EXTREME NETWORKS

Verify Governance workflow

Ludovico Stevens

Solutions Engineering

April 2025

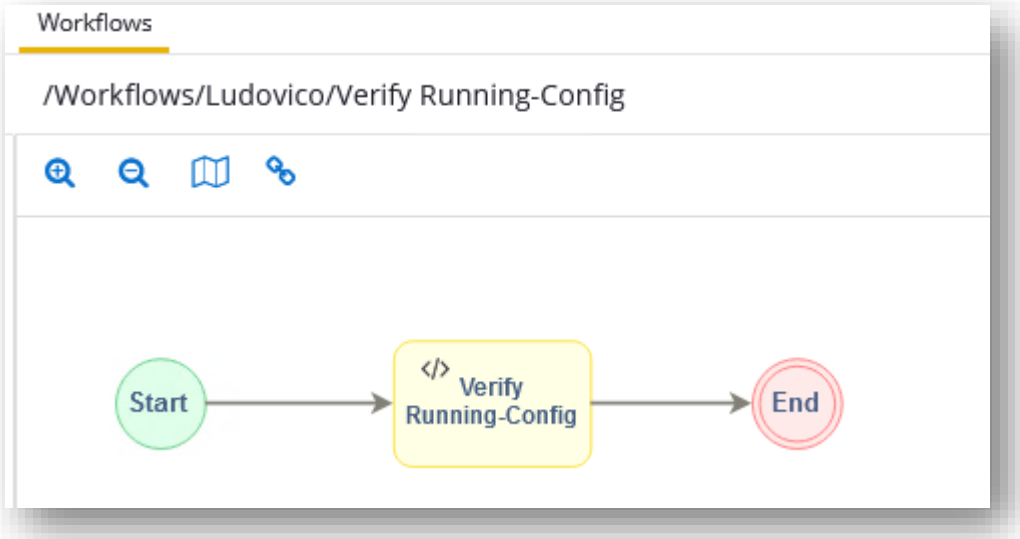
ADVANCE WITH US

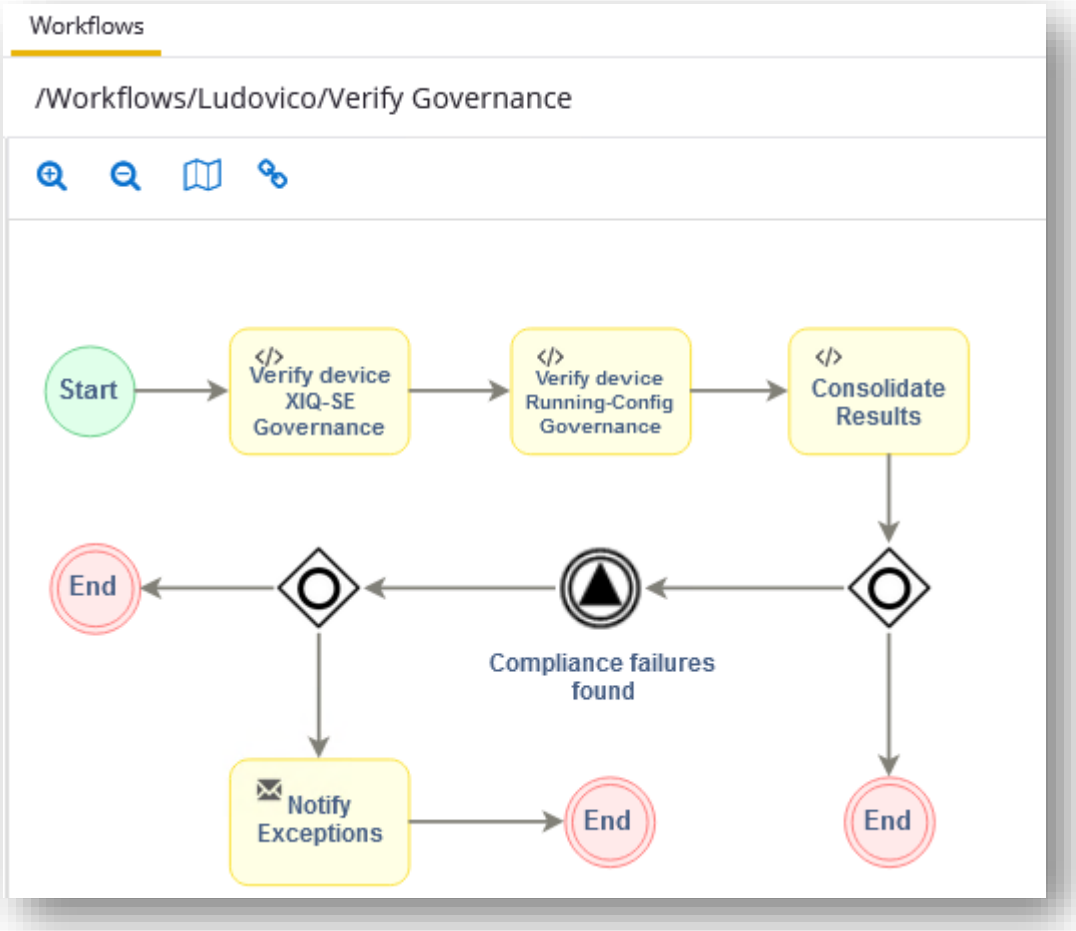
Verify Governance workflow

- **Workflow to validate governance compliance of all devices deployed in CSV file**
- **For each S/N in CSV:**
- Check switch added to XIQ-SE
- Check in right site path
- Check with expected IP
- Check with correct name
- Check XIQ-SE nickname matches
- Check in correct sysLocation (based on site or input)
- Check with correct sysContact (based on site or input)
- Check added to AccessControl
- Check added in right Engine Group
- Check added with correct RADIUS template
- Check added with correct Access Type
- Check added to correct Location Group
- Check added to Policy Domain
- Check added in right domain
- Check added to Policy VLAN Island
- Check in correct VLAN Island
- Child workflow "Verify Running-Config" will be executed to verify grep patterns:
- Check switch config for correct RADIUS servers
- Check switch config for correct RADIUS clients
- Check for custom config patterns in running config (these patterns support remediation)

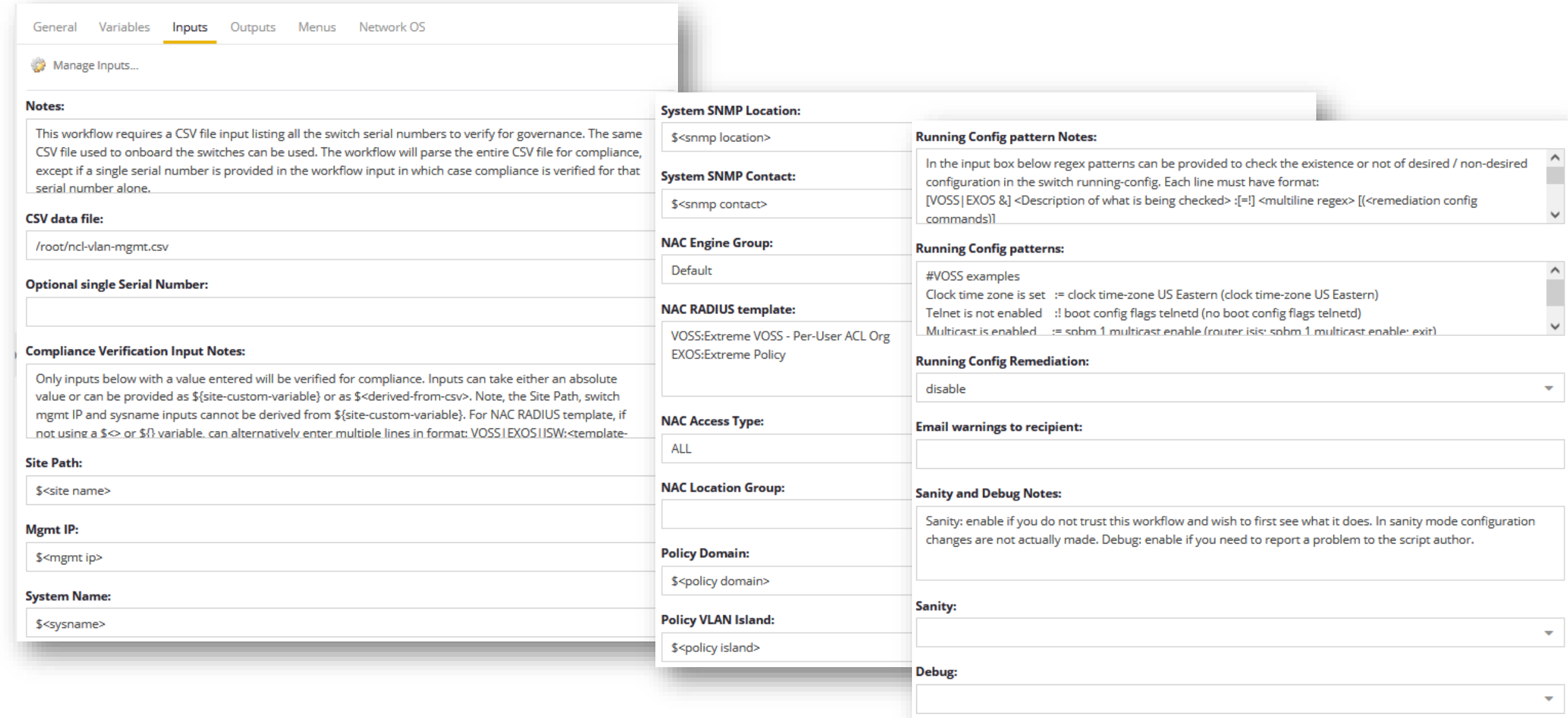
Verify Governance workflow & Verify Running-Config workflow

- Two workflows go hand in hand
- **Verify Governance workflow** is the main “parent” workflow that you run. This workflow reads the CSV file and performs XIQ-SE checks for every device in the CSV file. It then executes 1 or more instances of the “child” **Verify Running-Config workflow** to make checks in the device config file and consolidates all results.
- The **Verify Governance workflow** will not run unless the **Verify Running-Config workflow** is also installed.
- The **Verify Running-Config workflow** can also be used independently to just validate config elements on 1 or more devices.





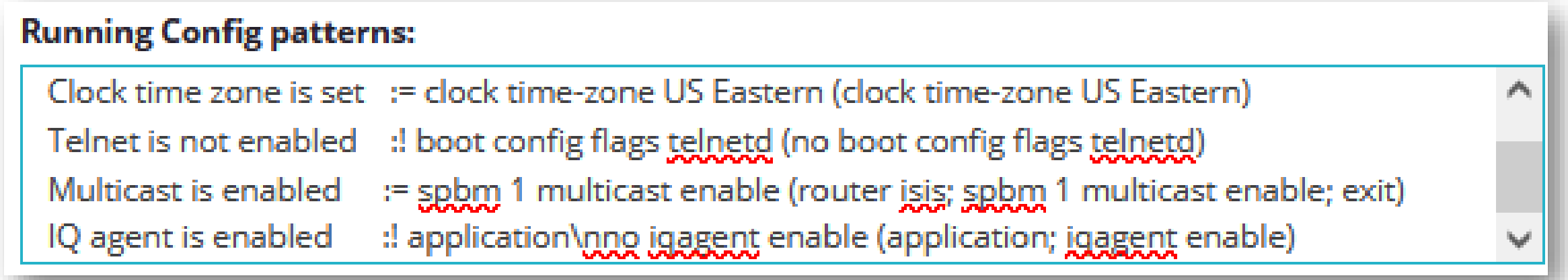
Workflow inputs



Workflow inputs

- This workflow requires a CSV file input listing all the switch serial numbers to verify for governance. The same CSV file used to onboard the switches can be used. The workflow will parse the entire CSV file for compliance, except if a single serial number is provided in the workflow input in which case compliance is verified for that serial number alone.
- Only inputs below with a value entered will be verified for compliance. Inputs can take either an absolute value or can be provided as ${site-custom-variable} or as $<derived-from-csv>. Note, the Site Path, switch mgmt IP and sysname inputs cannot be derived from ${site-custom-variable}. For sysLocation and sysContact if the input value is "ztp" then the device sysLocation and sysContact are checked against the device's site sysLocation and sysContact. For NAC RADIUS template, if not using a $<> or ${} variable, can alternatively enter multiple lines in format: VOSS|EXOS|ISW:<template-name>

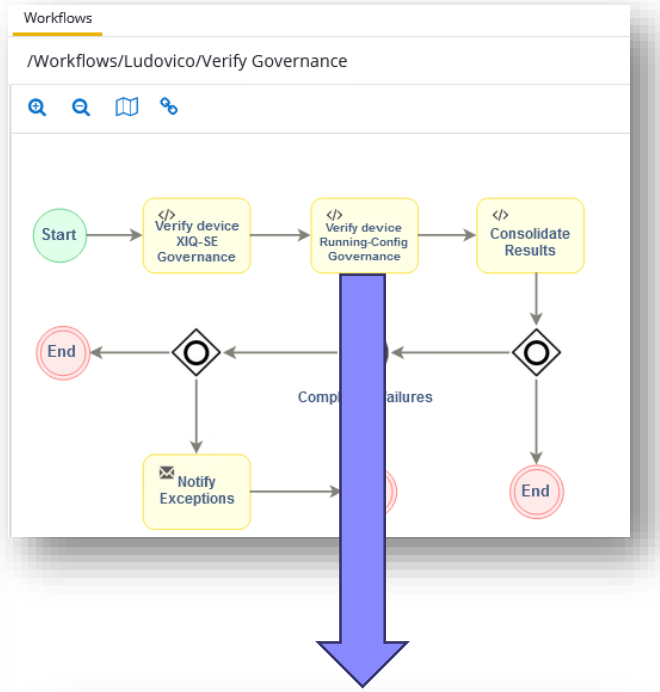
Workflow Running Config patterns input



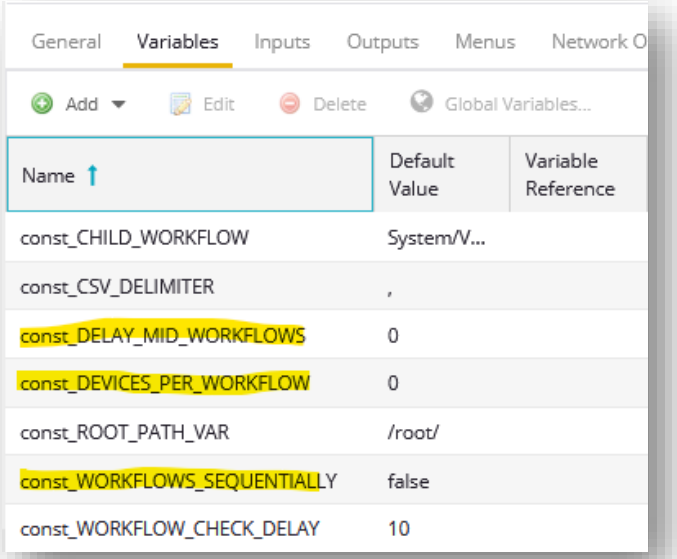
- The input box Running Config patterns allows to check the existence or not of desired / non-desired configuration in the switch running-config. Each line must have format:
  - [VOSS|EXOS &] <Description of what is being checked> :[=!] <multiline regex> [(<remediation config commands)]
  - Default examples shown above
- The VOSS/EXOS keys, if provided must be followed by "&"; this allows a pattern to be checked for VOSS or EXOS only, if the workflow is parsing both family types in the CSV file.
- If "**:=**" is used, the pattern is expected to be found whereas if "**:!**" is used then the pattern is expected not to be found. A warning is generated for the patterns when the expectations are found to be false.
- If remediation is required, the necessary config command(s) can be appended inside brackets (). If too many entries are required in this input box, a file path on XIQ-SE file system may be provided instead.

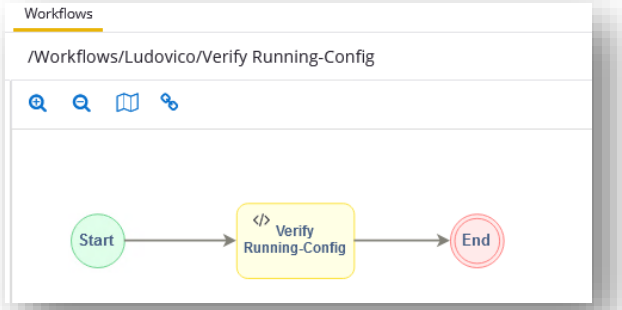
Tuning child workflow execution in scaled environments

- What if there are hundreds or thousands of switches in the CSV ?
- Normally, the parent **Verify Governance workflow** will run one instance of the child **Verify Running-Config workflow** against all switches.
- If you run a workflow against, say 20, switches, what XIQ-SE does is that it will run it for the 1st 10 switches, and once these have completed, it will run for the other 10.
- If you run 2 workflows, one against 10 switches and the other against 10 switches, they all run at the same time. So faster, but.. I might not want to push this too far…
- The number of child workflow instances can be controlled via variables:

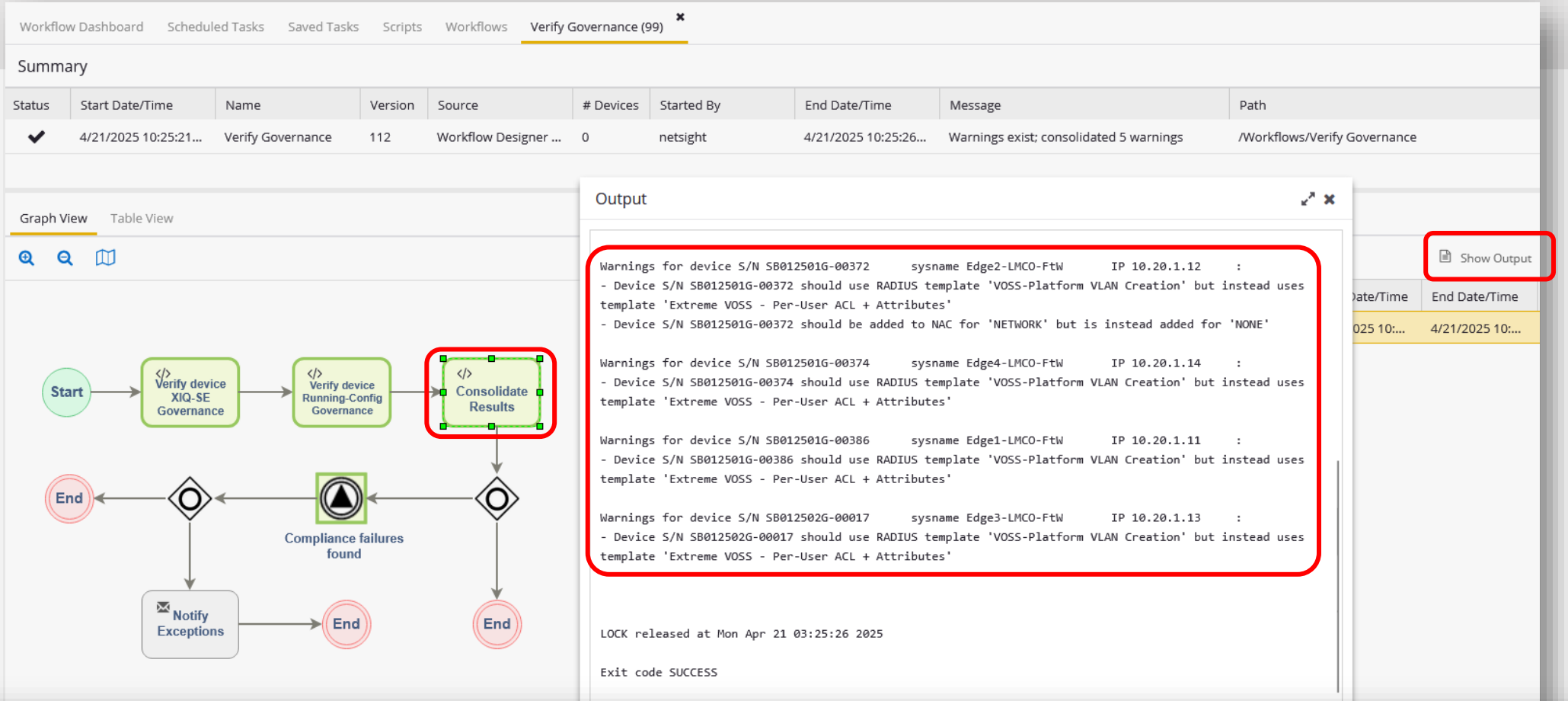


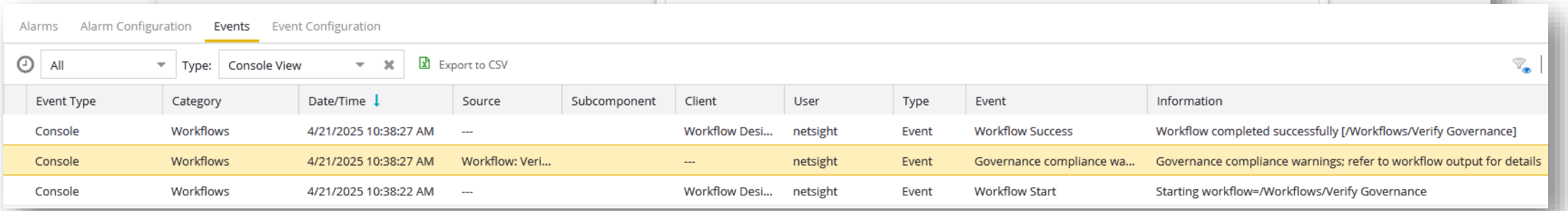
- If DEVICES_PER_WORKFLOW = 0, then it will run 1 child workflow against all the switches which are listed in the CSV. It will go through all switches in batches of 10 as described above.
- If you set DEVICES_PER_WORKFLOW=10, it will run a number of child workflows (number of switches in CSV / 10) all at the same time, each against 10 switches.
- If you want to stagger them, you can provide a non-zero value for DELAY_MID_WORKFLOW, but they can still overlap, depending on how this timer compares to execution time.
- If you want them to run sequentially, without overlapping at all, you set WORKFLOWS_SEQUENTIALLY to true.





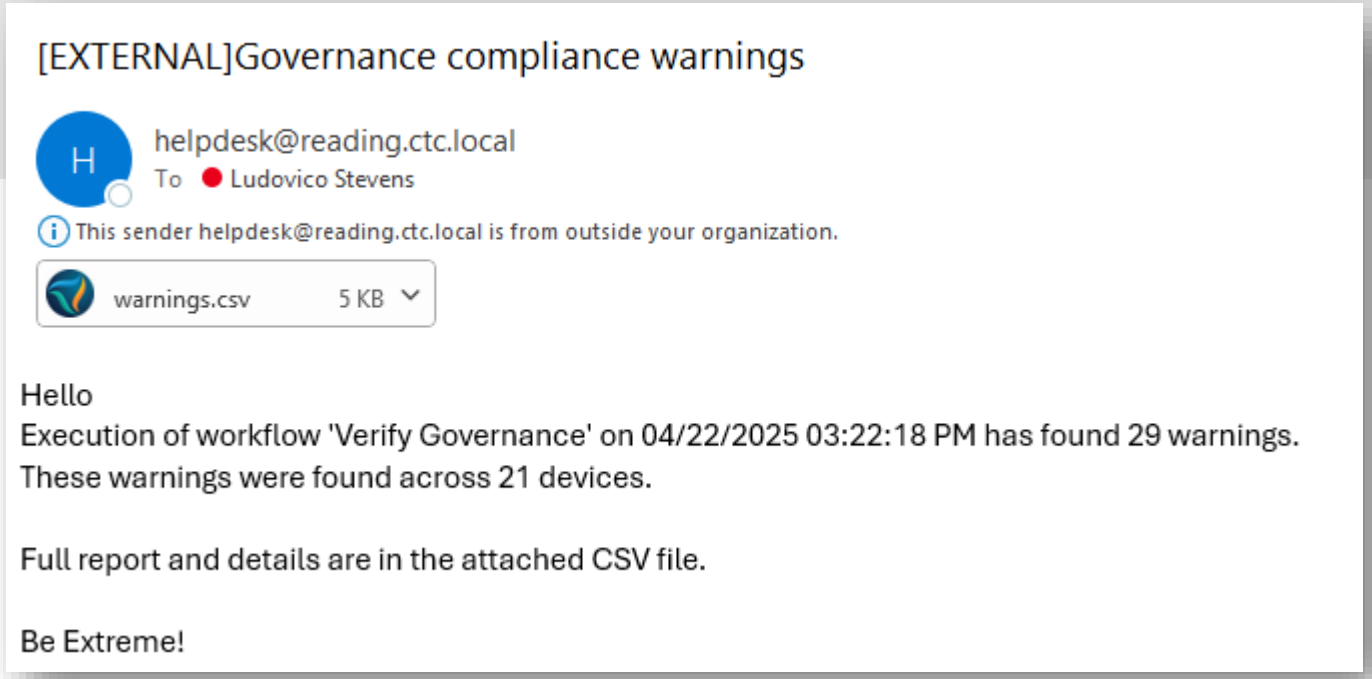
After workflow execution





Workflow email report

- If an email address is provided and warnings are detected, an email will be sent, with a CSV file attachment detailing all the warnings



[EXTERNAL]Governance compliance warnings

H helpdesk@reading.ctc.local
To Ludovico Stevens

This sender helpdesk@reading.ctc.local is from outside your organization.

warnings.csv 5 KB

Hello
Execution of workflow 'Verify Governance' on 04/22/2025 03:22:18 PM has found 29 warnings.
These warnings were found across 21 devices.

Full report and details are in the attached CSV file.

Be Extreme!

File Edit Data Selection Find View Tools Go To Preferences Contact Us Help warnings.csv - Modern CSV (Free)

warnings.csv ×

	0	1	2	3	4
0	S/N	Sysname	IP	Warning	Remediation
1	SB012501G-00372	Edge2-LMCO-FtW	10.20.1.12	Device S/N SB012501G-00372 should use RADIUS template 'VOSS-Platform VLAN Creation' but instead uses template 'Extreme ...	
2	SB012501G-00372	Edge2-LMCO-FtW	10.20.1.12	Device S/N SB012501G-00372 should be added to NAC for 'NETWORK' but is instead added for 'NONE'	
3	SB012501G-00374	Edge4-LMCO-FtW	10.20.1.14	Device S/N SB012501G-00374 should use RADIUS template 'VOSS-Platform VLAN Creation' but instead uses template 'Extreme ...	
4	SB012501G-00386	Edge1-LMCO-FtW	10.20.1.11	Device S/N SB012501G-00386 should use RADIUS template 'VOSS-Platform VLAN Creation' but instead uses template 'Extreme ...	
5	SB012502G-00017	Edge3-LMCO-FtW	10.20.1.13	Device S/N SB012502G-00017 should use RADIUS template 'VOSS-Platform VLAN Creation' but instead uses template 'Extreme ...	
6					

6 rows x 5 columns Selected: 1 cell Cell Length: 3 Filters: none Delimiter: comma (,) UTF-8 CRLF Editable