




# How to Use the Compliance Feature in Solarwinds using Network Configuration Manager (NCM) for DISA Security Technical Information Guides (STIG), National Institute of Standards and Technology (NIST), and Payment Card Industry (PCI) Guidelines and Requirements



































































Welcome to the Compliance feature of NCM. I have been working with this feature from the days of Cirrus. When I first started on this project, I was getting inspected about once every 6 months and found it took about two weeks of review, meetings, mitigation, and after action reports. Meanwhile, my production work was put on hold and started backing up. There had to be a better more efficient way of going about these inspections. So I looked at Solarwinds NCM (Cirrus) and started my journey. By the time I was down building the templates, rules, policies and reports, my inspection time when from around two weeks to three days.

These reports were developed for you as a template to give you a better understanding of how to use NCM to your benefit and provide reports to management on the status of you network. Some rules will require some customization given your environment and others can be run right from the get go. Some rules are using regular expressions and others use plain text strings to find a match or not match for the trigger condition.


Let us look at a sample report. On the left hand side you will have a list of all your devices you have selected for this report. The default is to select all "Cisco" devices on your network. The report will run against the configuration you have saved/backed up in NCM. If the rule fails or the condition for a positive result is not met then you will get one of these symbols:

- CAT I Finding: 
- CAT II Finding: 
- CAT III Finding: 

If the column is blank then the rule has passed and your system for this finding is now compliant.

STIG-V8R18-CSCO - Switchport Interfaces (searched 340 configs)										
NodeName	CSCO-R17-NET-NAC-009 - V05626 - Switchport Interfaces (34 violations)	CSCO-R17-NET-NAC-012 - V.05624 - Switch Interfaces (34 violations)	CSCO-R17-NET-VLAN-002 - V.03973 - Switch Interfaces (34 violations)	CSCO-R17-NET-VLAN-004 - V.03971 - Switch Interfaces (4 violations)	CSCO-R17-NET-VLAN-005 - V.03972 - Switch Interfaces (34 violations)	CSCO-R17-NET-VLAN-006 - V.05628 - Switch Interfaces (34 violations)	CSCO-R17-NET-VLAN-007 - V.05623 - Switch Interfaces (0 violations)	CSCO-R17-NET-VLAN-008 - V.05622 - Switch Interfaces (34 violations)	CSCO-R17-NET-VLAN-009 - V.03984 - Switch Interfaces (34 violations)	CSCO-R17-NET-VLAN-024 - V-18545 - Switch Interface (34 violations)
My Devices										
										
										
										
										
										
										
										

## How it Works:

In the first example, we see this rule looking for a string of characters matching **service call-home**. If this string is found then the rule will place a  warning symbol in the column on the report.

### Edit CSCO-R17-NET0405 - V-28784 - Service

Rules describe what is to be found (or not found) in configuration files. If the rule is not met, the rule violation will appear with the error level set below in the policy report.

#### IDENTIFY THIS RULE

Rule name:

Description:

Alert level:  Informational  Warning  Critical

Save in folder:

#### STRING MATCHING

Alert on the rule below if  String is found  String is NOT found

**Advanced Config Search**(block search and/or search)

String:

String type:  Regular Expression (Regex)  Find String

Strings can be a [Regular Expression](#), or a simple find expression using "\*" and "?". A policy rule may test for the line to be found, such as an access list, or not to be found, such as 'public' for a community string.

#### REMEDIATION

Remediation script:

When a rule violation is found, you will have the option of running this script. [More about remediation.](#)

In the second example, we see this rule looking for a couple TACACS servers for authentication. This is where some of the customization will need to be done. Replace the **[text]** with your specific organization requirements and conventions to validate the rule.

Edit CSCO-R17-NET0433 - V-15432 - AAA

Rules describe what is to be found (or not found) in configuration files. If the rule is not met, the rule violation will appear with the error level set below in the policy report.

**IDENTIFY THIS RULE**

Rule name:

Description:

Alert level:  Informational  Warning  Critical


Save in folder:

**STRING MATCHING**

Alert on the rule below if  String is found  String is NOT found

Advanced Config Search(block search and/or search)

AND/OR	PARENS (OPTIONAL)	MUST/MUST NOT CONTAIN	STRING TYPE	STRING	PARENS (OPTIONAL)
		must contain	Find string	aaa group server tacacs+ [Server-Group Name]	
and		must contain	Find string	server-private [Primary Server IP] key	X
and		must contain	Find string	server-private [Secondary Server IP] key	X

If the configuration fails to have the requested string of characters, then a  symbol will be placed in the column on your report.

**Notes:**

If you make a change on your device, you will need to download the current configuration prior to running the rule you are evaluating to get the correct results.

# The Manual Verification Reports

Some of the findings and criteria will need specific visual verification in order to pass the test. These will always trigger an alert. For most of these, I have configured an Access-List on the device that is a text based ACL and is not applied to the system. Using the **remarks** key word in the ACL cli is very helpful for documenting system items.

V8R18 - Cisco - Manual Verification

Last updated Tuesday, March 24, 2015 11:56:05 PM

REPORT DETAILS

Export

STIG-V8R18-CSCO - Manual Verification Required R8V16 (searched 204 configs)

NodeName	CSCO-R16-NET1288 - V-25890 - Manual Verification (34 violations)	CSCO-R16-NET1289 - V-25891 - Manual Verification (34 violations)	CSCO-R17-NET0162 - V-04622 - Manual Verification (34 violations)	CSCO-R17-NET0190 - V-03005 - Manual Verification (34 violations)	CSCO-R17-NET1030 - V-03072 - Manual Verification (34 violations)	CSCO-R17-NET1808 - V-17814 - VPN (34 violations)
My Devices	⚠	ℹ	✖	ℹ	ℹ	⚠
	⚠	ℹ	✖	ℹ	ℹ	⚠
	⚠	ℹ	✖	ℹ	ℹ	⚠
	⚠	ℹ	✖	ℹ	ℹ	⚠
	⚠	ℹ	✖	ℹ	ℹ	⚠
	⚠	ℹ	✖	ℹ	ℹ	⚠
	⚠	ℹ	✖	ℹ	ℹ	⚠
	⚠	ℹ	✖	ℹ	ℹ	⚠
	⚠	ℹ	✖	ℹ	ℹ	⚠
	⚠	ℹ	✖	ℹ	ℹ	⚠

## How do I Build My Own Reports

Please visit this document: How to Create a Policy Report - <https://thwack.solarwinds.com/docs/DOC-174979>

## Different Type of Reports

You will notice various report and rules will have a "NA" or "XX" in the title. These are rules and reports that are either *Not Applicable* or *Not Supported* by the device vendor. If you run into some of these you may delete them if you choose. I wanted to provide all the rules possible for coverage.

I hope this document has been helpful. If you have any questions or comments, feel free to contact me here on Thwack.

Regards,

CourtesyIT

