

Table of Contents

Reports	1
Show Report	2
Compliance report	3
API	4

Reports

Compliance

Dashboard **Reports** Policies Licensed nodes

Saved reports:

Report name: Public

Report type:

Compliance status:

Show report

Through reports you can view the results of compliance. The first screen you'll see is a form to create your reports, based on specific filters. You can show reports based on nodes, or policies. Each with their own sets of filters that can be combined. You can select this with the *Report type* dropdown.

You are able to save these filters as a saved report. Saved reports can be public or non-public. If a saved report is public then other people can view your report (but not edit it), if not then only you can see it. You can save a report with the "save"-button, and delete it with the "delete"-button if you so desire.

Note that if you edit the report name, it will edit the name of that report. If you have a saved report selected and want to create a new one, use the "Saved reports"-dropdown and select the empty option. This will allow you to create a new saved report.

Policy reports can be filtered on policy name:

Saved reports:

Report name: Public

Report type:

Policy name:

Compliance status:

Show report

And node reports can be filtered on node name, vendor, domain, fqdn, polling group and node model (the model as denoted by its config):

Saved reports:	<input type="text" value="cisco_diag_report"/>
Report name:	<input type="text" value="cisco_diag_report"/> <input checked="" type="checkbox"/> Public <input type="button" value="Save"/> <input type="button" value="Delete"/>
Report type:	<input type="text" value="nodes"/>
Hostname:	<input type="text" value="*"/>
Compliance status:	<input type="text" value="no"/>
Vendor:	<input type="text" value="Cisco_IOS"/>
Node group:	<input type="text" value="Cisco_IOS"/>
Polling group:	<input type="text" value="cisco_IOS"/>
Domain:	<input type="text" value="YCE"/>
Node model:	<input type="text"/>
Node fqdn:	<input type="text"/>

And of course you can filter on compliant and non-compliant policies and nodes. When your filters are set correctly you can view your report by clicking on the "Show report"-button.

Show Report

Policies

Policy name	Compliant?	Severity
cisco_diagnostics regexp	no	-
cisco_diagnostics	no	-
cisco_diagnostics_hostname	no	-
cisco_ios	no	-
cisco_more_diag	no	-
fortigate	no	-

1 / 1 250 items per page 1 - 19 of 19 items

Search Show report

Compliance checks

Hostname	Policy	Fqdn	Severity	Compliant?	Last check date	Last change date
clone_switch13	NEWEST_IOS		Medium	Not compliant	2020-05-12 10:30:45	2020-05-12 10:30:37
clone_switch2	NEWEST_IOS		Medium	Not compliant	2020-05-12 10:30:45	2020-05-12 10:30:37
clone_switch14	NEWEST_IOS		Medium	Not compliant	2020-05-12 10:30:45	2020-05-12 10:30:37
clone_switch4	NEWEST_IOS		Medium	Not compliant	2020-05-12 10:30:45	2020-05-12 10:30:37
clone_switch6	clone_switch4 NEWEST_IOS		Medium	Not compliant	2020-05-12 10:30:45	2020-05-12 10:30:37
clone_switch7	NEWEST_IOS		Medium	Not compliant	2020-05-12 10:30:45	2020-05-12 10:30:37
clone_switch8	NEWEST_IOS		Medium	Not compliant	2020-05-12 10:30:45	2020-05-12 10:30:37

Show report

You are brought to a form with two grids. The first shows all nodes or policies that match your filters, and whether they are compliant or not. A node is compliant only if all its policies are compliant, and in the same way a policy is only compliant if all its nodes are compliant. When you click on a node, you will see a list with all its policies, when you click on a policy, you will see a list with all its nodes. For each instance you will see the last time it was checked for compliancy, and the last time it changed from compliant to non-compliant, or vice versa.

Compliance rules all have a severity. The node or policy reports take all applicable non-compliant rules, and show their maximum severity (or simply a '-' if the node is compliant);

Both grids have a 'Show report'-button. This shows a detailed report of the last compliance check. You can see a detailed report for both a node, policy or policy-node combination. In the first two cases, it will combine all known records into one report.

Compliance report

Compliance report

pgels (System) of NetYCE

Report for policy NEWEST_IOS on node clone_switch2

Detail level: 0 1 2 3

```
Rule 'config_check' compliance error:
Condition 'A' not compliant
Condition line 'description tosti' in condition 'A' not found in block '' with path ''
```

Refresh Download Close

In case the policy on this node is compliant you will see a simple confirmation. In case the policy is not, you will see a detailed breakdown of what is wrong. You can download this report to save it to your system.

In the case of reports on entire nodes and policies, these reports have the potential to grow quite big. The detail level allows you to specify how much detail you want to see in your overall report, based on indentation. 0 shows as little as possible, 3 shows everything. When you click on the download button, it will download what you see on screen.

API

You can also request reports through the netYCE API. For more information, see the [Cmpl API Reference](#).

From:
<http://wiki.netyce.com/> - **Yce-Wiki version 7**

Permanent link:
<http://wiki.netyce.com/doku.php/menu:operate:compliance:reports>

Last update: **2020/05/22 11:49**

