

Table of Contents

Verify telnet is disabled 3

Verify telnet is disabled

Disabling Telnet and enabling SSH is one of the best practices suggested by the official Cisco Hardening Guide for IOS devices to secure the management plane. Below example helps in validating telnet configuration disabled using NetYCE Compliance module

campus01-b02-access01 and campus01-b02-access02 are the two reference devices which we are using for this example. One has telnet configuration enabled and other does not.

Example config

campus01-b02-access01#

```
campus01-b02-access01#show run | b line vty
line vty 0 4
  privilege level 15
  logging synchronous
  transport input ssh
!
```

campus01-b02-access02#

```
campus01-b02-access02#show run | b line vty
line vty 0 4
  access-class 12 in
  privilege level 15
  logging synchronous
  transport input all
!
```

How its done

Below are the steps to create new policy.

Operate → Compliance → Policies → New→

Edit Policy

Name:

Sample 3 : Telnet disable

Description:

Enabled:

☒

Run compliance on config change:

☒

Signal type:

☒ Trap

☐ Syslog

☐ Email

☐ REST API

Signal trigger:

☒ From compliant to non-compliant

☐ From non-compliant to compliant

☐ From non-compliant to non-compliant

☐ From compliant to compliant

Close

Apply

OK

Click on the Node Group to select the relevant group of devices to add. Node group named “building2_access” holds the nodes of both the nodes:

Node group	Tag	Scope
building2_access		all

New

Delete

Rule → New

Edit Rule

Name:

Telnet check

Rule type:

Configuration

▼

Vendor:

Cisco_IOS

▼

Severity:

Minor

▼

Description:

☐ Search based on lines

☒ Search based on config blocks

Rule start:

line vty .*

Rule end:

!

Close

Apply

OK

Edit condition

Name:

A

Type:

ConfigBlock

☒ Enabled

☐ This is a logical condition

☒ Lines contain regular expressions

Must not contain

▼

transport input telnet|all

Close

Apply

OK

Report/test results:

Below is how to create reports to see the results of the compliance policies.

Operate → Compliance → Reports → New → Report Name “test” → Report type “Policies” → Policy Name “Sample 2 : Login banner” → Show Report

Report

Policies

Policy name	Compliant?	Severity	Last change date
Sample1- Verify ACL for remote access	no	Minor	2021-01-11 13:24:49

1

/ 1

250 items per page

1 of 1 items

Search

Show report

Compliance checks

Hostname	Policy	Fqdn	Severit...	Compliant...	Last check date	Last change date
campus01-b02-access02	Sample1- Verify ACL for remote access	campus01-b02-access...	-	Compliant	2021-01-11 13:24:49	2021-01-11 13:24:49
campus01-b02-access01	Sample1- Verify ACL for remote access	campus01-b02-access...	Minor	Not compliant	2021-01-11 13:24:49	2021-01-11 13:24:49

This was a simple example to understand how to implement compliance policy to verify if telnet access is disabled or enabled on the network devices.

From:

<https://wiki.netyce.com/> - **Technical documentation**

Permanent link:

<https://wiki.netyce.com/doku.php/guides:user:compliance:examples:telnet>

Last update:

2022/04/29 08:39

