**SOP: Updating Device Software/IOS through HPNA**

# VERSION CONTROL:

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Name | Remarks |
| 1.0 | 5/2018 | Suryakant Sahoo and Deepa Vaidyanathan | First version |
| 1.1 | 5/2018 | Norman | 1st review |

Contents

[VERSION CONTROL: 1](#_Toc513834931)

[PURPOSE: 2](#_Toc513834932)

[AUDIENCE: 2](#_Toc513834933)

[REQUIREMENTS: 2](#_Toc513834934)

[NOTES: 2](#_Toc513834935)

[1. WHY SHOULD I USE HPNA TO UPDATE DEVICE SOFTWARE? 3](#_Toc513834936)

[2. PROCESS 3](#_Toc513834937)

[3. ANALYSIS AND REPORTING 3](#_Toc513834938)

[3.1 Creating Software Level In HPNA: 3](#_Toc513834939)

[3.2 Running Policy Compliance Check For The Software Levels: 5](#_Toc513834940)

[3.3 Generating Device Software Report: 6](#_Toc513834941)

[3.4 Creating Policy To Detect Vulnerabilities On Device Software: 6](#_Toc513834942)

[3.5 Running The Compliance Check: 6](#_Toc513834943)

[3.6 Generating Software Compliance Report: 7](#_Toc513834944)

[4. WORKFLOW SETUP 7](#_Toc513834945)

[5. UPDATING DEVICE SOFTWARE 7](#_Toc513834946)

[5.1 Checking If Required Image Is Available In HPNA 8](#_Toc513834947)

[5.2 Loading Software Image in HPNA 9](#_Toc513834948)

[5.3 Preparing To Update Device Software: 10](#_Toc513834949)

[5.4 Running the Update Device Software Task 11](#_Toc513834950)

[5.5 Verify the Process Has Been Executed Successfully 15](#_Toc513834951)

# PURPOSE:

The purpose of this document is to provide the necessary steps for identifying old, obsolete and vulnerable device software and upgrade Cisco IOS and similar software through the use of HPNA.

# AUDIENCE:

1. Network Analysts/Engineer checking device software vulnerabilities on one or multiple devices and upgrading the same.

# REQUIREMENTS:

1. Analyst has access to HPNA;
2. Analyst is familiar with basic HPNA operation and
   * How to consult its help documents;
   * How to schedule jobs
3. Analyst understands Cisco IOS/Nexus commands;
4. Analyst already have necessary permissions to configure devices through an SSH client (e.g. putty)
5. Nice to have:
   * Analyst understands how to create regex expressions.
   * Analyst understands basic Boolean/programming logic.

# NOTES:

1. **HPNA works best on Internet Explorer and has compatibility issues with other browsers due to Flash being disabled by default on Cargill installs.**
2. **Some options shown here may require additional permissions. Please check with Infra-NW-HP Tools team if you need additional permissions or if some options are not available.**

# WHY SHOULD I USE HPNA TO UPDATE DEVICE SOFTWARE?

HPNA will help you identify and update old, obsolete and vulnerable device software/IOS:

* Identify and generate a report consisting of the list devices running security vulnerable software/IOS.
* Update software/IOS to the latest/secure version on multiple devices at a time;

# PROCESS

To efficiently identify vulnerable/obsolete software on the devices and update device software using HPNA you’ll have to follow below steps:

1. **Analysis and Reporting:**

* Create/Update new policies or software level(s). Should be a continuous process based on source. E.g., Grid, Lifecycle team, TGRC Team etc.
* Run a policy compliance check for the software levels/software compliance.
* Generate a Compliance Report or Device Software Report. Devices with Security risks and vulnerabilities will be identified.

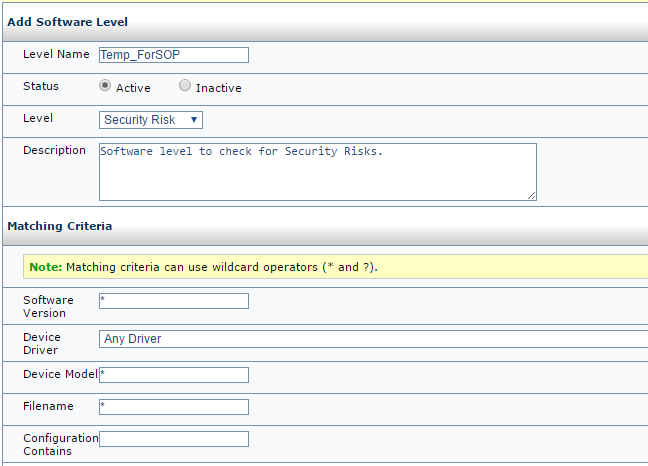
1. **Updating Device Software:**

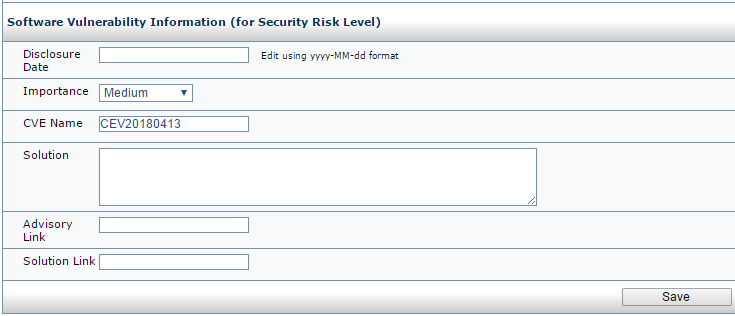
* For devices that needs update, load Software image in HPNA (or choose from existing image).
* Run file system diagnostics on the device(s) that needs update.
* Workflow creation in HPNA.
* Run Update Device Software task in HPNA. Device reboot can be scheduled to run later.

# ANALYSIS AND REPORTING

## 3.1 Creating Software Level In HPNA:

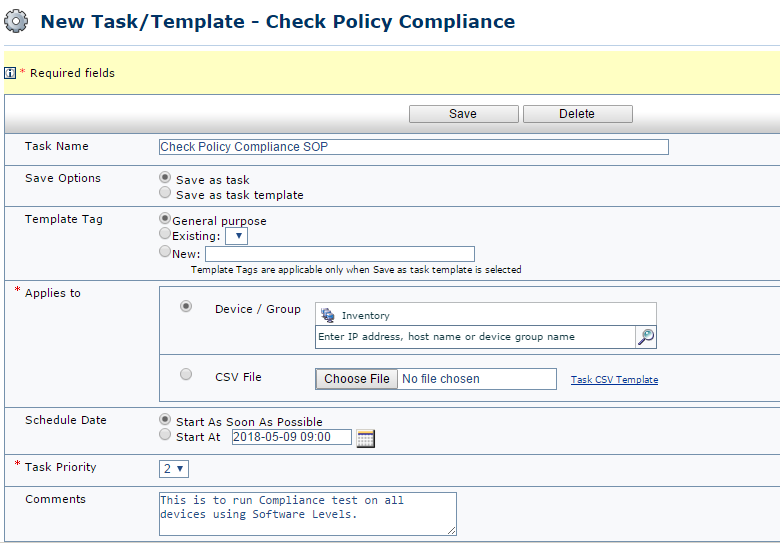
* + Log into HPNA with your DS ID (<https://hpna.admin.cargill.com/> ) ;
  + On top bar, click on Policies 🡺 Software Levels;
  + Click on **Add Level**.
  + Type the name of your level on **Level Name**; Start its name with **Temp\_** to sign that this group can be erased after some time.
  + Mark **Status** as active to activate the Level during next Policy checks.
  + Select a **Level** as per your requirement/source.
  + Provide the level **Description.**
  + Fill in the **Matching Criteria** as per requirement/source.
  + Fill in the Software Version, Device Driver, Device Model, File Name and Configuration Contains depending on the requirement/source. Fill wildcard \* to run for all types or leave it blank. For Drivers select All Drivers to select all drivers.
  + Under **Software Vulnerability Information (for Security Risk Level)**
  + Fill in the **Disclosure Date** as per source.
  + Mark **Importance** depending on the priority of handling the device.
  + Give in any unique **CEV Number**. Eg. CEV20180413 (CEVyyyymmdd).
  + Click on **Save** to save your Add Level Form.

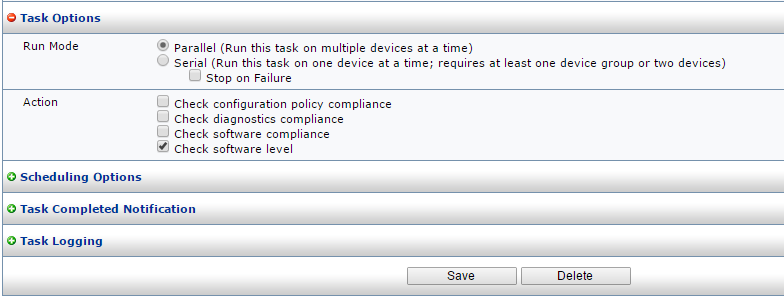




## 3.2 Running Policy Compliance Check For The Software Levels:

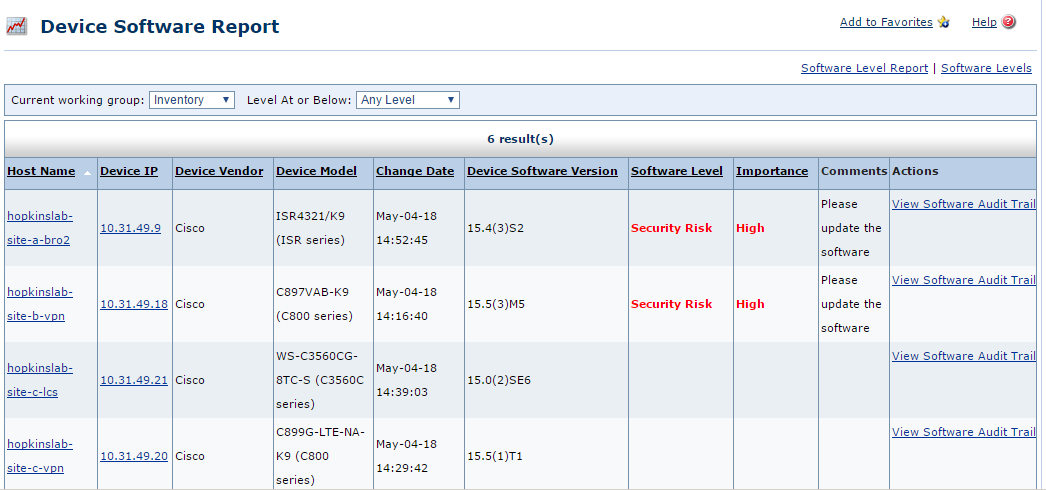
* + Log into HPNA with your DS ID (<https://hpna.admin.cargill.com/> ) ;
  + On top bar, click on Policies 🡺 Policy Tasks 🡺 Check Policy Compliance;
  + Give a **Task Name** or let it be the same just add unique key words to recognize later if required.
  + Under **Applies To**, select the **Device/Group** 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 Software Level.**
  + 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.





## 3.3 Generating Device Software Report:

* + Log into HPNA with your DS ID (<https://hpna.admin.cargill.com/> )
  + On top bar, click on Reports 🡺 Device Software
  + A **Device Software Report** will get generated with device details like Hostname, IP, Vendor, Model, Change Date and Software Version. Identified Software Level, Importance and Comments as defined while creating Software Levels will also be stated in the report.
  + You can select/change the **Current Working Group** and **Level at or below** as required. Select Inventory for all devices and Any Level for visibility of the complete report.

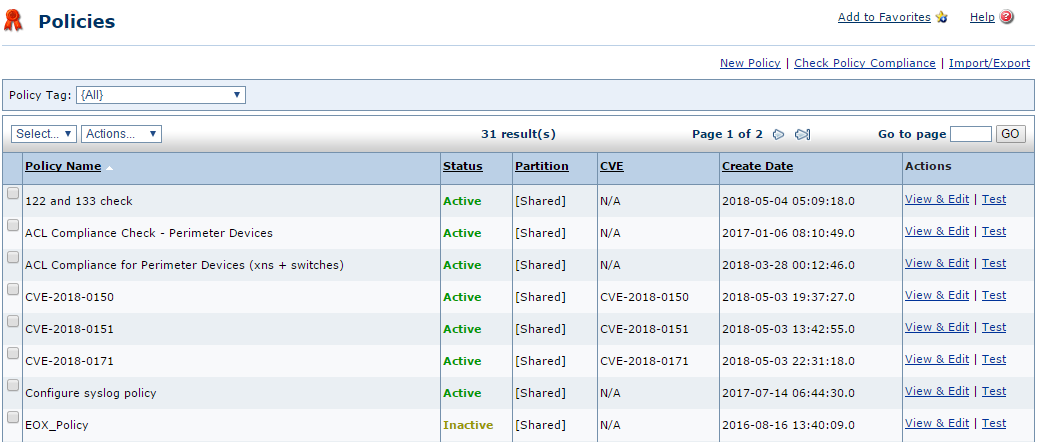


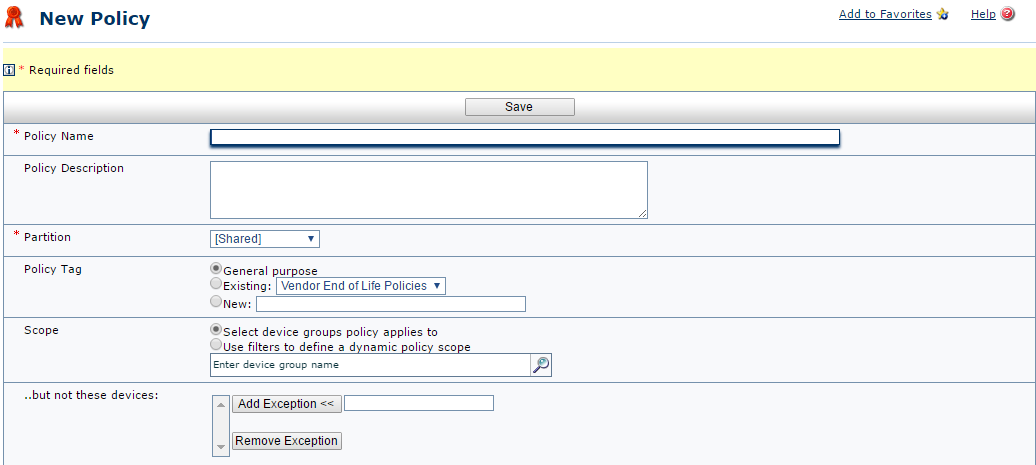
## 3.4 Creating Policy To Detect Vulnerabilities On Device Software:

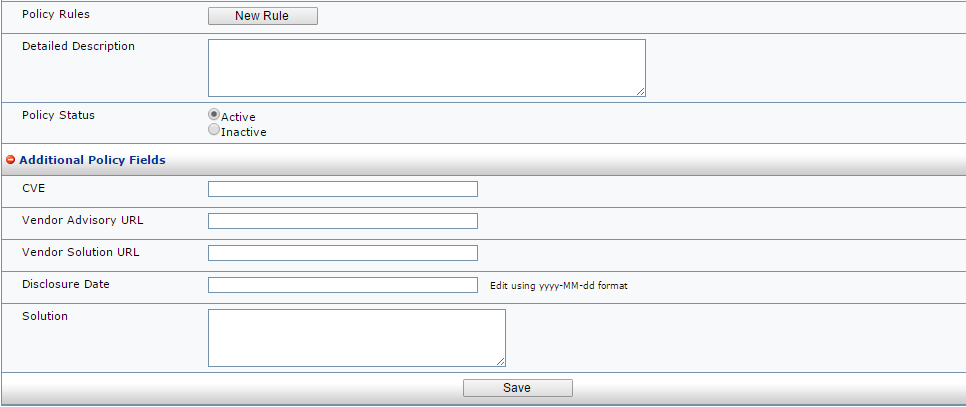
* + Log into HPNA with your DS ID (<https://hpna.admin.cargill.com/> ) ;
  + On top bar, click on Policies.
  + To view the policies already created, click on **Policy List.**
  + To create a new policy, click on the **New Policy**.
  + On the form that shows up, enter the name for the new policy.
  + **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.

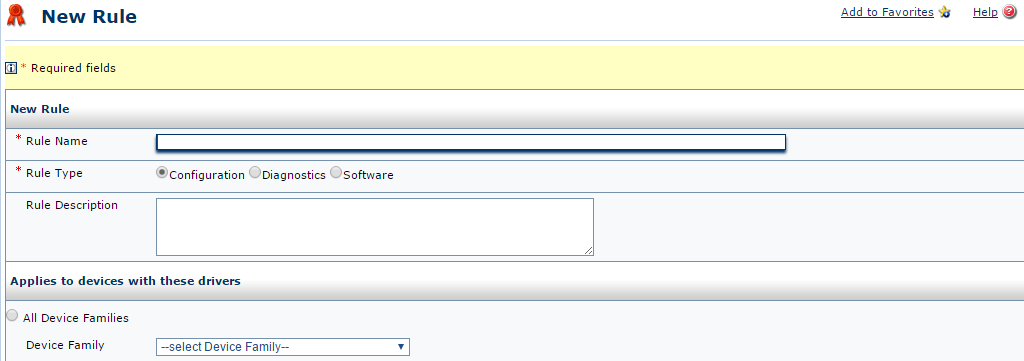


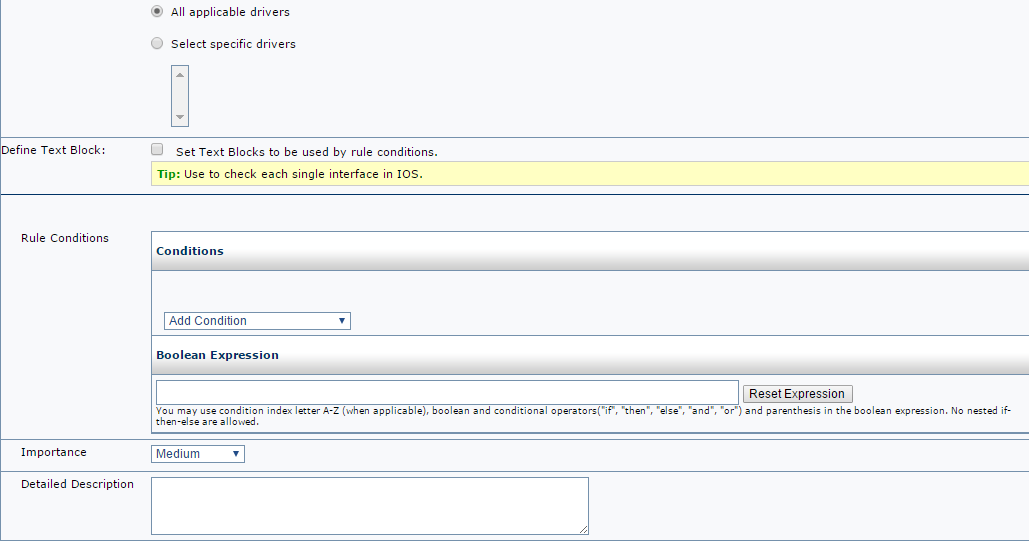


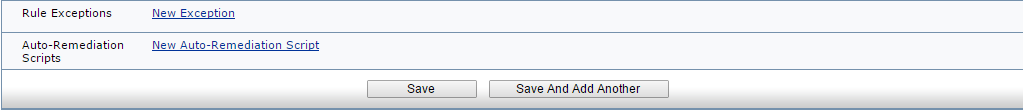


**When the New Exception link is clicked, a new page opens, where the below fields appear:**

* + **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.

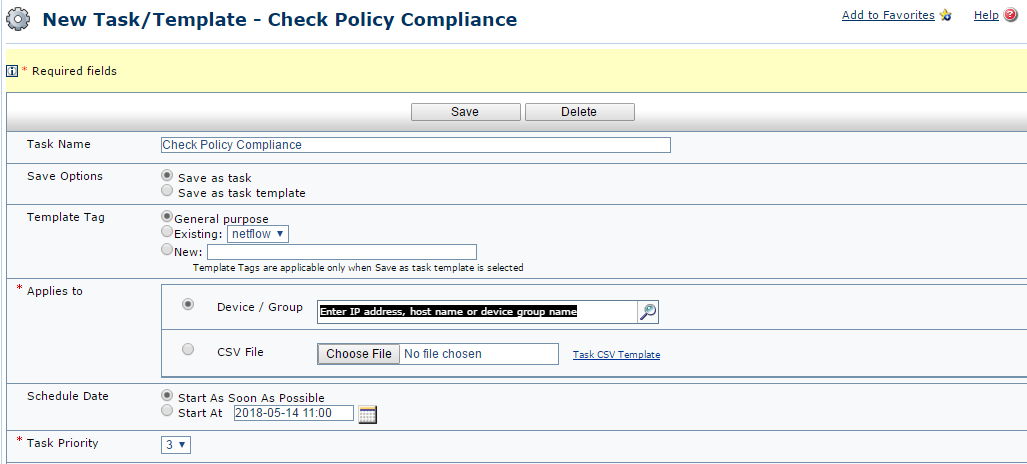


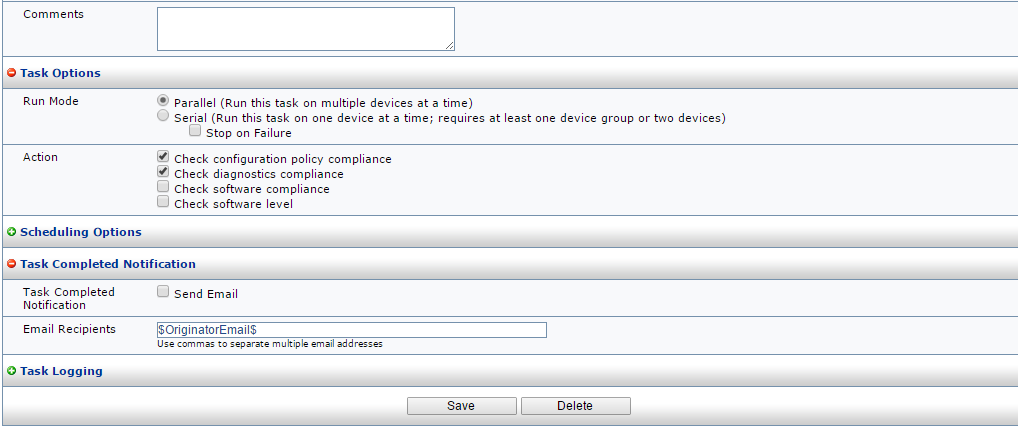




## 3.5 Running the Compliance Check:

* + 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.





## 3.6 Generating Software Compliance Report:

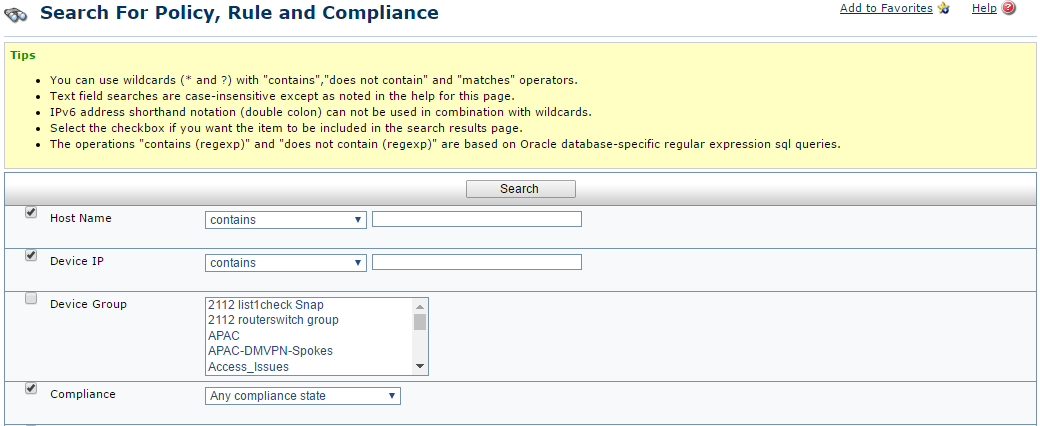
* + Log into HPNA with your DS ID (<https://hpna.admin.cargill.com/> )
  + On top bar, click on Reports 🡺 Search For 🡺 Compliances
  + **Host Name**: Select an operator and enter the Host Name. Operators include: Contains, Does not contain, Matches, Equals, Does not equal, Contains (regex), Does not 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.

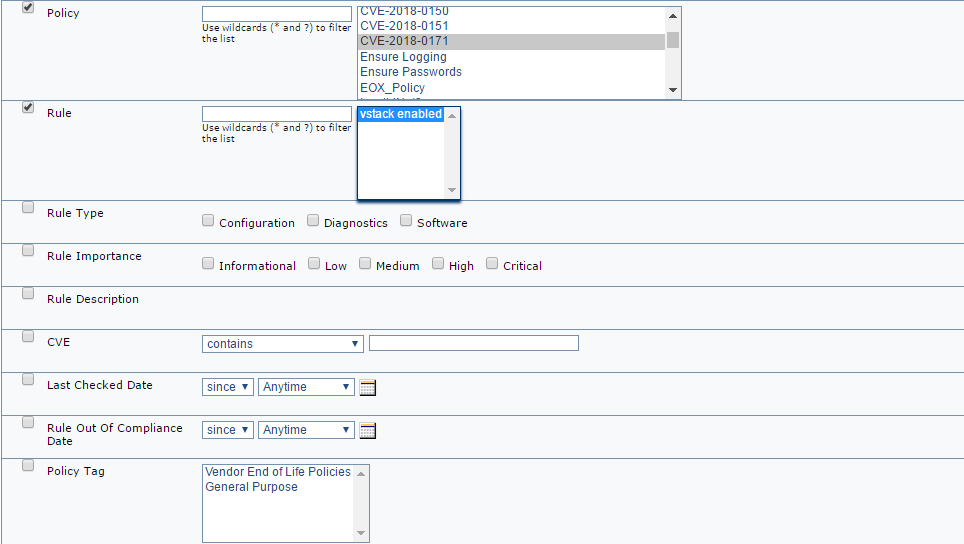
Note: Wildcards do not work with the “equals” and “does not equal” operators.

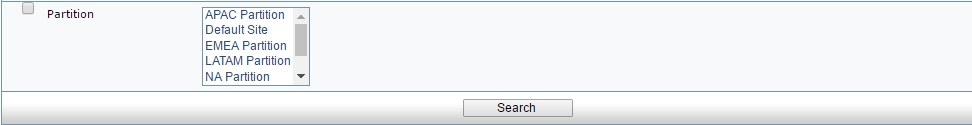
* + **Device IP**: Select an operator and enter the device’s IP address. Operators include: Contains, Does not contain, Matches, Equals, Does not equal, Contains (regex), Does not contain (regex).
  + **Device ID**: The device ID specification. Operators include: Equals, Is less than, Is greater than.
  + **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.

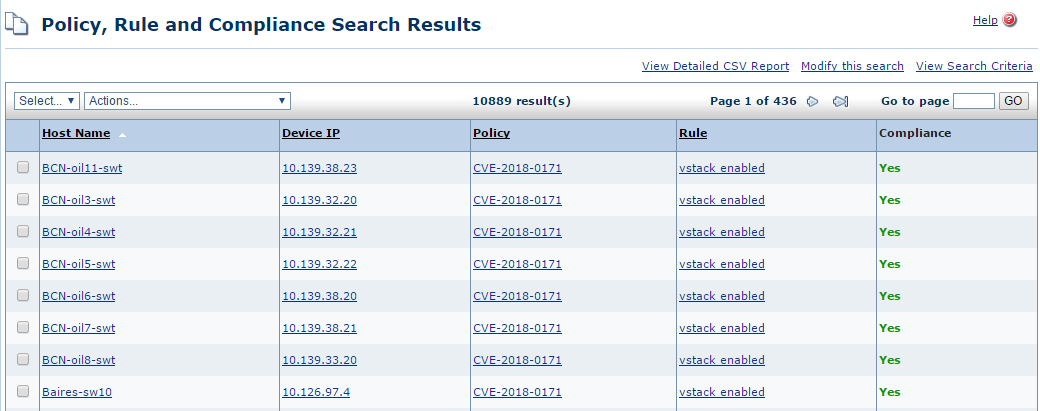
Select the following operators:

* + 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.









# WORKFLOW SETUP

The HP Network Automation (NA) Workflow Integration & Routing Engine (WIRE) manages the process of network configuration, that network changes are made according to predefined policies, completed in the correct sequence, and approved by the appropriate people. Workflow indicates an ordered sequence of tasks that begins with the originator of a task submitting the task for approval, and ends with the approver approving or rejecting it. While the originator of a task is a limited access user, the approver (an individual or a group of individuals) is a power user or a full access user.

The following flow chart describes the workflow process:

Admin sets up the workflow setup

The task originator schedules a task with a request for approval

The task is reviewed and approved by the approver/ approvers

# UPDATING DEVICE SOFTWARE

HPNA contains a Software Image repository with Image sets that can be used when upgrading software. When updating a device, you’ll be able to verify if the required image has already been loaded by other analysts and reuse them while executing your tasks. If the image required by your project/task is not available, you’ll have to upload it before proceeding.

**SOFTWARE IMAGE TYPES AND NAMING CONVENTION**

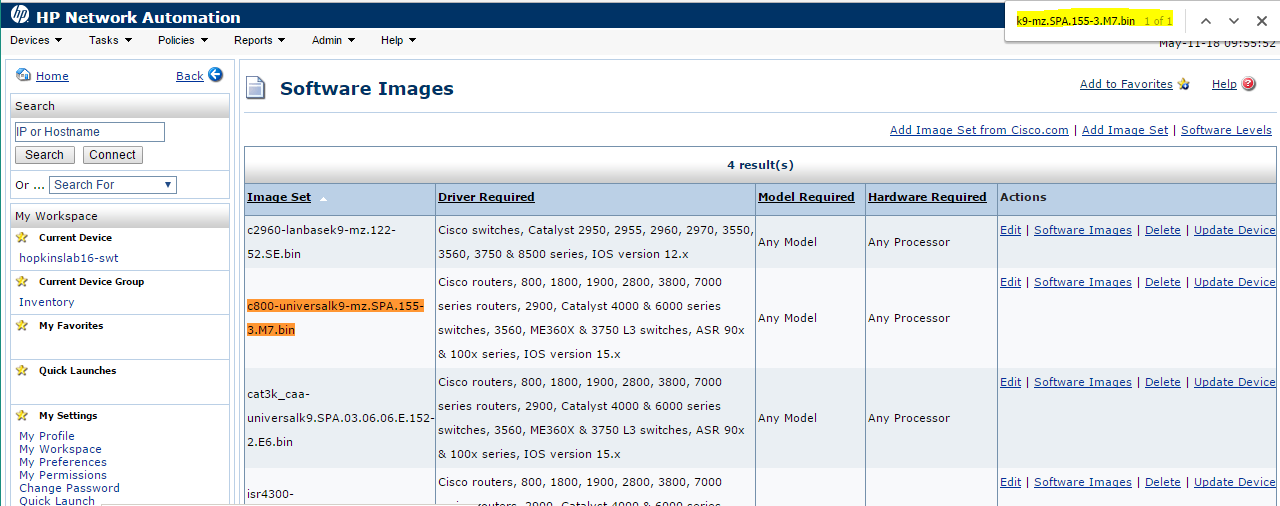
There will be three types of images hosted in HPNA:

* GRID: All Grid images are software versions validated and supported by engineering team to run on CNET, either through grid review or during projects and other assignments. These images will have the **GRID\_** prefix;
* CUSTOM: All images that were not validated by engineering team should receive the **CUSTOM\_** prefix, so they’re properly identified as non-standard OSs. Custom images may be required during tests, PoCs, troubleshooting or grid update.
* OBSOLETE: All images that were once in the grid and then retired should be identified with the **OBSOLETE\_** prefix, so it is clear these images are not part of standards anymore. Although no devices should be “updated” to run an obsolete version, there may be valid reasons why these images are needed.

Note: Some devices automatically reboot after a software update.

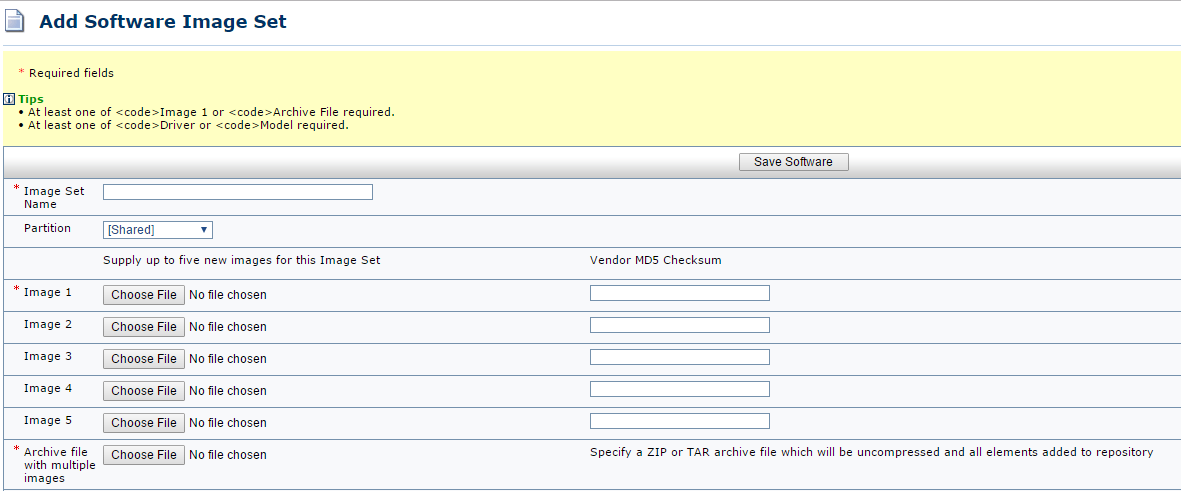
## Checking If Required Image Is Available In HPNA

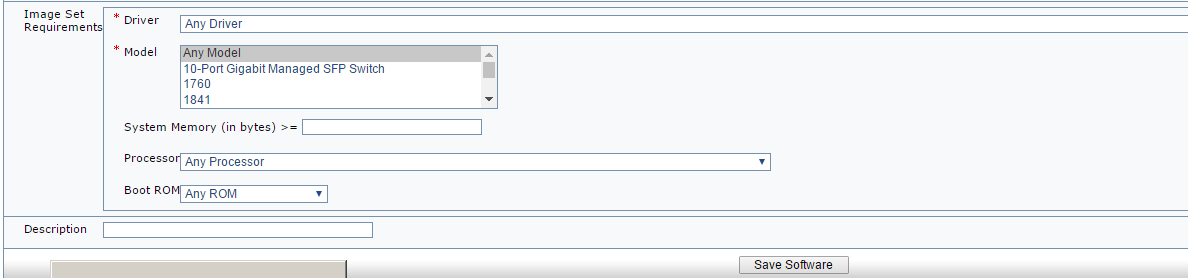
* + Log into HPNA with your DS ID (<https://hpna.admin.cargill.com/> ) ;
  + On top bar, click on Devices 🡺 Device Tools 🡺 Software Images
  + Use CTRL+F to search on the screen if the required software image is already existing in HPNA.



## 5.2 Loading Software Image in HPNA

* + Log into HPNA with your DS ID (<https://hpna.admin.cargill.com/> ) ;
  + On top bar, click on Devices 🡺 Device Tools 🡺 Software Images
  + Click on **Add Image Set.**
  + Write an **Image Set Name.** Remember to follow the naming convention and prepend the image name with GRID/CUSTOM/OBSOLETE. Example: OBSOLETE\_ Cisco IOS 15.3(3)M3
  + Select a **Partition** from the dropdown menu. Different partitions will be listed here only if they are configured. If you want to use all partitions, select Shared.
  + Up to 5 software images can be uploaded.
  + **Vendor MD5 Checksum**: Checksum is a 128-bit checksum computed using the MD5 algorithm. MD5 is a cryptographically secure algorithm.
  + Specify a ZIP or a TAR **Archive file** to expand the archive file and add all contained files to the image set.
  + Under **Image Requirements**, select a driver and model required by the image. Consult Cisco website for information. Peer review it with engineering team.
  + System memory, processor and boot ROM can also be filled if required.
  + Add a **Description** for better clarity.
  + Click **Save Software** to save the software.

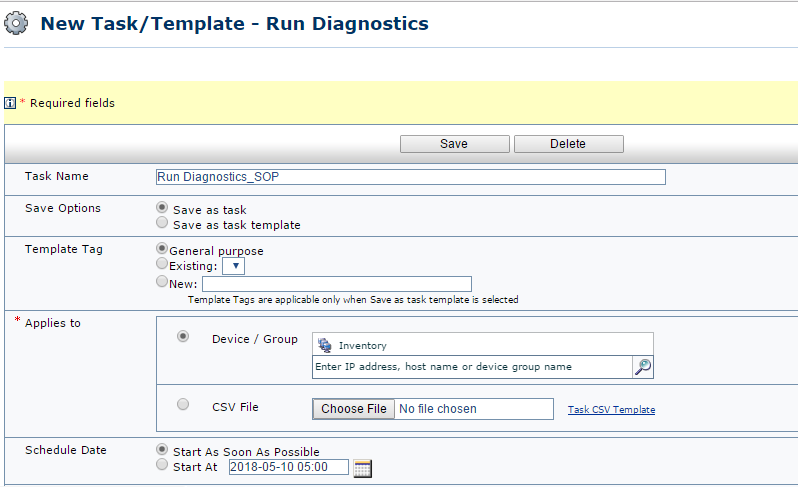


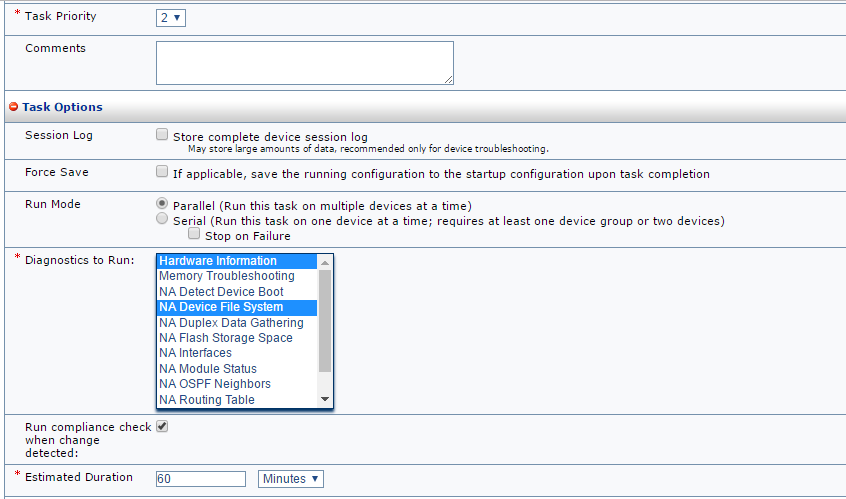


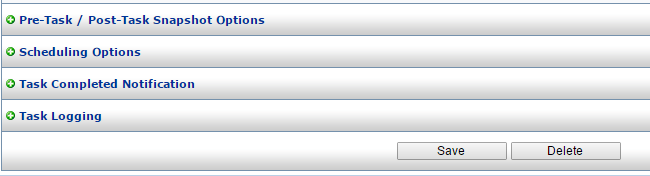
## 5.3 Preparing To Update Device Software:

Run a file system diagnostics to collect device(s) information:

* + Log into HPNA with your DS ID (<https://hpna.admin.cargill.com/> )
  + On top bar, click on Tasks 🡺 New Tasks 🡺 Run Diagnostics
  + Give the **Task Name** (include the CRQ or INC number if possible).
  + In **Applies To**, select one or multiple **Device/Group** that you want to run this diagnostics for.
  + Choose appropriate **Task Priority**. 1 being the highest.
  + Under **Task Options**, check **Session log** if you want to have detailed log generated.
  + Let the **Run Mode** be set as parallel.
  + In **Diagnostic to Run** press **CRTL** andselect **NA Device File System,** then **Hardware Information**.
  + There are more options available that can be used to Take Snapshot, Schedule, get Notifications and Logging that can be used if and when required.
  + Click on **Save** to save the task and run the diagnostics.



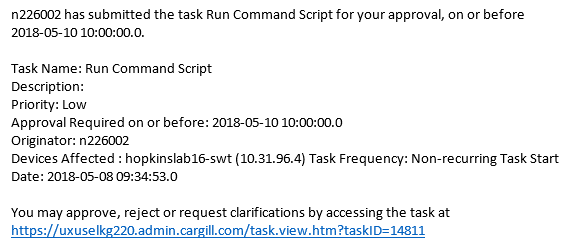




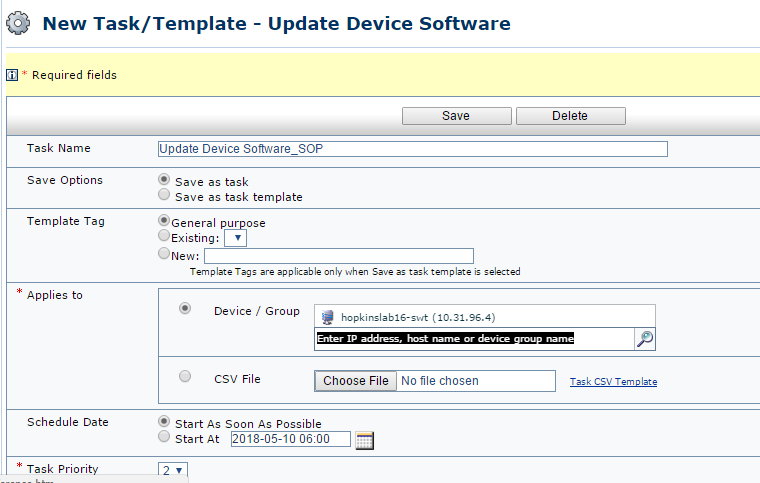
## 5.4 Running the Update Device Software Task

* + Log into HPNA with your DS ID (<https://hpna.admin.cargill.com/> )
  + On top bar, click on Tasks 🡺 New Tasks 🡺 Update Device Software
  + Give the **Task Name** (include the CRQ or INC number if possible)
  + In **Applies To**, select **Device/Group** that you want to run this update for. To select all, choose Inventory. Here, single device is selected.
  + Choose appropriate **Task Priority**. 1 being the highest.
  + Under **Task Options**, check **Session log** if you want to have detailed log generated.
  + Use **Force Save** if needed.
  + Let the **Run Mode** be set as parallel.
  + HPNA will detect an **image set** automatically, if not, please select one.
  + Under the **Deployment Table**, Run a new **file system diagnostic** to update the total, free, and net memory numbers.
  + (Optional) Select from the **preprocessing** and **postprocessing** tasks (for example, the Cisco IOS squeeze command) supported by the device to compact the device memory. These tasks do not remove files from the device. Ensure that sufficient memory will be available for the update.
  + Select files and folders to add to the device by dragging them from the **Software Image Repository** to a file system under **On Device**. (To undo a move, drag the item back to the Software Image Repository.)
  + In the **On Device** area, mark files for special treatment by right-clicking a file name, and then selecting Mark for deletion, **Mark as boot image**, or **Mark as OS image**. (To undo a selection, select Remove marker.)
  + **Summary** will displays the changes to be made.
  + If selected, the **Verify** option verifies images using commands available on the device. The MD5 checksum on the device is compared to the MD5 checksum stored in the database.
  + If NA should **reboot** each device after applying a software update, select the Reboot device after deploying software check box, and then enter the estimated reboot time, otherwise let it be unchecked. Note: Some devices automatically reboot after a software update. This setting does not impact the behavior of those devices.
  + **Estimated Reboot Time** is the maximum time that NA should wait between initiating a device reboot and initiating a snapshot of the updated device configuration.
  + **Estimated Duration,** enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.
  + **Device credentials** options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials
  + **Approval options** are only displayed if the task is part of a **Workflow** Approval Rule. An approval mail will be sent to the Users/Admins who are marked as approvers in the workflow. Mail subject e.g., NA request for approval.

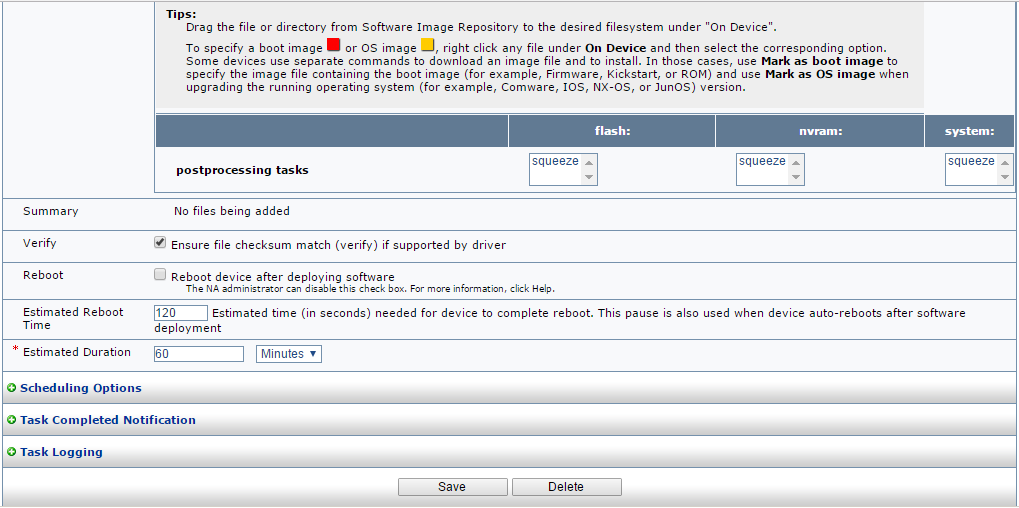
**Please find below an example screenshot of the mail sent to the approver**

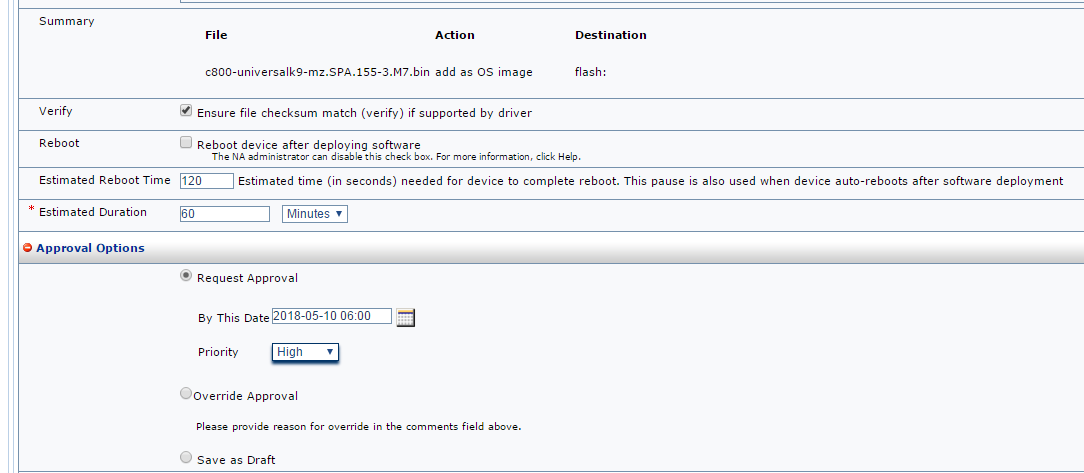


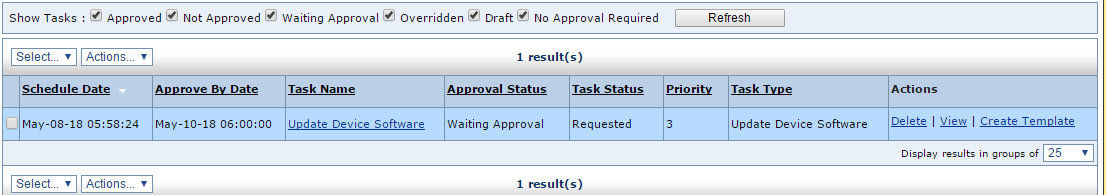
* + **Request Approval** is checked by default if the task needs approval before it can run. **To change the date** by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority
  + If the task allows override, select this option to **override the approval** process. We should use override approval only on test devices or in emergencies.
  + **Save as Draft**, If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
  + You can use **Scheduling Options** to schedule the task for a later time or to run it periodically.
  + If you want NA to send an email message upon task completion, select the Send Email check box under **Task Completed Notification**. Enter a comma-separated list of email addresses to receive the message.
  + **Task Logging**, if available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Note: when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing.
  + Click **Save** to save and run the update task. Note: Snapshot will be taken before and after the Software Update. Status of which task is running will be shown.

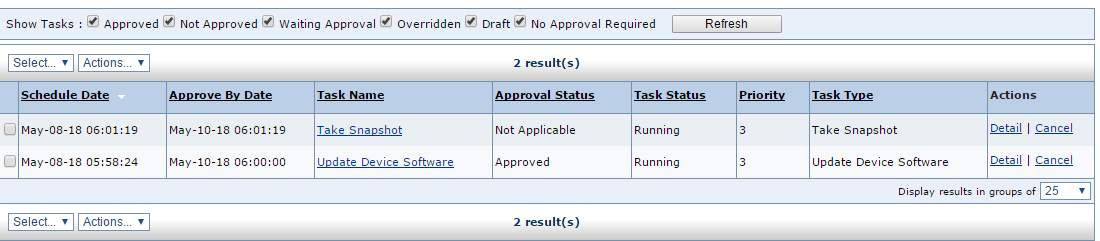












## 5.5 Verify the Process Has Been Executed Successfully

After Update Device Software Task is succeeded and the rebooting of the device is complete,   
we can check in the device form and verify the change of software version.

* + Log into HPNA with your DS ID (<https://hpna.admin.cargill.com/> ) ;
  + Use the search bar to search for the device.
  + In the Device Home View you would be able to verify if the Software Version is changed to the required/upgraded version.

