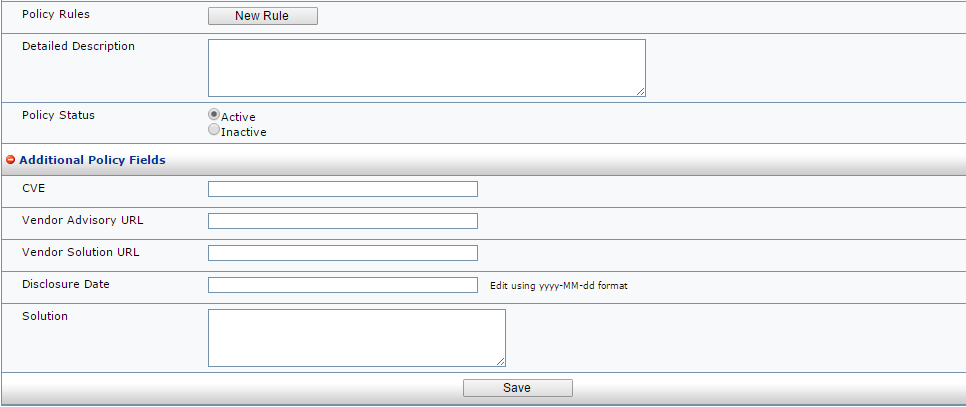
* + Log into HPNA with your DS ID (<https://hpna.admin.cargill.com/> ) ;
  + On top bar, click on Policies.
  + To view the policies already created, click on **Policy List.**
  + To create a new policy, click on the **New Policy**.
  + On the form that shows up, enter the name for the new policy.
  + **Policy Description**: Enter a description of the policy.
  + **Partition**: Select a Partition from the drop-down menu. (Note: This field is only displayed if you have configured one or more Partitions.)
  + **Policy Tag**: Select one of the following options:
    1. General purpose — If you do not want to tag a policy, it is used as a general purpose policy.
    2. Existing — Select a tag from the drop-down menu.
    3. New — Create a new policy tag by entering a tag name.
  + **Scope**: Select one of the following options:
    1. Select the device groups to which this policy applies — Use the Device Selector to select groups.
    2. Use filters to define a dynamic policy scope —When defining a policy, you can define the policy scope the same way you define a Dynamic Group.
  + **But not these devices**: Enter the IP address or hostname of the device in the right-hand box and then click Add Exception <<. To remove a device, select the IP address or hostname of the device in the left-hand box and click Remove Exception.
  + **Policy Rules**: The Policy Rules table displays all rules that will be applied by the policy. The policy applies all rules to each saved device selected for this policy.
  + **New Rule button**: To create a new rule for this policy, click the New Rule button. The New Rule page opens.
  + **Detailed Description**: Enter a detailed description of the policy. This field enables you to add a detailed description of the policy.
  + **Policy Status**: Click one of the following options:
    1. Active — Marks the policy active (the default).
    2. Inactive — Deactivates the policy.
  + **Additional Policy Fields**:
  + **CVE**: Enter the CVE (Common Vulnerabilities and Exposures) name. CVE is a list of standardized names for vulnerabilities and other information on security exposures.
  + **Vendor Advisory URL**: Enter the URL to an external reference for advisory information on a vulnerability.
  + **Vendor Solution URL**: Enter a URL to an external reference for more information on possible solutions to the vulnerability.
  + **Disclosure Date**: Enter the date when the software vulnerability was flagged in the following format: yyyy-mm-dd.
  + **Solution**: Enter detailed solution information.

**When you click the New Rule button, a new form with the below fields appears:**

* + **Rule Name:** Enter the rule name.
  + **Rule Type:** Select a rule type. For example, you can define a rule based on the configuration text or data model elements pulled from configuration text of the selected device(s). Options include:
    1. Configuration — If selected, the configuration rule checks to see if the selected device(s) configuration text is in compliance with the current configuration rule.
    2. Diagnostics — If selected, the rule checks to see if the selected device(s) Diagnostic text is in compliance with current Diagnostic rule.
    3. Software — If selected, the rule checks to see if the selected device(s) are in compliance with the current software rule.
  + **Rule Description:** Enter a description of the rule.
  + Applies to devices with these drivers:
  + **All Device Families:** Click the radio button if you want to apply the rule to all device families. By default, NA parses configuration and device information into normalized elements for its data model.
  + **Device Family:** Select the device family to which the rule applies from the drop-down menu, for example BayStack, Cisco IOS or Nortel ASF. Select one of the following options:
    1. All applicable drivers — If checked (the default), NA chooses all applicable drivers. Keep in mind that a rule applies only to devices that are assigned a specific driver.
    2. Select specific drivers — If checked, select one or more drivers from the list. Keep in mind that a configuration rule applies only to the configuration for devices that are assigned a specific driver.
  + **Define Text Block:** Enables you to set text blocks to be used by configuration block conditions. If you select the Set Text Blocks option, the Block Start Pattern and the Block End Pattern fields are displayed.
  + **Rule Conditions:** Select one or more conditions from the drop-down menu, for example Config Text, Flash Memory, and Host Name.
  + Click the Reset Expression button to reset the expression to the default.
  + **Importance**: Select the importance level. This indicates the non-compliance risk rating for the policy rule. Options include:
    1. Informational — Events that typically do not require a response.
    2. Low — Events that may require a response as time permits.
    3. Medium — Events that require a timely response, typically within 72 hours (the default).
    4. High — Events that require an urgent response, typically within 24 hours.
    5. Critical — Events that require an immediate response.
  + **Detailed Description:** Enter a description of the rule.
  + **Rule Exceptions:** Displays a list of rule exceptions, if applicable.
  + To add an Exception Rule, click the New Exception link. The New Rule Exception page opens.
  + **Auto-Remediation Scripts:** The Auto-remediation pop-up window accesses the data on the Policy Rule page to show variable mappings, generate sample code, and validate the script before it is saved.
  + Click the Save button to save the rule, or the Save And Add Another button to save the current rule and add a new one.

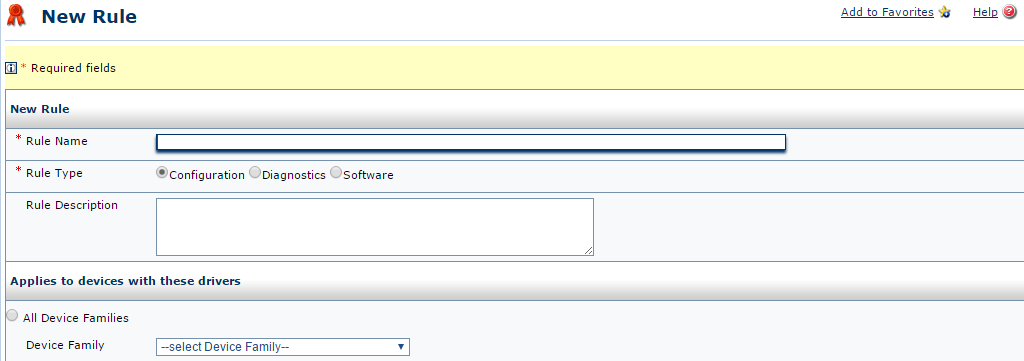


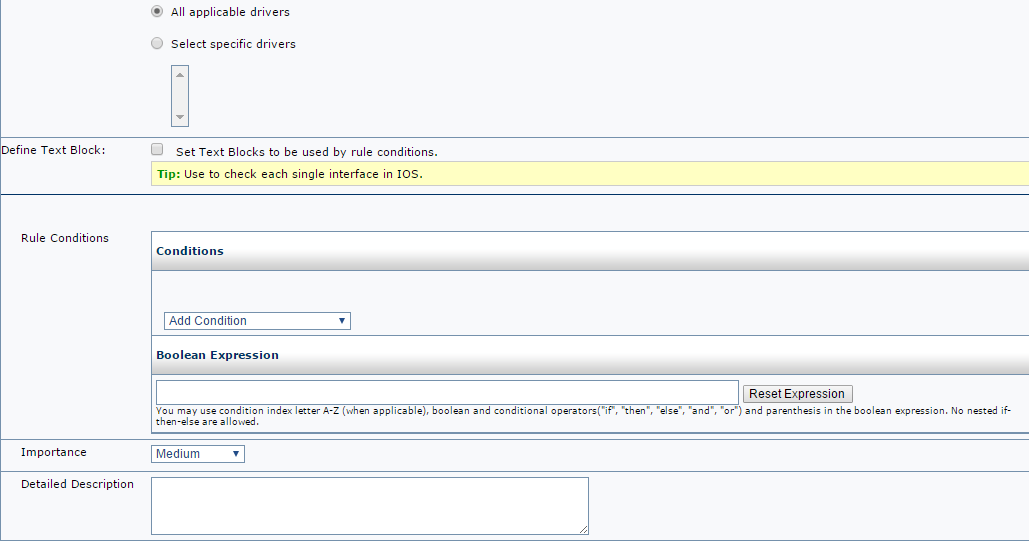


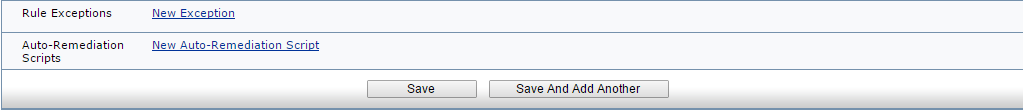


**When the New Exception link is clicked, a new page opens, where the below fields appear:**

* + **Device:** Enter the IP address or hostname of the device to which this exception rule applies.
  + **Expires on:** If checked, choose the month, day, year, hour, and minute after which this exception is disregarded by the rule.
  + **Ignore text matching this pattern when checking the configuration rule:** If checked, enter text. All text in a device’s configuration that matches the text you entered is not subject to this configuration rule.
  + **Ignore this device entirely when checking the configuration rule:** If checked, NA skips this device when checking the configuration rule.

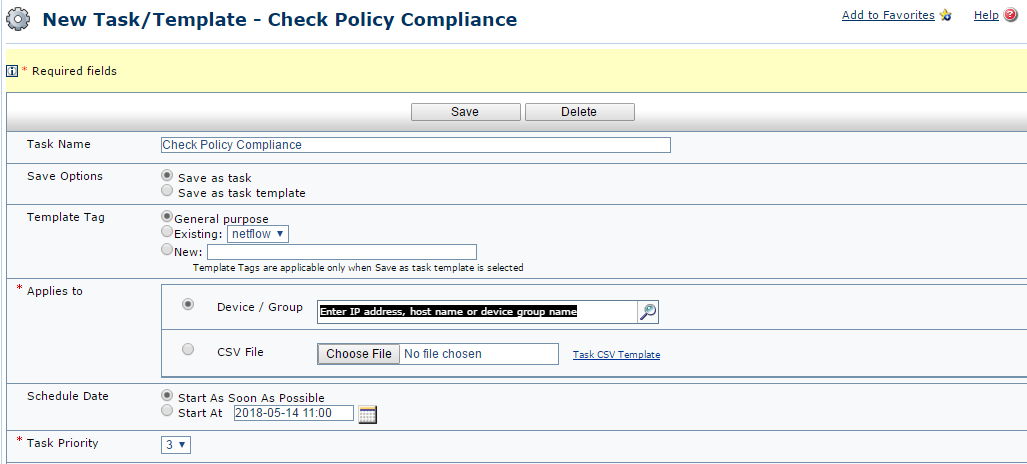


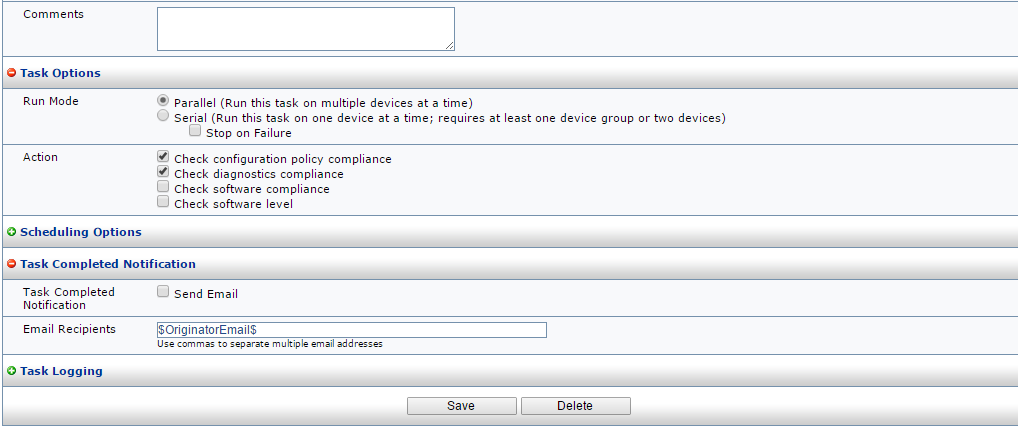




## Running the Compliance Check:

* + Log into HPNA with your DS ID (<https://hpna.admin.cargill.com/> ) ;
  + On top bar, click on Policies 🡺 Policy Tasks 🡺 Check Policy Compliance;
  + Give a **Task Name** or let it be the same just add unique key words to recognize later if required.
  + Under **Applies To**, select the **Device/Group** and select Inventory (for all devices) or any specific group that is present in HPNA. You can also select individual device.
  + Select the **Task Priority**, 1 being the highest.
  + Add **Comments** if required.
  + Under **Tasks Options**, Let the **Run Mode** set as parallel.
  + In **Actions**, check only the **Check Configuration Policy Compliance** or **Check Diagnostic Compliance,** depending on your requirement.
  + You can use **Scheduling Options** to schedule the task for a later time or to run it periodically.
  + By using the **Task Completed Notification**, you can provide email address, to which a mail would be sent once the task is complete. If not required, let it be blank.
  + You can store a variety of log for this task using the **Task Logging** if required, otherwise let it be unchecked.
  + Select **Save** to save and Run the compliance check task.





## Generating Compliance Report:

* + Log into HPNA with your DS ID (<https://hpna.admin.cargill.com/> )
  + On top bar, click on Reports 🡺 Search For 🡺 Compliances
  + **Host Name**: Select an operator and enter the Host Name. Operators include: Contains, Does not contain, Matches, Equals, Does not equal, Contains (regex), Does not contain (regex).
  + You can use **wildcard characters**. The ? stands for any one character in that position, while the \* stands for any number of characters in that position, for example: usa-ny-ny-\*, 10.0.\*.2, and ?jones.

Note: Wildcards do not work with the “equals” and “does not equal” operators.

* + **Device IP**: Select an operator and enter the device’s IP address. Operators include: Contains, Does not contain, Matches, Equals, Does not equal, Contains (regex), Does not contain (regex).
  + **Device ID**: The device ID specification. Operators include: Equals, Is less than, Is greater than.
  + **Device Group**: Use the Device Selector to select groups.
  + **Compliance**: Select one of the following options:
    1. Any compliance state
    2. Device in compliance
    3. Device not in compliance
    4. Device not checked yet
    5. Device has no applicable policy
  + **Policy**: Enter the name of the policy or select a policy from the drop-down menu.
  + **Rule**: Enter a policy configuration rule or select one from the drop-down menu.
  + **Rule Type**: Select one or more of the following options:
    1. Configuration
    2. Diagnostics
    3. Software
  + **Rule Importance**: Select one or more Importance levels. Options include:
    1. Informational — Events that typically do not require a response.
    2. Low — Events that may require a response as time permits.
    3. Medium — Events that require a timely response, typically within 72 hours.
    4. High — Events that require an urgent response, typically within 24 hours.
    5. Critical — Events that require an immediate response.
  + **Rule Description**: Include rule description in search results.
  + **CVE**: Enter the CVE (Common Vulnerabilities and Exposures) name, along with an operator. CVE is a list of standardized names for vulnerabilities and other information on security exposures
  + **Last Checked Date**: Select the following operators:
    1. Since or Until
    2. Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago
    3. Note: Clicking the calendar icon opens the calendar, where you can select a date and time.
  + **Rule Out Of Compliance Date**: The rule out of compliance date is the time that NA detects that a device is out of compliance with a particular rule.

Select the following operators:

* + 1. Since or Until
    2. Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago
    3. Note: Clicking the calendar icon opens the calendar, where you can select a date and time.
  + **Policy Tag**: Select a Policy Tag. Policy tags enable you to search for compliance entries related to policies with selected tags.
  + **Partition**: Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory.

