

Table of Contents

Verify that passwords encrypted 3

Verify that passwords encrypted

The *service password-encryption* global configuration command directs the Cisco IOS software to encrypt the passwords, Challenge Handshake Authentication Protocol (CHAP) secrets, and similar data that are saved in its configuration file. Such encryption is useful in order to prevent casual observers from reading passwords, such as when they look at the screen over the muster of an administrator.

Below example helps in validating 'service password encryption' is enabled using NetYCE Compliance module

Example config

campus01-b02-access01 and *campus01-b02-access02* are the two reference devices which we are using for this example. One has password encryption configured and other does not.

Below command output gives us the information.

campus01-b02-access01#

```
campus01-b02-access01#show run | i password-encryption
no service password-encryption
```

campus01-b02-access02#

```
campus01-b02-access02#show run | i password-encryption
service password-encryption
campus01-b02-access02#
```

How its done

Below are the steps to create new policy.

Operate → Compliance → Policies → New→

Edit Policy

Name:

Sample 4 : Service Password Encryption

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:

Service Password Encryption

Rule type:

Configuration

Vendor:

Cisco_IOS

Severity:

Minor

Description:

☒ Search based on lines

☐ Search based on config blocks

Rule start:

Rule end:

Close

Apply

OK

Edit condition

Name: A

Type: ConfigBlock

☒ Enabled

☐ This is a logical condition

☐ Lines contain regular expressions

☐ Match in exact order

Must contain

service password-encryption

Must not contain any additional lines containing:

Close

Apply

OK

Edit condition

Name: and

Type: And

☒ Enabled

☒ This is a logical condition

Match in exact order

Edit condition

Name:

B

Type:

ConfigBlock

☒ Enabled

☐ This is a logical condition

☐ Lines contain regular expressions

Must not contain

no service password-encryption

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 4 : Service Password Encryption” → Show Report

Report

Policies

Policy name	Compliant?	Severity	Last change date
Sample 4 : Service Password Encryption	no	Minor	2021-01-18 08:28:11

1 / 1

250 items per page

1 of 1 items

SearchShow report

Compliance checks

Hostname	Policy	Fqdn	Severit...	Compliant...	Last check date	Last change date
campus01-b02-access02	Sample 4 : Service Password Encrypt...	campus01-b02-access...	-	Compliant	2021-01-18 08:28:11	2021-01-18 08:28:11
campus01-b02-access01	Sample 4 : Service Password Encrypt...	campus01-b02-access...	Minor	Not compliant	2021-01-18 08:28:11	2021-01-18 08:28:11

Close

This was a simple example to understand how to implement compliance policy to verify password encryption configuration.

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

Permanent link:
https://wiki.netyce.com/doku.php/guides:user:compliance:examples:pwd_encrypt

Last update: 2022/04/29 08:39

