

GestióIP IPAM

v3.5

IP address management software

Network Configuration Backup and Management Module User Guide

v1.3

www.gestioip.net

Table of Contents

1 Introduction.....	4
1.1 Features.....	4
2 Configuration.....	4
2.1 Enable Device Configuration Management.....	4
2.1.1 License key.....	4
2.1.1.1 Introduce the license key.....	5
2.2 Configure GestióIP Configuration Management.....	6
2.2.1 Device User Groups.....	7
2.2.1.1 Create, edit, delete Device User Groups.....	7
2.2.2 Configuration Backup Server.....	8
2.2.2.1 Create, edit, delete Configuration Backup Server.....	8
2.2.2.1.1 Backup Server behind NAT.....	9
2.2.3 Job Groups.....	10
2.2.3.1 Create, edit, delete <i>Job Groups</i>	10
2.2.4 Show Job details.....	11
2.2.5 Search through configurations.....	11
2.2.6 Diff configuration/command outputs (of the same or different devices).....	12
2.2.7 Show the Job execution logfiles.....	13
2.3 CM Dashboard.....	14
2.4 Configuration Management for devices.....	15
2.4.1 Configure Configuration Management for devices.....	15
2.4.1.1 Enable Configuration Management for a device.....	15
2.4.1.2 Assign Jobs to devices.....	16
2.4.1.3 Delete Jobs from devices.....	17
2.4.1.4 Disable Configuration Management for a device.....	17
2.4.1.5 Delete Configuration Management for a device.....	17
2.4.2 Mass update.....	17
2.4.2.1 Enable CM.....	18
2.4.2.2 Disable CM.....	19
3 Working with Jobs.....	20
3.1 Assigned Jobs.....	21
3.1.1 Show last Job execution log.....	21
3.1.2 Show/download stored configurations/Job outputs.....	21
3.1.3 Diff stored configurations/Job outputs.....	21
3.1.4 Search through stored device configurations/Job outputs.....	22
3.1.5 Execute an assigned Job.....	22
3.2 Restore configurations or upload files to devices.....	22
3.3 Execute unassigned device Jobs.....	23
3.3.1 List the content of the backup directory.....	23
3.4 Run Jobs automatically/schedule Jobs.....	24
3.4.1 fetch_config.pl arguments.....	24
3.4.2 logfiles fetch_config.pl.....	26
3.4.3 Configure cron jobs.....	26
3.5 Bulk changes.....	27
4 XML files/Device Type Groups.....	28

4.1 XML files parameters.....	28
4.1.1 Using wildcards/special characters.....	33
4.2 Create new Jobs for an existing Device Type Group.....	34
4.3 Create XML files/Create Device Type Groups.....	37
4.4 Check XML files syntax.....	37
4.4.1 Support.....	38
4.4.2 Share your XML file.....	38
5 Troubleshooting.....	39
5.1 Server timeout.....	39
5.2 Jobs do not appear.....	39
5.3 Running Jobs.....	39
5.3.1 Background.....	39
6 Configuration Backup Server.....	41
6.1 Installation of the FTP, TFTP and SSH (SCP) server software.....	41
6.1.1 Debian/Ubuntu.....	41
6.1.1.1 FTP server.....	41
6.1.1.2 TFPT server.....	42
6.1.1.3 SSH (SCP) server.....	43
6.1.2 OpenSuse.....	44
6.1.2.1 FTP server.....	44
6.1.2.2 TFTP server.....	45
6.1.2.3 SSH (SCP) server.....	45
6.1.3 Fedora/Redhat/CentOS.....	46
6.1.3.1 FTP server.....	46
6.1.3.2 TFPT server.....	47
6.1.3.3 SSH (SCP) server.....	48
6.2 Firewall.....	49

1 Introduction

GestióIP's Device Configuration Management Module allows to automatically backup and manage configurations of network devices like switches, router, load balancer or firewalls. It furthermore permits to execute commands on the devices and to optionally store the command's output. This offers many possibilities. You can, for example, create a Job which executes every day a command like “show arp” to create a MAC-address/port-history for your switches or you can make bulk changes like changing the password of multiple devices.

1.1 Features

The Device Configuration Management Module offers the following main features:

- Automatic configuration backups for multiple devices.
- Automatic execution of commands for multiple devices.
- Configuration down and upload.
- Diff between stored configurations or stored Job outputs.
- Search through stored configurations or stored Job outputs.
- Configuration history.
- XML files to easily create custom Jobs.

2 Configuration

2.1 Enable Device Configuration Management

2.1.1 License key

The Configuration Management Module (CMM) is a “non-free” component of GestióIP. To enable the CMM you need to purchase a license key.

Go to http://www.gestioip.net/configuration_backup_and_management.html to apply for a license key or to request a free trial key.

The license key is associated with the hostname of the GestióIP server.

To show the hostname of the GestióIP server execute the command “hostname” from a terminal or go to “Manage” → “GestióIP”. The hostname appears in front of the textbox “Licence Key”. The

hostname in the example of Fig. 1 is “server_name”.

2.1.1.1 Introduce the license key

1. Go to “Manage” → “GestióIP”
2. Set “configuration management support” to “yes”
3. Introduce the license key in the field “License Key *server_name*”
4. Click “set”
5. Click the “network” item in top menu to make the new “CM” item appear.

The screenshot shows a web-based configuration interface. At the top, there is a dropdown menu labeled 'configuration management support' with 'yes' selected. Below this is a text input field for the 'Licence Key' (labeled '"server_name"') containing the value 'f5bbf3dc99d5273ba61f423e281d0e5e_82337793.1034483'. Further down are three text input fields for directory paths: 'Configuration backup directory' with '/usr/share/gestioip/conf', 'Log directory' with '/usr/share/gestioip/var/log', and 'Device XML directory' with '/usr/share/gestioip/var/devices'. At the bottom left of the form is a 'set' button.

Figure 1: Enable Configuration Management globally

Enabling Device Configuration Management creates the new top menu item “CM” as well as the new host column “CM” for the “host-list-view”. The CM column indicates the last Job execution status with a colored symbol (green dot: OK, red dot: error, gray dot: never executed, gray “x”: disabled). By clicking over the symbol, one access to device's “manage-Job-page”.

2.2 Configure GestióIP Configuration Management

The “CM” item appears in the top menu after enabling the Configuration Management Module.

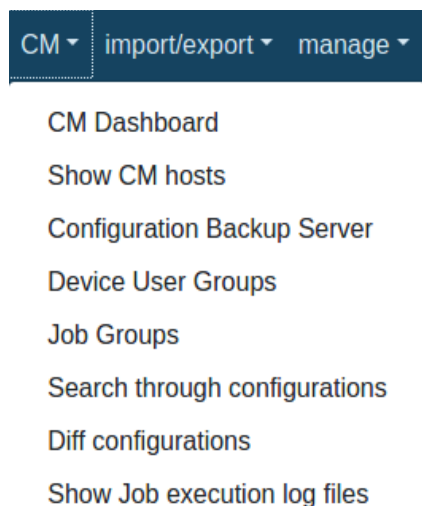


Figure 2: CM Menu

The CM menu offers the following options:

- Access the Dashboard
- Show CM hosts - list/manage devices with configured Configuration Management.
- Manage *Device User Groups*.
- Manage *Configuration Backup Server*.
- Manage *Job Groups*.
- Show Job details.
- Search through stored configurations or command outputs.
- Diff configurations/command outputs (of the same or different devices).
- Show the Job execution logfiles.

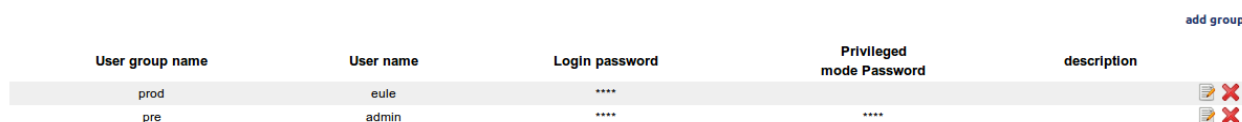
Before you can assign backup or other Jobs to devices, you need to create at least one *Device User Group*, one *Configuration Backup Server* and one *Job Group*. Furthermore there must exist an adequate *Device Type Group* with Jobs for the specific device model (see 4).

2.2.1 Device User Groups

Device User Groups are used to store the credential information (user, login password, enable password) for the different devices.

2.2.1.1 Create, edit, delete Device User Groups

To create, edit or delete *Device User Groups* access to “CM” → “Device User Groups”





The screenshot shows a table with the following columns: User group name, User name, Login password, Privileged mode Password, and description. There are two rows of data. The first row has 'prod' as the group name, 'eule' as the user name, and four asterisks for the passwords. The second row has 'pre' as the group name, 'admin' as the user name, and four asterisks for the passwords. To the right of each row are edit (pencil icon) and delete (red X icon) buttons. An 'add group' link is visible in the top right corner.


User group name	User name	Login password	Privileged mode Password	description
prod	eule	****		
pre	admin	****	****	

Figure 3: show Device User Groups

To add a new *Device User Group* click “add group”.

To edit a *Device User Group* click over the  (edit)-button.

To delete a *Device User Group* click over the  (delete)-button.



The screenshot shows a form with the following fields: User group name (cisco_prod), User name (admin), Login password (masked with asterisks), retype Login password (masked with asterisks), Privileged mode Password (masked with asterisks), retype Privileged mode Password (masked with asterisks), and description (User Group Cisco production devices). An 'add' button is located at the bottom left.

Figure 4: Device User Group form

- **User group name:** descriptive name for the group (mandatory).
- **User Name:** user name to logon to the devices (optional).
- **Login password:** password to logon to the devices (optional).
- **Privileged mode Password:** password to access to privileged mode of the devices (e.g. Cisco “enable” mode). Leave this field blank if the device does not have a privileged mode.

Note: *Device User Groups* which are assigned to a device can not be deleted. Click the delete-

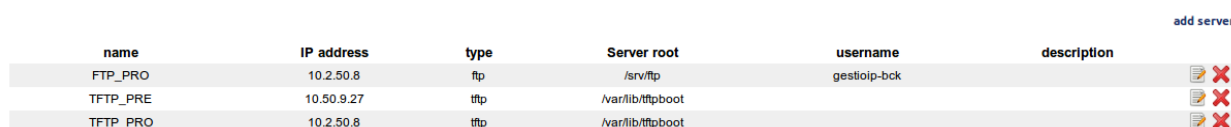
button to list the devices which are using that group.

2.2.2 Configuration Backup Server

Configuration Backup Servers are used to store the configuration backups and command outputs. It is always the GestióIP server. The configuration allows to specify parameters like the type of the server (e.g. backup protocol: FTP, TFTP, SCP) or the IP address of the GestióIP server to which the devices should send their configuration to. (in the case that the GestióIP server disposes about multiple networks interfaces). The adequate server software must be installed on the GestióIP server. See 6 for examples how to install the server software on the GestióIP server.

2.2.2.1 Create, edit, delete Configuration Backup Server

To create, edit or delete Configuration Backup Servers access to “CM” → “Configuration Backup Server”









name	IP address	type	Server root	username	description	
FTP_PRO	10.2.50.8	ftp	/srv/ftp	gestioip-bck		 
TFTP_PRE	10.50.9.27	tftp	/var/lib/tftpboot			 
TFTP_PRO	10.2.50.8	tftp	/var/lib/tftpboot			 

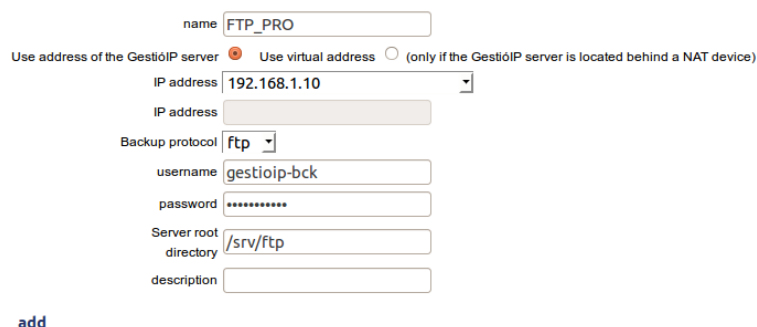
Figure 5: show Configuration Backup Server

In this example, the GestióIP server has a FTP and a TFTP server installed and has two network interfaces which are connected to the production (10.2.50.8) and to the pre-production (10.50.9.27) environment.

Click “add server” to create a new Configuration Backup Server.

To edit a server click the  (edit)-button.

To delete a server click the  (delete)-button.



name

Use address of the GestióIP server ☒ Use virtual address ☐ (only if the GestióIP server is located behind a NAT device)

IP address

IP address

Backup protocol

username

password

Server root directory

description

[add](#)

Figure 6: Creation of a FTP Configuration Backup Server

name

Use address of the GestioIP server ☒ Use virtual address ☐ (only if the GestioIP server is located behind a NAT device)

IP address

IP address

Backup protocol

Server root directory

description

[add](#)

Figure 7: Creation of a TFTP Configuration Backup Server

- **name:** descriptive name for the server (mandatory).
- **IP address:** IP address of the server to which the devices should connect to (see 2.2.2.1.1) (mandatory).
- **backup protocol:** Server type (FTP, TFTP or SCP (SSH)) (mandatory).
- **username:** username to authenticate with the server (only FTP and SCP) (optional).
- **password:** username's password to authenticate with the server (only FTP and SCP) (optional).
- **Server Root directory:** root directory of the server. The directory to which the configuration backups/command-outputs will be uploaded. (mandatory).
- **description:** an optional description.

See 6 for the values “username” and “Server Root directory”.

Note: *Configuration Backup Server* which are assigned to devices can not be deleted. Click the delete-button to list the devices which are using that server.

2.2.2.1.1 Backup Server behind NAT

If the GestioIP server resides in a LAN with private addresses and the devices to backup are located outside of the LAN, select “Use virtual address” and specify the outer virtual address of the NAT device which is linked to the GestioIP server (see Fig. 8).

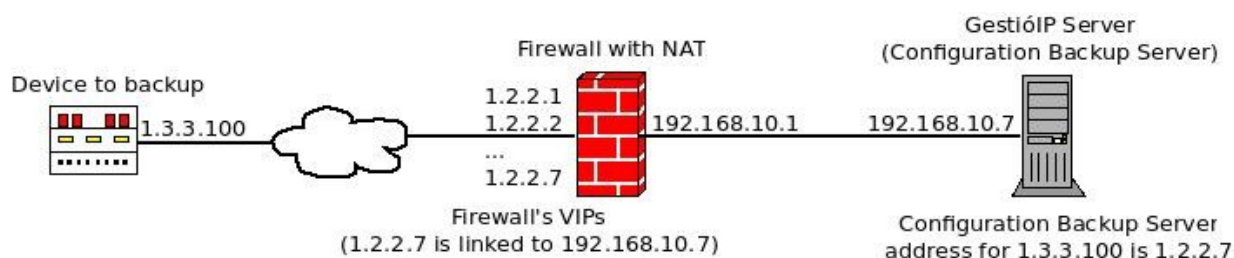


Figure 8: Backup devices in front of a Firewall with NAT

In this example, the “virtual IP address” would be 1.2.2.7.

2.2.3 Job Groups

Job Groups are used to group Jobs to execute them by the same task. For example, you can create a *Job Group* “backup daily” and assign the backup-Jobs which should be executed daily to this group (see 3.4.3).

2.2.3.1 Create, edit, delete Job Groups

To create, edit or delete *Job Groups* access to “CM” → “Job Groups”

ID	name	description	devices	
19	arp stat	daily arp statistic	show	
1	backup daily	daily backup at 01:45h	show	

Figure 9: show Job Groups

ID: Job Group ID. The ID is used to specify the *Job Group* for the automatic Job execution. It will be created automatically.

name: descriptive name (mandatory).

description: a short description.

devices: clicking “show” lists the hosts which are using this *Job Group*.

Click “add Job Group” to create a new Job Group.

To edit a Job Group click over the (edit)-button.

To delete a Job Group click over the (delete)-button.

2.2.4 Show Job details

Jobs are defined in the *Device Type Group* XML files (see 4). To show the commands which are defined for a specific Job go to “CM” → “Show Job Details”.

Show Job details

Device Type Group: Brocade Fabric OS

Job: Backup running config via FTP

[send](#)

Figure 10: show Job details

Select the *Device Type Group* and the Job which should be displayed and click “send”.

```

Device Group values

deviceGroupName: Brocade Fabric OS
deviceGroupId: 10
models: DS4100
loginPrompt:
enablePrompt: >
enableCommand: enable
usernameExpr: [[GENERIC_USERNAME_EXPR]]
passwordExpr: [[GENERIC_PASSWORD_EXPR]]
logoutCommand: exit
pagerExpr:
pagerDisableCmd:

Job Details "copyRunFtp"

comment: Backup running config via FTP
Command 1: configupload -all -ftp [[SERVER_IP]],[[SERVER_USERNAME]],[[SERVER_ROOT]],[[CONFIG_NAME]],[[SERVER_PASSWORD]]
Return 1: configUpload complete

XML file: /usr/share/gestioip/var/devices/10_brocade_fabric_OS.xml

```

Figure 11: Job details

2.2.5 Search through configurations

The search form offers the possibility to execute a search through the stored configurations/Job outputs.

Access to “CM” → “Search through configurations” to access to the search form.

Device Type Group

Job

Job Group

search string

search only through last logfiles ☒

send

Figure 12: search through configuration/command outputs

The form permits to search through the configurations/Job outputs of

- all Jobs of a *Device Type Group*
- a specific Job
- a *Job Group*
- a combination of the fields

The checkbox “search only through last logfiles” offers the possibility to search either through all stored configurations or through only the last ones.

Note: To search through the configurations/Job outputs for a specific device go to the “manage-Jobs-page” (“CM” → “Show CM hosts” → click over the colored CM-symbol).

2.2.6 Diff configuration/command outputs (of the same or different devices)

To diff configurations/command outputs click over “CM” → “Diff configurations”.

Step I: Select the devices/Jobs to diff configurations from.

To find a specific Job more easily you can order the Jobs by the IP addresses or by the hostnames.

Choose two jobs to diff configurations/outputs from

Job I 192.168.80.36 (Planta6) - Enterasys/copyRunTftp

Job II 192.168.80.36 (Planta6) - Enterasys/copyRunTftp

send

order entries by hostname

Figure 13: Diff configurations step I

Step II: Select the configurations which should be diffed and click “diff”.

Choose the configurations/outputs you want to diff

Planta6 (copyRunTftp) 05/05/2014 - 15:58 (01)

planta7(copyRunTftp) 19/05/2014 - 09:49 (01)

send

Figure 14: Diff configurations step II

Note: You also can diff the configurations/Job outputs for a specific device from the “manage-Jobs-page” (“CM” → “Show CM hosts” → click over the colored CM-symbol).

2.2.7 Show the Job execution logfiles.

To show the Job execution log files click over “CM” → “Show Job execution log files”.

Select the log file which should be shown and click “show”.

Job execution log files

from

03/08/2014 - 05:45:01

02/08/2014 - 05:45:02

01/08/2014 - 05:45:02

31/07/2014 - 05:45:01

30/07/2014 - 05:45:01

29/07/2014 - 05:45:02

28/07/2014 - 05:45:02

27/07/2014 - 05:45:01

26/07/2014 - 05:45:01

25/07/2014 - 05:45:01

show

Figure 15: Show Job execution log

Note: You can also access to the last execution log for a specific Job from the “manage-Jobs-page”.

2.3 CM Dashboard

The CM Dashboard gives an overview of the results of the execution of defined Jobs.

It offers the possibility to show the Job execution results for a specific date (Fig. 16) or for a time range (Fig. 17).

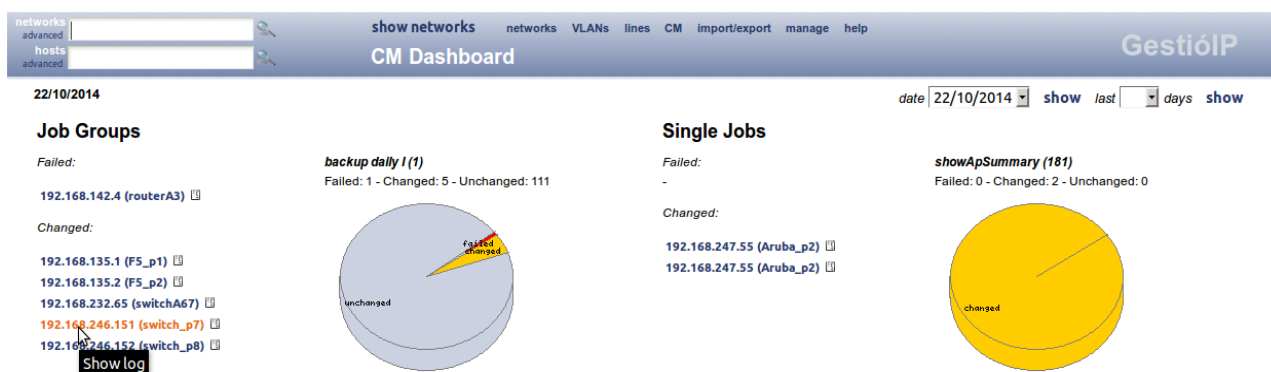



Figure 16: CM Dashboard (specific date)

Click over the IP addresses to access to the log file for a specific Job of this device.

Click over the -symbol to access to the devices Job-Management-Page.

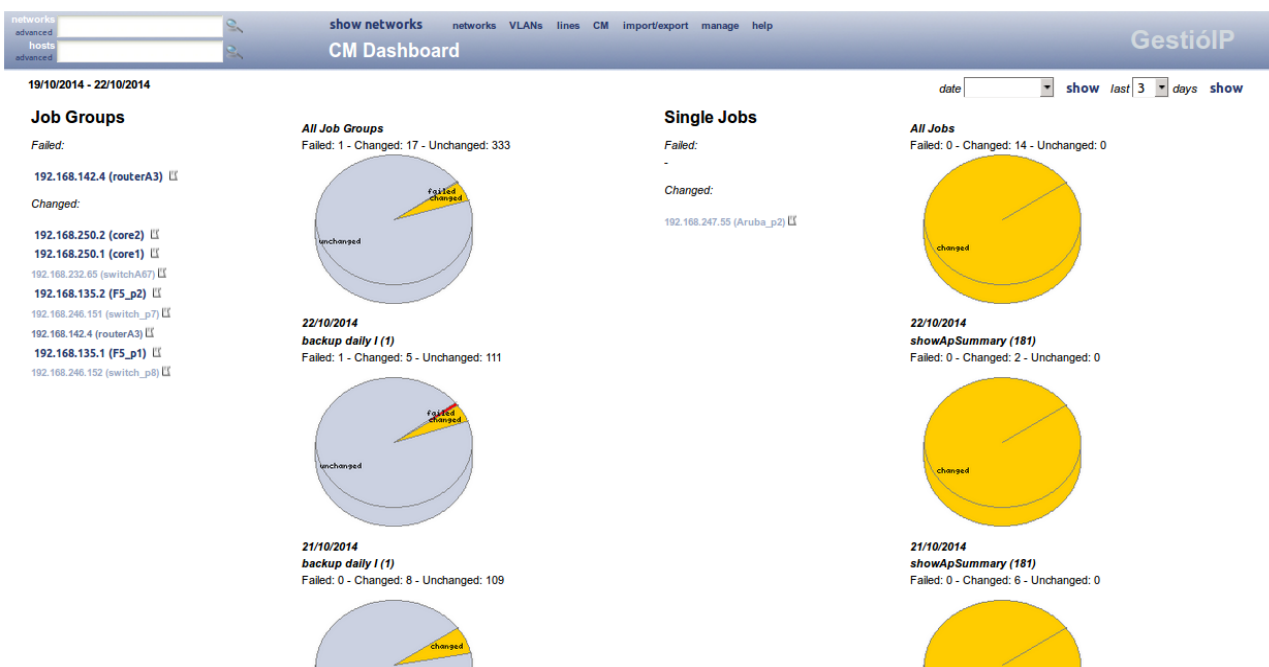


Figure 17: CM Dashboard (time range)

The “time range view” gives an overview of the Jobs which were executed within a specific time range.

The IP addresses appear in three different shades of colors.

Failed:

red – no successful execution within the time range

orange – more then one failed Job execution within the time range

dark blue – one failed Job execution within the time range

Changed:

light blue – configuration changes during all Job executions

darker blue – configuration changes during some Job executions


dark blue – configuration changes during one Job execution

Only the IP addresses which appear in dark blue offer links to the log files. To access to the log files for IPs with multiple fails/changes, click over the graph for a specific date.

2.4 Configuration Management for devices

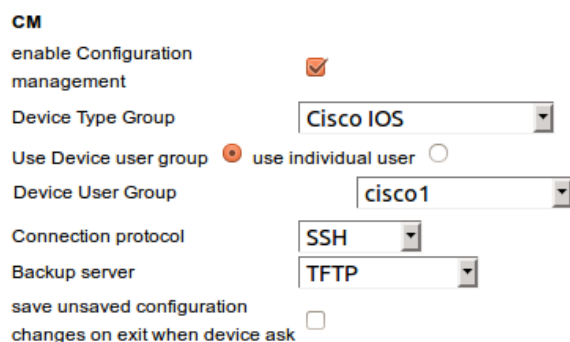
All device specific CM configuration (*Device Type Group*, *Configuration Backup Server*, ...) as well as the association of Jobs to devices is made from the “edit-host-form”.

2.4.1 Configure Configuration Management for devices

Go to host-list-view (“networks” → click over the adequate network) or execute a search for the device which should be configured. Access to the “edit-host-form” by clicking on the "edit" icon  behind the device's IP address.

2.4.1.1 Enable Configuration Management for a device

To enable CM for a device access to the “edit-host-form”.



CM

enable Configuration management ☒

Device Type Group

Use Device user group ☒ use individual user ☐

Device User Group

Connection protocol

Backup server

save unsaved configuration ☐

changes on exit when device ask ☐

Figure 18: CM configuration for devices

1. Check the “enable Configuration Management” checkbox to enable the Configuration Management for this device.
2. Select the adequate *Device Type Group* for the device. The *Device Type Group* determine which Jobs are available for the device. *Device Type Groups* are defined in form of XML files. If there is no predefined XML file for your device model available, you can create a new XML file for your device model (see 4.3).
3. Select the *Device User Group* which holds the correct user information to access to the device or configure the user information for this device individually.
4. Select the *connection protocol* which should be used by the *Configuration Backup Server* to connect to the device.
5. Select the *Configuration Backup Server* where the device configurations and the Job outputs should be stored.
6. Before a Job logs-out from the device, the device might ask if unsaved configuration changes should be stored. Check the checkbox “save unsaved configuration changes on exit when device ask” to force the Job to save unsaved configuration changes before logging-out.

Hint: You can use host mass update feature to configure CM for multiple devices simultaneously.

2.4.1.2 Assign Jobs to devices

You can assign up to 30 Jobs to a device.

Job	Backup running config via TFTP
description	backup config
Job Group	backup daily
✕	
+	

Figure 19: assign Jobs

- **Job:** the Job which should be assigned to the device (mandatory)
- **description:** a description (optional)
- **Job Group:** Device Job Group for this Job (optional)

Click the + (add)-button to assign more Jobs to the device.

Click “change” to save the changes.

Note: configuration-restore/file upload Jobs can only be executed manually and must not configured as assigned Job.

2.4.1.3 Delete Jobs from devices

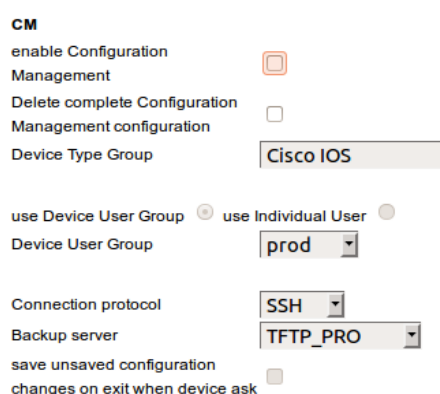
To delete Jobs from devices click the  (delete)-button.

This will clean the specific Job form.

Click “change” to save the changes

2.4.1.4 Disable Configuration Management for a device

Disabling CM for a device causes that the Jobs will not longer be processed by the automatic Job execution.



CM

enable Configuration Management ☐

Delete complete Configuration Management configuration ☐

Device Type Group

use Device User Group ☒ use Individual User ☐

Device User Group

Connection protocol

Backup server

save unsaved configuration changes on exit when device ask ☐

Figure 20: Disable CM for a device

To disable CM for a device uncheck the “enable Configuration Management” checkbox and click “save”. The CM configuration and the Jobs will be deactivated but not deleted.

2.4.1.5 Delete Configuration Management for a device

To delete the CM configuration for a device uncheck the “enable Configuration Management” checkbox and check the checkbox “Delete complete Configuration Management configuration” (see Fig. 20). Click “save” to save the changes. This will delete the CM configuration as well as all Jobs which are assigned to this device.

2.4.2 Mass update

To configure CM for multiple devices you can use the mass-update feature.

2.4.2.1 Enable CM

CM-mass-update will always overwrite the *Device Type Group*. Execute the CM mass update only for devices of the same *Device Type Group*.

To use the mass-update execute the following steps:

1. List the devices which should be configured by entering host-list-view, cm-hosts-list-view or by executing a host-search.
2. Check the checkboxes in front of the devices which should be configured.
3. Select “edit” and “CM” in the mass-update-form at the bottom of the page.
4. Click “mass update”

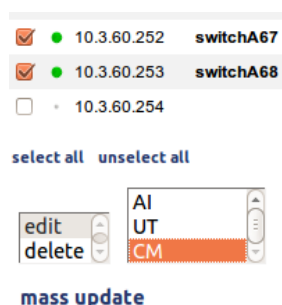


Figure 21: Mass update

Select a *Device Type Group*. The *Device Type Group* determines which Jobs are available for the device.

If you don't want to overwrite the the *Device User Group*, *Connection Protocol*, *Device Backup Server* or the value of “save unsaved configuration changes...” check the appropriate checkboxes “exclude from update” behind the fields.

 The screenshot shows a form titled 'Device Jobs'. It contains several settings:

- 'enable Configuration management' with a checked checkbox.
- 'Device Type Group' with a dropdown menu.
- 'use Device User Group' with a radio button selected, and 'use Individual User' with an unselected radio button. There is also an 'exclude from update' checkbox.
- 'Device User Group' with a dropdown menu.
- 'Connection protocol' with a dropdown menu and an 'exclude from update' checkbox.
- 'Backup server' with a dropdown menu and an 'exclude from update' checkbox.
- 'save unsaved configuration changes on exit when device ask' with an unselected checkbox and an 'exclude from update' checkbox.

Figure 22: mass update - change cm values

Select the Jobs, insert optionally a description and select a *Device Job Group*.

Click “change” to save the changes.

2.4.2.2 Disable CM

To disable CM for multiple devices go to CM mass update form for the devices you want to edit (see 2.4.2.1)

Uncheck the checkbox “enable Configuration Management”.

If you want that the complete CM configuration as well as the Jobs which are associated with the devices are deleted, check the checkbox “Delete complete Configuration”.

Click “change” to save the changes.

Device Jobs

enable Configuration management ☐

Delete complete Configuration Management configuration ☒

Device Type Group

use Device User Group ☒ use Individual User ☐ ☐ exclude from update

Device User Group

Connection protocol ☐ exclude from update

Backup server ☐ exclude from update

save unsaved configuration changes on exit when device ask ☐ ☐ exclude from update

Figure 23: mass update - disable CM

If you only want to delete the associated Jobs from the devices check the checkbox “Delete old Jobs from devices” (you must always select a *Device Type Group*) and click “change”.

Other Jobs

Delete old Jobs from devices ☐

Job

description

Job Group

✖

+

Figure 24: Mass Update - Jobs

3 Working with Jobs

Access to the “manage-Jobs-page” of a device: “CM” → “show cm hosts” → click over the Job status symbol behind the device's IP address (CM-column).

The “manage-Jobs-page” offers the following options:

Assigned Jobs:

- Show Job's last execution log.
- Show stored device configurations/Job outputs. *
- Diff two stored device configurations/Job outputs. *
- Search strings through the stored device configurations/Job outputs. *
- Execute the Job.

* only *Job Types* “configuration backup” and “fetch command output”, not available for binary configurations

Other:

- Upload a stored configuration/a file to the device.
- Run unassigned Jobs on the device (the Jobs must be defined for the device's *Device Type Group*).
- List the directory/show the path of the directory where all configurations for this device are stored.

The screenshot displays two job entries in the GestióIP interface. Each entry includes a status icon, job name, description, type, job group, last execution time, and a 'Show job details' link. To the right of each job entry are four interactive sections: 'Show configuration' or 'Show command output' with a date selector and a 'show' button; 'Diff configurations' or 'Diff command outputs' with two date selectors and a 'diff' button; a 'Search' section with a dropdown menu (set to 'All files'), a text input field, and a 'search' button; and an 'Execute job now' section with a 'run job now' button and radio buttons for log mode (default, verbose, debug).

Job 1: Backup running config via TFTP
 Description: backup daily
 Type: copy_file
 Job Group: backup daily (1)
 Last execution: 2014-08-24 18:14:12
 Show job details

Job 2: arp -an
 Description: ARP stat
 Type: fetch_command_output
 Job Group: ARP stat (2)
 Last execution: 2014-08-23 11:12:18
 Show job details

Figure 25: assigned Device Jobs

3.1 Assigned Jobs

3.1.1 Show last Job execution log

Click over the colored symbol if front of the Job to show the last execution log for this Job. The color indicates, if the Job was executed successfully (green), with errors (red) or if the Job was never executed (gray). To access to older logfile go to “CM” → “Show job execution logfiles”.

3.1.2 Show/download stored configurations/Job outputs

Select the configuration/Job output from the “Show configuration/Show command output” select-box and click “show”. This will show the configuration on a web-page as well as a link to download the configuration/Job output.

3.1.3 Diff stored configurations/Job outputs

Select the configurations/Job outputs which should be diffed from the “Diff configurations/Diff command output” select-box and click “diff”.

The diff page shows two types off diffs. A “Unix-like” diff of the lines which differ and a comparison chart of the complete files.

Note: Binary configurations can not be shown nor diffed

The screenshot displays the 'Diff' interface with two panels. The top panel shows a 'diff' command being executed on two files: '01/08/2014 - 05:45 (01)' and '22/06/2014 - 05:45 (01)'. The bottom panel shows the resulting diff output, which is a comparison of two configuration files: '/usr/share/gestiop/conf/DEFAULT/1974/201408010545_01_1974_153.conf (newer)' and '/usr/share/gestiop/conf/DEFAULT/1974/201406220545_01_1974_153.conf (older)'. The diff output is shown in two columns, with line numbers on the left and the configuration content on the right. The content is color-coded to show differences: green for lines that are the same, red for lines that are different, and yellow for lines that are added or removed. The configuration content includes various settings such as 'version 12.2', 'no service pad', 'service timestamps debug datetime localtime', 'service timestamps log datetime localtime', and 'service password-encryption'.

Figure 26: Diff configurations/Job outputs

Checkbox “ignore comments”

The checkbox “ignore comments” forces GestióIP to ignore changed comments. A line is considered as comment, when it starts with "!", "#" or "/".

This lines will not be shown in the first diff box and will be shown, but not be highlighted, in the second diff box.

The screenshot shows the diff tool interface. At the top, there are two file selection boxes, both containing '30/06/2020'. To the right of these boxes is a 'diff' button and an unchecked checkbox labeled 'ignore comments'. Below this, a diff result is displayed in a box. The diff shows two files: '</usr/share/gestioip/config/DEFAULT/5111/202006301810_03_5111_285.txt (newer)' and '>/usr/share/gestioip/config/DEFAULT/5111/202006301755_02_5111_285.txt (older)'. The diff shows a change from '2c2' to '25,26c25,26'. The configuration values for RX and TX packets are shown as unchanged.

```
</usr/share/gestioip/config/DEFAULT/5111/202006301810_03_5111_285.txt (newer)
>/usr/share/gestioip/config/DEFAULT/5111/202006301755_02_5111_285.txt (older)
2c2
< llast config change 1.2.4.4
---
> llast config change 1.2.3.4
25,26c25,26
< RX packets:131401 errors:0 dropped:0 overruns:0 frame:0
< TX packets:60288 errors:0 dropped:0 overruns:0 carrier:0
```

Figure 27: diff result with “ignore comments” unchecked

The screenshot shows the diff tool interface with the 'ignore comments' checkbox checked. The file selection boxes and the 'diff' button are the same. The diff result box is empty, indicating that all changes were ignored.

```
</usr/share/gestioip/config/DEFAULT/5111/202006301810_03_5111_285.txt (newer)
>/usr/share/gestioip/config/DEFAULT/5111/202006301755_02_5111_285.txt (older)
---
25,26c25,26
< RX packets:131401 errors:0 dropped:0 overruns:0 frame:0
< TX packets:60288 errors:0 dropped:0 overruns:0 carrier:0
```

Figure 28: diff result with “ignore comments” checked

3.1.4 Search through stored device configurations/Job outputs

Select either “all files” to execute a search through all stored backups or select a specific configuration/Job-output (see Fig. 25), introduce a search string and click “search”.

```
gtw4. ( ) 201408010545_01_1974_153.conf show
neighbor route-map WAN-PRINCIPAL in
neighbor route-map PREPEND out
route-map WAN-PRINCIPAL permit 10
route-map IBGP-BACKUP permit 10
route-map PREPEND permit 10
route-map IBGP-PRINCIPAL permit 10
route-map WAN-BACKUP permit 10
```

Figure 29: Output of a search for "route-map"

Click “show” to show the complete file.

3.1.5 Execute an assigned Job

To execute a assigned Job manually select the log-level and click “run job now”.

3.2 Restore configurations or upload files to devices

Use this form to restore backedup configurations or to upload files to the devices.

- Select a adequate Job (the Job must be defined in the device's XML file) (see 4.2, Example 2).
- Select “Upload a stored configuration” to restore a configuration which was backedup by the CM-system or choose “Choose configuration or file to upload” to restore/upload a local file from your workstation to the device.
- Choose a log mode.
- Click “upload”.

Upload configuration or file to device

Job Select the adequat upload job

Upload a stored configuration ☒ Choose configuration or file to upload ☐

log mode

default ☒ verbose ☐ debug ☐

upload

Figure 30: Upload configuration form

3.3 Execute unassigned device Jobs

The “Run a job on this device”-form offers the possibility to run a Job which is available for the device's *Device Type Group* independently if the Job is assigned to the device or not.

Execute the Job by clicking “run job now”. Running a Job may take, depending on the job, up to 45s. The result page will be shown when the Job has finished. It offers links to access to the stored configuration/Job-output and informs about errors which might have occurred.

Run a job on this device

Job

log mode

default ☒ verbose ☐ debug ☐

run job now

Figure 31: Execute a unassigned Job manually

Hint: Access to the outputs of unassigned Jobs via the link “Configuration backup directory” on the bottom of the page.

3.3.1 List the content of the backup directory

To list all backedup configurations/Job outputs click the link “Configuration Backup Directory” at the bottom of the “manage-Jobs-page”.

Configuration backup directory: </usr/share/gestioip/conf/DEFAULT/6071>

Figure 32: Access to the configuration backup directory

3.4 Run Jobs automatically/schedule Jobs

Jobs can be executed automatically. The automatic execution of the Jobs is made by the script `/usr/share/gestioip/bin/fetch_config.pl`.

To run Jobs automatically configure cron jobs for the script `/usr/share/gestioip/bin/fetch_config.pl` (see 3.4.3).

The configuration file for all scripts in `/usr/share/gestioip/bin` is `/usr/share/gestioip/etc/ip_update_gestioip.conf`.

Before running the script `fetch_config.pl` you must first configure the following parameters in `ip_update_gestioip.conf`:

```
sid_gestioip=gestioip
user_gestioip=gestioip
pass_gestioip=XXXXXX
bbdd_host_gestioip=localhost
bbdd_port_gestioip=3306
```

```
mail_destinatarios=user@domain.org (optional)
client=client's name
```

3.4.1 fetch_config.pl arguments

The script `fetch_config.pl` offers the following arguments:

-c, --csv_hosts=list

Coma separated list of IPs to process. If you only specify the `-c` option, all Jobs associated to this devices will be executed

-d, --debug=LEVEL

Debug level 1-3 (e.g. `-d 2`).

-g, --group_id=job_group_id

ID of the *Job Group* for which the commands should be executed. Consult the *Job Group* ID from *Job Group* list view (“CM” → “Job Groups”) or from the “manage-Jobs-form”. In Fig. 33, the *Job Group* ID is 1 (1).

-h, --help

Print help.

-i, --id=job_id

ID of the Job that should be executed. To execute a specific Job for a specific device. You find the Job ID by hovering over the Job name from the “manage-Jobs-page”. In Fig. 33, the Job has the ID 23.

--jobname=job_short_name

Execute a Job by it's shortname (shortname example: copyRunTftp2)(see Fig. 33). Without --csv_host option, the Job will be executed for all devices which have a Job with this name associated (independent of the *Device Job Group*).

-l, --log_file_name=file_name

To specify the log file name.

-m, --mail

Send the Job execution log via email to the addresses specified in the configuration file “ip_update_gestioip.conf (parameter “mail_destinatarios”).

--name_client=clientname

Name of the client for which the script should be executed. If there are no clients configured, the clientname is “DEFAULT”

-r, --run_unassociated_job

Run a Job by its name, independently if it is a defined job. Requires options --jobname and --csv_hosts.

-u, --upload_config_file=config_name

Configuration file to upload to the device (only for “upload” Jobs). Requires options --jobname and --csv_hosts.

-v, --verbose

Run the script in “verbose” mode.

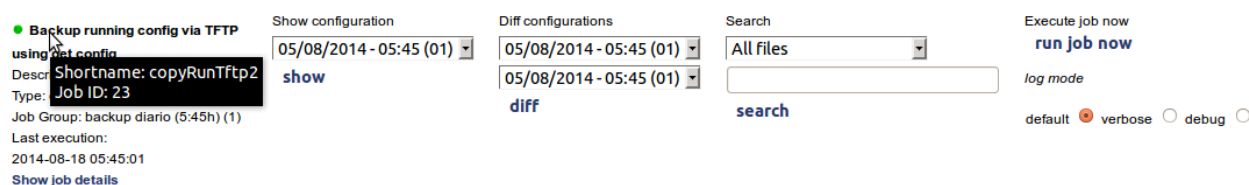


Figure 33: Find the Job ID, Job short name and Job Group ID

Examples:

Execute all Jobs of *Device Job Group* 1 and send the logfile via mail to the mail_destinatarios:
`fetch_config.pl --group_id 1 -m`

Execute a specific Job for a specific device by the Job ID in “verbose” mode:

```
fetch_config.pl --id 33 -v
```

Run all associated Jobs with the name “copyRunTftp” (on all devices which have this Job associated):

```
fetch_config.pl --name copyRunTftp
```

Run a Job on a device which is not associated with the device (but defined for device's *Device Type Group*):

```
fetch_config.pl --csv_hosts 192.168.32.8 --jobname copyRunTftp --run_unassociated_job
```

Run all Jobs which are associated with the specified devices:

```
fetch_config.pl --csv_hosts 192.168.32.8,192.168.55.4,10.3.20.9
```

3.4.2 logfiles fetch_config.pl

Every run of fetch_config.pl creates a logfile. The logfiles are stored in /usr/share/gestioip/var/log.

Example:

20140821101642_1_fetch_config.log – logfile from 21/08/2014 10:16:42

Running the script with the -v (verbose) option creates an additional logfile which holds the output of the device. This may be useful for troubleshooting purposes. This additional log files terminating in “_stdout” (20140821101629_1_fetch_config.log_stdout).

Hint: Create a cron-job to delete old logfiles:

```
35 3 * * * find /usr/share/gestioip/var/log -type f -mtime +30 -delete > /dev/null 2>&1
```

This cron-job will delete every day at 3:35h all files from the log directory which are older than 30 days.

3.4.3 Configure cron jobs

To execute the Jobs automatically you need to configure con-jobs.

Example:

Configuration of a cron job which runs all Jobs of the *Device Job Group* with ID “1” and sends the Job execution report via mail every day at 05:45h am.

```
45 5 * * * /usr/share/gestioip/bin/fetch_config.pl -g 1 -m >/dev/null 2>&1
```

Note: the execution of fetch_config.pl for one Job takes normally about 10-15s per Job. Count with

around 20 minutes for 100 Jobs or around 3,5 hours for 1000 Jobs. To speed up the execution you can define multiple *Job Groups* and run an instances of `fetch_config` for each *Job Group* in parallel.

Example:

If you want to run backup Jobs for 3000 devices create three different *Job Groups* (e.g. backup1 (ID: 6), backup2 (ID: 7) and backup3 (ID: 8)), assign 1000 Jobs to each *Job Group* and create a cron job for each *Job Group*.

```
15 3 * * * /usr/share/gestioip/bin/fetch_config.pl -g 6 -m >/dev/null 2>&1
15 3 * * * /usr/share/gestioip/bin/fetch_config.pl -g 7 -m >/dev/null 2>&1
15 3 * * * /usr/share/gestioip/bin/fetch_config.pl -g 8 -m >/dev/null 2>&1
```

3.5 Bulk changes

The CM Module allows to execute bulk changes for multiple devices. The bulk changes can only be executed from the command line by running the script `fetch_config.pl`.

To execute a bulk change you need to:

1. Create the adequate *Jobs* which should be executed.
2. Create a *Job Group* to group the *Jobs* to execute them together.
3. Assign the *Job* and the *Device Job Group* to the devices
4. Execute `fetch_config.pl` with the “-g” (job-group-id) – option from command line (see 3.4).

Example: Change the SNMP RO community string of multiple devices running Cisco IOS:

1. Create an adequate Job (in the XML file `1_cisco_ios.xml`):

```
<changeSnmpRoCommunity>
  <comment>Change SNMP RO community string</comment>
  <jobType>task</jobType>

  <command>conf t</command>
  <return>(config)#</return>
  <command>no snmp-server community public R0</command>
  <return>(config)#</return>
  <command>snmp-server community XXXX R0</command>
  <return>(config)#</return>
  <command>exit</command>
```

```
<return>[[ENABLE_PROMPT]]</return>
</changeSnmpRoCommunity>
```

2. Create a Job Group (“CM” → “Job Groups”) (see 2.2.3).
3. Assign the *Job* and the *Device Job Group* to the devices. You can use the mass-update feature for this task (see 2.4.2).
4. Run `fetch_config.pl` from the command line (replace *GID* by the *Job Group ID*).
\$ `/usr/share/gestioip/fetch_config.pl -g GID`
5. Delete the password from the XML file.

4 XML files/Device Type Groups

The XML files define the *Device Type Group* values for a device model. All *Device Type Group* specific configuration is made within the XML files.

The XML files define parameters like devices prompts, global commands like the “pager disable command” and the Jobs for the specific *Device Type Group*.

GestióIP comes with a several predefined XML files. If there is no XML file for your device model available you can create your own XML files (see 4.3).

The XML files are located in `/usr/share/gestioip/var/devices/`.

4.1 XML files parameters

The XML files offer the following attributes:

Main container

```
<deviceGroupValues>
```

Device Type Group Name - this value will be displayed in the Device Type Group select box of the Web interface

Mandatory

```
<deviceGroupName>Cisco IOS</deviceGroupName>
```

Device Group ID - Internal ID of the Device Group - must be identical with XML file's serial number e.g. `17_MyOS.xml` -> XML file's serial number = Device Type Group ID = 17

Device Type Group ID must be unique for every Device Type Group

Mandatory

<deviceGroupID>1</deviceGroupID>

List of models for which this XML file is compatible

Optional

<models>IOS,PIX/ASA 7.x/8.x</models>

Login Prompt - prompt which is displayed after login but which does not have sufficient privileges to execute the commands. Leave this parameter blank if the commands can be executed directly after logging-in without changing to "enable"-mode (leave it blank if no command like "enable" is required).

Optional

<loginPrompt>></loginPrompt>

Enable Prompt - privileged prompt of level from which the commands can be executed.

Mandatory

<enablePrompt>#|(enable)</enablePrompt>

In the case that after a successful login appear a message which requires a confirmation instead of the login or enable prompt, configure an expression which matches this message here. The message will be confirmed by the fetch_config.pl script with an return

Optional

<loginConfirmationExpr>Terminal type?</loginConfirmationExpr>

Enable command - command to gain the privileges to execute the commands

Mandatory if both parameter <loginPrompt> and <enablePrompt> are set

(leave this parameter blank if only <enablePrompt> is set.

<enableCommand>enable</enableCommand>

Username expression - expression which matches logins 'username: ' string. The value of [[GENERIC_USERNAME_EXPR]] should match for most devices and needs normally not to be changed

Optional

<usernameExpr>[[GENERIC_USERNAME_EXPR]]</usernameExpr>

Password expression - expression which matches logins 'password: ' string . The value [[GENERIC_PASSWORD_EXPR]] should match for most devices and need normally not be changed

Optional

<passwordExpr>[[GENERIC_PASSWORD_EXPR]]</passwordExpr>

Logout Command - command to logout from the remote session

Mandatory

<logoutCommand>exit</logoutCommand>

GestióIP 3.5 – Network Configuration Backup and Management Module

Pager expression - Expression which indicates that there will come more command output

Optional

```
<pagerExpr>--More--</pagerExpr>
```

Pager Disable command - command to disable paging

Optional (Because some devices do not use paging. For devices which have paging enabled it is mandatory)

```
<pagerDisableCmd>terminal length 0</pagerDisableCmd>
```

Unsaved changes question - Expression that matches the question if the unsaved configuration changes should be saved before logging out

Optional

```
<unsavedChangesMessage>The system has unsaved changes|Would you like to save them now|Do you wish to save your configuration changes</unsavedChangesMessage>
```

Definition of the Jobs for the devices of this Device Type Group

```
<jobs>
```

Job short name - arbitrary Job name

Mandatory

```
<copyRunTftp>
```

Job comment - this value will be displayed in the "Job" select box of the Web interface

Mandatory

```
<comment>Backup running config via TFTP</comment>
```

Job Type - This attributes determines how the Job will be internally processed.

There are four Job Types available:

copy_file - Use this value if the Job should copy a configuration/a file from the device to the server. Example: backup the configuration of a device via FTP or TFTP.

fetch_command_output - Use this value if the Job should execute a command on the device and store the command's output. Example: fetch and store the output of the command "show arp"

task - Use this value if the Job should execute a command on the device without storing the command output. Example: bulk-change to change the password for multiple devices

copy_local - to copy a file which is already saved on the Backup Server locally to the backup directory. To integrate configuration files which can not be fetched by GestióIP within the Configuration Management Module. *copy_local* Jobs do not connect to the devices nor execute commands on the devices. *copy_local* Jobs do only accept the attributes `<comment>`, `<jobType>`, `<localSourceFile>` and `<localSourceCommand>`. See *25_juniper_ive.xml* and *35_pfsense.xml* for examples.

copy_local allows also to executes local scripts:

Example:

```
#
```

GestióIP 3.5 – Network Configuration Backup and Management Module

`<localSourceCommand>/usr/share/gestioip/bin/create_pfsense_backup.sh</localSourceCommand>`

Would execute the command `create_pfsense_backup.sh` . The script downloads the configuration and copies it to a by parameter specified location . `fetch_config.pl` executes the script with the following arguments: `device_ip backup_file_name user_name login_pass`

NOTE: Upload Jobs (jobs which copy configurations from the backup server to the device, for example to restore a backedup configuration) MUST have the jobType "task"

Mandatory

`<jobType>copy_file</jobType>`

Saved configuration may only differ with actual configuration in an "unimportant" string like "saved_cfg_timestamp"

This option allows to configure a string which match lines which should not be compared when determining if the configuration has changed.

Optional

`<diffConfigIgnore>saved_cfg_timestamp</diffConfigIgnore>`

Command timeout - will replace the default command execution timeout of 92s

`<commandTimeout>120</commandTimeout>`

Backup file Extension - if you want to save the file with a specific extension (eg. tar.gz) on the Backup Server. Depending on the Job Type, the file will be automatically stored with the extension ".conf" (type "copy_file") or ".txt" (type "fetch_command_output"), independently of the extension of the original config file. Use this option to force the backupfile to be stored on the server with another extension than .conf or .txt.

Optional

`<configExtension>tar.gz</configExtension>`

The Date format parameter allows to specify the format of the date which should replace the [[DATE]] variable.

Supported date specifiers:

%d - Day of the month, zero-padded (01-31)

%H - Hour in 24h format (00-23)

%I - Hour in 12h format (01-12)

%m - Month as a decimal number (01-12)

%M - Minute (00-59)

%y - Year, last two digits (00-99)

%Y - Year, four digits (2014)

Example: with `<dateFormat>` set to "Y%m%d", ipso-backup_[[DATE]].tar.gz will be translated to ipso-backup_20140425.tar.gz.

Optional

<dateFormat>%Y%m%d</dateFormat>

Name of the configuration file on the device. Normally the destination file will be specified with the `[[CONFIG_NAME]]` variable (e.g. "copy configs/device_cm.cfg tftp://[[SERVER_IP]]/[[CONFIG_NAME]]"). In the case that the device does not permit to specify the destination file name you must indicate the name of the configuration file which will be copied to the device with the `[[DEST_CONFIG_NAME]]` variable. (e.g. "set backup remote manual [[DEST_CONFIG_NAME]] ftp-passwd [[SERVER_PASSWORD]]").

`[[DEST_CONFIG_NAME]]` variable will be replaced by the value of the `<destConfigName>`-attribute.

Optional

<destConfigName>ipso-backup_[[DATE]].tgz</destConfigName>

You can use the following variables within the `<command>` and `<return>` attributes:

[[ENABLE_PROMPT]] - Will be replaced by the enable prompt (which is defined above (enablePrompt))

[[CONFIG_NAME]] - Will be replaced by the correct name under which the configuration will be stored on the Backup Server (dest file)

[[SERVER_IP]] - Will be replaced by the Backup Server's IP address

[[SERVER_USERNAME]] - Will be replaced by the Backup server's username

[[SERVER_PASSWORD]] - Will be replaced by the Backup server's password

[[UPLOAD_CONFIG_NAME]] - Will be replaced by the filename of the configuration or file which should be uploaded to a device (only required for configuration "upload" or file "upload" jobs)

[[DEVICE_USERNAME]] - Will be replaced by the username (as defined in the Device User Group)

[[IGNORE_ERRORS]] - The default behavior is that the command execution is stopped when a command output matches an error expression. Add this variable to a command, if the command execution should NOT be stopped after an error expression match.

Example: `<command>delete configs/device_cm.cfg[[IGNORE_ERRORS]]</command>`

[[SLEEPsss]] - Wait sss seconds after executing the command. This value can ONLY be used within the `<command>` attribute.

Example: `<command>copy config backup server[[SLEEP60]]</command>` - Wait 60s before executing the next command which comes after "copy config backup server"

[[FILE_CONTENT:/path/ascii_file]] - Will be replaced with the content of "/path/ascii_file"

[[DATE]] - Will be replaced by the date in the format specified in the `<dateFormat></dateFormat>` attribute. This variable can only be used within the `<command>` or `<destConfigName>` attribute. Requires the `<dateFormat></dateFormat>` attribute

[[DEST_CONFIG_NAME]] - Will be replaced by the value of the `<destConfigName>`-attribute

List of commands and returns

command – command which should be executed on the device

```
<command>copy running-config tftp:</command>
```

return – expression which matches the expected return from the executed command

```
<return>Address or name of remote host</return>
```

Example: Copy the running configuration of a Cisco IOS device to a TFTP server

```
<command>copy running-config tftp:</command>
```

```
<return>Address or name of remote host</return>
```

```
<command>[[SERVER_IP]]</command>
```

```
<return>Destination filename</return>
```

```
<command>[[CONFIG_NAME]]</command>
```

```
<return>!!\r*\n*.*bytes copied.*</return>
```

4.1.1 Using wildcards/special characters

The XML attributes support wildcards. This is especially useful when creating the <return> expression, but wildcards can be used with any other attribute, too.

The following characters can be used as wildcards:

. (any character except newline)

* (match 0 or more times)

+ (match 1 or more times)

? (match 0 or 1 times)

\r\n (matches newline)

If you want to match for one of this characters you need to escape them.

Examples:

Expression/characters to match	match-expression
?	\?
Transfer successful.	Transfer successful\.
<i>newline</i>	\r\n (use always \r\n together)
!!	!!\r*\n*.*bytes copied.*

1030 bytes copied in 2.489 secs (395 bytes/sec)	
---	--

Use the pipe “|” character to specify alternative expressions.

Example:

```
<enablePrompt>#|(enable)</enablePrompt>
```

will match prompts like

```
Switch-A> (enable)
```

or

```
Switch-A#
```

4.2 Create new Jobs for an existing Device Type Group

To create new Jobs for an existing *Device Type Group* open the XML file for this group with your favorite editor and add the new Job in the “Job” section of the file.

Mandatory parameters are the arbitrary Job-name, the Job-Type, the comment and at least one command and one return. A “command” attribute must always be followed by by a “return” attribute (number of commands and returns must be the same). See 4.1 for a full list of the available parameters.

To best method to determine the commands and returns is to execute the commands which should be executed by the Job manually and create the commands and returns on the basis of the output of the commands.

Example 1: create a backup Job for an Enterasys Matrix device

```
$ telnet 192.168.30.35
Trying 192.168.30.35...
Connected to 192.168.30.35.
Escape character is '^['.
```

```
Username:admin
```

```
Password:*****
```

```
Enterasys SecureStack C2
```

```
Command Line Interface
```

Enterasys Networks, Inc.
50 Minuteman Rd.
Andover, MA 01810-1008 U.S.A.

Phone: +1 978 684 1000
E-mail: support@enterasys.com
WWW: http://www.enterasys.com

(c) Copyright Enterasys Networks, Inc. 2011

Chassis Serial Number: 111111111111X
Chassis Firmware Revision: 05.02.17.0006

```
Matrix(rw)->delete configs/device_cm.cfg
Matrix(rw)->show config outfile configs/device_cm.cfg
Matrix(rw)->copy configs/device_cm.cfg tftp://192.168.42.58/conf_bck_test.cfg
File transfer operation completed successfully.
Matrix(rw)->delete configs/device_cm.cfg
Matrix(rw)->exit
Connection closed by foreign host
```

In this example, the first command is executed to make sure that the file “device_cm.cfg” does not already exist: `Matrix(rw)->delete configs/device_cm.cfg` – As this command will produce an (not critical) error in the case that the file doesn't exist, we use the variable `[[IGNORE_ERRORS]]` within this command to avoid that the execution of the command will be stopped after an error.

Because the return of the command is the privileged mode prompt (`Matrix(rw)->`), we use the variable `[[ENABLE_PROMPT]]` as return value. The privileged mode prompt value is defined by the `<enablePrompt>`-attribute in the “global” section of the XML file.

Command “`copy configs/device_cm.cfg tftp://192.168.22.58/conf_bck_test.cfg`”: In the XML file, the IP address of the server can be replaced by the value `[[SERVER_IP]]`, the name of the configuration file MUST be replaced by the variable `[[CONFIG_NAME]]`. `[[SERVER_IP]]` will be replaced by the IP of the device's *Configuration Backup Server*, `[[CONFIG_NAME]]` will be replaced by an internal name created by the `fetch_config.pl` script.

The return of this command is “File transfer operation completed successfully”. So the return attribute value must match this string: `<return>File transfer operation completed successfully</return>` (e.g. `<return>completed successfully</return>` would also work).

As the Job is a “backup Job”, `<jobType>` must be set to “copy_file” (see 4.1).

Here the complete Job:

```

<copyRunTftp>
  <comment>Backup running config via TFTP</comment>
  <jobType>copy_file</jobType>

  <command>delete configs/device_cm.cfg[[IGNORE_ERRORS]]</command>
  <return>[[ENABLE_PROMPT]]</return>
  <command>show config outfile configs/device_cm.cfg</command>
  <return>[[ENABLE_PROMPT]]</return>
  <command>copy configs/device_cm.cfg tftp://[[SERVER_IP]]/
[[CONFIG_NAME]]</command>
  <return>File transfer operation completed successfully</return>
  <command>delete configs/device_cm.cfg</command>
  <return>[[ENABLE_PROMPT]]</return>
</copyRunTftp>

```

Example 2: Restore-configuration (upload) Job for a device running Cisco IOS:

Restore-configuration Jobs work like all other Jobs. The *Configuration Backup Server* (the GestióIP server) connects to the device and executes the commands on the device.

Execute the commands from which the Job should be created manually:

```

Router#copy tftp: running-config
Address or name of remote host []? 64.104.207.171
Source filename []? backup_cfg_for_my_router
Destination filename [running-config]?
Accessing tftp://10.66.64.10/backup_cfg_for_my_router...
Loading backup_cfg_for_router from 64.104.207.171 (via FastEthernet0/0): !
[OK - 1030 bytes]

```

1030 bytes copied in 9.612 secs (107 bytes/sec)

Router#

The jobType for restore-configuration Jobs must always be set to “task”.

The first command to restore a configuration from a TFTP server is `copy tftp: running-config`, the return value of the command is “Address or name of remote host []?”. The next “command” is the IP address of the *Configuration Backup Server* ([`Server_IP`]), after this, the Cisco device returns the string “Source filename []?”. The “Source file” is the backedup configuration on the *Configuration Backup Server*. Specify the “Source file” with the variable [`UPLOAD_CONFIG_NAME`]. The variable [`UPLOAD_CONFIG_NAME`] will be replaced by the name of the configuration which was specified on the web interface or on the command line. The Cisco device returns the string `Destination filename` which can here be answered with “ENTER” (empty `<command>` attribute).

Here the complete Job:

```
<copyTftpRun>
  <comment>Backup running config via TFTP</comment>
  <jobType>task</jobType>

  <command>copy tftp: running-config</command>
  <return>Address or name of remote host</return>
  <command>[[SERVER_IP]]</command>
  <return>Source filename</return>
  <command>[[UPLOAD_CONFIG_NAME]]</command>
  <return>Destination filename</return>
  <command></command>
  <return>OK</return>
</copyTftpRun>
```

Hint: After editing a XML file run always the script “check_xml_files.pl” which you find in the same directory as the XML files to check the XML file's syntax (see 4.4).

4.3 Create XML files/Create Device Type Groups

The easiest way to create a new *Device Type Group* (a new XML file) is to copy an existing one and adapt it to the device's model specific parameters.

Give the XML-file a significant name to be able to identify easily which *Device Type Group* is defined by this file (Example: 1_cisco_ios.xml for devices running Cisco IOS). The serial number must be unique and must be the same as the <deviceGroupID> attribute (1_cisco_ios.xml => <deviceGroupID>1</deviceGroupID>).

If you create new XML files use always serial numbers > 1000. This makes sure that new XML files which are included in the updates will not conflict with the serial numbers of self created XML files.

Adapt the *Device Type Group's* global variables like <enablePrompt> and create the required Jobs (see 4.2).

The XML file must have the extension .xml.

4.4 Check XML files syntax

To check the syntax of the XML files run the script “check_xml_files.pl” which you find in the

same directory as the XML files (/usr/share/gestioip/var/devices/check_xml_files.pl).

Run the script always after editing or creating a XML file.

Execute the script without arguments to check all XML files or specify a XML file as argument to check a specific file.

Example:

```
$ /usr/share/gestioip/var/devices/check_xml_files.pl 19_f5_bigip.xml
Checking 19_f5_bigip.xml...
  copyScfFtp: OK
>>>>>ERROR: Job: copyUscScp: no jobType defined - Job will be ignored
  copyScfFtpExport: OK
  copyScfScp: OK
19_f5_bigip.xml OK
$
```

Note: The check_xml_files.pl script only checks the syntax of the XML file and *not* the syntax of the commands which should be executed on the device.

4.4.1 Support

The project provides support for defining new Jobs and for the creation of new XML files.

If you have trouble creating XML files or define new Jobs send a mail to contact@gestioip.net.

The mail with the support request **MUST** include the following information:

- The device vendor, model and OS/firmware version.
- The copy of the **complete output of the session** (from login to logout) with the successful execution of the commands of which the new Job should be created from (see session example in 4.2).

If you already have created the Job, execute it from the “Manage-Jobs-page” in verbose mode and include also

- The XML-file with the new Job which you have created.
- The two execution log files of the last run of the Job in verbose mode (...fetch_config.log andfetch_config.log_stdout)(see 3.4.2). To obtain the log files, execute the Job in verbose mode from the “manage-Jobs-page” (see 3.3) or execute the Job from commadline (see 3.4).

4.4.2 Share your XML file

Please share your XML files.

If you have created new XML files or if you have created new Jobs please send the XML files to contact@gestioip.net so that they can be included within the next update of GestióIP.

Thanks a lot!!

5 Troubleshooting

5.1 Server timeout

The new versions of Fedora, Redhat and Centos work with a small default Apache server timeout. Set the timeout to 300s.

Open `/etc/httpd/conf/httpd.conf` with an editor and add the following line at the beginning of the file:

```
Timeout 300
```

Save the file and restart the Apache webserver (`sudo apachectl restart`)

5.2 Jobs do not appear

If you created a new Job (via the XML files), and the Job does not appear in the Job list of it's *Device Type Group*, check the syntax of the XML file by running the “`check_xml_files.pl`” script (see 4.4).

5.3 Running Jobs

5.3.1 Background

The *Configuration Backup Server* connects via the *connection protocol* to the device and executes the commands of the Job on the device (in the case of a backup Job). That means that configurations are uploaded from the device to the server (and not downloaded by the server).

Make sure that the firewalls permit the connections between the devices and the server (see 6.2)

If errors occur during the automatic execution of a Job, the Job status button will change to a red color.

To gather information why a Job was not correctly executed check the Job execution log file (see 3.1.1). If the log file doesn't offer sufficient information run the Job manually with “verbose” log mode from the “manage-Job-page” (see 3.1.5). Click the link “Show log” to access to the Job's log file.

Error while fetching configuration detected

ERROR: Login failed: Username/Password incorrect

Check the log file for further information

[Show log](#)

Figure 34: Job execution failed

Hint: You also can also run `fetch_config.pl` manually from the command line (see 3.4).

If a Job which was executed manually from the “manage-Jobs-page” runs in a timeout (result-page does not load), this is probably a problem with the Job definition in the XML file. To debug this problem consult the logfiles (`/usr/share/gestioip/var/log`) and run `check_xml_files.pl` (see 4.4).

6 Configuration Backup Server

The *Configuration Backup Server* is always the server with the GestióIP installation.

Make sure that there is enough disk space available.

To receive configurations/command outputs there must be the adequate server software (FTP/TFTP/SSH server) on the GestióIP server installed and running.

Examples for Backup Server software:

FTP – vsftpd

TFTP - tftpd

SCP – openssh

This servers are for all Linux distributions as package available.

6.1 Installation of the FTP, TFTP and SSH (SCP) server software

The installation of the server software can be made with the distribution specific packet manager. After the installation the owner and the permissions of the server root directory must be set.

<i>Server</i>	<i>Document Root Owner</i>	<i>Document Root permissions</i>
FTP	ftp_backup_user:apache_server_group	770
TFTP	tftp_server_user:apache_server_group	770
SSH (SCP)	scp_backup_user:apache_server_group	770

6.1.1 Debian/Ubuntu

Working with Ubuntu 14.04.

6.1.1.1 FTP server

Install the FTP server

```
sudo apt-get install vsftpd
```

Create the server root directory (if not exists)

```
sudo mkdir /srv/ftp
```

Create a user to connect to the server

```
sudo useradd -G www-data -d /srv/ftp gestioip-bck
sudo passwd gestioip-bck
```

Change the owner and the permissions of the server root directory

```
sudo chown gestioip-bck:www-data /srv/ftp/
sudo chmod 770 /srv/ftp/
```

Open /etc/vsftpd.conf with an editor and configure the following parameters:

```
pam_service_name=ftp
listen=YES
local_enable=YES
local_umask=0002
anonymous_enabled=NO
write_enable=YES
```

Restart the FTP server

```
sudo service vsftpd restart (>=12.04)
sudo /etc/init.d/vsftpd restart (10.04)
```

GestióIP Configuration Backup Server configuration:

Backup protocol: ftp

Server root directory: /srv/ftp

Username: gestioip-bck

6.1.1.2 TFTP server

Install the TFTP server

```
sudo apt-get install xinetd tftpd tftp
```

Create the configuration file /etc/xinetd.d/tftp with the following content (sudo vi /etc/xinetd.d/tftp):

```
service tftp
{
    protocol = udp
```

```
port = 69
socket_type = dgram
wait = yes
user = nobody
server = /usr/sbin/in.tftpd
server_args = /var/lib/tftpboot -s
disable = no
}
```

Create the server root directory:

```
sudo mkdir /var/lib/tftpboot
sudo chgrp -R www-data /var/lib/tftpboot
sudo chmod -R 775 /var/lib/tftpboot
```

Restart the TFTP server (vía xinetd):

```
sudo service xinetd stop
sudo service xinetd start
```

GestióIP Configuration Backup Server configuration:

Backup protocol: tftp

Server root directory: /var/lib/tftpboot

6.1.1.3 SSH (SCP) server

If not already installed, install the openssh server

```
sudo apt-get install openssh-server
```

Create the server root directory:

```
sudo mkdir -p /home/gestioip-scp-bck/gestioip-backup
```

Create a user to connect to the server:

```
sudo useradd -d /home/gestioip-scp-bck gestioip-scp-bck
sudo usermod -G www-data gestioip-scp-bck
sudo passwd gestioip-scp-bck
```

Change owner and permissions of the server root directory:

```
sudo chown -R gestioip-scp-bck:www-data /home/gestioip-scp-bck
```

```
sudo chmod -R 770 /home/gestioip-scp-bck/
```

GestióIP Configuration Backup Server configuration:

Backup protocol: scp

Server root directory: /home/gestioip-scp-bck/gestioip-backup

Username: gestioip-scp-bck

6.1.2 OpenSuse

6.1.2.1 FTP server

Install the FTP server:

```
sudo zypper install vsftpd xinetd
```

Edit /etc/xinetd.d/vsftpd: set “disable” to “no”.

```
disable = no
```

Create a user to connect to the server:

```
sudo /usr/sbin/useradd -d /srv/ftp gestioip-bck
```

```
sudo passwd gestioip-bck
```

Change the owner of the server root directory:

```
sudo chown gestioip-bck:www /srv/ftp/
```

```
sudo chmod g+w /srv/ftp/
```

Open /etc/vsftpd.conf with an editor and configure the following parameters:

```
pam_service_name=vsftpd
```

```
listen=NO
```

```
write_enable=YES
```

```
local_enable=YES
```

```
local_umask=0002
```

```
anonymous_enable=NO
```

Enable xinetd:

```
sudo chkconfig xinetd on
```

Restart the TFTP server (via xinetd):

```
sudo /usr/sbin/rcxinetd restart
```

GestióIP Configuration Backup Server configuration:

Backup protocol: ftp

Server root directory: /srv/ftp

Username: gestioip-bck

6.1.2.2 TFTP server

Install the TFTP server with YAST2 (will install xinetd, too) or with zypper:

```
zypper install tftp yast2-tftp-server xinetd
```

Edit /etc/xinetd.d/tftp: set “disable” to “no”.

```
disable = no
```

Change ownership and set permissions for the server root directory:

```
sudo chgrp -R www /srv/tftpboot
```

```
sudo chmod 775 /srv/tftpboot
```

Enable xinetd:

```
sudo chkconfig xinetd on
```

Restart the TFTP server (via xinetd):

```
sudo /usr/sbin/rcxinetd restart
```

GestióIP Configuration Backup Server configuration:

Backup protocol: tftp

Server root directory: /srv/tftpboot

6.1.2.3 SSH (SCP) server

If not already installed, install the openssh server and start it:

```
sudo zypper install openssh  
sudo service sshd start
```

Create the server root directory:

```
sudo mkdir -p /home/gestioip-scp-bck/gestioip-backup
```

Create a user to connect to the server:

```
sudo /usr/bin/useradd -d /home/gestioip-scp-bck gestioip-scp-bck  
sudo /usr/sbin/usermod -G www gestioip-scp-bck  
sudo passwd gestioip-scp-bck
```

Change owner and permissions of the server root directory:

```
sudo chown -R gestioip-scp-bck:www /home/gestioip-scp-bck  
sudo chmod -R 770 /home/gestioip-scp-bck/
```

GestióIP Configuration Backup Server configuration:

Backup protocol: scp

Server root directory: /home/gestioip-scp-bck/gestioip-backup

Username: gestioip-scp-bck

6.1.3 Fedora/Redhat/CentOS

6.1.3.1 FTP server

Install the FTP server:

```
sudo yum install vsftpd
```

Create the server root directory (if not exists):

```
sudo mkdir /srv/ftp
```

Create a user to connect to the server:

```
sudo /usr/sbin/useradd -d /srv/ftp gestioip-bck  
sudo passwd gestioip-bck
```

Change the owner of the server root directory:

```
sudo chown gestioip-bck:apache /srv/ftp/  
sudo chmod g+w /srv/ftp/
```

Open /etc/vsftpd/vsftpd.conf with an editor and configure the following parameters:

```
pam_service_name=vsftpd  
listen=YES  
write_enable=YES  
local_enable=YES  
local_umask=0002  
anonymous_enable=NO
```

Enable the FTP server on boot and start the FTP server:

Fedora

```
sudo systemctl enable vsftpd.service  
sudo systemctl start vsftpd.service
```

Redhat/Centos

```
sudo service vsftpd restart  
sudo chkconfig vsftpd on
```

GestióIP Configuration Backup Server configuration:

Backup protocol: ftp

Server root directory: /srv/ftp

Username: gestioip-bck

6.1.3.2 TFTP server

Install the TFTP server:

```
sudo yum install tftp-server
```

Edit /etc/xinetd.d/tftp: set “disable” to “no”.

```
disable = no
```

Change ownership and set permissions for the server root directory:

```
sudo chgrp -R apache /var/lib/tftpboot  
sudo chmod -R 775 /var/lib/tftpboot
```


Start the tftp service:

Fedora

```
sudo systemctl start xinetd.service  
sudo systemctl enable xinetd.service
```

Redhat/Centos

```
sudo service xinetd start  
sudo chkconfig xinetd on
```

GestióIP Configuration Backup Server configuration:

Backup protocol: tftp

Server root directory: /var/lib/tftpboot

6.1.3.3 SSH (SCP) server

If not already installed, install the openssh server

```
sudo yum install openssh-server
```

Create the server root directory:

```
sudo mkdir -p /home/gestioip-scp-bck/gestioip-backup
```

Create a user to connect to the server:

```
sudo useradd -d /home/gestioip-scp-bck gestioip-scp-bck  
sudo usermod -G apache gestioip-scp-bck  
sudo passwd gestioip-scp-bck
```

Change owner and permissions of the server root directory:

```
sudo chown -R gestioip-scp-bck:apache /home/gestioip-scp-bck/gestioip-backup  
sudo chmod -R 770 /home/gestioip-scp-bck/
```

GestióIP Configuration Backup Server configuration:

Backup protocol: scp

Server root directory: /home/gestioip-scp/gestioip-backup

Username: gestioip-scp-bck

6.2 Firewall

The firewall must permit that the server can logon to the device (*connection protocol*) as well as it must permit, that the device can copy it's configuration/the command-outputs to the server (*backup protocol*). Make sure that the following connections are allowed by the firewalls.

server → device:*connection protocol*

device → server:*backup protocol*

Examples:

If the server connects with SSH to the device, the server must be able to reach the device on port 22 (TCP):

server → device:22

If the server connects with TELNET to the device, the server must be able to reach the device on port 23 (TCP):

server → device:23

If the device copies it's configuration via FTP to the server, the device must be able to reach the server on port 21 (TCP)

device → server:21

If the device copies it's configuration via TFTP to the server, the device must be able to reach the server on port 69 (UDP)

device → server:69 (UDP)

