

Deployment Guide

NetMRI Policy Deployment Guide



Table of Contents

Introduction	2
Prerequisites	2
PCI compliance	2
DISA-STIG Compliance	13
Auto Device Remediation	19
Testing the triggered job by changing a device configuration manually	29
Device CVE/PSIRT - Advisor	35
Device Life Cycle Management	44

Introduction

This deployment guide will show you how to use the NetMRI policy feature to analyze the discovered intermediary device (ie routers, switches, firewalls, etc) configurations for any policy violations like PCI (payment card industry), DISA STIG (Defense Information Systems Agency Security Technical Information Guides), and CVE/PSIRT (Common Vulnerabilities and Exposures/Product Security Incident Response Team) violations. In addition, this deployment guide will show how to configure NetMRI to auto remediate any misconfigurations and provide life cycle management information on the discovered devices.

Rules and Policy

The NetMRI Policy Design Center provides you with the ability to test the configuration of devices in your network against a specific set of rules and identify where the device does not comply with those rules. **Rules** are the individual tests and are grouped into a set called a **Policy**. Policies are deployed to analyze one or more Device Groups in the NetMRI system (see the topic “Introducing Device Groups” in the Infoblox NetMRI Administrator Guide, Part 3 Device and Network Exploration, Devices & Interfaces for more information on Device Groups.)

Rules are written in one of three forms: A Simple Rule looks for configuration statements that are required to be present and/or are required to be absent in the device's configuration. A Rule Logic Builder rule combines several tests and combines their evaluation with logical operators like AND, OR, NOT, etc. These two rule types are stored internally as XML documents, so the third way to write rules is directly in XML. Consult the Infoblox NetMRI Administrator Guide, Part 5 Network Compliance for more details.

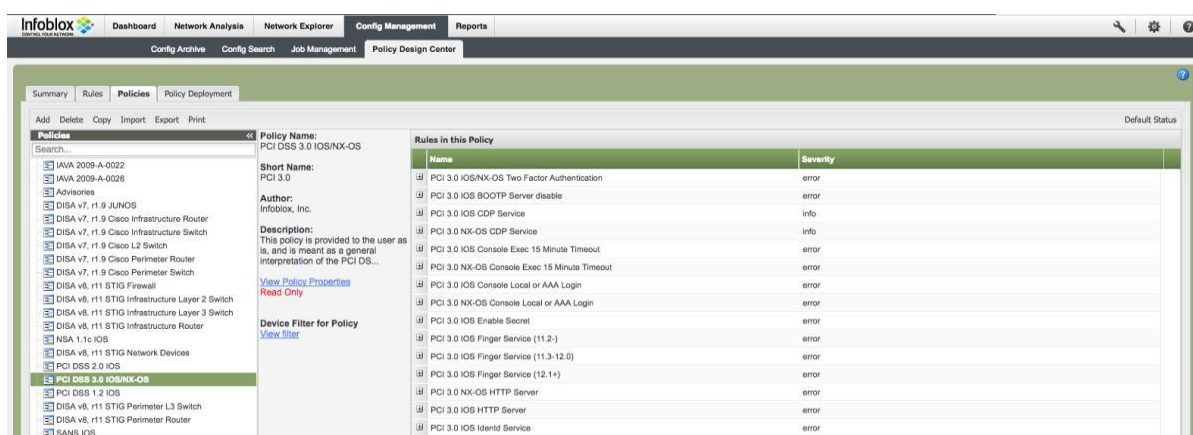
Prerequisites

- The NetMRI appliance must be configured to discover the required devices.
- The discovered devices have been placed into the default device groups or user-created device groups.
- Mail server settings are configured.
- The NetMRI appliance must have a backup of the discovered devices' configuration files.
- In the deployment sections, lab devices are used as examples to illustrate the features

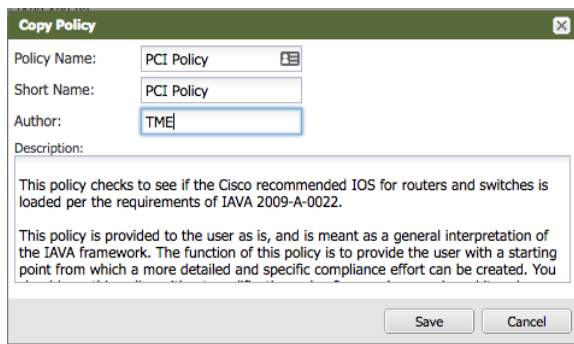
PCI compliance

If you have an enterprise network where credit card information traffic flows through it, then you must adhere to a **version of the PCI DSS** standards. NetMRI has built-in policies for PCI **DSS** compliance. The following instructions show you how to implement PCI policies. The predefined policies are examples built mainly for Cisco and Juniper. For other vendors you may need to create additional rules following the given examples.

1. Navigate to Config Management → Policy Design Center → Policies → PCI DSS 3.0 IOS/NX-OS.

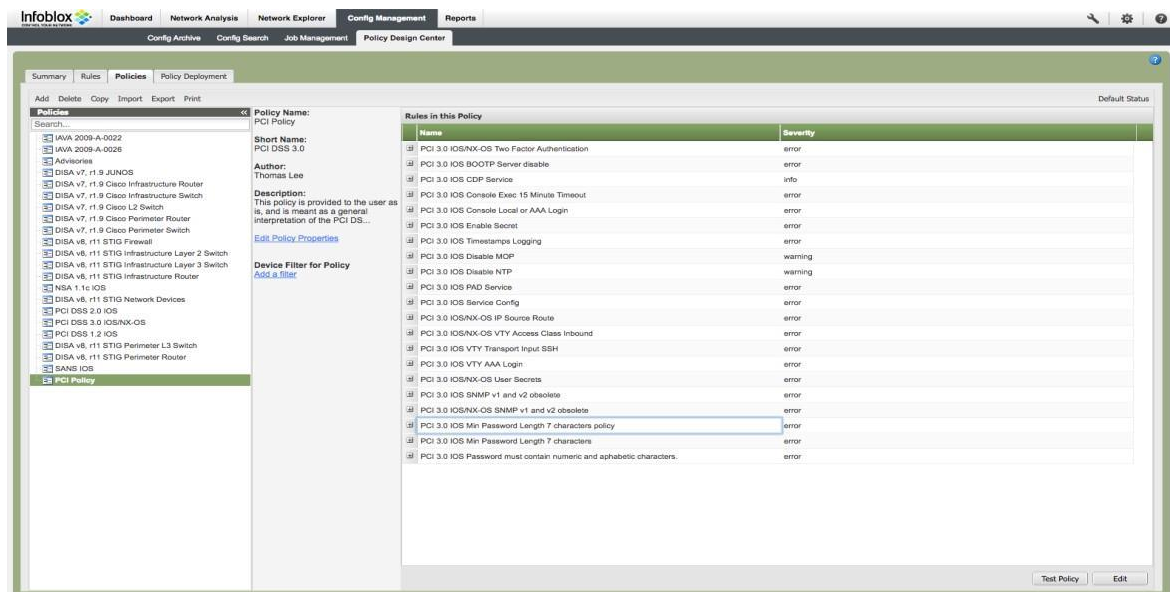


2. Make sure the PCI 3.0 policy is highlighted. Click on the Copy button to copy this default policy to a user created policy. Fill out the Policy Name, Short Name (max Short Name length is 12 characters), and Author. Click Save.



The 'Copy Policy' dialog box is shown. It has fields for 'Policy Name', 'Short Name', and 'Author'. The 'Policy Name' field contains 'PCI Policy'. The 'Short Name' field contains 'PCI Policy'. The 'Author' field contains 'TME'. There is a 'Description' text area with the following text: 'This policy checks to see if the Cisco recommended IOS for routers and switches is loaded per the requirements of IAVA 2009-A-0022. This policy is provided to the user as is, and is meant as a general interpretation of the IAVA framework. The function of this policy is to provide the user with a starting point from which a more detailed and specific compliance effort can be created. You'. At the bottom are 'Save' and 'Cancel' buttons.

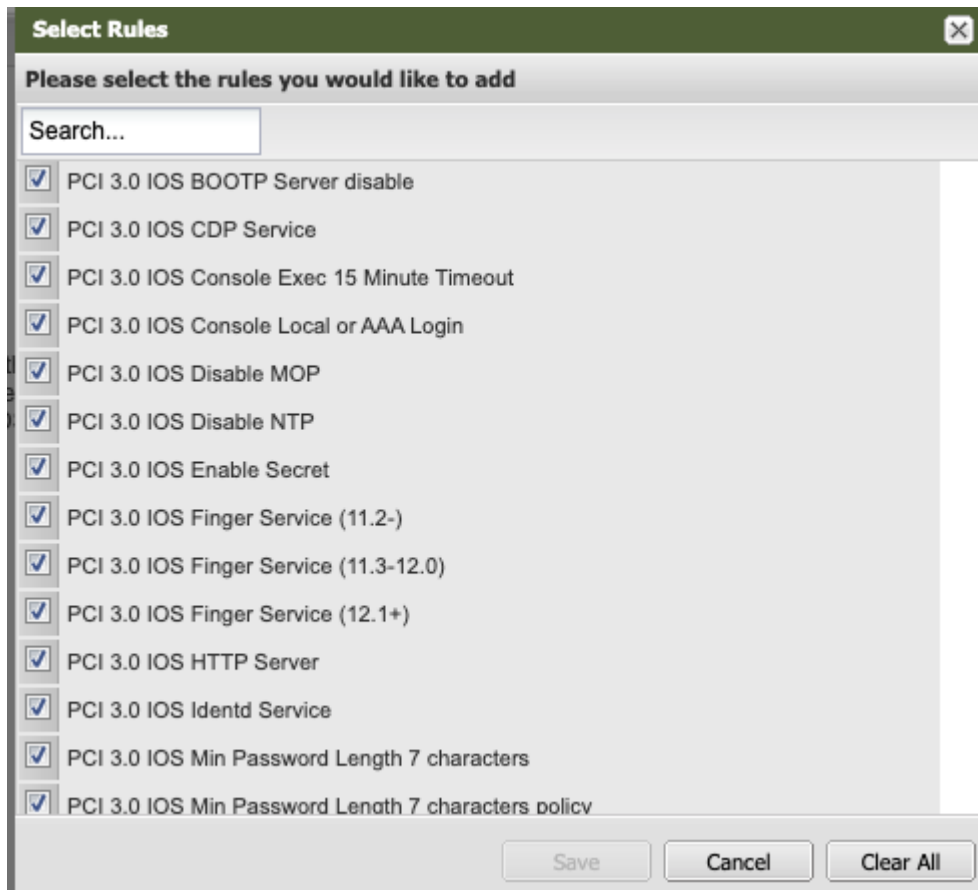
3. Highlight the newly created Filter policy called PCI Policy.



The Infoblox Policy Design Center interface is shown. The 'Policies' tab is selected. On the left, a list of policies is shown, with 'PCI Policy' highlighted. On the right, the details for 'PCI Policy' are shown. The 'Policy Name' is 'PCI Policy', the 'Short Name' is 'PCI DSS 3.0', and the 'Author' is 'Thomas Lee'. The 'Description' is: 'This policy is provided to the user as is, and is meant as a general interpretation of the PCI DSS...'. Below the description is a 'Device Filter for Policy' section with a link to 'Add a Filter'. On the right, a table titled 'Rules in this Policy' lists various rules with their names and severities.

Name	Severity
PCI 3.0 IOS/NX-OS Two Factor Authentication	error
PCI 3.0 IOS BOOTP Server disable	error
PCI 3.0 IOS CDP Service	info
PCI 3.0 IOS Console EXEC 15 Minute Timeout	error
PCI 3.0 IOS Console Local or AAA Login	error
PCI 3.0 IOS Enable Secret	error
PCI 3.0 IOS Timestamp Logging	error
PCI 3.0 IOS Disable MOP	warning
PCI 3.0 IOS Disable NTP	warning
PCI 3.0 IOS PAD Service	error
PCI 3.0 IOS Service Config	error
PCI 3.0 IOS/NX-OS IP Source Route	error
PCI 3.0 IOS/NX-OS VTY Access Class Inbound	error
PCI 3.0 IOS VTY Transport Input SSH	error
PCI 3.0 IOS VTY AAA Login	error
PCI 3.0 IOS/NX-OS User Secrets	error
PCI 3.0 IOS SNMP v1 and v2 obsolete	error
PCI 3.0 IOS/NX-OS SNMP v1 and v2 obsolete	error
PCI 3.0 IOS Min Password Length 7 characters policy	error
PCI 3.0 IOS Min Password Length 7 characters	error
PCI 3.0 IOS Password must contain numeric and alphabetic characters.	error

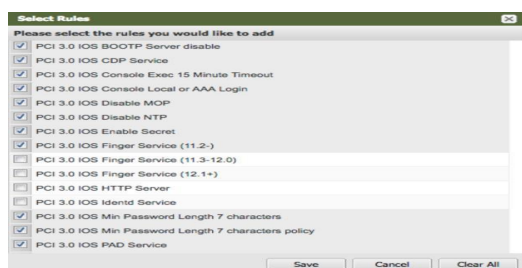
4. Click on the Edit button on the lower right corner of the screen to edit this policy and the following screen appears:



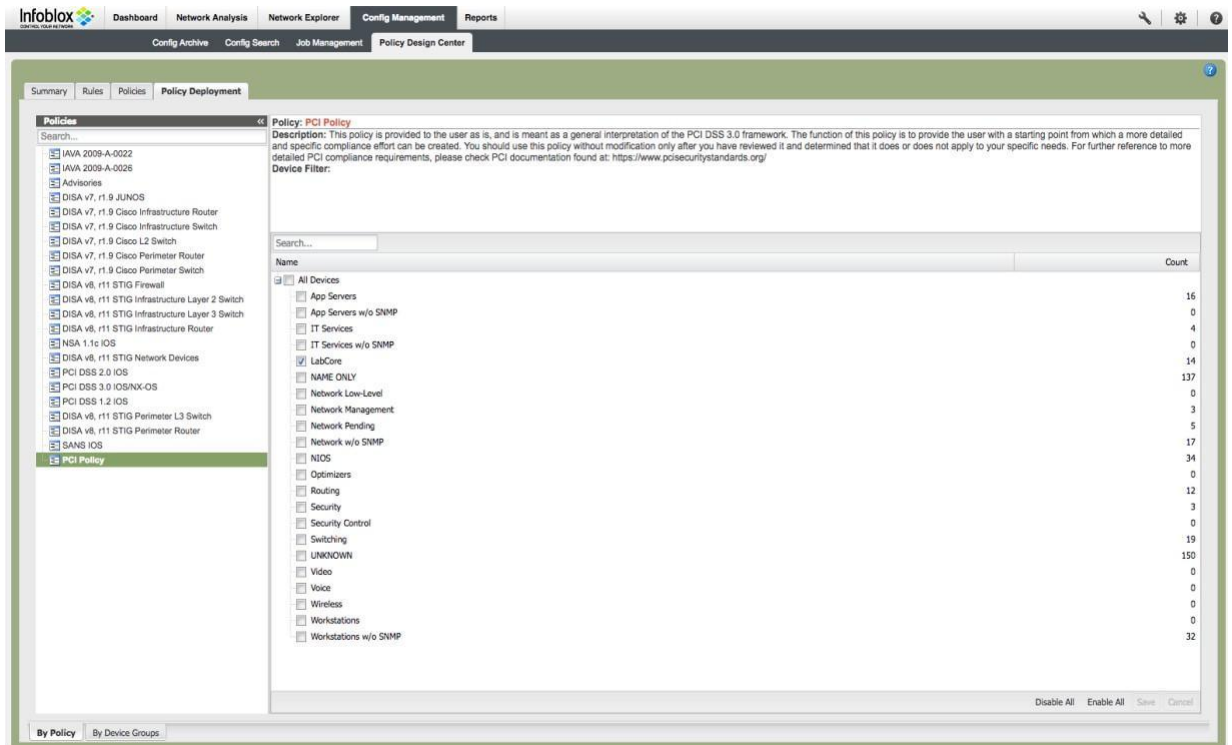
5. Select the rules that you want to add or not by clicking on the check box. Click Save. Note: To familiarize yourself with this feature, you can choose any number of the rules below for your Cisco IOS devices:
 - a. PCI 3.0 IOS BOOTP Server disable
 - b. PCI 3.0 IOS CDP Service
 - c. PCI 3.0 IOS HTTP Server
 - d. PCI 3.0 IOS Min Password Length 7 characters

If you have Cisco NX-OS devices, you can choose any number of the rules below:

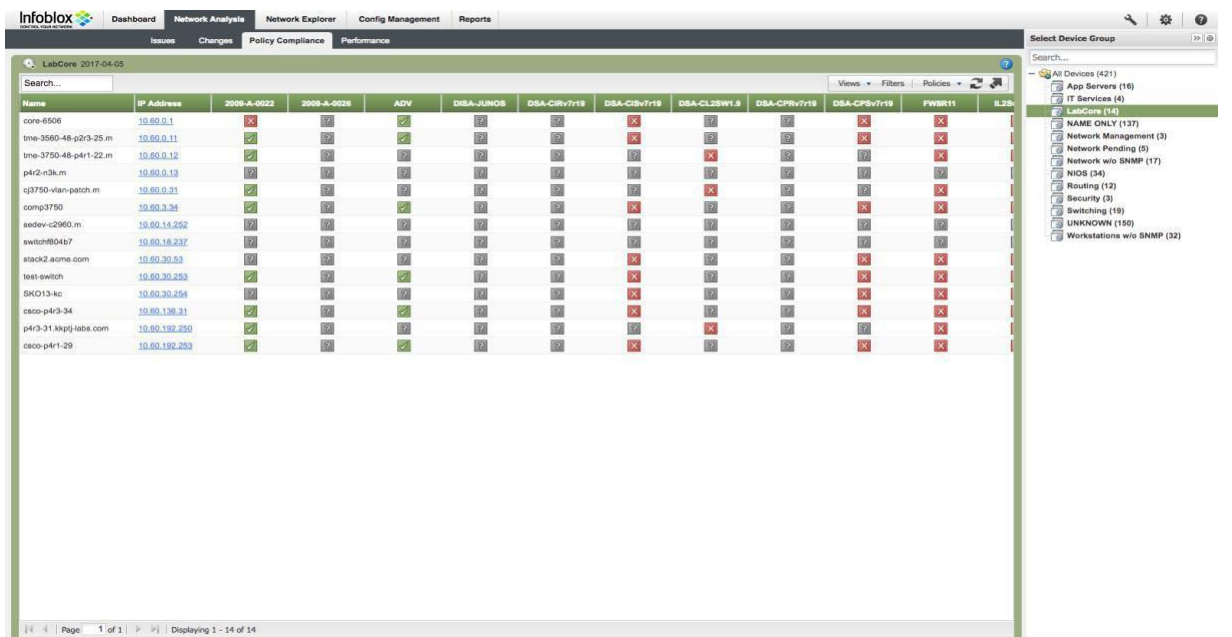
- a. PCI 3.0 IOS/NX-OS SNMP v1 and v2 obsolete
- b. PCI 3.0 NX-OS CDP Service
- c. PCI 3.0 NX-OS Disable NTP
- d. PCI 3.0 NX-OS HTTP Server



- Click on the Policy Deployment tab to deploy the policy to the chosen device group. Notice the LabCore device group is selected. The LabCore device group is a user-defined device group and is used as an example. The Save button will be ungrayed when a change is detected. Click Save if needed.



- Navigate to Network Analysis → Policy Compliance. By default, all deployed policies will be displayed for the selected device group. The status on the Policy Compliance screen will be 'Deployed' after initially deploying a policy and the status will only update when analysis is complete. It may take a few minutes before the newly created policy returns data.



- Click on the Policies drop down menu to select the PCI Policy.

The screenshot shows the Infoblox Network Analyst interface. The 'Policy Compliance' tab is active. A table lists various devices and their compliance status across different policy frameworks. A dropdown menu is open, showing a list of policies. The 'PCI Policy' is selected at the bottom of the list.

Name	IP Address	2009-A-0022	2009-A-0026	ADV	DISA-JUNOS	DISA-CISv7r19	DISA-CISv7r19	DISA-CL2SW1.9	DISA-CPRv7r19	DISA-CPRv7r19
core-6506	10.60.0.1	X	?	?	?	?	?	?	?	?
lme-3560-48-p2r3-25.m	10.60.0.11	?	?	?	?	?	?	?	?	?
lme-3750-48-p4r1-22.m	10.60.0.12	?	?	?	?	?	?	?	?	?
p4r2-r3k.m	10.60.0.13	?	?	?	?	?	?	?	?	?
q3750-vlan-patch.m	10.60.0.31	?	?	?	?	?	?	?	?	?
comp3750	10.60.3.34	?	?	?	?	?	?	?	?	?
sedev-c2960.m	10.60.14.252	?	?	?	?	?	?	?	?	?
switch#04b7	10.60.18.237	?	?	?	?	?	?	?	?	?
stack2.acme.com	10.60.30.53	?	?	?	?	?	?	?	?	?
test-switch	10.60.30.253	?	?	?	?	?	?	?	?	?
SKO13-ic	10.60.30.254	?	?	?	?	?	?	?	?	?
cisco-p4r3-34	10.60.136.31	?	?	?	?	?	?	?	?	?
p4r3-31.kkpg-labs.com	10.60.192.250	?	?	?	?	?	?	?	?	?
cisco-p4r1-29	10.60.192.253	?	?	?	?	?	?	?	?	?

Policy: PCI Policy
Description: This policy is provided to the user as is, and is meant as a general interpretation of the PCI DSS 3.0 framework. The function of this policy is to provide the user with a starting point from which a more detailed and specific compliance effort can be created. You should use this policy without modification only after you have reviewed it and determined that it does or does not apply to your specific needs. For further reference to more detailed PCI compliance requirements, please check PCI documentation found at: <https://www.pcisecuritystandards.org/>

- The following should appear.

The screenshot shows the Infoblox Network Analyst interface. The 'Policy Compliance' tab is active. The 'PCI Policy' is selected, and the table displays compliance results for various devices across different policy frameworks.

Name	IP Address	IOS-AAR-033	IOS-BTP-031	IOS-CDP-031	IOS-CON-035	IOS-CON-036	IOS-ENA-031	IOS-LOG-032	IOS-NMOP-031	IOS-NTP-038	IOS-PAD-031	IOS-PAD-031
core-6506	10.60.0.1	X	X	X	?	?	?	?	?	?	?	?
lme-3560-48-p2r3-25.m	10.60.0.11	X	X	X	?	?	?	?	?	?	?	?
lme-3750-48-p4r1-22.m	10.60.0.12	X	X	X	?	?	?	?	?	?	?	?
q3750-vlan-patch.m	10.60.0.31	X	X	X	?	?	?	?	?	?	?	?
comp3750	10.60.3.34	X	X	X	?	?	?	?	?	?	?	?
stack2.acme.com	10.60.30.53	X	X	X	?	?	?	?	?	?	?	?
test-switch	10.60.30.253	X	X	X	?	?	?	?	?	?	?	?
SKO13-ic	10.60.30.254	X	X	X	?	?	?	?	?	?	?	?
cisco-p4r3-34	10.60.136.31	?	X	X	?	?	?	?	?	?	?	?
p4r3-31.kkpg-labs.com	10.60.192.250	X	X	X	?	?	?	?	?	?	?	?
cisco-p4r1-29	10.60.192.253	?	X	X	?	?	?	?	?	?	?	?

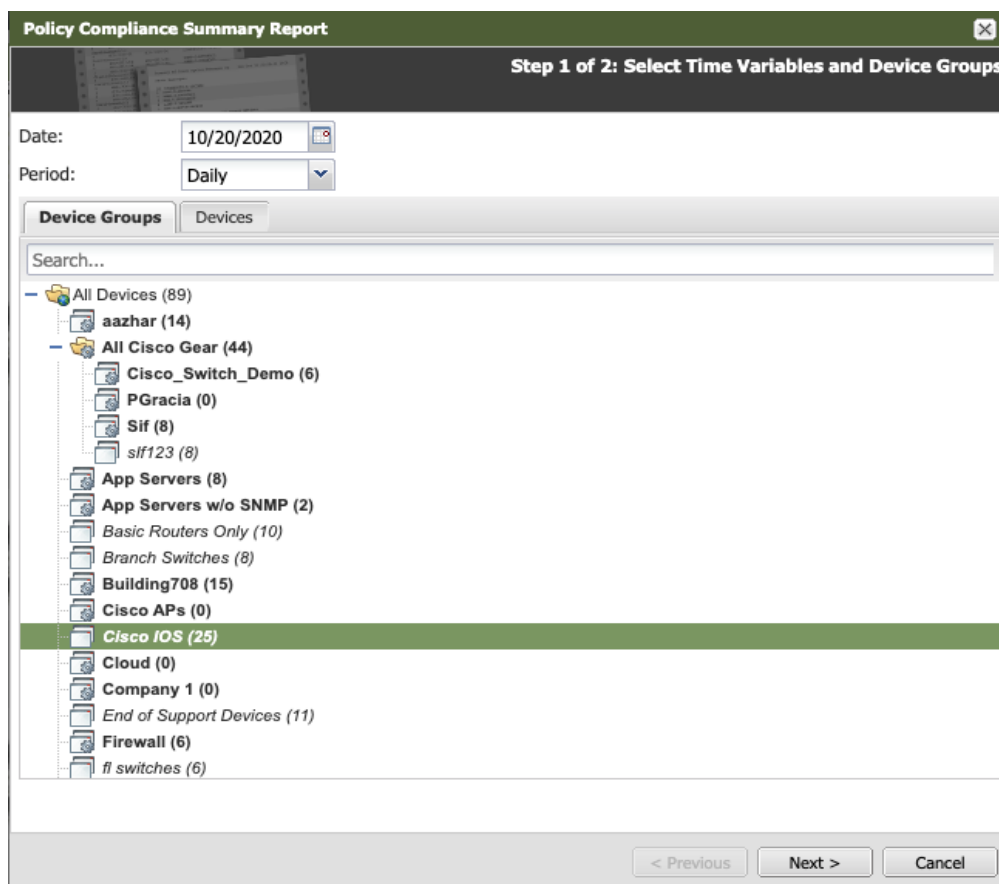
10. You can move the mouse over to any of the colored boxes to get detailed information of the policy analysis or you can click on any of the boxes to get more detail in a new window.. Here is a legend of the various colored boxes:

- a. Red X: Error
- b. Blue X: Info
- c. Yellow X: Warning
- d. Green ✓: Pass

11. To run a report navigate to Reports → Report Gallery and move the mouse pointer over the Policy Compliance Summary report.



12. Click on the 'Run' link. Select the device group and then click on the 'Next' button.



13. Select the policies that you want to run by highlighting the selected policy and clicking on the right arrow. Click on the 'Run' button.

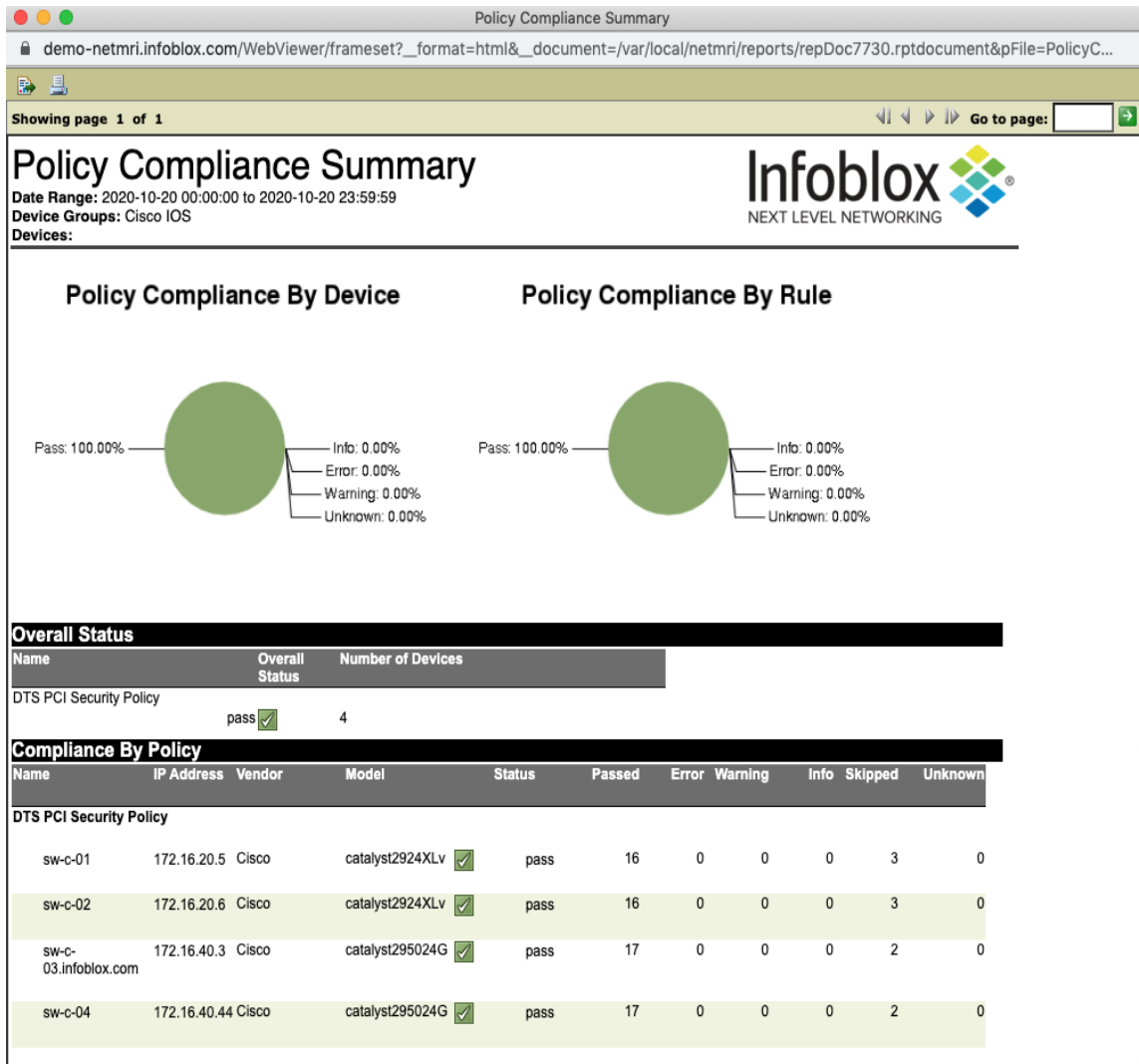
Policy Compliance Summary Report [X]

Step 2 of 2: Select Policies

Policies	Selected Policies	Clear
<ul style="list-style-type: none">● DISA v7, r1.9 JUNOS● DISA v8, r20 STIG Firewall● DISA v8, r20 STIG Infrastructure Layer 2 Switch● DISA v8, r20 STIG Network Devices● DISA v8, r21 STIG Infrastructure Layer 3 Switch● DISA v8, r21 STIG Infrastructure Router● DISA v8, r23 STIG Perimeter L3 Switch● DISA v8, r23 STIG Perimeter Router● DTS Operations Policy● DTS PCI Security Policy● DTS Sample Rules● enable● External Logging● Global Policy● Grego● HoR IOS Blocked End Host● Hostname policy bdb● IAVA 2009-A-0022● IAVA 2009-A-0026● IB_10127 High CVE-2018-5743● IB_10472 High CVE-2018-10239● IB_10531 Low CVE-2019-6469● IB_10622 High CVE-2019-11477● IB_10622 Med CVE-2019-11478	<ul style="list-style-type: none">● DTS PCI Security Policy	

< Previous Run Cancel

14. The report will show on the screen. At the upper left of the screen, you can choose to download the report in PDF, Excel, or MS Word format in addition to printing the report.



- Click on the schedule button under the Policy Comp[liance Summary report to schedule the report. Select the device group. Click Next.

Policy Compliance Summary Report

Step 1 of 4: Select Time Variables and Device Groups

Date:10/20/2020

Period:Daily

Device Groups

Devices

Search...

All Devices (89)

aazhar (14)

All Cisco Gear (44)

Cisco_Switch_Demo (6)

PGracia (0)

Sif (8)

sif123 (8)

App Servers (8)

App Servers w/o SNMP (2)

Basic Routers Only (10)

Branch Switches (8)

Building708 (15)

Cisco APs (0)

Cisco IOS (25)

Cloud (0)

Company 1 (0)

End of Support Devices (11)

Firewall (6)

fl switches (6)

< Previous

Next >

Cancel

16. Select the policies that you want to run by highlighting the selected policy and clicking on the right arrow. Click on the 'Next' button.

Policy Compliance Summary Report Step 2 of 4: Select Policies

Policies

- DISA v7, r1.9 JUNOS
- DISA v8, r20 STIG Firewall
- DISA v8, r20 STIG Infrastructure Layer 2 Switch
- DISA v8, r20 STIG Network Devices
- DISA v8, r21 STIG Infrastructure Layer 3 Switch
- DISA v8, r21 STIG Infrastructure Router
- DISA v8, r23 STIG Perimeter L3 Switch
- DISA v8, r23 STIG Perimeter Router
- DTS Operations Policy
- DTS PCI Security Policy
- DTS Sample Rules
- enable
- External Logging
- Global Policy
- Grego
- HoR IOS Blocked End Host
- Hostname policy bdb
- IAVA 2009-A-0022
- IAVA 2009-A-0026
- IB_10127 High CVE-2018-5743
- IB_10472 High CVE-2018-10239
- IB_10531 Low CVE-2019-6469
- IB_10622 High CVE-2019-11477
- IB_10622 Med CVE-2019-11478

Selected Policies Clear

DTS PCI Security Policy

< Previous Next > Cancel

17. Enter the email address of the destination of this report. Click Next.

Policy Compliance Summary Report Step 3 of 4: Select Report Scheduling

Report Name: Policy Compliance Summary

To Emails:

To Users: InfobloxTest InfobloxTest ()
Japan tokyo ()
MohammadTest MohammadTest ()
NETMRISPT-4456 NETMRISPT-4456 ()
Ahmad Abou Zaher (aabouzaher@infoblox.com)

Output Format: pdf

Recurrence Pattern: Weekly

Execution Time: 6:00 AM

☐ Sunday ☐ Tuesday ☐ Thursday ☐ Saturday
☒ Monday ☐ Wednesday ☐ Friday

< Previous Next > Cancel

18. Verify the settings of the scheduled report. If configurations are correct, click Schedule.

Policy Compliance Summary Report

Step 4 of 4: Summary of Scheduled Report

Report Name:	Policy Compliance Summary
Date:	10/20/2020
Period:	Daily
Device Groups:	Cisco IOS
Devices:	
Policies:	DTS PCI Security Policy
To Emails:	
To Users:	715
Schedule:	Weekly - Monday at 06:00 AM

< Previous

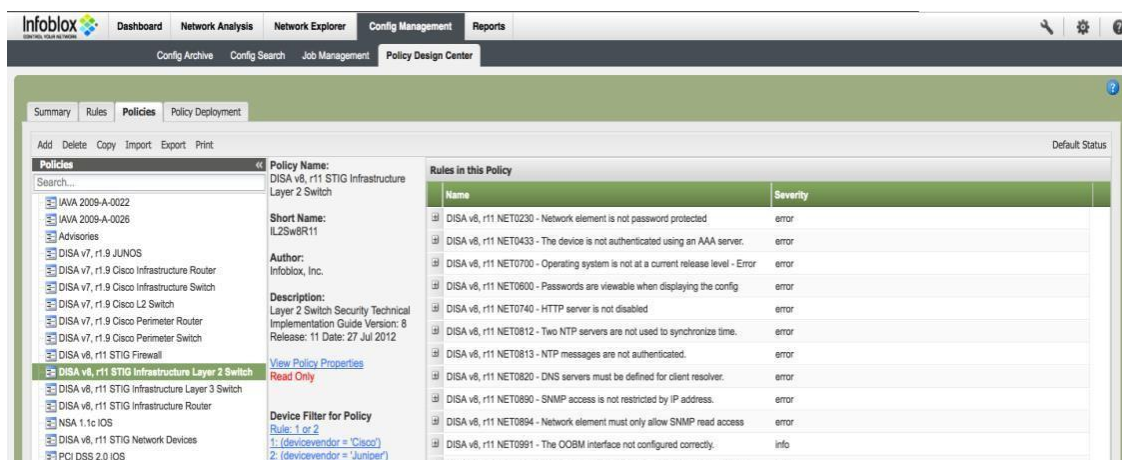
Schedule

Cancel

DISA-STIG Compliance

STIGs are nothing more than alternate configurations that make commonly used applications more secure. All DoD IT assets must meet STIG compliance in some fashion before they are allowed to operate on DoD networks. In the example below, we use a DISA STIG policy for layer 2 switches. The following instructions will show you how to implement DISA STIGs compliance:

1. Navigate to Config Management → Policy Design Center → Policies → DISA v8,r11 STIG Infrastructure Layer 2 Switch.



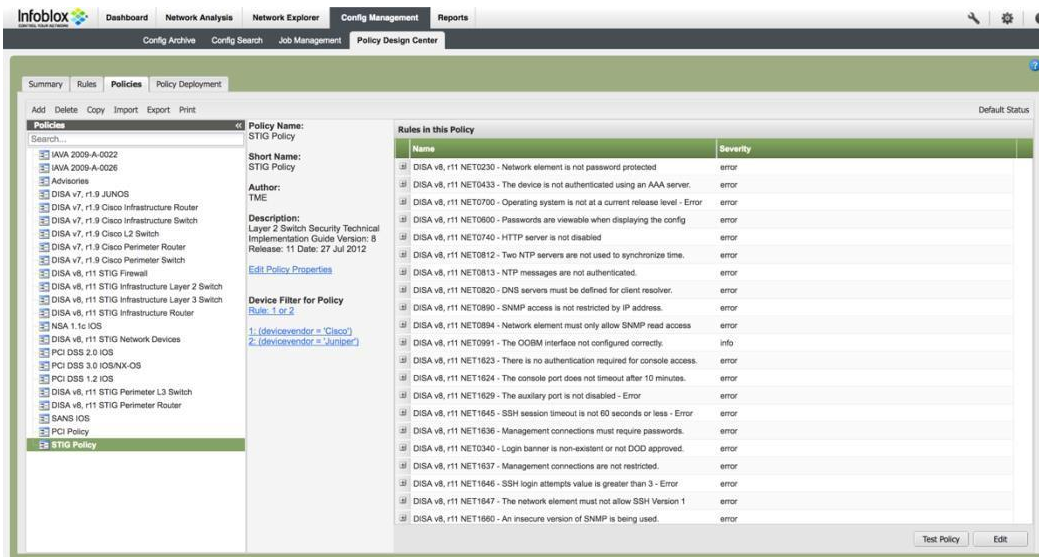
2. Make sure the selected DISA STIG policy is highlighted. Click on the Copy button to copy this default policy to a user created policy. Fill out the Policy Name, Short Name (Short Name is limited to 12 characters), and Author. Click Save.

The 'Copy Policy' dialog box is shown, allowing a user to create a new policy based on the selected one. The fields are as follows:

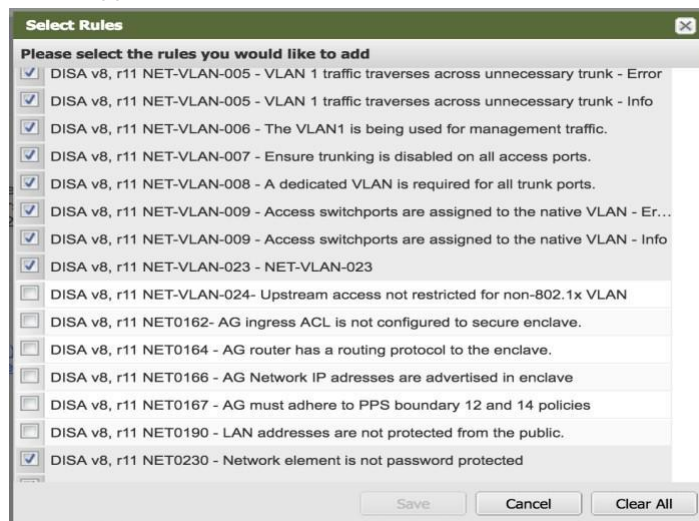
- Policy Name: STIG Policy
- Short Name: STIG Policy
- Author: TME
- Description: Layer 2 Switch Security Technical Implementation Guide
Version: 8
Release: 11
Date: 27 Jul 2012

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

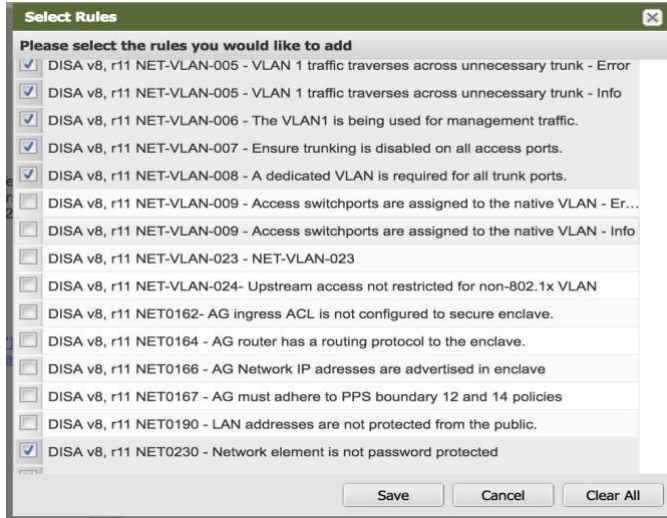
3. Highlight the newly created policy called STIG Policy.



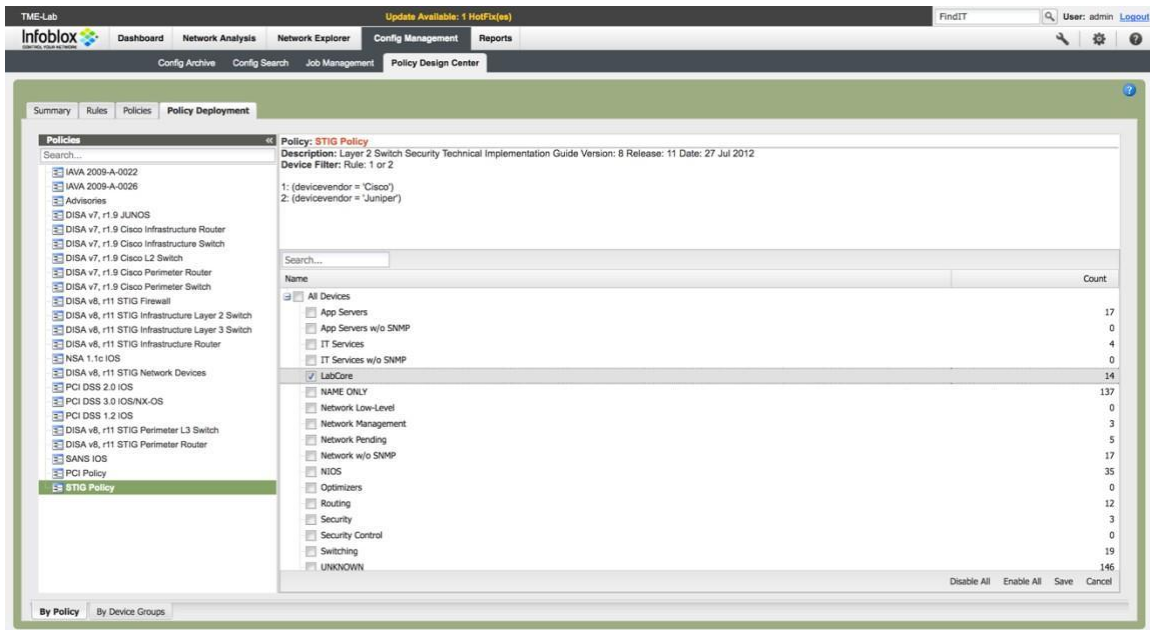
4. Click on the Edit button on the lower right corner of the screen to edit this policy and the following screen appears:



5. Select the rules that you want to add by clicking on the check box. Click Save Note: To familiarize yourself with this feature, you can choose any number of the rules below for your Cisco IOS devices:
- DISA v8, r11 NET0230 Network element is not password protected
 - DISA v8, r11 NET0600-Passwords are viewable when displaying the config
 - DISA v8, r11 NET0710-The Cisco discovery protocol (CDP) is not disabled
 - DISA v8, r11 NET0740-HTTP server is not disabled

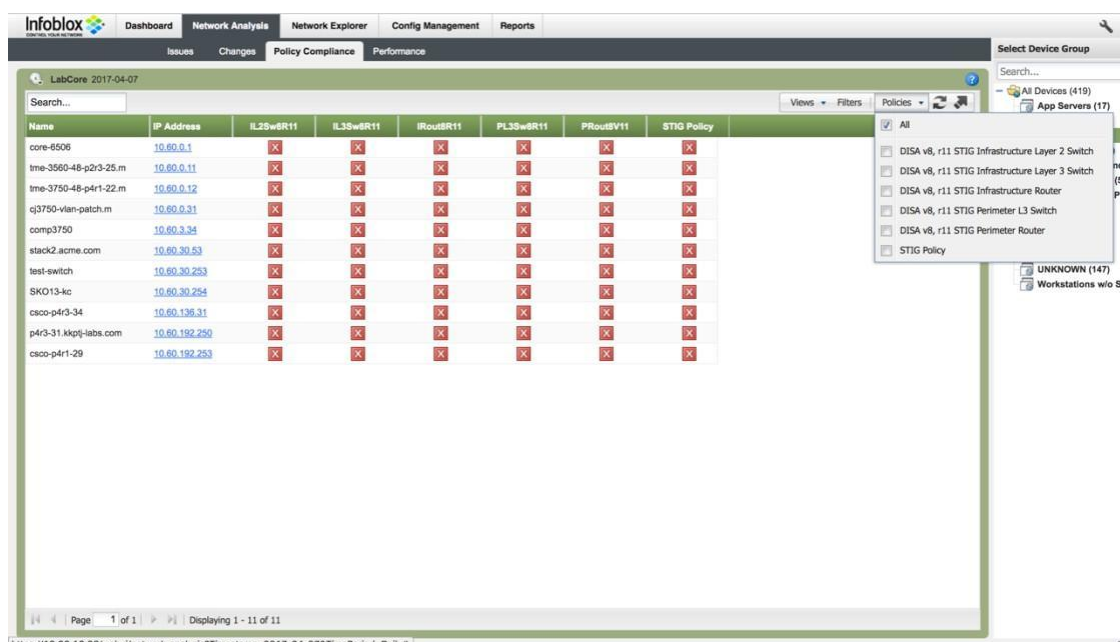


6. Click on the Policy Deployment tab to deploy the policy to the chosen device group. Notice the LabCore device group is selected. The Save button will be ungrayed when a change is detected. Click Save if needed.

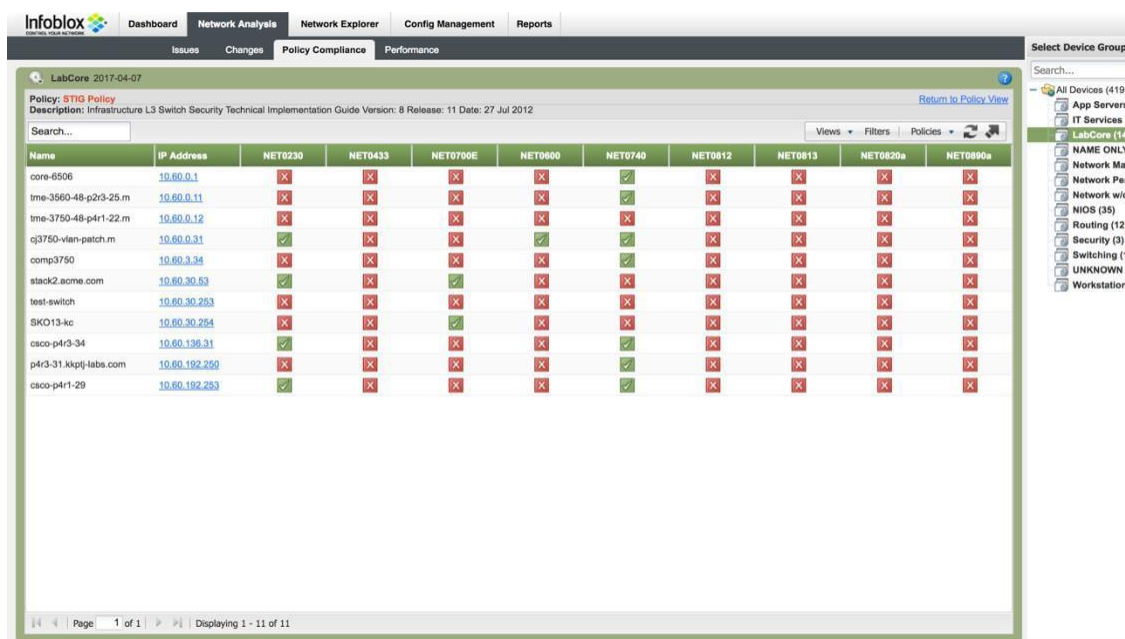


7. After waiting 10 minutes or more for processing, navigate to Network Analysis → Policy Compliance. By default, all deployed policies will be displayed for the selected device group.

8. Click on the Policies drop down menu to select the STIG Policy.

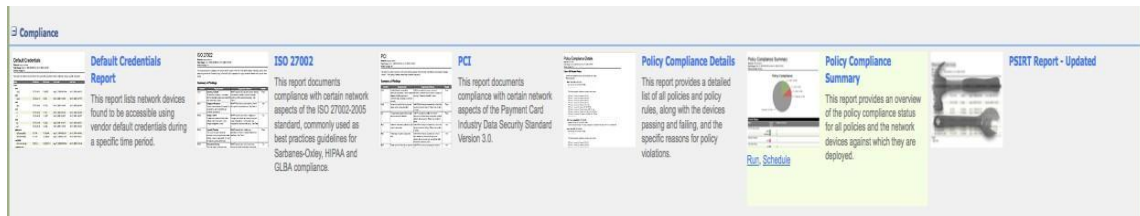


9. The following should appear.

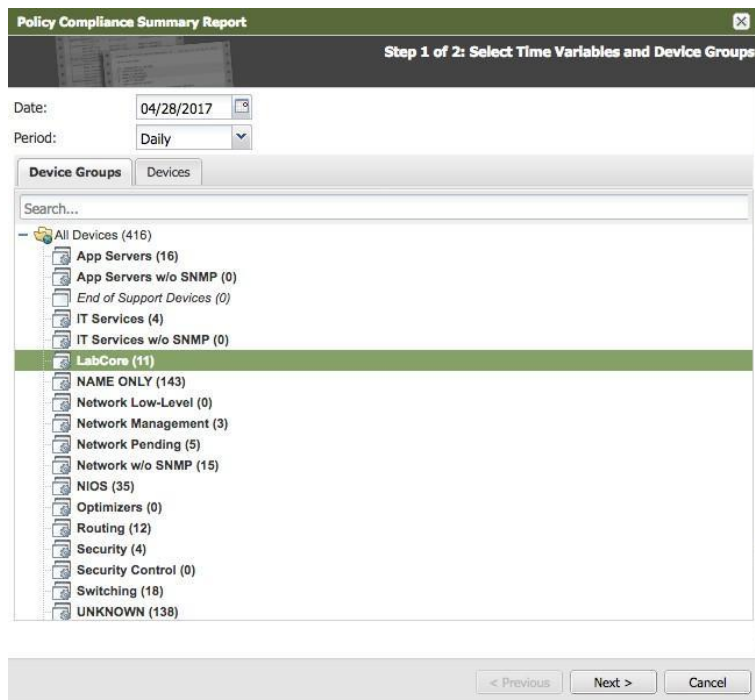


10. You can move the mouse over to any of the colored boxes to get detailed information of the policy analysis or you can also click any of the boxes to get details in a new window. Here is a legend of the various colored boxes:
 - a. Red X: Error
 - b. Blue X: Info
 - c. Yellow X: Warning
 - d. Green ✓: Pass

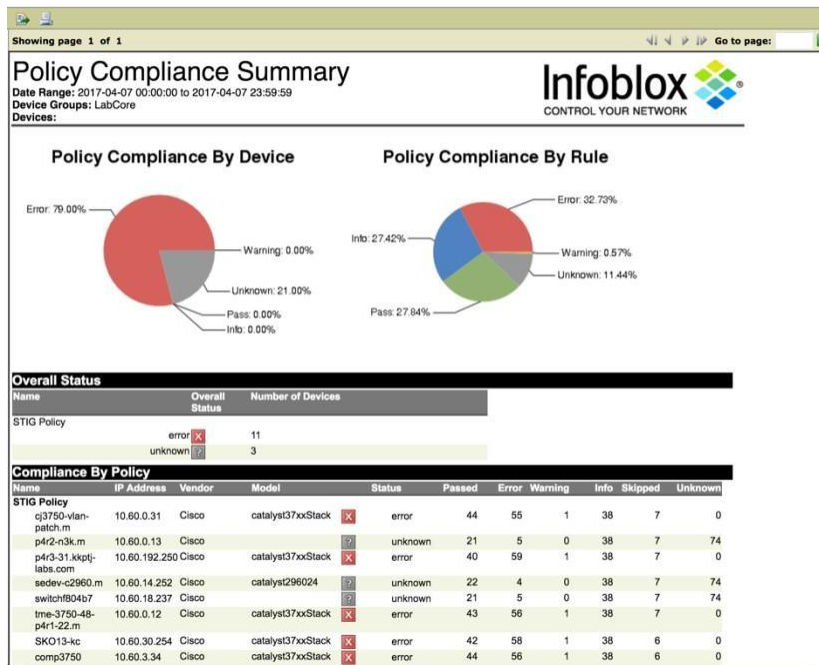
11. To run the Compliance Summary report, navigate to Reports → Report Gallery and move mouse pointer to the Policy Compliance Summary.



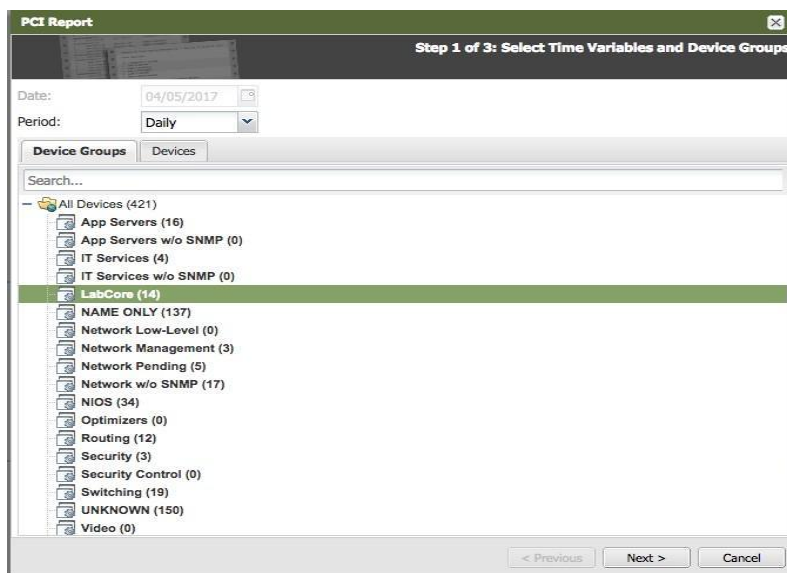
12. Click on the 'Run' button.



13. The report will show on the screen. At the upper left of the screen, you can choose to download the report in PDF, Excel, or MS Word in addition to printing the report.



14. Click on the schedule button under the Compliance Summary Report description. Select the device group. Click Next.



15. Enter the email address of the destination of this report. Click Next.

The screenshot shows a window titled "Policy Compliance Summary Report" with a subtitle "Step 3 of 4: Select Report Scheduling". The window contains the following fields and options:

- Report Name: Policy Compliance Summary
- To Emails: management@xyzcorp.com
- To Users: NetMRI Admin (), dave signori (), support support (), tac tac (), Thomas Lee (thomasl@infoblox.com)
- Output Format: pdf
- Recurrence Pattern: Weekly
- Execution Time: 6:00 AM
- Days of the week: ☐ Sunday, ☐ Tuesday, ☐ Thursday, ☐ Saturday, ☒ Monday, ☐ Wednesday, ☐ Friday

At the bottom right, there are three buttons: "< Previous", "Next >", and "Cancel".

16. Verify the settings of the scheduled report. If configurations are correct, click Schedule. At this time this report will be run and sent out to the email address on the date below and the time below.

The screenshot shows a window titled "Policy Compliance Summary Report" with a subtitle "Step 4 of 4: Summary of Scheduled Report". The window displays a summary of the scheduled report settings:

- Report Name: Policy Compliance Summary
- Date: 04/07/2017
- Period: Daily
- Device Groups: LabCore
- Devices:
- Policies: STIG Policy
- To Emails: management@xyzcorp.com
- To Users:
- Schedule: Weekly - Monday at 06:00 AM

At the bottom right, there are three buttons: "< Previous", "Schedule", and "Cancel".

Auto Device Remediation

NetMRI triggered jobs allow a script or template with predefined or custom variables to execute against a device when a "triggering source event" occurs. Triggering sources consist of the following:

- Policy rule violations.
- Custom and standard Issues.

Note: In order for the auto device remediation to work as quickly as possible, the device must be configured to send syslog data to the NetMRI appliance. Otherwise, NetMRI will detect the change on the next change detection interval. For example, in Cisco IOS, the configuration statement is 'logging <IP address of syslog server>'.

In this example, we create a triggered script to delete any instances of SNMP community name public or private as a community string in any configuration of the devices. In this exercise, we're going to create a rule to test for the presence of the SNMP community string and test it against a device along with a script to delete the public and/or private SNMP community string.

1. Navigate to Config Management → Policy Design Center → Rules and look for the rule called IOS SNMP Community Strings.
2. Here is that rule:

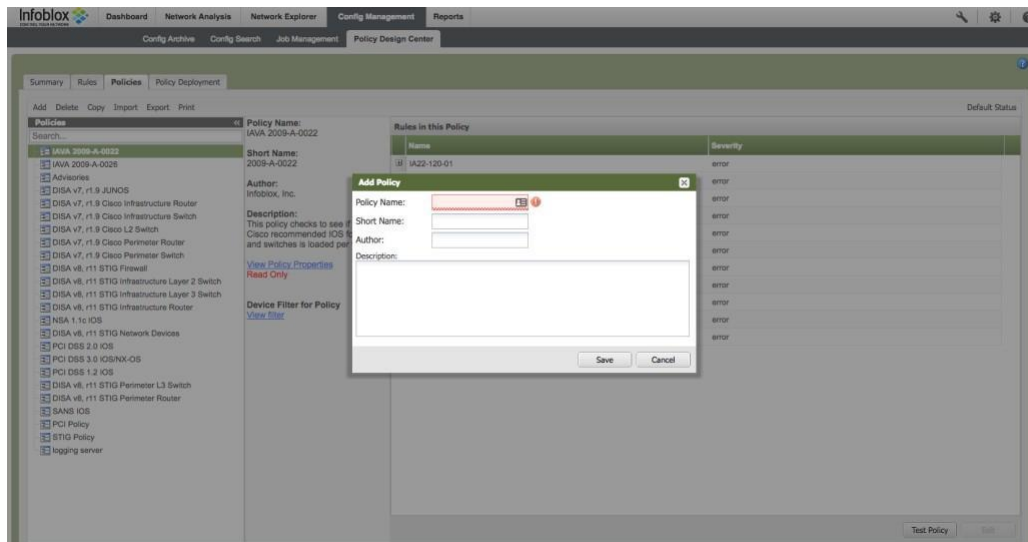
The screenshot displays the 'Rule Logic Builder' interface for a rule named 'IOS SNMP Community Strings'. The left sidebar contains metadata: Rule Name (IOS SNMP Community Strings), Short Name (IOS-SNMP-001), Author (Infoblox, Inc.), Severity (error), Description (If using SNMP, do not use default community strings. References: NSA; SANS 5.7.2, 5.7.3 This ru...), Remediation (Do not use default well-known community strings for SNMP), View Rule Properties (Read Only), Device Filter for Rule (Rule: 1 and 2 and 3, 1: (devicevendor matches 'Cisco'), 2: (devicesysdescr contains 'IOS'), 3: devicetype in (Router, Switch-Router, Switch)), and Used in these policies (NSA 1.1c IOS, SANS IOS). The main panel shows the logic: 'Enforce This Rule: If (1) then 2'. It contains two steps: Step 1 is 'Config File Match' with the condition 'Must Contain AT LEAST ONE of These Lines' and the pattern '^snmp-server'. Step 2 is 'Config File Match' with the condition 'May Not Contain Any of These Lines' and the pattern '^snmp-server community (public|private)'.

#	Type	Note
1	Config File Match	Must Contain AT LEAST ONE of These Lines ^snmp-server
2	Config File Match	May Not Contain Any of These Lines ^snmp-server community (public private)

Now, we're going to create a policy using that rule and test it against the devices. At this point, the rule should pass.

1. Navigate to Config Management → Policy Design Center → Policies and create a policy that uses the IOS SNMP Community String rule.

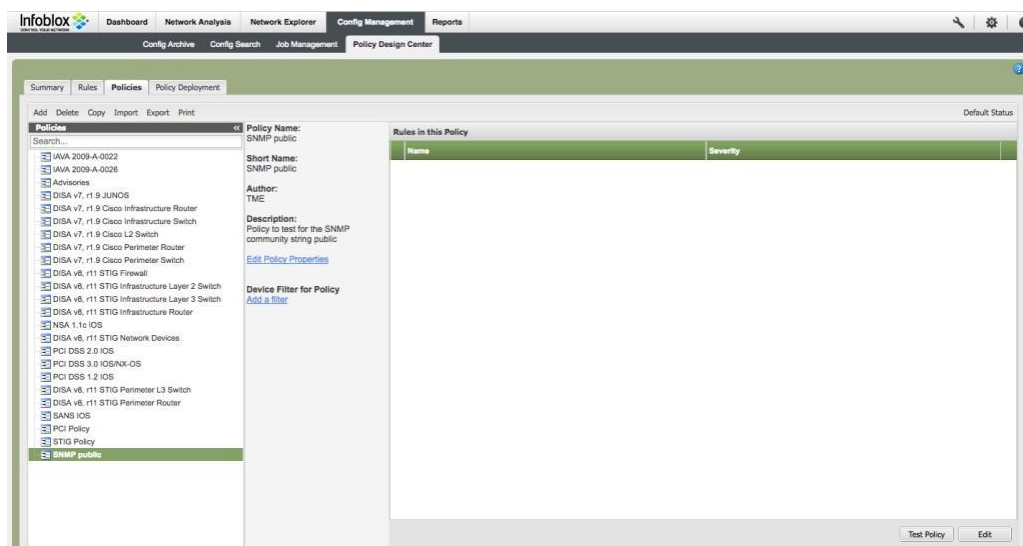
- Click on the 'Add' button and you should see the following screen:



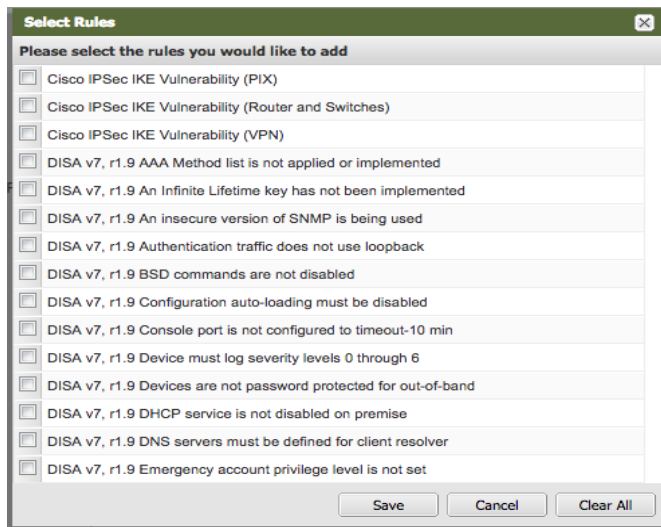
- Enter the Policy Name, Short Name, Author, and description. Click 'Save' afterwards.



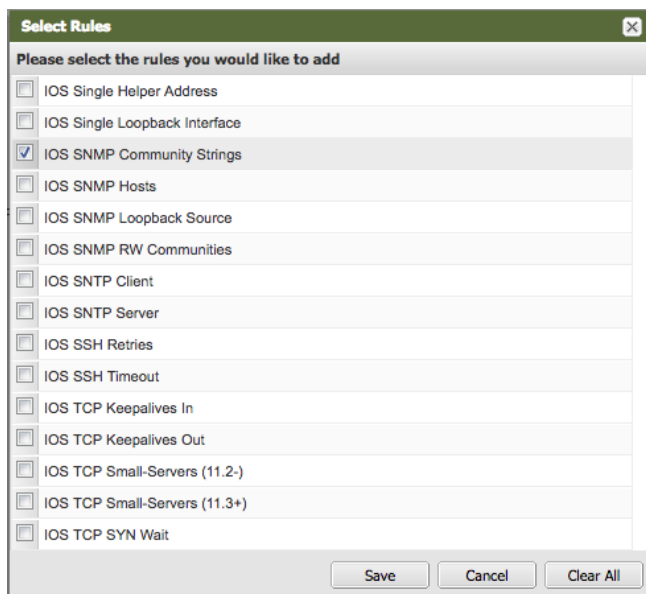
- Highlight the newly created policy and you should see a blank rules screen:



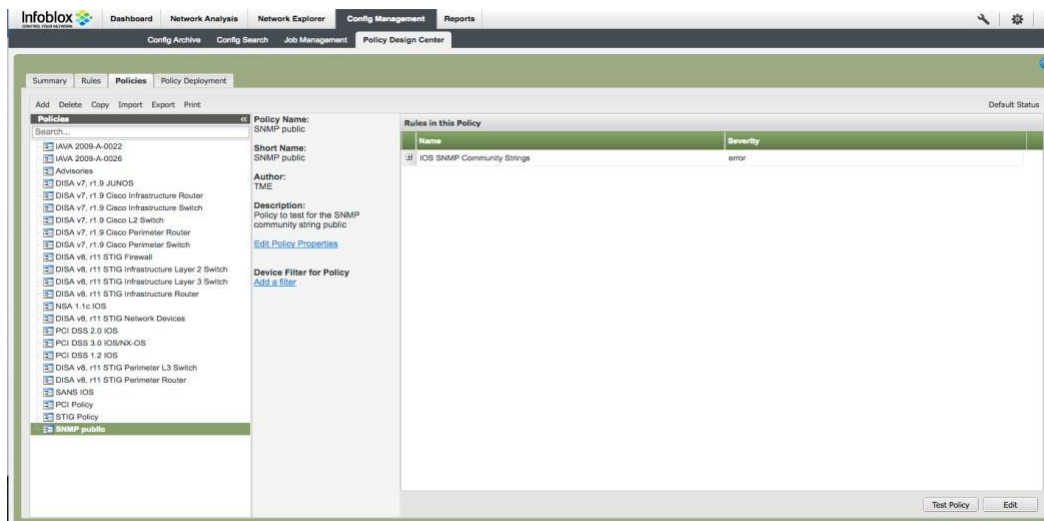
- Click on the Edit button in the lower right corner of the screen. A small screen will appear.



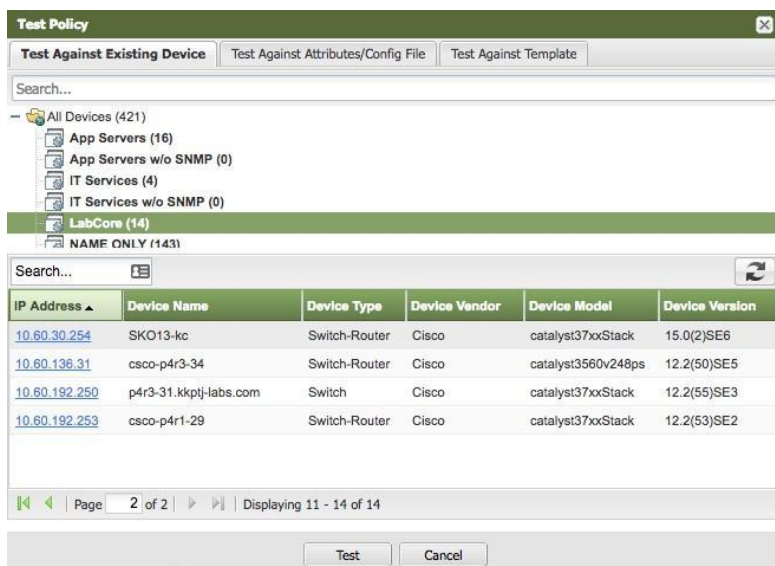
- Scroll down and click on the IOS SNMP Community Strings rule and then click Save.



7. The following screen appears:



8. Test the policy against a device configuration. Click on the 'Test Policy' button on the lower right corner of the previous screen. The following small screen appears.



- For this example, we selected the device group 'LabCore' and then the switch with the IP address of 10.60.30.254. Click on the 'Test' button. The following screen will appear:

Infoblox Configuration Policy Test Results
2017-04-17 18:02:41

Policy SNMP public
Policy to test for the SNMP community string public

☒ **Pass**

Policy Summary:

Pass	1 (100.00%)
Fail	0 (0.00%)
Error	0 (0.00%)
Warning	0 (0.00%)
Info	0 (0.00%)
Skip	0 (0.00%)
Unknown	0 (0.00%)
Checked	1 (100.00%)

Rules Summary:

IOS SNMP Community Strings:IOS-SNMP-001	Pass	<input checked="" type="checkbox"/>
---	------	-------------------------------------

Device SK013-kc
IP: 10.60.30.254
Model: catalyst37xxStack
Version: 15.0(2)SE6
Last Check: 2017-04-17 18:00:14

Rule IOS SNMP Community Strings
If using SNMP, do not use default community strings. References: NSA, SANS 5.7.2, 5.7.3 This rule is provided to the user as is, and is meant as a general interpretation of the NSA 1.1c and SANS frameworks. The function of this rule is to provide the user with a starting point from which a more detailed and specific compliance effort can be created. You should use this rule without modification only after you have reviewed it and determined that it does or does not apply to your specific needs.

Filter:
Rule: 1 and 2 and 3
1: (devicevendor matches 'Cisco')
2: (devicesysdescr contains 'IOS')
3: devicetype in (Router, Switch-Router, Switch)

☒ **Pass**

Remediation:
Do not use default well-known community strings for SNMP.

Logic:
Running config file contains some:
"snmp-server
Running config file does not contain any:
"snmp-server community (public|private)

- We want to be sure that the policy passes on this device before deploying.
- Highlight and deploy the SNMP public private policy against the LabCore device group, by checking the box next to the **LabCore** device group in the **Policy Deployment** tab, and click **Save**.

Infoblox Dashboard Network Analysis Network Explorer Config Management Reports

Config Archive Config Search Job Management Policy Design Center

Summary Rules Policies Policy Deployment

Policies
Search...
 JAVA 2009-A-0022
 JAVA 2009-A-0026
 Advisories
 DISA v7, r1.9 JUNOS
 DISA v7, r1.9 Cisco Infrastructure Router
 DISA v7, r1.9 Cisco Infrastructure Switch
 DISA v7, r1.9 Cisco L2 Switch
 DISA v7, r1.9 Cisco Perimeter Router
 DISA v7, r1.9 Cisco Perimeter Switch
 DISA v8, r11 STIG Firewall
 DISA v8, r11 STIG Infrastructure Layer 2 Switch
 DISA v8, r11 STIG Infrastructure Layer 3 Switch
 DISA v8, r11 STIG Infrastructure Router
 NSA 1.1c IOS
 DISA v8, r11 STIG Network Devices
 PCI DSS 2.0 IOS
 PCI DSS 3.0 IOS/XX-OS
 PCI DSS 1.2 IOS
 DISA v8, r11 STIG Perimeter L3 Switch
 DISA v8, r11 STIG Perimeter Router
 SANS IOS
 PCI Policy
 STIG Policy
SNMP public private

Policy: SNMP public private
Description: Policy to test for the SNMP community string public or private
Device Filter:

Search...

Name	Count
<input type="checkbox"/> All Devices	
<input type="checkbox"/> App Servers	16
<input type="checkbox"/> App Servers w/o SNMP	0
<input type="checkbox"/> IT Services	4
<input type="checkbox"/> IT Services w/o SNMP	0
<input checked="" type="checkbox"/> LabCore	14
<input type="checkbox"/> NAME ONLY	143
<input type="checkbox"/> Network Low-Level	0
<input type="checkbox"/> Network Management	3
<input type="checkbox"/> Network Pending	5
<input type="checkbox"/> Network w/o SNMP	17
<input type="checkbox"/> NIOS	35
<input type="checkbox"/> Optimizers	0
<input type="checkbox"/> Routing	12
<input type="checkbox"/> Security	4
<input type="checkbox"/> Security Control	0
<input type="checkbox"/> Switching	19
<input type="checkbox"/> UNKNOWN	141

Disable All Enable All Save Cancel

By Policy By Device Groups

12. Wait for your deployed policy to pass for all devices in the LabCore device group.

The screenshot shows the Infoblox GUI with the 'Policy Compliance' tab selected. The policy is 'SNMP public private' with a description 'Policy to test for the SNMP community string public or private'. A table lists 11 devices, all of which are compliant (indicated by green checkmarks).

Name	IP Address	ios snmp
core-6506	10.60.0.1	✓
tme-3560-48-p2r3-25.m	10.60.0.11	✓
tme-3750-48-p4r1-22.m	10.60.0.12	✓
cj3750-vlan-patch.m	10.60.0.31	✓
comp3750	10.60.3.34	✓
stack2.acme.com	10.60.30.53	✓
test-switch	10.60.30.253	✓
SKO13-ko	10.60.30.294	✓
cisco-p4r3-34	10.60.136.31	✓
p4r3-31.kkptj-labs.com	10.60.192.250	✓
cisco-p4r1-29	10.60.192.253	✓

13. Create a script to delete the SNMP public and/or private community strings. Navigate to Config Management → Job Management → Scripts. Click on the '+' button to add a script.

The screenshot shows the Infoblox GUI with the 'Scripts' tab selected under 'Job Management'. A table lists 22 scripts, including various compliance and configuration tasks.

Actions	Name	Language	Run Level	Created By	Updated By	Updated On	Last Run
2009 Extended DST Compliance		CCS	High	admin	admin	2017-03-13 16:15:18	
Ad Hoc Command Batch		CCS	High	admin	admin	2017-03-13 16:15:17	
Assign Port to VLAN		Perl	High	admin	admin	2017-03-13 16:15:29	
Catalyst 3750 Bad Stack Switch		CCS	High	admin	admin	2017-03-13 16:15:18	
Catalyst Port ErrDisabled		CCS	High	admin	admin	2017-03-13 16:15:18	
Example 1 - Cisco Set User Password		CCS	High	admin	admin	2017-03-13 16:15:18	
Example 1 - Cisco Set User Password (Perl)		Perl	High	admin	admin	2017-03-13 16:15:19	
Example 2 - Multi-Vendor Set User Password		CCS	High	admin	admin	2017-03-13 16:15:19	
Example 2 - Multi-Vendor Set User Password (Perl)		Perl	High	admin	admin	2017-03-13 16:15:19	
Example 3 - Cisco Set Existing User Password		CCS	High	admin	admin	2017-03-13 16:15:19	
Example 3 - Cisco Set Existing User Password (Perl)		Perl	High	admin	admin	2017-03-13 16:15:19	
Example 4 - Cisco Set Duplex		CCS	High	admin	admin	2017-03-13 16:15:20	
Example 4 - Cisco Set Duplex (Perl)		Perl	High	admin	admin	2017-03-13 16:15:20	
Example 5 - Cisco Set Duplex Redux		CCS	High	admin	admin	2017-03-13 16:15:20	
Example 5 - Cisco Set Duplex Redux (Perl)		Perl	High	admin	admin	2017-03-13 16:15:20	
Example 6 - Cisco Set Port Fast		CCS	High	admin	admin	2017-03-13 16:15:20	
Example 6 - Cisco Set Port Fast (Perl)		Perl	High	admin	admin	2017-03-13 16:15:21	
Example 7 - Cisco Set Port Fast Redux		CCS	High	admin	admin	2017-03-13 16:15:21	
Example 7 - Cisco Set Port Fast Redux (Perl)		Perl	High	admin	admin	2017-03-13 16:15:21	
HTTP Server Running On Switch or Server		CCS	High	admin	admin	2017-03-13 16:15:30	
Invalid User Account Issue		CCS	High	admin	admin	2017-03-13 16:15:21	
IOS ACL Archive		CCS	High	admin	admin	2017-03-13 16:15:22	

- Enter the name of the script, run level of high, description, and the script itself. When finished, click on the 'Save & Close' button.

Add New Script

Tip: use the [Regular Expression Test](#) page to check trigger variable and trigger templates.

Name:

Run Level:

Category:

Description:

Language:

#Script-Description:

```
# Remove the SNMP community string public

#####

Action: Remove Logging Statement
Action-Commands:

Config t
no snmp-server community public
no snmp-server community private
end
write mem

#####
```

Save & Close Save Export Cancel

- Navigate to Config Management --> Job Management --> Triggered Jobs and click the + sign in the upper right-hand corner to add a Triggered Job.

TM6-Lab

Infoblox

Dashboard Network Analysis Network Explorer Config Management Reports

Config Archive Config Search Job Management Policy Design Center

Scripts Library Config Templates Lists Scheduled Jobs **Triggered Jobs** Job History Custom Issues

Search...

Actions	Name	Level	Enabled	Active Window	Trigger Type	Trigger Event	Device Groups	Action	Created On	Updated On
⚙️	IOS SSH Settings	High	No	24/7	Policy Rule	IOS SSH Retries	All	Schedule Job	2015-12-10 16:49:11	2015-12-10 16:41
⚙️	Isolate Rogue DHCP Server	High	Yes	24/7	Issue	Rogue DHCP Server Located (Devices)	All	Schedule Job	2017-03-13 16:15:38	2017-03-13 16:11
⚙️	Locate Rogue DHCP Server	High	Yes	24/7	Issue	Rogue DHCP Server Detected (Devices)	All	Auto-Run	2017-03-13 16:15:44	2017-03-13 16:11
⚙️	Provision Bare Metal Device	High	Yes	24/7	Issue	Bare Metal Device Found (Devices)	All	Schedule Job	2017-03-13 16:15:51	2017-03-13 16:11

Page 1 of 1 | Displaying 1 - 4 of 4

Updated at 2017-04-18 10:46:15

16. Select “Policy Rule” as the Trigger Source from the drop down and select the IOS SNMP Public Private rule within the Policy Rule Selection box, and click Next.

The screenshot shows the 'Triggered Job Wizard' window with the 'Select Trigger' tab active. The 'Trigger Source' dropdown is set to 'Policy Rule'. Below it, the 'Policy Rule Selection' box contains a list of rules, with 'ios snmp public private' selected. To the right, the 'Selected Policy Rule Information' box displays details for the selected rule, including its name, short name, description, filter, and remediation text. At the bottom right, there are buttons for '< Previous', 'Next >', and 'Cancel'.

Policy Rule Selection	
Search...	
Name	
IOS Service Config	
IOS Service Sequence-Numbers (12.0+)	
IOS Single Helper Address	
IOS Single Loopback Interface	
IOS SNMP Community Strings	
IOS SNMP Hosts	
IOS SNMP Loopback Source	
ios snmp public private	
IOS SNMP RW Communities	
IOS SNMP Client	
IOS SNMP Server	

Selected Policy Rule Information	
Rule Name:	ios snmp public private
Rule Short Name:	ios snmp
Rule Description:	If using SNMP, do not use default community strings. References: NSA; SANS 5.7.2, 5.7.3 This rule is provided to the user as is, and is meant as a general interpretation of the NSA 1.1c and SANS frameworks. The function of this rule is to provide the user with a starting point from which a more detailed and specific compliance effort can be created. You should use this rule without modification only after you have reviewed it and determined that it does or does not apply to your specific needs.
Rule Filter:	Rule: 1 and 2 and 3 1: (devicevendor matches 'Cisco') 2: (devicesysdescr contains 'IOS') 3: devicetype in (Router, Switch-Router, Switch)
Rule Remediation Text:	Do not use default well-known community strings for SNMP.

17. Select the “LabCore” group and make sure that the “Active Time Window” indicates 24/7, and click Next.

The screenshot shows the 'Triggered Job Wizard' window with the 'Trigger Filters' tab active. The 'Device Groups' list includes 'All Devices (421)', 'App Servers (16)', 'IT Services (4)', 'LabCore (11)', and 'NAME ONLY (144)'. The 'Active Time Window' dropdown is set to '24/7'. At the bottom right, there are buttons for '< Previous', 'Next >', and 'Cancel'.

Device Groups:
All Devices (421)
App Servers (16)
IT Services (4)
LabCore (11)
NAME ONLY (144)

Active Time Window: 24/7

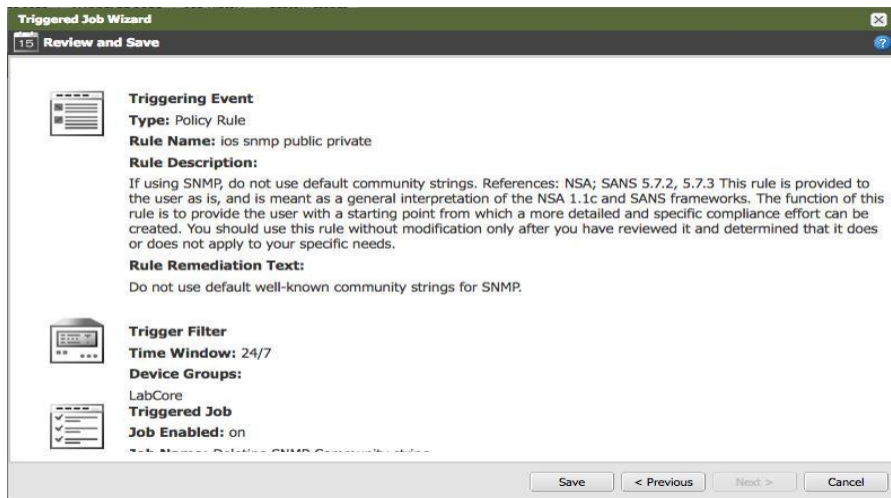
18. In the “Define Job” pane, you can add details like a custom name and a description. However, make sure that the “Enabled” box **is** checked and that you have selected script created in step 2. Click Next.

The screenshot shows the 'Define Job' pane of the 'Triggered Job Wizard'. The 'Job Name' section has 'Use Custom Name' selected with the text 'Deleting SNMP Community string' and 'Use Script Name' unselected. The 'Enabled' checkbox is checked. The 'Job Description' text box contains 'Deletes public and/or private SNMP community strings'. Below this, the 'Scripts' tab is active, showing a list of scripts. The script 'Remove SNMP Community string public and private...' is selected. The right pane shows the details for this script, stating 'No input required'. Navigation buttons at the bottom are '< Previous', 'Next >', and 'Cancel'.

19. From the “Schedule Job Execution” pane, make sure that you select “Run Job Immediately” from the “Trigger Action” drop down, and click Next.

The screenshot shows the 'Schedule Job Execution' pane of the 'Triggered Job Wizard'. The 'Trigger Action' dropdown menu is set to 'Run Job Immediately'. The pane is mostly empty with a large white area for scheduling details. Navigation buttons at the bottom are '< Previous', 'Next >', and 'Cancel'.

20. Review the properties of the job and click Save.



Testing the triggered job by changing a device configuration manually

You will log into a device via telnet and issue a couple of commands to change the configuration. The steps below would also cause a configuration backup to occur. NetMRI will not backup configurations if no changes have occurred.

1. Open up a terminal window on your PC.
2. Telnet to a switch in the device group. In this example the switch is called SKO13-kc and the IP address is 10.60.30.254.
3. The username is admin and the password is 'infoblox'.
4. If necessary, go into enable mode by entering "enable" at the prompt. The enable password is "infoblox".
5. Type "config t" at the prompt to configure the device.
6. Enter the following command to add the SNMP public community string:
SKO13-kc(config)# snmp-server community public ro
7. Exit config mode and issue a "write mem" command.

8. Leave the terminal session open, and issue a “term mon” command.

```
ip http secure-server
!
!
ip sla enable reaction-alerts
logging trap debugging
logging host 10.60.16.96
!
snmp-server community infoblox RO
!
!
line con 0
line vty 0 4
  exec-timeout 30 0
  login local
  transport preferred ssh
line vty 5 15
  exec-timeout 30 0
  login local
  transport preferred ssh
!
!
monitor session 1 source interface Gi1/0/1 , Gi1/0/25 ~ 26
monitor session 1 destination interface Gi1/0/2 , Gi1/0/27
ntp server 10.60.2.2
end

SK013-kc#config t
Enter configuration commands, one per line. End with CNTL/Z.
SK013-kc(config)#snmp-server community public ro
SK013-kc(config)#exit
SK013-kc#write mem
Building configuration...
[OK]
SK013-kc#term mon
SK013-kc#
Apr 18 19:22:13.096: %SYS-5-CONFIG_I: Configured from console by admin on vty1 (
10.60.16.96)Connection closed by foreign host.
sc-l-thomasl:downloads thomasl$
```

This will show you when NetMRI logs into the device and removes the SNMP statement. This should occur about 15 minutes after the change.

9. Navigate to Config Management → Config Archive and look for your configuration change.

The screenshot shows the Infoblox Config Archive interface. On the left, there is a 'Device Group' sidebar with a search bar and a list of device groups: All Devices (426), App Servers (16), IT Services (4), NAME ONLY (148), Network Management (3), Network Pending (5), Network w/o SNMP (15), NIOS (35), Routing (12), and Security (4). Below this is a table of devices with columns for IP Address, Device Name, and Device Type. The table lists 11 devices, including SK013-kc. On the right, the 'Config Archive' section is active, displaying a message: 'Select a Device Group Filter and Device from the list to the left'. Below this message is a note: 'Note: devices only appear in this list if config collection is enabled for this device and a successful configuration collection has occurred.' At the bottom right, there are buttons for 'Compare Second Device', 'Compare', 'Set Baseline', 'Rollback', 'Delete', and 'Export...'.

IP Address	Device Name	Device Type
10.60.0.31	cj3750-vlan-patch.m	Switch (99%)
10.60.3.34	comp3750	Switch-Router (99%)
10.60.0.1	core-6506	Switch-Router (99%)
10.60.182.253	cisco-p4r1-29	Switch-Router (99%)
10.60.136.31	cisco-p4r3-34	Switch-Router (99%)
10.60.192.250	p4r3-31.kltp-labs.com	Switch (99%)
10.60.30.254	SK013-kc	Switch-Router (99%)
10.60.30.53	stack2.acme.com	Switch-Router (99%)
10.60.30.253	test-switch	Switch-Router (99%)
10.60.0.11	tme-3560-48-p2r3-25.m	Switch-Router (99%)
10.60.0.12	tme-3750-48-p4r1-22.m	Switch (99%)

10. Select the switch that was modified. In our example that is SKO13-kc.

The screenshot shows the Infoblox Config Management interface. On the left, a tree view shows the device hierarchy: All Devices (426) > LabCore (11) > SKO13-kc (1). The main table displays configuration files for SKO13-kc. The table has columns: Actions, BL, Status, Config Type, First Seen, Last Collected, and Edited By. The table shows a list of configuration files, with the most recent one being 'Running Config Saved? Yes'.

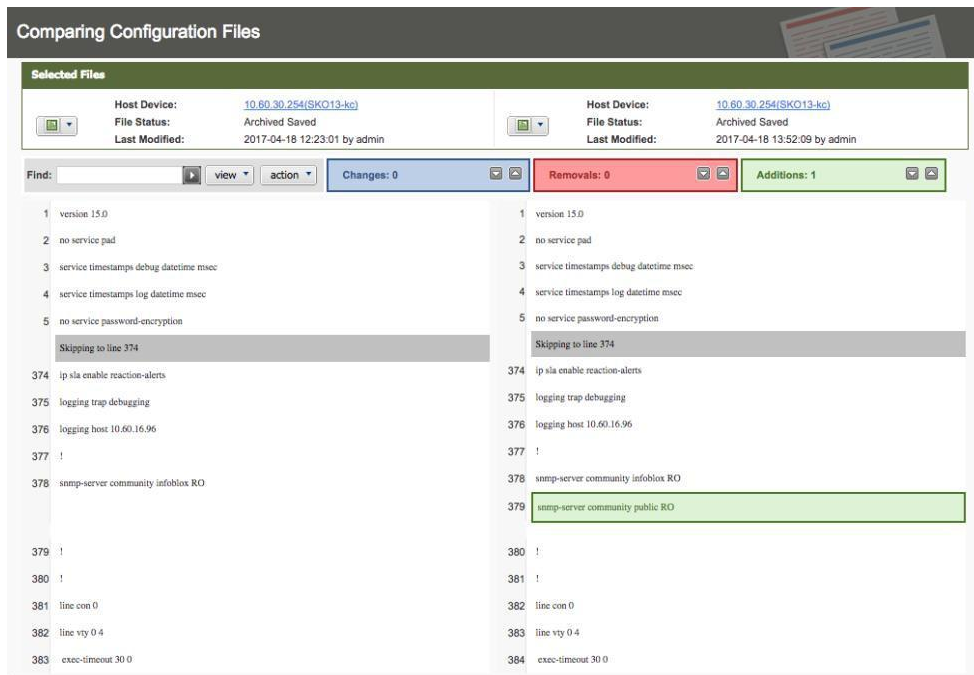
Actions	BL	Status	Config Type	First Seen	Last Collected	Edited By
<input type="checkbox"/>	Current	Running		2017-04-18 13:57...	2017-04-18 13:57...	admin
<input type="checkbox"/>	Current	Saved		2017-04-18 13:57...	2017-04-18 13:57...	admin
<input type="checkbox"/>	Archived	Running		2017-04-18 13:52...	2017-04-18 13:52...	admin
<input type="checkbox"/>	Archived	Saved		2017-04-18 13:52...	2017-04-18 13:52...	admin
<input type="checkbox"/>	Archived	Running		2017-04-18 12:23...	2017-04-18 12:23...	admin
<input type="checkbox"/>	Archived	Saved		2017-04-18 12:23...	2017-04-18 12:23...	admin
<input type="checkbox"/>	Archived	Running		2017-04-18 12:17...	2017-04-18 12:17...	admin
<input type="checkbox"/>	Archived	Saved		2017-04-18 12:17...	2017-04-18 12:17...	admin
<input type="checkbox"/>	Archived	Running		2017-04-18 11:33:15	2017-04-18 11:33:15	admin
<input type="checkbox"/>	Archived	Saved		2017-04-18 11:33:15	2017-04-18 11:33:15	admin
<input type="checkbox"/>	Archived	Running		2017-04-18 11:26:15	2017-04-18 11:26:15	admin
<input type="checkbox"/>	Archived	Saved		2017-04-18 11:26:15	2017-04-18 11:26:15	admin
<input type="checkbox"/>	Archived	Running		2017-04-17 20:02...	2017-04-17 20:02...	admin
<input type="checkbox"/>	Archived	Saved		2017-04-17 20:02...	2017-04-17 20:02...	admin
<input type="checkbox"/>	Archived	Running		2017-04-17 19:49...	2017-04-17 19:49...	thomasl
<input type="checkbox"/>	Archived	Saved		2017-04-17 19:49...	2017-04-17 19:49...	thomasl
<input type="checkbox"/>	Archived	Running		2017-04-17 18:02...	2017-04-17 18:02...	thomasl
<input type="checkbox"/>	Archived	Saved		2017-04-17 18:02...	2017-04-17 18:02...	thomasl
<input type="checkbox"/>	Archived	Running		2017-04-17 17:57...	2017-04-17 18:00...	thomasl
<input type="checkbox"/>	Archived	Saved		2017-04-17 17:57...	2017-04-17 18:00...	thomasl
<input type="checkbox"/>	Archived	Running		2017-04-17 17:18...	2017-04-17 17:18...	thomasl

11. Select the configuration files to compare.

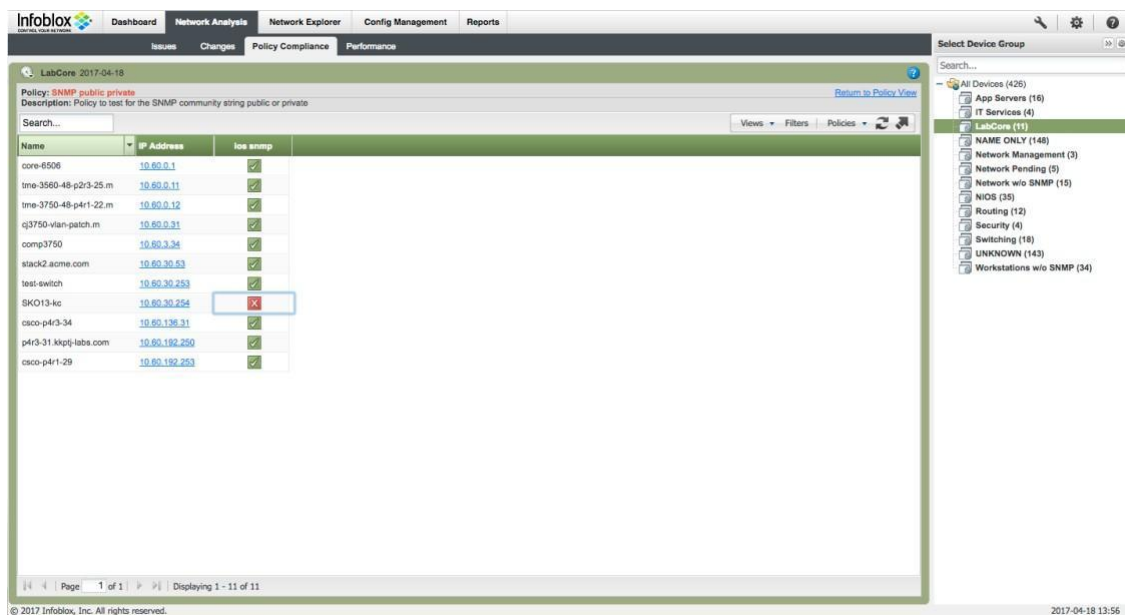
The screenshot shows the Infoblox Config Management interface, similar to the previous one, but with the configuration files selected for comparison. The table shows a list of configuration files, with the most recent one being 'Running Config Saved? Yes'. The 'Compare' button is visible at the bottom right.

Actions	BL	Status	Config Type	First Seen	Last Collected	Edited By
<input type="checkbox"/>	Current	Running		2017-04-18 13:57...	2017-04-18 13:57...	admin
<input type="checkbox"/>	Current	Saved		2017-04-18 13:57...	2017-04-18 13:57...	admin
<input checked="" type="checkbox"/>	Archived	Running		2017-04-18 13:52...	2017-04-18 13:52...	admin
<input checked="" type="checkbox"/>	Archived	Saved		2017-04-18 13:52...	2017-04-18 13:52...	admin
<input checked="" type="checkbox"/>	Archived	Running		2017-04-18 12:23...	2017-04-18 12:23...	admin
<input checked="" type="checkbox"/>	Archived	Saved		2017-04-18 12:23...	2017-04-18 12:23...	admin
<input checked="" type="checkbox"/>	Archived	Running		2017-04-18 12:17...	2017-04-18 12:17...	admin
<input checked="" type="checkbox"/>	Archived	Saved		2017-04-18 12:17...	2017-04-18 12:17...	admin
<input checked="" type="checkbox"/>	Archived	Running		2017-04-18 11:33:15	2017-04-18 11:33:15	admin
<input checked="" type="checkbox"/>	Archived	Saved		2017-04-18 11:33:15	2017-04-18 11:33:15	admin
<input checked="" type="checkbox"/>	Archived	Running		2017-04-18 11:26:15	2017-04-18 11:26:15	admin
<input checked="" type="checkbox"/>	Archived	Saved		2017-04-18 11:26:15	2017-04-18 11:26:15	admin
<input checked="" type="checkbox"/>	Archived	Running		2017-04-17 20:02...	2017-04-17 20:02...	admin
<input checked="" type="checkbox"/>	Archived	Saved		2017-04-17 20:02...	2017-04-17 20:02...	admin
<input checked="" type="checkbox"/>	Archived	Running		2017-04-17 19:49...	2017-04-17 19:49...	thomasl
<input checked="" type="checkbox"/>	Archived	Saved		2017-04-17 19:49...	2017-04-17 19:49...	thomasl
<input checked="" type="checkbox"/>	Archived	Running		2017-04-17 18:02...	2017-04-17 18:02...	thomasl
<input checked="" type="checkbox"/>	Archived	Saved		2017-04-17 18:02...	2017-04-17 18:02...	thomasl
<input checked="" type="checkbox"/>	Archived	Running		2017-04-17 17:57...	2017-04-17 18:00...	thomasl
<input checked="" type="checkbox"/>	Archived	Saved		2017-04-17 17:57...	2017-04-17 18:00...	thomasl
<input checked="" type="checkbox"/>	Archived	Running		2017-04-17 17:18...	2017-04-17 17:18...	thomasl

12. Click on the 'Compare' button. Notice the change?



13. After this change occurred, you can navigate to Network Analysis → Policy Compliance to look for the indication of a policy compliance issue. You may need to refresh the screen until the red 'X' appears. This may take about 5 minutes.



14. Click on the red X and you get an explanation of the violation.

The screenshot shows the 'Configuration Policy Analysis' page in the Infoblox web interface. The page title is 'Configuration Policy Analysis' with a timestamp of '2017-04-18 13:54:56'. The device being analyzed is 'SKO13-1c' with IP '10.60.30.254', model 'catalyst37xxStack', and version '15.0(2)SE6'. The last check was on '2017-04-18 13:54:56'.

Rule ios snmp public private
 If using SNMP, do not use default community strings. References: NSA; SANS 5.7.2, 5.7.3 This rule is provided to the user as is, and is meant as a general interpretation of the NSA 1.1c and SANS frameworks. The function of this rule is to provide the user with a starting point from which a more detailed and specific compliance effort can be created. You should use this rule without modification only after you have reviewed it and determined that it does or does not apply to your specific needs.

Filter:
 Rule: 1 and 2 and 3
 1: (devicevendor matches 'Cisco')
 2: (devicesysdescr contains '108')
 3: devicetype in (Router, Switch-Router, Switch)

Error
Message:
 Line 379 matches expression '^snmp-server community (public |private)'.

Remediation:
 Do not use default well-known community strings for SNMP.

Logic:
 Running config file contains some:
 "snmp-server
 Running config file does not contain any:
 "snmp-server community (public |private)

15. The triggered jobs process may take a few minutes to revert your changes to that specific device. Navigate to Network Analysis → Changes to view changes. Also, this change will trigger a configuration backup.

The screenshot shows the 'Network Analysis - Changes' page in the Infoblox web interface. The page has tabs for 'Issues', 'Changes', 'Policy Compliance', and 'Performance'. The 'Changes' tab is selected, showing a table of configuration changes.

Actions	Change Window	IP Address	Name	Vendor	Model	Device Type	User	Change Method	Change Type	Config
⚙️	2017-04-18 13:57:09	10.60.30.254	SKO13-1c	Cisco	catalyst37xxStack	Switch-Router (99%)	admin	Syslog.Config	Admin	Runnir
⚙️	2017-04-18 13:51:49	10.60.30.254	SKO13-1c	Cisco	catalyst37xxStack	Switch-Router (99%)	admin	Syslog.Config	Admin	Runnir
⚙️	2017-04-18 12:22:14	10.60.30.254	SKO13-1c	Cisco	catalyst37xxStack	Switch-Router (99%)	admin	Syslog.Config	Admin	Runnir
⚙️	2017-04-18 12:16:53	10.60.30.254	SKO13-1c	Cisco	catalyst37xxStack	Switch-Router (99%)	admin	Syslog.Config	Admin	Runnir
⚙️	2017-04-18 11:32:16	10.60.30.254	SKO13-1c	Cisco	catalyst37xxStack	Switch-Router (99%)	admin	Syslog.Config	Admin	Runnir
⚙️	2017-04-18 11:25:37	10.60.30.254	SKO13-1c	Cisco	catalyst37xxStack	Switch-Router (99%)	admin	Syslog.Config	Admin	Runnir

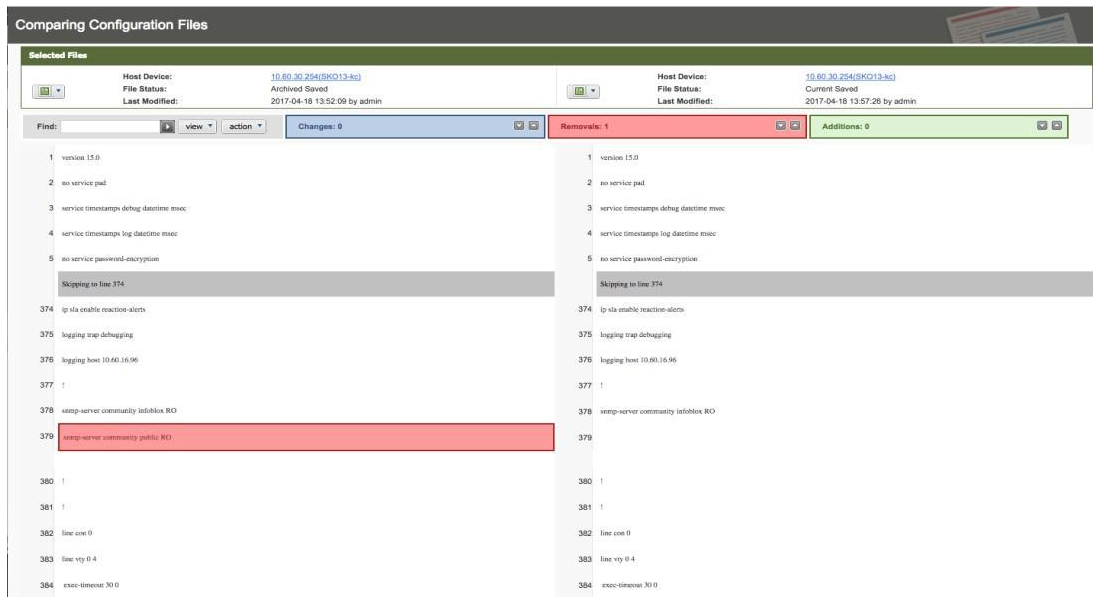
Page: 1 of 1 | Displaying 1 - 6 of 6 | Updated at 2017-04-18 14:13:08

Detected Change
 A bar chart showing the detected change for device 10.60.30.254. The y-axis represents the number of changes (1 to 7), and the x-axis represents the device IP address.

Most Changed Devices
 A bar chart showing the most changed devices. The y-axis represents the number of changes (1 to 7), and the x-axis represents the device IP address. The device 10.60.30.254 is the most changed device with 6 changes.

Change Type: All | View: Changed Devices

- Click on the wheel of the latest change and select 'View Saved Configuration Difference'. You see the SNMP public community string command is removed per the policy and triggered job.



- You can see a record of the triggered job being run to fix the SNMP misconfiguration. Navigate to Config Management → Job Management → Job History.

Scripts

Library

Config Templates

Lists

Scheduled Jobs

Triggered Jobs

Job History

Custom Issues

Search...

Views

Filters

Status	Job ID	Name	Script	Initiated By	Approved By	Start Time	End Time	Summary Count
✓ OK	4	Deleting SNMP Community string [Triggered Job][Run Now]	Remove SNMP Community string public and private	admin	admin	2017-04-18 13:57:00	2017-04-18 13:57:21	Total: 1, Pending: 0, OK: 1, Error: 0, Other: 0
✓ OK	3	Deleting SNMP Community string [Triggered Job][Run Now]	Remove SNMP Community string public and private	admin	admin	2017-04-18 12:22:00	2017-04-18 12:22:23	Total: 1, Pending: 0, OK: 1, Error: 0, Other: 0
✓ OK	2	Deleting SNMP Community string [Triggered Job][Run Now]	Remove SNMP Community string public and private	admin	admin	2017-04-18 11:32:00	2017-04-18 11:32:26	Total: 1, Pending: 0, OK: 1, Error: 0, Other: 0
✓ OK	1	Remove SNMP Community string public and private [Triggered Job][Run Now]	Remove SNMP Community string public and private	admin	admin	2017-04-17 20:02:00	2017-04-17 20:02:25	Total: 1, Pending: 0, OK: 1, Error: 0, Other: 0

- Click on the name of the latest job. The following screen appears:

Job Viewer

Job ID: 4 **Start Time:** 2017-04-18 13:57:00
Script: Remove SNMP Community string public and private **End Time:** 2017-04-18 13:57:21
Job Count: 1 **Status:** ✓ OK

[Details](#) [Issues](#) [Files](#)

Job Details

2017/04/28

Deleting SNMP Community string [Triggered Job][Run Now] - Remove SNMP Community string public and private

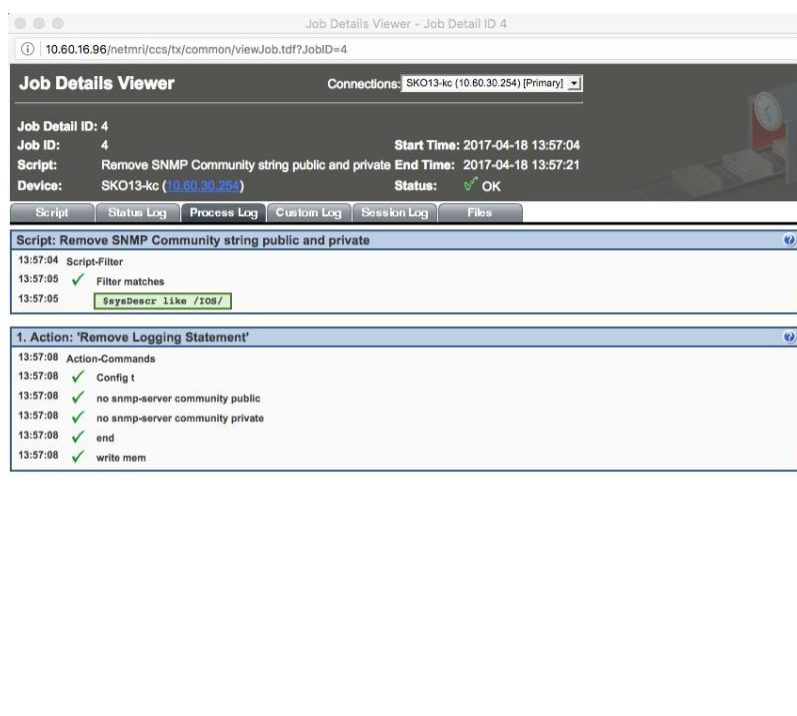
Search...

Status	Start Time	End Time	IP Address	Device Name	Actions
✓ OK	2017-04-18 13:57:04	2017-04-18 13:57:21	10.60.30.254	SKO13-kc	

Page 1 of 1 | Displaying 1 - 1 of 1

[Cancel All](#) [Rerun Errors](#) [Reschedule Errors](#)

19. Click on the 'OK' link. The following screen appears:



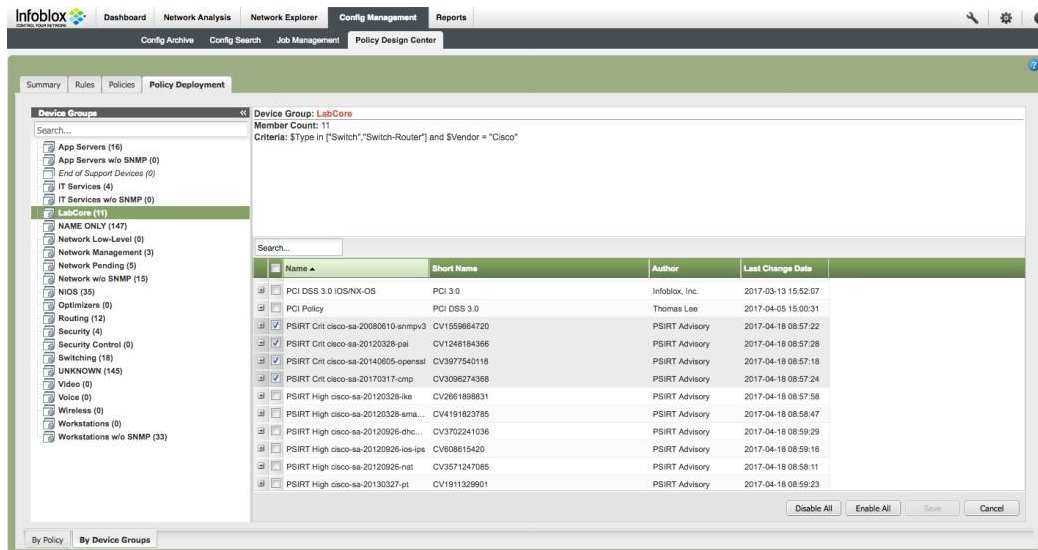
20. The screen above shows NetMRI logging in and running the script. You can click on the Script tab, Status Log tab, Custom Log tab, Session Log tab, and Files tab to see the details of each.

Device CVE/PSIRT - Advisor

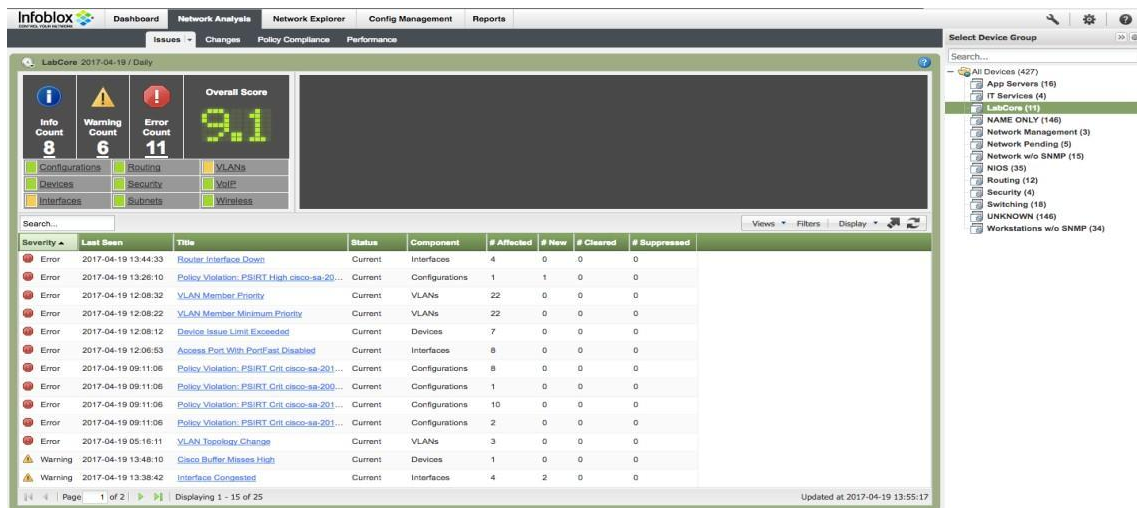
Network vendors provide Security Advisory information with increasing cadence and complexity. Your team needs to make sense of this data, determine which vulnerabilities impact your network's security posture, and take timely action to keep your network secure. For many, internal and external compliance requirements make this challenge even more complex. EmpoweredAdvisor™ from Empowered Networks for NetMRI helps you ensure your network is secure & compliant, with Always-On Analysis, Alerts & Advice, based on Security Advisories.

After installation of the EmpoweredAdvisor, you can do the following to gather the PSIRT information on your devices. In this example, we are using the LabCore device group and assigning the PSIRT policies to view any device vulnerabilities, but you can assign the PSIRT policies to any or all of the device groups in your NetMRI.

1. Navigate to Config Management → Policy Design Center. Make sure the left pane is viewing By Device Groups.



2. From the screen shot above, highlight the device group and then scroll down on the right pane to the PSIRT section. Click on each PSIRT policy that you want to evaluate. Click Save when it becomes ungrayed.
3. After about 10 minutes or more depending upon the size of the device group and/or number of PSIRT policies enabled, navigate to Network Analysis → Issues to view Issues.



- Click on the Views pull-down menu and select PSIRT Violations. This will show only the PSIRT violations.

The screenshot shows the Infoblox GUI with the 'Views' menu open. The 'PSIRT Violations' option is highlighted. The main dashboard displays an overall score of 9.1 and a list of issues. The 'Issues' tab is active, showing a table of violations.

Severity	Last Seen	Title	Status	Component	# Affected	# New	# Cleared	# Suppressed
Error	2017-04-19 13:44:33	Router Interface Down	Current	Interfaces	4	0	0	0
Error	2017-04-19 13:26:10	Policy Violation: PSIRT High cisco-sa-20...	Current	Configurations	1	1	0	0
Error	2017-04-19 12:08:32	VLAN Member Priority	Current	VLANs	22	0	0	0
Error	2017-04-19 12:08:22	VLAN Member Minimum Priority	Current	VLANs	22	0	0	0
Error	2017-04-19 12:08:12	Device Issue Limit Exceeded	Current	Devices	7	0	0	0
Error	2017-04-19 12:06:53	Access Port With PortFast Disabled	Current	Interfaces	8	0	0	0
Error	2017-04-19 09:11:06	Policy Violation: PSIRT Crit cisco-sa-201...	Current	Configurations	8	0	0	0
Error	2017-04-19 09:11:06	Policy Violation: PSIRT Crit cisco-sa-200...	Current	Configurations	1	0	0	0
Error	2017-04-19 09:11:06	Policy Violation: PSIRT Crit cisco-sa-201...	Current	Configurations	10	0	0	0
Error	2017-04-19 09:11:06	Policy Violation: PSIRT Crit cisco-sa-201...	Current	Configurations	2	0	0	0
Error	2017-04-19 05:16:11	VLAN Toolbody Change	Current	VLANs	3	0	0	0
Warning	2017-04-19 13:48:10	Cisco Buffer Misses High	Current	Devices	1	0	0	0
Warning	2017-04-19 13:38:42	Interface Congested	Current	Interfaces	4	2	0	0

- After selecting the PSIRT view, you will see the following:

The screenshot shows the Infoblox GUI with the 'PSIRT Violations' view selected. The main dashboard displays an overall score of 9.1 and a list of issues. The 'Issues' tab is active, showing a table of violations.

Severity	Last Seen	Title	Status	Component	# Affected	# New	# Cleared	# Suppressed
Error	2017-04-19 09:11:06	Policy Violation: PSIRT Crit cisco-sa-200...	Current	Configurations	1	0	0	0
Error	2017-04-19 09:11:06	Policy Violation: PSIRT Crit cisco-sa-201...	Current	Configurations	8	0	0	0
Error	2017-04-19 09:11:06	Policy Violation: PSIRT Crit cisco-sa-201...	Current	Configurations	2	0	0	0
Error	2017-04-19 09:11:06	Policy Violation: PSIRT Crit cisco-sa-201...	Current	Configurations	10	0	0	0
Error	2017-04-19 13:26:10	Policy Violation: PSIRT High cisco-sa-20...	Current	Configurations	1	1	0	0

- Click on one of the links to view the affected devices.

Policy Violation: PSIRT Crit cisco-sa-20120328-pal
Showing details for LabCore group

Component: Configurations Correctness: -2.0
Severity: Error Stability: 0.0
Last Seen: 2017-04-19 09:11:06

In Device Group
Search...
All Devices (427)
 Routing (12)
 Switching (18)

Components Affected by Issue (Current)
Search...
Views: Filters: Display: [Icons]

Device Name	Device Type	IP Address	Rules	Passed	Error	Warning	Info	Details	Last Seen	Diff	Sup?
lme-3750-45-pd1-22.m	Switch (99%)	10.60.0.12	5	4	1	0	0	View	2017-04-19 09:11:06	Same	
lme-3660-45-pd3-25.m	Switch-Router (99%)	10.60.0.11	5	4	1	0	0	View	2017-04-19 09:11:06	Same	
pd3-31.klapr-laba.com	Switch (99%)	10.60.192.250	5	4	1	0	0	View	2017-04-19 09:11:06	Same	
coms3750	Switch-Router (99%)	10.60.3.34	5	4	1	0	0	View	2017-04-19 09:11:06	Same	
lme-switch	Switch-Router (99%)	10.60.30.253	5	4	1	0	0	View	2017-04-19 09:11:06	Same	
cisco-pd1-23	Switch-Router (99%)	10.60.192.253	5	4	1	0	0	View	2017-04-19 09:11:06	Same	
cisco-pd3-34	Switch-Router (99%)	10.60.192.26	5	4	1	0	0	View	2017-04-19 09:11:06	Same	
q3750-vlanc-switch.m	Switch (99%)	10.60.0.21	5	4	1	0	0	View	2017-04-19 09:11:06	Same	

Page: 1 of 1 | Displaying 1 - 8 of 8 | Updated at 2017-04-19 14:09:05

History | Description

- Click on one of the View links under the Details column.

Infoblox Configuration Policy Analysis
2017-04-19 09:11:06

Policy Violation: PSIRT Crit cisco-sa-20120328-pal
Cisco IOS Software Command Authorization Bypass CVE-2012-0384, Cisco IOS Software Command Authorization Bypass Vulnerability

Filter:
rules: 1
1: id=Vendor matches 'Cisco'

Error
Last Check: 2017-04-19 09:10:58

Policy Summary:

Category	Count	Percentage
Pass	4	(80.00%)
Fail	1	(20.00%)
Error	1	(20.00%)
Warning	0	(0.00%)
Info	0	(0.00%)
Debug	0	(0.00%)
Unknown	0	(0.00%)
Checked	5	(100.00%)

Rules Summary:

Rule	Result
PSIRT cisco-sa-20120328-pal Rule 1 CV1251609625	Pass
PSIRT cisco-sa-20120328-pal Rule 2 CV1545163038	Pass
PSIRT cisco-sa-20120328-pal Rule 3 CV110462254	Pass
PSIRT cisco-sa-20120328-pal Rule 4 CV987321223	Pass
PSIRT cisco-sa-20120328-pal Rule 5 CV1824588525	Error

Device: C3750-vlanc-switch.m
IP: 10.60.0.21
Model: c3750v37x3chack
Version: 12.2(55)SE3
Last Check: 2017-04-19 14:07:21

Rule PSIRT cisco-sa-20120328-pal Rule 5
Cisco IOS Software Command Authorization Bypass

Filter:
rules: 1
1: id=Vendor matches 'Cisco'

Error

Remediation:
<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20120328-bundle>

Logic:
(srcIpAnySec &= 'Cisco IOS Software, C3750 Software (C3750E-UNIVERSAL-K9-M), Version 12.2(55)SE3, RELEASE SOFTWARE (fcl) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2011 by Cisco Systems, Inc. Compiled the 05-May-11 13:48 by prod_rel_team')

- Scroll down the screen if necessary to view the error details. This screen shows the title of the PSIRT, filter used to choose the device to evaluate, the remediation link, and the logic for evaluating the filtered device.

Rule PSIRT cisco-sa-20120328-pal Rule 5
Cisco IOS Software Command Authorization Bypass

Filter:
rules: 1
1: id=Vendor matches 'Cisco'

Error

Remediation:
<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20120328-bundle>

Logic:
(srcIpAnySec &= 'Cisco IOS Software, C3750 Software (C3750E-UNIVERSAL-K9-M), Version 12.2(55)SE3, RELEASE SOFTWARE (fcl) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2011 by Cisco Systems, Inc. Compiled the 05-May-11 13:48 by prod_rel_team')

- Copy and paste the remediation URL. In this case it is:
<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20120328-bundle>

- Here is the result of the URL:

Cisco Security

Cisco Security Advisories

Vulnerabilities

Filter By Product

Quick Search

Advanced Search

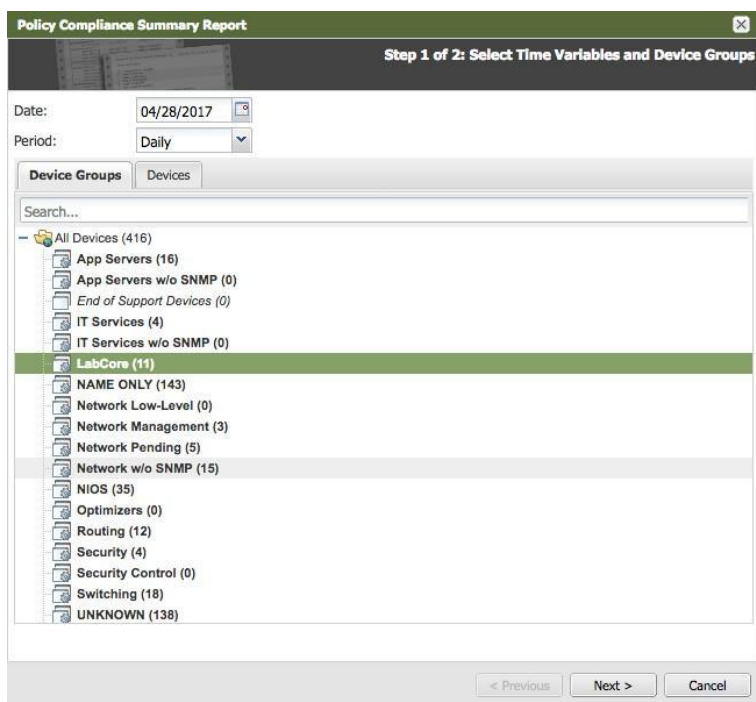
ADVISORY	IMPACT	CVE	LAST UPDATED	VERSION
<input type="text" value="Search Advisory Name"/>	<div>All</div>	<input type="text" value="Search CVE"/>	<div>Most Recent</div>	
<div><div></div><div>Cisco IOS XR Software Cisco Discovery Protocol Format String Vulnerability</div></div>	High	CVE-2020-3118	2020 Oct 20	1.1
<div><div></div><div>Cisco Webex Teams Client for Windows DLL Hijacking Vulnerability</div></div>	High	CVE-2020-3535	2020 Oct 07	1.0
<div><div></div><div>Cisco Identity Services Engine Authorization Bypass Vulnerability</div></div>	High	CVE-2020-3467	2020 Oct 07	1.0
<div><div></div><div>Cisco Video Surveillance 8000 Series IP Cameras Cisco Discovery Protocol Remote Code Execution and Denial of Service Vulnerability</div></div>	High	CVE-2020-3544	2020 Oct 07	1.0

Feedback

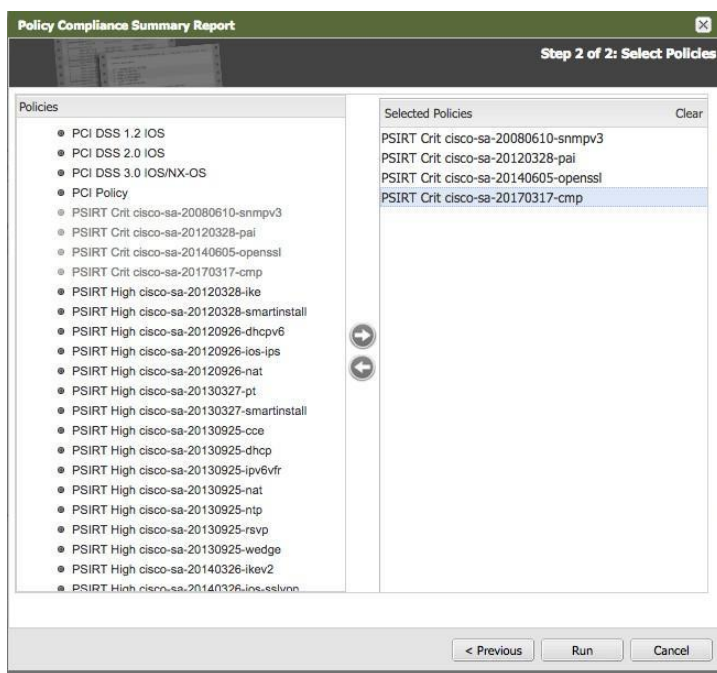
11. From this screen, you can find out details of the vulnerability and fix for the vulnerability.
12. In addition, you can run a Policy Compliance Summary report to show the number of devices in a device group that have vulnerabilities. Navigate to Reports → Report Gallery. Move the mouse pointer to the Policy Compliance Summary report.



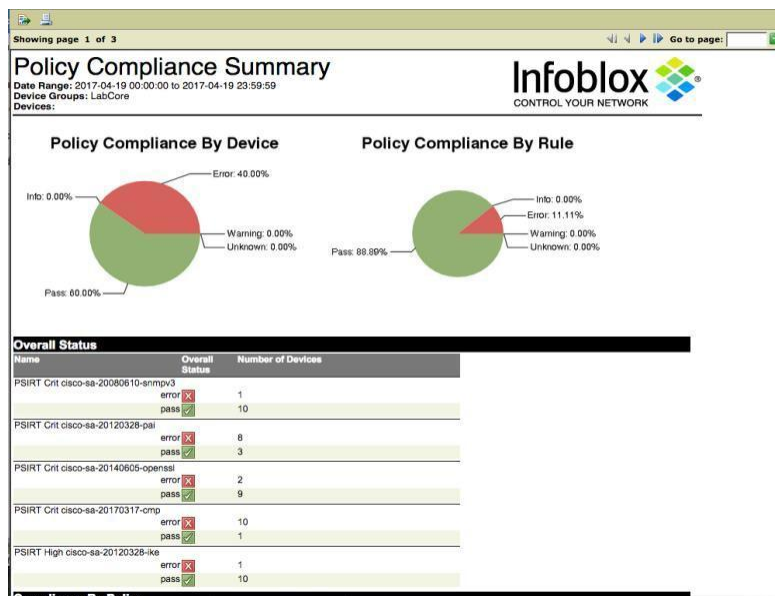
13. Click on the 'Next' link.



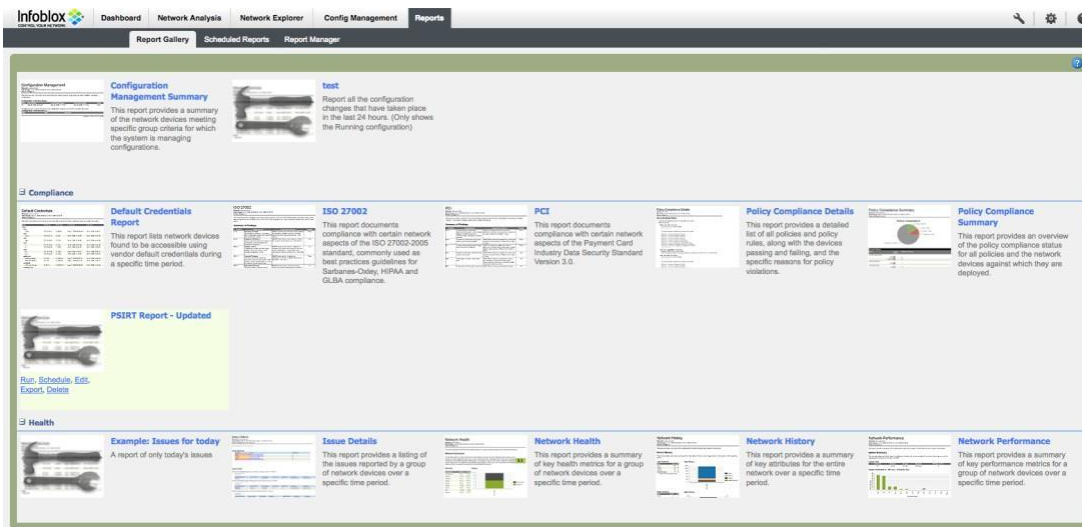
14. Select the PSIRTs that were used in the screen shot in step 1 as an example



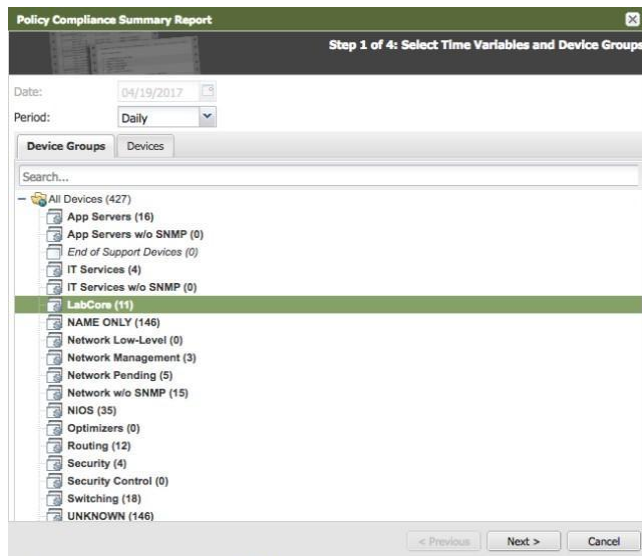
15. Click on the 'Run' button. The following screen appears. At the upper left of the screen, you can choose to download the report in PDF, Excel, or MS Word in addition to printing the report.



16. You can have the report scheduled to be sent out via email. Highlight the PSIRT Report and click on the schedule button.



17. Select the device group. Click Schedule.



18. Select the PSIRT policies and click Next.

Policy Compliance Summary Report Step 2 of 4: Select Policies

Policies

- IB_6112 Med CVE-2016-9131
- JN Crit CVE-2013-6618
- JN High CVE-2014-3818
- JN Med CVE-2013-7313
- NSA 1.1c IOS
- PCI DSS 1.2 IOS
- PCI DSS 2.0 IOS
- PCI DSS 3.0 IOS/NX-OS
- PCI Policy
- PSIRT Crit cisco-sa-20080610-snmpv3
- PSIRT Crit cisco-sa-20120328-pai
- PSIRT Crit cisco-sa-20140605-openssl
- PSIRT Crit cisco-sa-20170317-cmp
- PSIRT High cisco-sa-20120328-ike
- PSIRT High cisco-sa-20120328-smartinstall
- PSIRT High cisco-sa-20120926-dhcpv6
- PSIRT High cisco-sa-20120926-ios-ips
- PSIRT High cisco-sa-20120926-nat
- PSIRT High cisco-sa-20130327-pt
- PSIRT High cisco-sa-20130327-smartinstall
- PSIRT High cisco-sa-20130925-ccs
- PSIRT High cisco-sa-20130925-dhcp
- PSIRT High cisco-sa-20130925-ipv6vfr
- PSIRT High cisco-sa-20130925-nat

Selected Policies Clear

- PSIRT Crit cisco-sa-20080610-snmpv3
- PSIRT Crit cisco-sa-20120328-pai
- PSIRT Crit cisco-sa-20140605-openssl
- PSIRT Crit cisco-sa-20170317-cmp
- PSIRT High cisco-sa-20120328-ike

< Previous Next > Cancel

19. Enter the email address, output format, recurrence pattern, execution time, and day of week. Click Next.

Policy Compliance Summary Report Step 3 of 4: Select Report Scheduling

Report Name: Policy Compliance Summary

To Emails: management@xyzcorp.com

To Users: NetMRI Admin ()
dave signori ()
psirt psirt ()
support support ()
test test ()

Output Format: pdf

Recurrence Pattern: Weekly

Execution Time: 6:00 AM

☐ Sunday ☐ Tuesday ☐ Thursday ☐ Saturday
☒ Monday ☐ Wednesday ☐ Friday

< Previous Next > Cancel

20. Verify the settings are correct. Click Schedule.

Policy Compliance Summary Report
Step 4 of 4: Summary of Scheduled Report

Report Name: Policy Compliance Summary
Date: 04/19/2017
Period: Daily
Device Groups: LabCore

Devices:
Policies: PSIRT Crit cisco-sa-20080610-snmpv3, PSIRT Crit cisco-sa-20120328-pal, PSIRT Crit cisco-sa-20140605-openssl, PSIRT Crit cisco-sa-20170317-cmp, PSIRT High cisco-sa-20120328-ike

To Emails: management@xyzcorp.com
To Users:
Schedule: Weekly - Monday at 06:00 AM

< Previous Schedule Cancel

Device Life Cycle Management

After installation of the Empowered Networks' Empowered Advisor, you can do the following to gather the Life Cycle information on your devices. In this example, we are using the LabCore device group.

1. Navigate to Network Explorer → Inventory. Select the device group and then select All Devices.

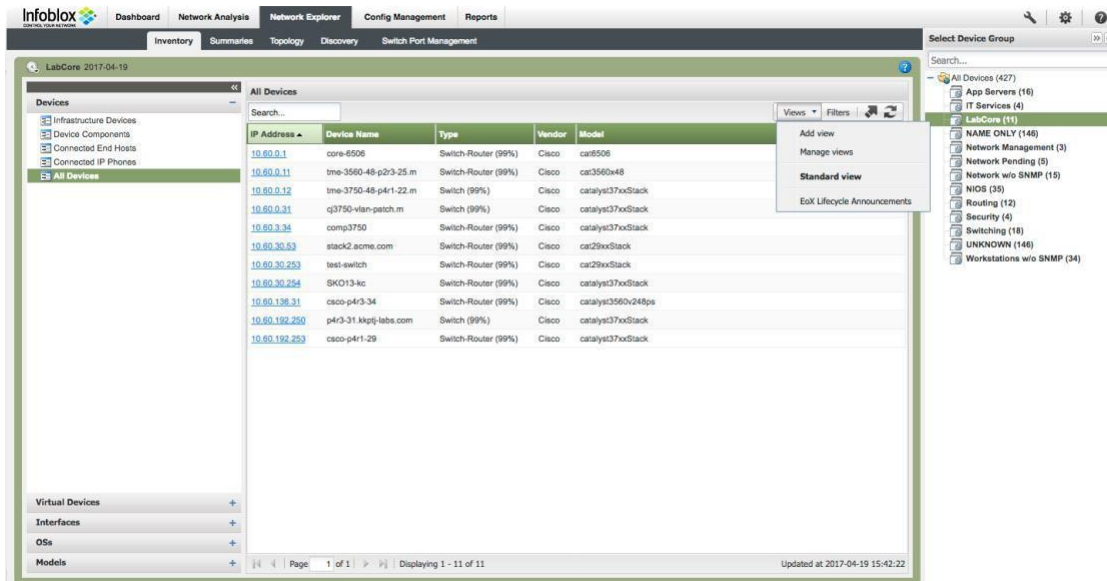
The screenshot shows the Infoblox Network Explorer interface. The 'Inventory' tab is selected, and the 'All Devices' list is displayed. The list includes columns for IP Address, Device Name, Type, Vendor, and Model. The following table represents the data shown in the screenshot:

IP Address	Device Name	Type	Vendor	Model
10.60.0.1	core-6506	Switch-Router (99%)	Cisco	cat6506
10.60.0.11	tme-3560-48-p2r3-25.m	Switch-Router (99%)	Cisco	cat3560w48
10.60.0.12	tme-3750-48-p4r1-22.m	Switch (99%)	Cisco	catalyst37xxStack
10.60.0.31	q3750-vlan-patch.m	Switch (99%)	Cisco	catalyst37xxStack
10.60.3.34	comp3750	Switch-Router (99%)	Cisco	catalyst37xxStack
10.60.30.63	stack2.acme.com	Switch-Router (99%)	Cisco	cat29xxStack
10.60.30.253	test-switch	Switch-Router (99%)	Cisco	cat29xxStack
10.60.30.254	SKO13-ko	Switch-Router (99%)	Cisco	catalyst37xxStack
10.60.136.31	cisco-p4r3-34	Switch-Router (99%)	Cisco	catalyst3560v248ps
10.60.192.250	p4r3-31.kopj-labs.com	Switch (99%)	Cisco	catalyst37xxStack
10.60.192.253	cisco-p4r1-29	Switch-Router (99%)	Cisco	catalyst37xxStack

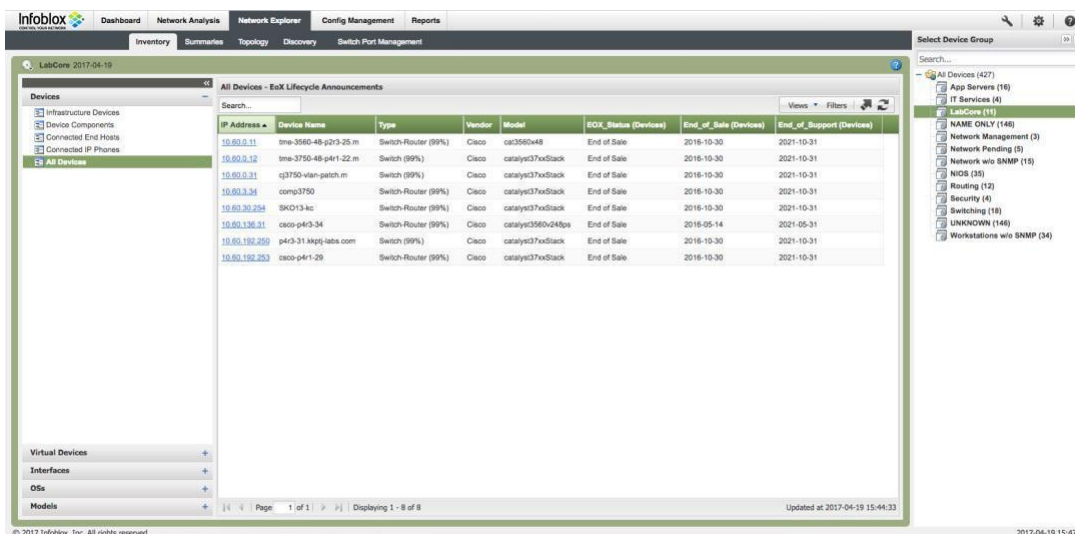
Virtual Devices: +
Interfaces: +
OSs: +
Models: +

Page 1 of 1 | Displaying 1 - 11 of 11 | Updated at 2017-04-19 15:42:22

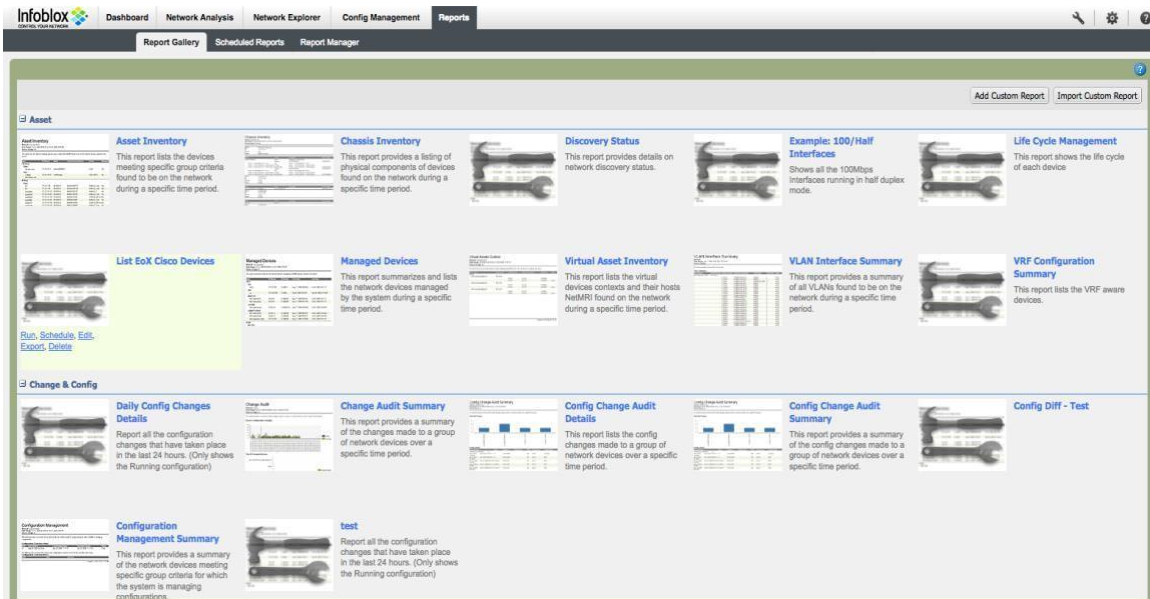
- Click on the Views drop down menu and select EoX Lifecycle Announcements view.



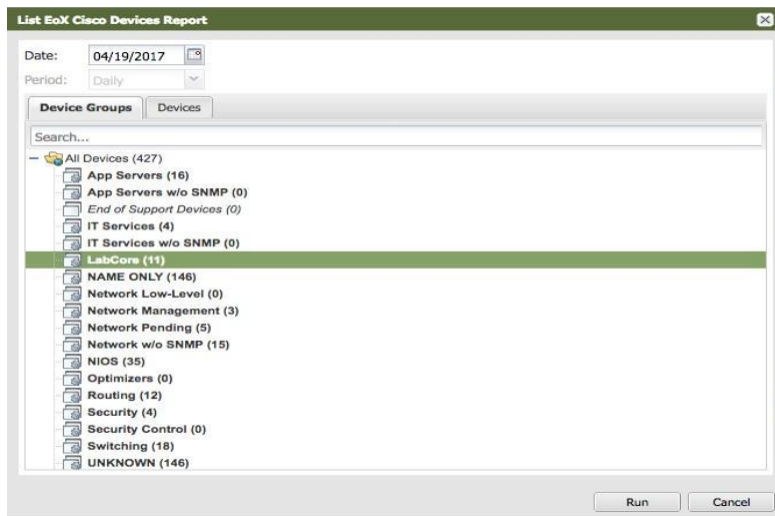
- Here are the results. In this device group, all of the devices are end-of-sale. The end-of-sale date is listed along with the end-of-support date. This information will allow you to plan a budget to replace the affected switches.



- You can run a report on the end-of-life devices. Navigate to Reports → Report Gallery → Asset → List EoX Cisco Devices.



- Click on the Run button in the screen above. Select the device group and then click on the Run button.



- The following screen appears.

List EoX Cisco Devices

Date Range: 2017-04-19 00:00:00 to 2017-04-19 23:59:59
Device Groups: LabCore

Search...

Views Filters

Name	Model	Type	Vendor	SNMP ByLocation	EoX_Status	End_of_Sale	End_of_Support
lme-3750-48-p4r1-22.m	catalyst3750Stack	Switch	Cisco		End of Sale	2016-10-30	2021-10-31
lme-3560-48-p2r3-25.m	cat3560e48	Switch-Router	Cisco		End of Sale	2016-10-30	2021-10-31
p4r3-31.kkplg-labs.com	catalyst3750Stack	Switch	Cisco		End of Sale	2016-10-30	2021-10-31
SKO13-ko	catalyst3750Stack	Switch-Router	Cisco		End of Sale	2016-10-30	2021-10-31
comp3750	catalyst3750Stack	Switch-Router	Cisco	Lab	End of Sale	2016-10-30	2021-10-31
cisco-p4r1-29	catalyst3750Stack	Switch-Router	Cisco		End of Sale	2016-10-30	2021-10-31
q3750-vlan-patch.m	catalyst3750Stack	Switch	Cisco		End of Sale	2016-10-30	2021-10-31
cisco-p4r3-34	catalyst3560v248ps	Switch-Router	Cisco		End of Sale	2016-05-14	2021-05-31

- This report can also be scheduled and sent to an email address on a periodic basis. Highlight the List EoX Cisco Devices report and click on the Schedule button.

Infoblox Dashboard Network Analysis Network Explorer Config Management Reports

Report Gallery Scheduled Reports Report Manager

Add Custom Report Import Custom Report

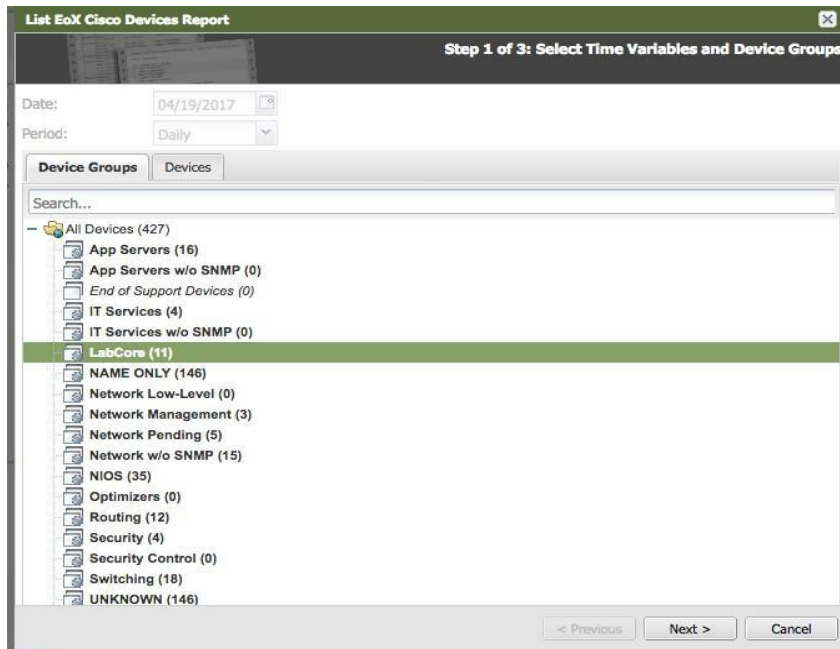
Asset

- Asset Inventory**
This report lists the devices meeting specific group criteria found to be on the network during a specific time period.
- Chassis Inventory**
This report provides a listing of physical components of devices found on the network during a specific time period.
- Discovery Status**
This report provides details on network discovery status.
- Example: 100/Half Interfaces**
Shows all the 100Mbps interfaces running in half duplex mode.
- Life Cycle Management**
This report shows the life cycle of each device.
- List EoX Cisco Devices**
Run Schedule Edit Export Data
- Managed Devices**
This report summarizes and lists the network devices managed by the system during a specific time period.
- Virtual Asset Inventory**
This report lists the virtual devices contexts and their hosts found on the network during a specific time period.
- VLAN Interface Summary**
This report provides a summary of all VLANs found to be on the network during a specific time period.
- VRF Configuration Summary**
This report lists the VRF aware devices.

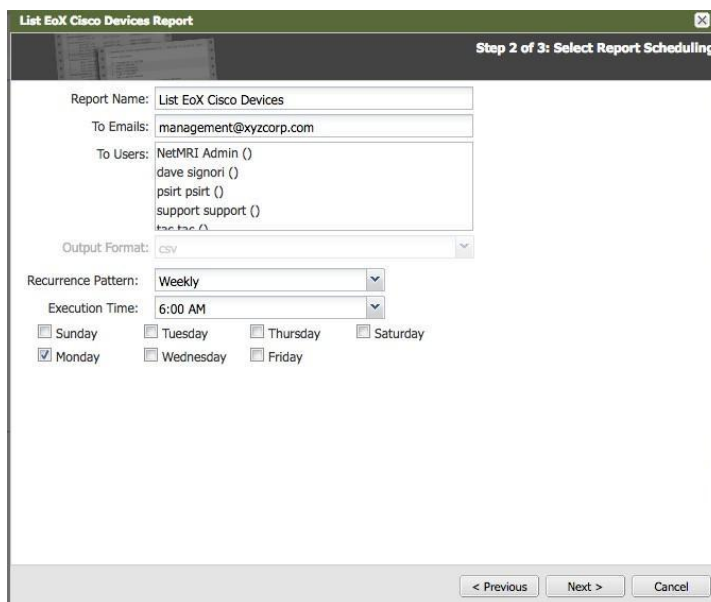
Change & Config

- Daily Config Changes Details**
Report all the configuration changes that have taken place in the last 24 hours. (Only shows the Running configuration)
- Change Audit Summary**
This report provides a summary of the changes made to a group of network devices over a specific time period.
- Config Change Audit Details**
This report lists the config changes made to a group of network devices over a specific time period.
- Config Change Audit Summary**
This report provides a summary of the config changes made to a group of network devices over a specific time period.
- Config Diff - Test**
- Configuration Management Summary**
This report provides a summary of the network devices meeting specific group criteria for which the system is managing configurations.
- test**
Report all the configuration changes that have taken place in the last 24 hours. (Only shows the Running configuration)

8. Select the Device Group and click Next.



9. Type in the email address and select the recurrence pattern, execution time, and day. Click Next.



10. Verify the settings are correct. Click Schedule.

List EoX Cisco Devices Report [X]

Step 3 of 3: Summary of Scheduled Report

Report Name: List EoX Cisco Devices

Date: 04/19/2017

Period: Daily

Device Groups: LabCore

Devices:

To Emails: management@xyzcorp.com

To Users:

Schedule: Weekly - Monday at 06:00 AM

< Previous Schedule Cancel



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 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | 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).