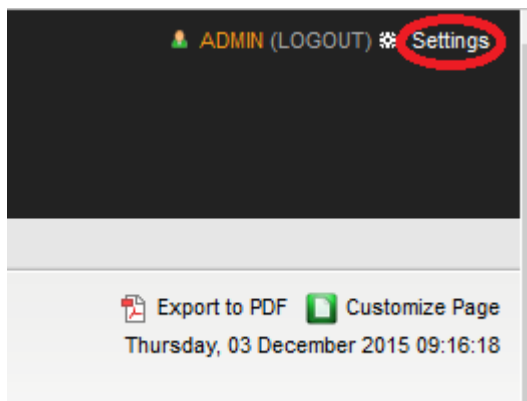


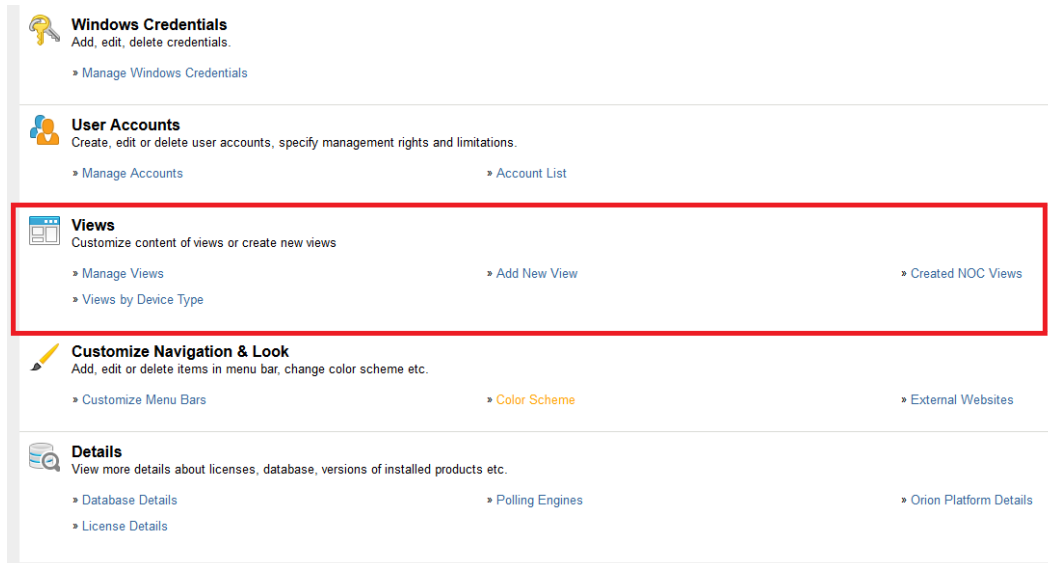
How to Create a DISA STIG Dashboard

This document was developed to assist you in creating a dashboard for you various NCM Compliance Policies.

Step 1. Navigate to the settings menu located at the far upper right hand corner of you web console.



Step 2. Navigate to Views located at the bottom of your web console. Select “Add New View”



Step 3. Give the new View a Name. I chose Network Audit for this view. Leave the summary page option. Click “Submit” when done.

Admin > Views > Manage Views >

Add New View

Name of New View

Type of View ▾

SUBMIT

VIEW TYPES:

Summary
Summary views display network-wide information.

Node Details
Node Details views display information about a single node.

Volume Details
Volume Details views display information about a single volume.

Active Alert Details
Active Alert Details views display information about single active alert.

Step 4. Here you will need to add “Policy Violations” to your various columns. I have three columns selected. Once you have added these to your columns click “Done”.

Customize Network Audit

Name

Type of view: **Summary**

Left Navigation

Is there a lot of content on this view? Break it up into smaller pages with tabs on the left.

Enable left navigation

Column 1 ✕

Resources

- Policy Violations
- Policy Violations

Width: px

Column 2 ✕

Resources

- Policy Violations
- Policy Violations

Width: px

Column 3 ✕

Resources

- Policy Violations
- Policy Violations

Width: px

TIP: You can use up to 6 columns

NOC View > List of created NOC views
Network Operations Center (NOC) is a view specially designed for Orion status overview
In case that NOC view mode and left navigation is enabled, the view will automatically rotate through the content of each tab(page).

Enable NOC view mode

View Limitation
You can create a view limitation that will limit the network devices that can be displayed on this view. Account limitations for the logged-in account will also be applied to this view when it is displayed.

No View Limitation defined.

Step 5. Navigate to the “Customize Navigation & Look” section. Click on “Customize Menu Bars” selection.

The screenshot shows a navigation menu with several sections:

- Windows Credentials**: Add, edit, delete credentials. [Manage Windows Credentials](#)
- User Accounts**: Create, edit or delete user accounts, specify management rights and limitations. [Manage Accounts](#) [Account List](#)
- Views**: Customize content of views or create new views. [Manage Views](#) [Add New View](#) [Created NOC Views](#)
[Views by Device Type](#)
- Customize Navigation & Look** (highlighted with a red border): Add, edit or delete items in menu bar, change color scheme etc. [Customize Menu Bars](#) [Color Scheme](#) [External Websites](#)
- Details**: View more details about licenses, database, versions of installed products etc. [Database Details](#) [Polling Engines](#) [Orion Platform Details](#)
[License Details](#)

Step 6. Navigate to the Menu Bar: NCM_TabMenu and click “Edit”.

The screenshot displays a list of menu bars, each with an 'Edit' (pencil icon) and 'Delete' (red X icon) button:

- Menu Bar: DeviceTracker_TabMenu**: Device Tracker Summary
- Menu Bar: FIREWALLS_TabMenu**: FSM Summary
- Menu Bar: Guest**: Summary Events Quality of Experience Environment
- Menu Bar: NCM_TabMenu** (highlighted with a red border): Config Summary Configuration Management Config Change Templates Reports Compliance Jobs Site Audit End of Support
- Menu Bar: Network_TabMenu**: NPM Summary Network Top 10 Wireless VSANs Overview

Step 7. Locate your view on the Available Items columns below. Drag the selection to the Selected Items column. Once you hover over the Selected Items column space will auto-magically appear for you to drop your selection. Select “Submit” when done.

Edit NCM_TabMenu Menu Bar

Drag items from the Available Items column to the Selected Items column to build your menu bar. Rearrange items by dragging them. Select the 'Submit' button to save changes.

Available items	Selected items
% Loss & Traffic	Config Summary
Accounts	Configuration Management
Admin	Config Change Templates
Alerts	Reports
All Interfaces	Compliance
All Maps <input type="button" value="Edit"/> <input type="button" value="X"/>	Jobs
All Nodes	Site Audit <input type="button" value="Edit"/> <input type="button" value="X"/>
All Volumes	End of Support
Custom Summary	<input type="button" value="SUBMIT"/> <input type="button" value="CANCEL"/>
Customize	<input type="text" value="Network Audit"/> <input type="button" value="Edit"/> <input type="button" value="X"/>
Device Tracker Summary	
Down Nodes	
EnergyWise	
Environment	
Errors & Discards	
Event Summary	
Events	
FSM Summary	
Groups	
<input type="text"/>	
Help	

1

2

3

Results:

Menu Bar: DeviceTracker_TabMenu

 Edit |  Delete

Device Tracker Summary

Menu Bar: FIREWALLS_TabMenu

 Edit |  Delete

FSM Summary

Menu Bar: Guest

 Edit |  Delete

Summary Events Quality of Experience Environment

Menu Bar: NCM_TabMenu

 Edit |  Delete

Config Summary Configuration Management Config Change Templates Reports Compliance Jobs Site Audit **Network Audit** End of Support

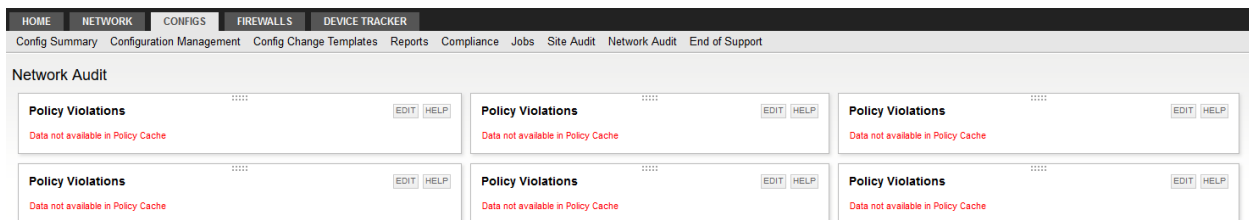
Menu Bar: Network_TabMenu

 Edit |  Delete

NPM Summary Network Top 10 Wireless VSANs Overview

NEW MENU BAR

Step 8. Navigate to the Configs Tab > Network Audit section. Select a Policy Violation window and click “Edit” within that window.



HOME NETWORK CONFIGS FIREWALLS DEVICE TRACKER

Config Summary Configuration Management Config Change Templates Reports Compliance Jobs Site Audit Network Audit End of Support

Network Audit

Policy Violations	Policy Violations	Policy Violations
Data not available in Policy Cache	Data not available in Policy Cache	Data not available in Policy Cache
EDIT HELP	EDIT HELP	EDIT HELP

Policy Violations	Policy Violations	Policy Violations
Data not available in Policy Cache	Data not available in Policy Cache	Data not available in Policy Cache
EDIT HELP	EDIT HELP	EDIT HELP

Step 9. Here I am using this particular window for Layer 2 Switches. I have selected all the Layer 2 Switch Reports for this window. Click “Submit” when done.

Edit Resource: Policy Violations

Title:

Subtitle:

Select Policy Reports:

- Basic Config Report
- STIG-V8R19-CSCO-OS-L2SW - Misc
- STIG-V8R19-CSCO-OS-L2SW - NTP and SNMP
- STIG-V8R19-CSCO-OS-L2SW - OOB Network
- STIG-V8R19-CSCO-OS-L2SW - Services
- STIG-V8R19-CSCO-OS-L2SW - SSH
- STIG-V8R19-CSCO-OS-L2SW - Switch Interfaces
- STIG-V8R19-CSCO-OS-L2SW - User Access
- STIG-V8R19-CSCO-OS-L2SW - VLAN 1
- STIG-V8R19-CSCO-OS-L2SW - VTY and Console
- STIG-V8R19-CSCO-OS-L2SW-ALL
- STIG-V8R19-CSCO-OS-PRTR - External Interface
- STIG-V8R19-CSCO-OS-PRTR - Inbound ACL
- STIG-V8R19-CSCO-OS-PRTR - Misc
- STIG-V8R19-CSCO-OS-PRTR - Multicast and IPV6
- STIG-V8R19-CSCO-OS-PRTR - NTP and SNMP
- STIG-V8R19-CSCO-OS-PRTR - OOB and VPN
- STIG-V8R19-CSCO-OS-PRTR - Outbound ACL
- STIG-V8R19-CSCO-OS-PRTR - Routing
- STIG-V8R19-CSCO-OS-PRTR - Services
- STIG-V8R19-CSCO-OS-PRTR - SSH and Log
- STIG-V8R19-CSCO-OS-PRTR - Tunneling
- STIG-V8R19-CSCO-OS-PRTR - User Access
- STIG-V8R19-CSCO-OS-PRTR - VLANS
- STIG-V8R19-CSCO-OS-PRTR - VTY
- STIG-V8R19-CSCO-OS-PRTR-ALL
- V8R18 - Juniper - Part 1 of 3
- V8R18 - Juniper - Part 2 of 3
- V8R18 - Juniper - Part 3 of 3

SUBMIT

Step 10. Repeat the above process as many times as you see fit to capture all your Compliance Reports and Policies. As you complete each Policy Window you will have a similar result below.

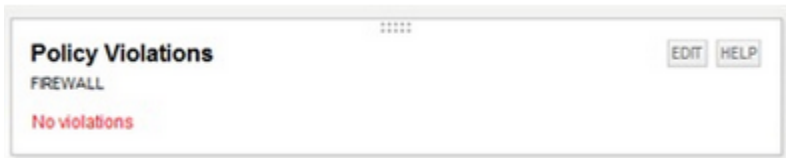
The image shows three screenshots of the Policy Violations report interface. Each screenshot displays a table of policy violations for a specific device type, categorized by severity (CAT I, CAT II, CAT III) and showing counts for each category. The first screenshot is for a Layer 2 Switch, the second for an Infrastructure Layer 3 Switch, and the third for a Perimeter Router. Each report includes a 'My Rules' section and a 'View All Policy Reports' link.

NAME	CAT III	CAT II	CAT I
-L2SW-AAA	1	0	0
-L2SW-Accounts	0	1	3
-L2SW-L2SW-Logging	2	0	0
-L2SW-L2SW-NTP	2	2	0
-L2SW-Misc Services	4	1	0
-L2SW-OOB Network	5	47	0
-L2SW-Other	29	0	0
-L2SW-SNMP	2	0	0
-L2SW-Switch Interfaces	0	33	0
-L2SW-VLAN 1	8	0	0
-L2SW-VTY and Console	0	0	1

NAME	CAT III	CAT II	CAT I
-L3SW-Accounts	2	2	4
-L3SW-ACL	2	4	0
-L3SW-INT-AAA	2	1	0
-L3SW-IPv6	4	3	0
-L3SW-Logging	1	0	0
-L3SW-Misc	5	4	0
-L3SW-NTP	3	0	0
-L3SW-OOB	4	20	0
-L3SW-Other	10	18	0
-L3SW-Port Security	2	2	0
-L3SW-Router Interfaces	2	0	0
-L3SW-Routing Protocol	6	4	2
-L3SW-SNMP	1	3	1
-L3SW-SSH	0	1	0
-L3SW-Switch Interfaces	6	12	2
-L3SW-VLAN1	2	4	0
-L3SW-VTY	0	3	2

NAME	CAT III	CAT II	CAT I
-PRTR-AAA	4	2	0
-PRTR-Access-List	0	108	0
-PRTR-Accounts	0	2	4
-PRTR-Inbound ACL	2	4	8
-PRTR-Logging	4	0	0
-PRTR-Misc Services	10	0	0
-PRTR-NTP	4	1	0
-PRTR-OOB	2	0	0
-PRTR-Outbound ACL	0	2	2
-PRTR-SNMP	2	2	0

**** Note **** At this time, if there are no policy violations for a selected window, you will receive the following result.



This will also occur if the auditing process is incomplete or “broken” efforts are being made to correct this anomaly and simply report “0” in the column.

Thank you for your time and please do not forget to “Like” and/or “Rate” this items how you see fit.

Respectfully,
CourtesyIT