

TRAFwatcher Manual

TRAFwatcher Manual

Table of Contents

Preface	viii
Target audience	viii
Conventions used in this manual	viii
1. Introduction	1
About	1
Main features	1
Minimum requirements	1
Hardware	1
Browser	1
2. Historical data	2
Control Panel	2
Limits	2
Latest threat overview	2
Subnets	2
Definitions	2
Configuration	3
Import subnets file	4
Add subnets metadata	4
Stats	5
Reports	5
Templates	5
Threat Analysis	7
Blackhole IP list	7
Removing IP addresses from the blackhole list	7
3. Configuration	8
Threat profiles	8
Add threat profiles metadata	9
Scripts	10
Creating scripts	10
Executing scripts	13
Login Script	13
Blackhole Script	13
Blackhole	15
4. ALARMmanager	16
Reports	16
Suppressed reports	16
Consolidated reports	16
Email Template	17
Introduction	17
Customizing the email	17
Alarm urgency level	18
Changing the urgency level priority	18
Adding a new urgency level	18
Add alarm urgency level metadata	19
Alarms	19
Add alarms metadata	20
Alarm profiles	21
Add alarm profile metadata	21
Console	22
Introduction	22
Console operation	22

5. System	25
Access Log	25
User access	25
Simultaneous access	25
Users	25
Editing users	25
Disabling users	26
User Groups	26
User profiles	27
Alarm Console	27
Backup/Restore	28
Local configuration backup	28
Local configuration restore	28
Remote backup	28
Remote restore	29
Restore status	29
Parameters	29
Active directory	30
ALARMmanager	30
Association agents	31
Auto login	31
Backup	31
BGP	31
Capture agent configuration	32
Circuit	32
Cisco WAAS	32
Configuration history	32
Data storage	33
dbn0/Altaia integration	34
Distributed architecture	35
EPM	35
Expiration warning	35
Grapher	36
HTTPS Configuration	36
Local preferences	36
Login redirection	37
Log level	37
Logo	37
Redundancy	37
Regional settings	38
Reports	38
SMS server	39
SMTP	40
SNMP	40
System Version Check	41
TACACS	41
Telcomanager Host Agent	41
Telcomanager JMX Agent	41
Theme	42
Threat Analysis	42
User access history	43
Web Services	43
Diagnostics	43
Network information	43

Connectivity tests	43
Packet Capture	43
Objects	44
Summarizer	44
Storage usage	44
Log files	45
Configuration Logs	45
Timezone	45
Support	45
Open request	45
Check for system updates	45
Remote support tunnel setup	46
About	46
6. License enabled features	47
Redundancy	47
Concepts	47
Enabling the redundancy	47
Distributed architecture	47
Concepts	47
Prerequisites	47
Deployment	48
7. Glossary	49
Abbreviations	49

List of Tables

1. Manual conventions	viii
2.1. New subnet form	3
2.2. Fields from subnet file	4
2.3. Metadata fields	4
2.4. Template Form	5
2.5. Suspect traffic report	7
3.1. Threat profile form	8
3.2. Metadata fields	9
3.3. Wildcard List	15
3.4. Blackhole form	15
4.1. Suppressed alarms report form	16
4.2. Consolidated alarm report form	16
4.3. Email template	17
4.4. Email variables	17
4.5. ALARM urgency level form	18
4.6. Metadata fields	19
4.7. TRAFwatcher alarm form	19
4.8. Metadata fields	21
4.9. Alarm profile form	21
4.10. Metadata fields	21
4.11. ALARMmanager console	22
5.1. User form	25
5.2. User form	26
5.3. User form	27
5.4. ALARMmanager console columns	27
5.5. FTP server form	28
5.6. S3 server form	29
5.7. Active directory form	30
5.8. ALARMmanager parameters form	30
5.9. Automatic association agent form	31
5.10. BGP form	31
5.11. Capture agent configuration form	32
5.12. Circuit form	32
5.13. Cisco WAAS form	32
5.14. Log history parameters	32
5.15. Data storage form	33
5.16. dbn0/Altaia integration form	34
5.17. Distributed architecture parameters form	35
5.18. EPM form	35
5.19. Expiration warning form	36
5.20. Grapher parameters form	36
5.21. Https parameters form	36
5.22. Local preferences form	36
5.23. Redundancy activation settings	37
5.24. Redundancy Commutation settings	37
5.25. Regional settings form	38
5.26. Scheduled reports configuration form	38
5.27. FTP Server configuration form	38
5.28. SMPP server form	39
5.29. SMTP parameters form	40
5.30. TRAP fields	41

5.31. Theme configuration	42
5.32. Threat analysis configuration	42
5.33. User access history form	43
5.34. Configurations API form	43
5.35. TRAFip's raw data form	43
5.36. Packet Capture	44
7.1. Abbreviations list	49

Preface

Target audience

This manual was designed for network administrators, network consultants and Telcomanager partners.

To fully understand this manual, the reader should have intermediate knowledge on network management and TCP/IP protocol.

Conventions used in this manual

This document uses the following conventions:

Table 1. Manual conventions

Item	Convention
Selecting a menu item	Menu → Submenu → Menu item
Commands, buttons and keywords	Boldface font.

Chapter 1. Introduction

About

TRAFwatcher is a module working with TRAFip to detect network threats.

Main features

- Support for NetFlow, jFlow, sFlow, IPFIX and Huawei netstream.
- Access to all system features through a web browser.
- High Availability can be provided through the use of the redundant solution, in which two appliances work in HOT-STANDBY.
- Mass graph image export.
- Flexible graph creation.
- Interactive HTML5 grapher, with features like vertical and horizontal zoom, auto-scale and aggregated charts.
- High performance database for historical data storage.
- Threat profiles that can be associated to subnets. So, alarms can be configured to trigger when an IP address reaches the defined thresholds.
- Creation of scripts to announce suspect IP addresses in blackhole.

Minimum requirements

These requisites are for the computers that will access the system through a web browser.

Hardware

- Processor Pentium 2 400 MHZ or above.
- 128 MB RAM memory.

Browser

- Internet explorer 9+.
- Chrome 4.0+.
- Firefox 7.0+.

Chapter 2. Historical data

This chapter describes the elements on the historical data tab.

Under this tab, you can access all the processed data for the monitored objects.

The data can be accessed through graphs and reports.

Control Panel

This tab displays the thresholds and the overview of all IPs currently identified as suspect traffic. They are separated by subnet.

Limits

For each subnet, it will be displayed a table containing the **Source bytes**, **Destination bytes**, **Source flows**, **Destination flows**, **Source packets**, **Destination packets**, **Source Ip Flood** and **Destination Ip Flood** thresholds, maximum values, averages and percentual distances between the averages and the maximum values.

If the subnet is using the automatic limit, it will be shown (**auto**) beside the threshold values.

The percentual distance between the maximum value and the average is calculated as follows:


$$\text{Distance} = [(\text{Maximum}/\text{Average}) - 1] * 100$$

Latest threat overview

It will be displayed the IPs (source or destination), the elapsed time, the detected attack type, the reached limit type, the limit value and the observed value.

Clicking on **Add to excluded list** button, the IP address will be excluded from the threat analysis.

To run the **Blackhole** script, click on the icon shown in **Blackhole** column.

To have detailed and consolidated statistics for each flow, generate a **Raw data report** by clicking on  icon.

Important

On this screen, it will be shown only the automatic subnets or the ones that are associated to a Threat Profile.

Subnets

The subnets object allows the analysis of IP block ranges.

Definitions

- **Subnet destination traffic**: composed by the sum of all flows in which the destination IP address belongs to the IP block range of the subnet.

- **Subnet source traffic:** composed by the sum of all flows in which the source IP address belongs to the IP block range of the subnet.
- **Absolute subnet traffic:** compound by the sum of all flows in which the source IP address or destination belongs to the subnet IP block.
- **External absolute traffic of the subnet:** consisting of the sum of all flows in which the IP address belongs to the subnet's IP block, but the source or destination IP address belongs to an unknown subnet.

Configuration

To manage the system subnets, access **Historical data** → **Subnets**.

Click the **Subnets** tree menu item to have the list of subnets configured.

To add a new subnet, click on **New** button and fill the form.

Table 2.1. New subnet form

Field	Description
Name	Subnet name.
Description	Subnet description.
IP address blocks	Subnets can have more than one address range. Ex: 10.0.0.0/24, 10.0.1.0/24, 2001:db8:abcd:2000::/64, 2001:cdba:9abc:5678::/64.
Traffic reference line (bps)	This value will be plotted in the object graph as a dotted red line.
Origin activity factor threshold	Limit of origin Activity factor .
Destination activity factor threshold	Limit of destination Activity factor .
Enable trend analysis	Use trend analysis default parameters or set them.
Enable TRAFWatcher	Select Yes to enable the threat analysis by TRAFwatcher.
Use auto limit	Select Yes and the system will calculate the thresholds automatically based on Tolerance Factor . If you select No , the threats detection will use the limits set manually in Threat profile .
Tolerance Factor	This field is only available when the Use auto limit is Yes . The Extreme factor is more tolerant. It means that the thresholds will be greater if this option is selected. To a moderate evaluation of threats, select the Moderate option.
Threat profile	This field is only available when the Use auto limit is No . Select a threat profile for this subnet to be used in threat analysis or leave blank.
Alarm profile	Alarm profile association.

Tip

You can enable TRAFwatcher in a lot of subnets simultaneously. To do this, access **Historical Data** → **Subnets**, select which subnets will be analysed by TRAFwatcher and click on **Enable TRAFwatcher** button.

Import subnets file

To import a file of subnets, access **Historical data** → **Subnets**.

Click the **Subnets** tree menu item.

Click the **Import** button and load the file.

A import subnets file has the following fields:

Table 2.2. Fields from subnet file

Field	Description
Name	Subnet name.
Description	Describe the subnet (optional).
IP address blocks	Subnets can have more than one address range. Input format: IP1/Mask1,IP2/Mask2. (IP/32 in the case of using a single IP). Ex: 10.0.0.1/32,10.0.1.0/24
Traffic reference line (bps)	Fill with an integer number greater than or equals to 0.
Enable TRAFwatchet	Fill with YES or NO .

Add subnets metadata

To access the metadata configuration page, access **Historical Data** → **Subnets**, click on **Subnet** tree menu item and click on **Metadata** button.

Click on **New** button to create a new metadata.

You can change the metadata configuration using the **Edit** button. To check the configuration history, click on **History** button.

To remove a metadata, click on **Delete** button.

Table 2.3. Metadata fields

Field	Description
Name	Enter the metadata name.
Description	Describe the metadata (optional).
Datatype	Choose the metadata type: Text , Integer or Enum (Enumerate).
Values	This field is only available when the Datatype is Enum . Enter a list of values, separating them by semicolon (;).

To associate the metadata to a subnet, access the subnets list and click on **Metadata** button beside the subnet that will be configured.

Then, fill the metadata according to its type.

Stats

Accessing a subnet through the left menu, the data display will show its stats for each 5 minutes.

It will be displayed the **Average** and the **Maximum** source and destination bytes, packets, flows and IP Flood.

At the top of the page, it will be shown the highest values.

Important

To obtain these values, it is necessary that the subnet be associated to a Threat Profile.

Important

Any subnet that exceeds the limit defined in the threat profile associated with her will have its cell highlighted in red.

Reports

Templates

For almost all reports available on the system, you have the option to save them as templates once you fill the report fields.

Saving

1. Open the desired report and select the Save template option.
2. Fill the fields below:

Table 2.4. Template Form

Fields	Values
Name	Report name.
Write permission	Select who can alter this report. The group option is based on user groups.
Read permission	Select who can read this report. The group option is based on user groups.
Send report by email	Send the report by email.
Send report to FTP server	Send the report to FTP server.
Attachment format	Choose the desired format: PDF or CSV.

3. Fill the other report fields and click the **Send** button.

After executing the steps above, the saved report is available at the **Template list** for each report type.

Scheduling

1. Open the Template list for the report or create a new report.
2. Select the Schedule template option.

3. Select the appropriate schedule option.

Schedule options

- One execution: It can be **Instant** or **Scheduled**. The data start and end times will be the start time and end times of the report.
- Daily: Define a **Scheduled report time** and every day, at this time, it will be executed a 1 day report. If the **Consider execution day** option is enabled, the execution day will be considered in this period.
- Weekly: Define a **Week-day** and time and every week, at this day and time, it will be executed a 7 days report. The data start and end times will be from Sunday 00h to Saturday 23h59min of the previous week. If the **Consider execution day** option is enabled, the execution day week will be considered in this period.
- Monthly: Define a **Execution day** and time and every month, at this day and time, it will be executed a 31 days report. The data start and end times will be from day 01 00h to the last day at 23h59min of the previous month. If the **Consider execution day** option is enabled, the execution day month will be considered in this period.

Tip

In order to schedule a report, you must save it as a template.

Tip

When a report is ready, it is sent an e-mail to users. The SMTP server should be configured and also each user email at the user configuration form.

Editing

After the template is saved, an **Edit** button appears at the template list and can be used to change the report parameters.

Visualizing reports

After the system runs a template, a new report instance is generated.

All report instances can be accessed through the Details button available for each template.

To visualise a report instance, follow the procedure below:

1. Click the **Details** button for the desired template.
2. Choose the desired output format between HTML, CSV and PDF.
3. Click the **Show** button for the desired report instance.

Managing disk space

The total space available and currently used by the template reports is listed below the template list.

The system has a reserved storage area that is shared for all reports.

You can increase or decrease this space by going to **System** → **Parameters** → **Data storage** .

You can delete generated reports by clicking the Details button at template list for the desired template.

Threat Analysis

The threat analysis report provides detailed information about suspect traffic. It displays source and destination IP addresses, when the suspect traffic between them started and when it was completed. Besides this, it shows which Threat profile parameter was exceeded: Bytes/s, Packets/s, Flows/s or IP addresses/s.

To generate a new report, access **Historical data** → **Reports** → **Threat analysis** .

The form will be already filled, but you can edit it. Then, click the **Send** button.

Table 2.5. Suspect traffic report

Field	Description
Start time	Enter the initial period time.
End time	Enter the final period time.
Filter by subnet	Select None to do not filter by subnet or select the desired one.
Number of lines	Choose a limit to the report output.
Attack type	You can choose between DNS amplification, High data flow between two IP address, High data flow between two IP address (Port 0), ICMP flood, IP Flood, NTP amplification, SNMP amplification and Syn flood.

Tip

You can generate **Raw data report** to have detailed and consolidated statistics for each flow and, to do it, click on icon shown next to IP address.

Blackhole IP list

This tab displays the IPs that were announced in blackhole manually or automatically.

For each IP, it will be displayed a table containing the time the IP had the suspected traffic detected, the time it was announced in blackhole and the time it was removed from blackhole.

At **System** → **Parameters** → **Threat Analysis** you can configure the maximum period, in minutes, in which an IP addresses will continue to be displayed in the list after their removal from blackhole.

Removing IP addresses from the blackhole list

To remove IP addresses from blackhole manually, click the icon shown in the Run removal script column.

Chapter 3. Configuration

Threat profiles

You can create threat profiles and associate them to subnets. In these profiles, you will define the rate per second limit of the data accumulated in the period set at **System** → **Parameters** → **Threat analysis** . Then, if one of the associated subnets reaches these limits, an alarm is triggered.

You can set the profile to detect if the **absolute traffic** thresholds were reached and **common attacks** as SYN flood, ICMP flood, DNS amplification, SNMP amplification, NTP amplification and **attacks on port 0**.

To create a new threat profile, access the **Configuration** → **Threat profiles** and click on **New** button.

Check the profile configuration history using the **History** button.

Edit the profiles using **Edit** button and remove them using **Remove** button.

Table 3.1. Threat profile form

Field	Description
Name	Define a name for the threat profile.
Source Mb/s	Limit of megabits sent per second to a host to trigger an alarm.
Destination Mb/s	Limit of megabits received per second by a host to trigger an alarm.
Source Packets/s	Limit of packets sent per second to a host to trigger an alarm.
Destination Packets/s	Limit of packets received per second by a host to trigger an alarm.
Source Flows/s	Limit of flows sent per second to a host to trigger an alarm.
Destination Flows/s	Limit of flows received per second by a host to trigger an alarm.
Source IP addresses number	Limit of connections sent to a host in 60 seconds.
Destination IP addresses number	Limit of connections received by a host in 60 seconds.
Syn flood threshold (flows/s)	Limit of flows containing the SYN flag sent per second to a single destination.
ICMP flood threshold (packets/s)	Limit of ICMP echo request sent per second to a single destination.
DNS amplification threshold (Mb/s)	Limit of DNS response sent per second to a single destination.
SNMP amplification threshold (Mb/s)	Limit of SNMP response sent per second to a single destination.
NTP amplification threshold (Mb/s)	Limit of NTP response sent per second to a single destination.

Field	Description
Source Mb/s - Port 0	Limit of megabits sent per second to a host on port 0 (zero).
Destination Mb/s - Port 0	Limit of megabits received per second by a host on port 0 (zero).
Source Packets/s - Port 0	Limit of packets sent per second to a host on port 0 (zero).
Destination Packets/s - Port 0	Limit of packets received per second by a host on port 0 (zero).
Source Flows/s - Port 0	Limit of flows sent per second to a host on port 0 (zero).
Destination Flows/s - Port 0	Limit of flows received per second by a host on port 0 (zero).
IP address list excluded from the analysis	Enter the IP addresses or subnets to be excluded from the threat analysis. Separate them by comma.
Subnets	Select the subnets to compose this profile.

Tip

To set the limits of the rates, you can use the **Average** and **Maximum** statistics displayed on **Stats** in the Subnet's graph selection area.

Add threat profiles metadata

To access the metadata configuration page, access **Configuration** → **Threat profiles** and click on **Metadata** button.

Click on **New** button to create a new metadata.

You can change the metadata configuration using the **Edit** button. To check the configuration history, click on **History** button.

To remove a metadata, click on **Delete** button.

Table 3.2. Metadata fields

Field	Description
Name	Enter the metadata name.
Description	Describe the metadata (optional).
Datatype	Choose the metadata type: Text , Integer or Enum (Enumerate).
Values	This field is only available when the Datatype is Enum . Enter a list of values, separating them by semicolon (;).

To associate the metadata to a threat profile, access the threat profiles list and click on **Metadata** button beside the profile that will be configured.

Then, fill the metadata according to its type.

Scripts

You can create and execute scripts of the following types: **Login** and **Blackhole**.

The script types will be shown in a selectbox on the left side menu. Selecting one of them, it will be listed the already created scripts.

Creating scripts

To create a new script, click on plus sign (+). The text box will have an example of the selected script type. Edit the text box and, after, select the execution mode (**Lua**, **Send/Expect** or **Text**, depending on the script type), click on **Run** and select the object in which the script will be executed.

Tip

You can save or remove a script at any time using the icons above the text box.

Functions

The system provides some functions to enhance the scripts possibilities:

- **tmlSnmp.snmpGet**: Executes SNMP GET on the device.
- **tmlSnmp.snmpGet2**: Executes SNMP GET on the device when the SNMP configuration is not default.
- **tmlSnmp.snmpWalk**: Executes SNMP WALK on the device.
- **tmlSnmp.snmpWalk2**: Executes SNMP WALK on the device when the SNMP configuration is not default.
- **tmlSSH.sshNew**: Connects to a remote system using SSH.
- **tmlTelnet.telnetNew**: Connects to a remote system using Telnet.
- **tmlUtils.processMapper**: Maps the device processes.
- **tmlUtils.removeTerminalEscape**: Remove terminal characters.
- **tmlDebug.log**: Prints the log on the **Debug** tab on **Result**.
- **tmlDebug vardump**: Prints the variable's log on the **Debug** tab on **Result**.
- **tmlJson.encode**: Converts a Lua table to a JSON string.
- **tmlJson.decode**: Converts a JSON string to a Lua table.
- **tmlPing.pingNew**: Sends ICMP echo messages.
- **tmlMsSql.msSqlNew**: Accesses the dbms (Database Management System) Microsoft SQL server.
- **setTimeout**: Changes the timeout connection.
- **tmlSocket.http**: Makes possible to execute HTTP requests. To do so, you must provide an URL and a request method. Possible request methods are **GET** and **POST** all uppercase.
- **tmlSequence.getNext**: Generates sequential numbers without repetition. Returns the current value plus 1 and the sequence begins with the number 1.

- **tmBGP.addToBlackHole**: Adds the subnet to the blackhole.
- **tmBGP.removeFromBlackHole**: Removes the subnet from the blackhole.

The Lua allowed functions for the scripts are:

- abs
- clock
- difftime
- exp
- floor
- ipairs
- max
- min
- next
- pairs
- pow
- sqrt
- time
- tonumber
- tostring
- type
- unpack

Variables

There are also variables that are available in every script and are filled according to the object that it is related.

They are stored in params table (params['variable_name']):

- **params['ipaddr']**: IP address.
- **params['name']**: Device's name.
- **params['description']**: Device's description.
- **params['type']**: Device's type.
- **params['snmp']['community']**: Device's SNMP community.
- **params['snmp']['version']**: Device's SNMP version.

- **params['snmp']['timeout']**: Device's SNMP Timeout.
- **params['snmp']['retries']**: Device's SNMP Retries.
- **params['snmp']['max_per_packet']**: Number of OIDs per packet.
- **params['snmp']['max_pps']**: Maximum packet rate (pps).
- **params['snmp']['window']**: Device's SNMP window.
- **params['snmp']['port']**: Device's SNMP port.
- **params['obj'][<MAPPER>][<DESCRIPTION>]['ifindex']**: Mapped object's ifIndex, where MAPPER is the mapper name and DESCRIPTION is the mapped object name (without the device name).
- **params['obj'][<MAPPER>][<DESCRIPTION>]['description']**: Mapped object's description, where MAPPER is the mapper name and DESCRIPTION is the mapped object name (without the device name).
- **params['username']**: Username for authentication.
- **params['passwd']**: Password for authentication.
- **params['enable_passwd']**: Enable password for authentication.
- **params['protocol']**: Protocol for connection.
- **params['alarm']['active']**: Alarm status. Returns **true** or **false**.
- **params['alarm']['name']**: Alarm name.
- **params['alarm']['urgency']**: Alarm urgency level.
- **params['alarm']['object']['name']**: Alarmed object name.
- **params['alarm']['object']['description']**: Alarmed object description.
- **params['alarm']['object']['type']**: In device alarms, it's the alarmed device type.
- **params['alarm']['object']['manufacturer']**: In device alarms, it's the alarmed device manufacturer.
- **params['alarm']['object']['device']['name']**: In mapped object alarms, it's the device name of the alarmed mapped object.
- **params['alarm']['object']['device']['description']**: In mapped object alarms, it's the device description of the alarmed mapped object.
- **params['alarm']['object']['device']['type']**: In mapped object alarms, it's the device type of the alarmed mapped object.
- **params['alarm']['object']['device']['manufacturer']**: In mapped object alarms, it's the device manufacturer of the alarmed mapped object.
- **params['blackhole']['ipaddr']**: IP blackhole announce or removal.
- **params['connection']**: Connection object used to access a device.

- **params['metadata']**[<METADATA_NAME>]: Device metadata value, where METADATA_NAME is the name of the metadata.

Executing scripts

To execute an already existing script, click on it on the left menu. You can edit it using the text box. So, click on **Run** and select the object in which the script will be executed.

Besides this, it's possible to check the last execution details using the tab **Result** at the bottom of the page.

Tip

You can save your changes using the Save icon above the text box.

Login Script

Check below the authentication script example Cisco Telnet written on Lua mode.

```
c = params['connection']
u = params['username']
p = params['passwd']

if (c:send(u) == false) then
    return nil
end
if (c:expect('Pass') == false) then
    return nil
end
if (c:send(p) == false) then
    return nil
end
if (c:expect('>') == false) then
    return nil
end
```

Blackhole Script

This type of script is used to announce IP addresses in blackhole list or to remove them.

It can be written on 3 modes: **Text**, **Lua** and **Send/Expect**.

At **Configuration** → **Blackhole**, you will associate a device to two scripts of this type, one of them will announce the IP in blackhole and the other one will remove it.

To configure the maximum period, in minutes, in which an IP address will be in blackhole before the removal script be executed, go to **System** → **Parameters** → **Threat Analysis** .

The following script is already configured in TRAFwatcher and it is a generic script for Cisco devices.

```
c = params['connection']
c:setTimeout(10)
```

```
if(c:send('enable') == false) then
  return false
end
if(c:expect('Password:') == false) then
  return false
end
if(c:send(params['enable_passwd']) == false) then
  return false
end
if(c:expect('#') == false) then
  return false
end

if(c:send('conf t') == false) then
  return false
end
if(c:expect('(config)') == false) then
  return false
end

for k,v in pairs(params['blackhole']) do
  if (c:send('ip route ' .. k .. ' 255.255.255.255 Null0') == false) then
    return false
  end
  if (c:expect('(config)') == false) then
    return false
  end
end

if (c:send('router bgp XXX') == false) then
  return false
end
if (c:expect('(config-router)') == false) then
  return false
end

for k,v in pairs(params['blackhole']) do
  if (c:send('network ' .. k .. ' mask 255.255.255.255
route-map blackhole') == false) then
    return false
  end
  if (c:expect('(config-router)') == false) then
    return false
  end
end

if (c:send('route-map blackhole permit 10') == false) then
  return false
end
if (c:expect('(config-route-map)') == false) then
  return false
end

if (c:send('set community 6939:666') == false) then
```

```

        return false
    end
    if (c:expect('(config-route-map)') == false) then
        return false
    end
    if (c:send('end') == false) then
        return false
    end
    if (c:expect('#') == false) then
        return false
    end
end

```

Wildcards

Table 3.3. Wildcard List

Variables	Description
%username%	User field from the device configuration form.
%passwd%	User password field from the device configuration form.
%enable_passwd%	Enable secret field from the device configuration form.
%blackhole_ipaddr%	IP address to be announced in Blackhole.
%blackhole_ipaddr_mask_N%	Network block of the IP address to be announced in Blackhole with the netmask N applied to it.

Blackhole

This feature allows you to use scripts to announce IP addresses in blackhole and to remove them from this list of suspect IP addresses.

Table 3.4. Blackhole form

Field	Description
Execution type	Select Manual to announce an specific IP address in blackhole manually through the Threat Analysis Report or Automatic to have the IP addresses automatically announced in blackhole by the system.
Script	Enter the script that will announce the IP address in blackhole list.
Removal script	Enter the script that will remove the IP address from blackhole list.
Device	Select the desired device.

Chapter 4. ALARMmanager

Reports

To access ALARMmanager reports, go to **ALARMmanager** → **Reports**

Suppressed reports

This report provides the logs for all the suppression operations performed by the users.

Table 4.1. Suppressed alarms report form

Field	Description
Output format	Select HTML, PDF or CSV format.
Object type	The object type for the alarms.
Start time	The start time for the report.
End time	The end time for the report.
Operation	Filter for the suppression operation.
User filter	Filter for the user that performed the operation.
Object filter	Filter for the object in which the operation was performed.
Alarm filter	Filter for the alarm in which the operation was performed.

Consolidated reports

This report provides a view of all alarm events in a detailed or resumed way.

This report can be saved as a template. For instruction on working with report templates, go to templates section on this manual.

Table 4.2. Consolidated alarm report form

Field	Description
Alarm filter	Use Regular Expressions and click the filter button to select the desired alarms.
Object filter	Use Regular Expressions to filter the desired objects.
Manufacturer	Filter by the manufacturer of the object. You have to use Regular Expressions to filter.
Manufacturer Type	Filter by manufacturer type of the object. You have to use Regular Expressions to filter.
Object type	Type of the object.
ifAlias filter	Filter based on interface ifAlias OID. You have to use Regular Expressions to filter.
Start time	The start of the analysis period.

Field	Description
End time	The end of the analysis period.
Period	If All day option is marked, this field is ignored, otherwise the data is selected within that range for each day.
Exclude weekends	Exclude weekend periods from the report data.
Active only	To display only active alarms.
Consolidated	This option will summarize all occurrences of an alarm for each object.
Generated by trap only	Shows only alarms generated by link down traps.
Output format	Select HTML, PDF or CSV format.
Groups	This field can be used to filter objects associated to some root groups.

Tip

To sort report results, click at each column header.

Email Template

Introduction

You can select the ALARMmanager email format and choose if you want to use the default template or to personalize it.

Table 4.3. Email template

Field	Description
Enable default email template	Select No to customize the email template.
Email content	You can choose the email format you will receive (HTML or Txt).

Customizing the email

When you are editing your email template, it's possible restore the default one just by clicking the **Restore default template** button.

If the email content is in the HTML format, you can visualize the preview before save the new template. To do this, click on the **Preview** button.

You will have the following keywords enclosed by '\$' and you may substitute them for your alarm configuration:

Table 4.4. Email variables

Variables	Description
\$date\$	Alarm start/end time.
\$objtype\$	Object type: Mapped object or Device. Service alarm does not have any type of object.

Variables	Description
\$object\$	Object name.
\$path\$	Shows the path for the object in the SLAview groups.
\$alarm\$	Alarm name.
\$action\$	Alarm state: active or inactive.
\$level\$	Alarm urgency level.
\$formula\$	Alarm formula.
\$varbind\$	Varbind.
\$suppressed\$	Indicates if alarm is suppressed.
\$color\$	Variable to be used in HTML email. Green to disabled and red to enabled.

Alarm urgency level

The urgency levels in the ALARMmanager application are customizable and you can configure as many as you want.

To manage the alarm levels access **ALARMmanager** → **Alarm urgency level** menu.

Here you have a list of pre-configured levels. You can edit levels or add new ones.

Changing the urgency level priority

To change an urgency level priority, select the desired level and click the UP or DOWN arrows located on the upper left corner.

Adding a new urgency level

To add a new urgency level, click the New and fill the form.

Table 4.5. ALARM urgency level form

Field	Description
Label	A label for the urgency level. This label is displayed on a column at the ALARMmanager console.
Background color	Background color that will be displayed in the ALARMmanager console.
Text color	Text color that will be displayed in the ALARMmanager console.
Beep	Enable sound warning for this alarm. The sound warning will be played by the ALARMmanager console if this function is also enabled at the console. To enable it, access ALARMmanager → Console → Enable sound warning
Alarms	Select the alarms that will receive this priority.

Field	Description
Service alarms	Select the service alarms that will receive this priority.

Add alarm urgency level metadata

To access the metadata configuration page, access **ALARMmanager** → **Alarm urgency level** and click on **Metadata** button.

Click on **New** button to create a new metadata.

You can change the metadata configuration using the **Edit** button. To check the configuration history, click on **History** button.

To remove a metadata, click on **Delete** button.

Table 4.6. Metadata fields

Field	Description
Name	Enter the metadata name.
Description	Describe the metadata (optional).
Datatype	Choose the metadata type: Text , Integer or Enum (Enumerate).
Values	This field is only available when the Datatype is Enum . Enter a list of values, separating them by semicolon (;).

To associate the metadata to an alarm urgency level, access the urgency levels list and click on **Metadata** button beside the level that will be configured.

Then, fill the metadata according to its type.

Alarms

TRAFwatcher already has 8 pre-configured **Possible threat** alarms: **DNS Amplification threshold reached**, **ICMP Flood threshold reached**, **IP Flood threshold reached**, **NTP Amplification threshold reached**, **Port 0 threshold reached**, **SNMP Amplification threshold reached**, **Syn Flood threshold reached** and **Traffic threshold reached**.

You can not remove these alarms, but you are able to edit their fields.

Table 4.7. TRAFwatcher alarm form

Field	Description
Name	Alarm name.
Alarm type	Select the alarm type.
Varbind	A free text field that can be used to recognize the alarms that are forwarded as traps.
Mail	Email will be sent to users. The SMTP server should be configured and also each user email at the user configuration form.

Field	Description
Mobile(SMS)	Shorter messages than the ones sent for emails will be sent. This alarm can be sent to an email to SMS gateway if the user SMS field is configured in the following format: 88888888@operator.com. If the SMS is a phone number, the SMPP or http protocol can also be used to send the message. To do that, you need to configure the following item: System → Parameters → SMS server .
Mobile(Telegram)	A message will be sent to a Telegram chat by a bot. To configure this feature, you must create a bot in Telegram, to do it, once you are on Telegram, start a conversation with the user @BotFather. Choose the option /newbot and follow the instructions to finish the bot creation. At the end write down the telegram bot token. Associate the bot to a chat where the messages will be sent. Access the user profile form, fill the "Telegram bot token" field and click Validate. If everything goes fine, the "Telegram chat ID" field will be automatically filled.
Trap	A trap will be sent for each alarm.
Mail delay	The email will be sent after the number of minutes defined in this field, starting from the activation time.
Mobile delay	The message will be sent after the number of minutes defined in this field, starting from the activation time.
Trap delay	The trap will be sent after the number of minutes defined in this field, starting from the activation time.
Disable mail for suppressed alarms	If the option "No" is selected, the email will be sent and the suppressed condition will be indicated in the email. The "Yes" option will prevent the email from being sent.
Disable mobile for suppressed alarms	If the option "No" is selected, the mobile messages will be sent and the suppressed condition will be indicated in the mobile. The "Yes" option will prevent the mobile messages from being sent.
Disable trap for suppressed alarms	If the option "No" is selected, the trap will be sent and the suppressed condition will be indicated in the trap. The "Yes" option will prevent the trap from being sent.
Urgency level	Select a level for the alarm.
Alarm profile	Select the alarm profiles this alarm should belong to.

Add alarms metadata

To access the metadata configuration page, access **Alarms** → **Alarms** and click on **Metadata** button.

Click on **New** button to create a new metadata.

You can change the metadata configuration using the **Edit** button. To check the configuration history, click on **History** button.

To remove a metadata, click on **Delete** button.

Table 4.8. Metadata fields

Field	Description
Name	Enter the metadata name.
Description	Describe the metadata (optional).
Datatype	Choose the metadata type: Text , Integer or Enum (Enumerate).
Values	This field is only available when the Datatype is Enum . Enter a list of values, separating them by semicolon (;).

To associate the metadata to an alarm, access the alarms list and click on **Metadata** button beside the alarm that will be configured.

Then, fill the metadata according to its type.

Alarm profiles

Profiles are used to tie together alarms and monitored objects.

To configure an alarm profile, select **Alarms** → **Alarm profile**, click the **New** button and fill out the form.

Table 4.9. Alarm profile form

Field	Description
Name	Define a name for the alarm profile.
Alarm	Select the desired alarms for this profile.
Subnet	Select the desired subnets for this profile.

Add alarm profile metadata

To access the metadata configuration page, access **Alarms** → **Alarm profile** and click on **Metadata** button.

Click on **New** button to create a new metadata.

You can change the metadata configuration using the **Edit** button. To check the configuration history, click on **History** button.

To remove a metadata, click on **Delete** button.

Table 4.10. Metadata fields

Field	Description
Name	Enter the metadata name.

Field	Description
Description	Describe the metadata (optional).
Datatype	Choose the metadata type: Text , Integer or Enum (Enumerate).
Values	This field is only available when the Datatype is Enum . Enter a list of values, separating them by semicolon (;).

To associate the metadata to an alarm profile, access the profiles list and click on **Metadata** button beside the alarm profile that will be configured.

Then, fill the metadata according to its type.

Console

Introduction

The ALARMmanager application works integrated to the systems and is capable of generating alarms based on formulas.

It also has the following features:

- HTML5 graphical interface.
- Alarm forwarding through email, mobile and traps.
- Alarms can trigger sounds.
- Alarm profiles to ease alarm association to managed objects.
- Alarm acknowledgment and comments.
- Alarm suppression to avoid emails, mobile messages and traps for repeated alarms.

Console operation

To access the operational alarm console, go to **ALARMmanager** → **Console**.

Authentication

A user must be authenticated to access ALARMmanager.

Console

The ALARMmanager console will display all the alarms that are active and also the inactive alarms that have not yet been inactive for the ALARMmanager storage period parameter. You will be able to visualize only the alarms that you have permissions to see and for the objects that you are allowed to visualize.

The console has the following columns:

Table 4.11. ALARMmanager console

Column	Description
START TIME	The time of the first occurrence.

Column	Description
END TIME	The time of the last occurrence. Displays ACTIVE if the alarm has not ended.
USER	User that acknowledged the alarm.
TYPE	Object type, can be device of mapped object.
OBJECT	Object name.
DESCRIPTION	If the object is an interface, displays its ifAlias.
PATH	Shows the first path for the object in the SLAview groups.
STATE	Alarm state, can be active or inactive.
ALARM	Alarm name.
LEVEL	The level for the alarm defined at the level configuration.
TRAP	Yes if it was generated by a trap and no otherwise.
COMMENTS	Comments by the operator. To insert a comment, click two times in that cell.

Alarm Acknowledgement

Once an alarm is acknowledged, the alarm line shows the username that performed the operation and this information can also be viewed at the consolidated alarm report. After acknowledging an alarm, you are able to insert comments for the alarm.

To acknowledge an alarm, right click the alarm to be acknowledged and then select the Acknowledge option on the menu. The alarm is then displayed at the acknowledged tab for all operators.

To acknowledge multiple alarms at once, select them with the left mouse button and then right click on the list to display the menu.

The alarm can be released from the operator only by an administrator user. To do it, the administrator should select the acknowledged alarm at the list and select the Unacknowledge alarm option from the menu.

Alarm Suppression

To suppress an alarm, follow the procedure below:

1. Select the desired alarms with the left mouse button. To choose more than one alarm, hold CTRL key and select the alarms with left mouse button.
2. Click with the right mouse button to show the popup menu. Click on Suppress alarms option on the popup menu.
3. Fill the suppression reason text box. You can also leave it blank.
4. Click on Confirm button.

You can check the logs for the suppression operations performed by the users at the suppressed alarms report

Alarm Comments

To insert comments for an alarm you first need to acknowledge it.

To insert a comment, follow the procedure below:

1. Click the Acknowledged alarm tab
2. Double click at the COMMENTS column for the alarm.
3. Fill the text box at the Alarm Comments window and click the Confirm button.

Enabling sound for an alarm

The sound alarm will function if there is an active, not acknowledged, critical or major alarm in the ALARMmanager console.

Select **ALARMmanager** → **Console** → **Enable sound warning** option.

Alarm synchronization

The ALARMmanager applet synchronizes its alarms with the system database every 2 minutes. This synchronization can be triggered immediately at **ALARMmanager** → **Console** → **Synchronize Alarms** menu.

Deleting alarms

ALARMmanager deletes automatically the alarms that have finished, but you will be able to visualize then at the console until the maximum inactive alarm storage time has passed. To configure that parameter go to **System** → **Parameters** → **ALARMmanager** menu.

The operator can delete the alarms at any time if they are in the inactive state by selecting the alarms with the right mouse button and clicking the Delete option on the menu.

Opening graphs

Select an alarm line and click the Open graphs button to open the objects graphs.

Alarm filter

This filter can be triggered from any object at any map. It will filter the object's alarms and also from the objects related to it hierarchically.

Tip

The urgency levels are displayed at the bottom of the page. When you click on one of them, it will filter all the alarms in this level. By clicking on it again, the filter is removed.

Chapter 5. System

Access Log

User access

This option displays a report summarized by day containing user access logs. Each report line is a link for a detailed report for the day.

Simultaneous access

This report displays the number of user logged in the system for each user group.

Users

The system has three user types:

User types

Administrator	Has full access to the system
Configurator	Can create, remove and edit any system objects. Cannot make changes to System configurations.
Operator	Can only visualize system monitored objects and reports.

When you associate groups to users, you will restrict this user visualization to objects within the group hierarchy.

Users can also be limited on the menus that they will access and on the number of simultaneous users that will access the system.

Editing users

1. Select **System** → **Users** → **User list** .
2. Click the New or Edit buttons and fill the form below:

Table 5.1. User form

Field	Description
Username	User login.
Name	User name.
Password	Password.
Password check	Repeat the password.
E-mail	E-mail to send alarms and when a scheduled report is available. You must configure the SMTP server .
SMS	Celular phone number to send alarms using the SMPP protocol or celular@teste.com to send

Field	Description
	short emails with alarms. The system can also send SMSs through the integration with a web portal.
Use compact graph	Visualize graphs in a default size or compact them.
Use group summarization	Enables the visualization of Group summarization for the user.
Local authentication	This field is visible only when Active Directory or TACACS is enabled. To configure the Active Directory, access System → Parameters → Active Directory and to configure the TACACS, access System → Parameters → TACACS .
Theme	Set user theme. Choose the Default Theme in System → Parameters → Theme
User group	Associate this user to a user group in order to restrict the number of simultaneous accesses to the system within the group.
Language	Set user language.
Profile	Set user profile to restrict alarm and service alarm visualization and notification.
Type	Choose the user type.
Menu	Use the Customize option to restrict the user to specific menus.
Subnets	Select the subnets the user will be able to access.

Disabling users

It is possible to disable an existing user, so it becomes inactive. An inactive user cannot log in again and will cease to receive any alerts from the system. To disable a user, use the **Disable** button beside the desired user.

User Groups

The user groups are used to manage how many users can login simultaneously to the system.

Procedure 5.1. Managing user groups

1. Select **System** → **Users** → **User group** .
2. Click the New or Edit buttons and fill the form below:

Table 5.2. User form

Field	Description
Name	User group name.
Description	User group description.

Field	Description
Limit simultaneous access	Select a number between 1 and 255. This will limit simultaneous access to the system within the users of this group.
Users	Specify the users that will be placed in the group. A user can belong to one group only.

User profiles

The user profiles are used to associate alarms to users.

Procedure 5.2. Managing user profiles

1. Select **System** → **Users** → **User profiles** .
2. Click the New or Edit buttons and fill the form below:

Table 5.3. User form

Field	Description
Name	User profile name.
Telegram bot token	Token obtained after creating a new bot in Telegram.
Telegram chat ID	Chat ID of the chat which the bot partakes.
Users	Associate users to this profile.
Profile -> Alarms	Associate pair of Profile -> Alarm to this profile.
Service alarms	Associate service alarms to this profile.

Alarm Console

You can select the columns that will be shown at ALARMmanager console. Furthermore, you are able to configure the order the columns will appear. For this purpose, click and drag the lines.

Table 5.4. ALARMmanager console columns

Column	Description
START TIME	The time of the first occurrence.
END TIME	The time of the last occurrence. Displays ACTIVE if the alarm has not ended.
USER	User that acknowledged the alarm.
TYPE	Object type, can be device of mapped object.
OBJECT	Object name.
DESCRIPTION	Object description.
IFALIAS	If the object is an interface, displays its ifAlias.
STATE	Alarm state, can be active or inactive.
ALARM	Alarm name.

Column	Description
LEVEL	The level for the alarm defined at the level configuration.
TRAP	Yes if it was generated by a trap and no otherwise.
COMMENTS	Comments by the operator. To insert a comment, click two times in that cell.
PATH	Shows the first path for the object in the SLAview groups.

Backup/Restore

You can perform backup and restore of all system data to and from an ftp server or a simple file download/upload with all system configurations.

Go to **System** → **Backup/Restore** to work with the following backup/restore options:

Local configuration backup

Click on this icon to display all current configuration backup files.

You can create a new file by clicking the Create new button.

The Setup button is used to set the number of backup files to keep.

Click the Download button to download the configuration file to your desktop.

The Copy to restore button is used to copy a configuration file to the restore area in order to restore this backup file.

Local configuration restore

This option is to be used to restore a backup file. By doing that, all current system configuration will be replaced by the definitions contained in the restored file.

To perform a system restore, you should either upload a configuration file from your local machine or copy an old backup file available in the system and then click the Restore button for that file.

Remote backup

This option can be used to save the system configuration files and historical database to a remote backup server. Select the type of protocol you want to use for the remote backup. The available options are **FTP** and **S3** protocols.

Table 5.5. FTP server form

Field	Description
IP version	Select IPv4 or IPv6.
Backup Server	IP address of the backup server.

Field	Description
Backup Directory	Directory on the backup server.
User	User to authenticate on the backup server.
User Password	Password.
Backup protocol	Protocol to be used for backups.
Protocol port number	Port number.
Server size (GB)	The server size in Gigabytes.
Activate backup	Select Yes to activate the backup feature.
Backup start time	Enter the time of the day to execute backups.

Table 5.6. S3 server form

Field	Description
IP version	Select IPv4 or IPv6.
Backup Server	IP address of the backup server.
Server size (GB)	The server size in Gigabytes.
Backup Server	IP address of the backup server.
Activate backup	Select Yes to activate the backup feature.
Backup start time	Enter the time of the day to execute backups.
Access key	User Access key.
Secret key	User Secret key.
Bucket name	Bucket name where backups will be stored.
Host base	S3 server URL.
Host bucket	Virtual-hosted.style URL.

Remote restore

Select a single system to perform data restore or click the Request complete restore to fetch data from both systems.

Important

- The ftp server must be online, since the data will be fetched from it.
- Only perform this operation on a new and empty TRAFip or SLAview installation, since all system data will be replaced.

Restore status

This option will display the restore status once you request a remote restore operation.

Parameters

This section is used to configure various system parameters that are used for different processes.

Active directory

This option will enable users to access TRAFip using the Active Directory Kerberos authentication method.

In order for a user to authenticate using this method, it must be configured in the system.

Table 5.7. Active directory form

Field	Description
Enable Active Directory authentication	Once Yes is selected, the Local authentication field will be available in the user form.
Server	Enter the server address. Example: kerberos.example.com
Domain	Enter the Active Directory domain. Example: ATHENAS.MIT.EDU

When this method is enabled, there isn't local authentication, it means **Operator** and **Configurator** users can only log in TRAFip using Active Directory.

Important

The **Administrator** user can choose to log locally or not, however, it's recommended to always have a **administrator** user with **Local authentication** enabled, when there is a external access control.

ALARMmanager

Table 5.8. ALARMmanager parameters form

Field	Description
Maximum events storage period	Number of hours that the occurrence table will hold occurrences. This table is used only for deep level debugging purposes, since the occurrences are not used after they are processed.
Maximum alarms storage period	After this period, the alarms will be deleted.
Maximum inactive alarms storage period	Once an alarm becomes inactive, it will be available at the ALARMmanager console for this period. After that, the alarm can be visualized at the ALARMmanager reports.

Alarm occurrences or events are generated by the following processes:

- SlaSumCaching: generates occurrences for all configurable alarms created with summarization variables.
- ICMPAgent: generates occurrences for the **Not replying ICMP** alarm.
- MIBget: generates occurrences for the **Not replying SNMP** alarm.
- ObjectMapper: generates occurrences for the **Object not found** alarm.

Caution

You can check the **Configurations** item under the **System** → **Diagnostics** → **Storage usage** section to check if the database is too big, indicating that the system is generating too many

alarms. If that is the case, you can decrease the alarm storage period or adjust the alarm settings to generate less alarms.

Association agents

Set two moments within the day to execute the automatic association for each agent type.

Table 5.9. Automatic association agent form

Field	Description
First execution time	Set the first execution time.
Second execution time	Set the second execution time.

Auto login

This feature enables the authentication bypass for URL requests coming from another system.

To enable this feature, follow the procedure below:

1. Go to **System** → **Parameters** → **Auto login**.
2. Select "Yes" on **Enable auto login** option.
3. Fill the referer URL in the format, which is the page from which the requests will be originated.
4. On your web server, fill the following URL: **http://<IP>/cgi-bin/login?dip=<USER>**.

Backup

- Data: Parameters to perform remote backup. Refer to remote backup section.
- Configuration: configure the number of old configuration backup files to keep in the system.

BGP

Advertise or withdraw routes from your routing tables.

Table 5.10. BGP form

Field	Description
Enable BGP	Select this option if you want to advertise or withdraw a route.
BGP identifier	Integer value that uniquely identifies the sender.
Local AS Number	Sender AS number
Peer AS number	Receiver AS number.
Peer ip	IP of the receiving router.
BGP Community	Set of generic tags that can be used to flag various administrative policies between BGP routers.

Capture agent configuration

Set the allowed number of simultaneous executing agents.

Table 5.11. Capture agent configuration form

Field	Description
Number of simultaneous executing agents	Choose a integer smaller than or equal to 10. The default is 3 .

Circuit

Set the Metadata to create the folder.

The circuits will be grouped according to the chosen metadata.

Table 5.12. Circuit form

Field	Description
Circuit name generation mode	Select Automatic to generate the circuit name automatically.
Script	This field is only available when the Circuit name generation mode is Automatic . Select the script. Create one in Scripts section.
Metadata for grouping	Select the metadata name.

Cisco WAAS

Cisco WAAS (Wide Area Application Services) is a Cisco Systems technology. It improves the performance of applications on a wide area network (WAN).

Table 5.13. Cisco WAAS form

Field	Description
Enable Cisco WAAS monitoring	Select Yes to enable the Cisco WAAS (Wide Area Application Services) monitoring, select No otherwise.

Configuration history

Set the storage period for different configuration areas.

Table 5.14. Log history parameters

Field	Description
Maximum configuration data storage period	This includes all configuration changes, except for the user related operations. This data can be displayed at System → Diagnostics → Configuration Logs .

Field	Description
Maximum user configuration data storage period	This is specific for user operations. This data can be displayed at System → Diagnostics → Configuration Logs by selecting the User option on Object type field.
Maximum summarization statistics storage period	This is related only to the summarization processes. This statistic can be checked at System → Diagnostics → Summarizer .

Data storage

In this area, you should configure the storage space that should be allocated for each type of system data.

The field **Available distribution space** will display the space that can still be distributed.

To check how much space each area is consuming, you should login to the desired system (TRAFip or SLAview) and access **System** → **Diagnostics** → **Storage Usage** . The TDB database item corresponds to the summarized data for each system.

You can perform redistribution of storage space between different areas at any time.

Table 5.15. Data storage form

Field	Description
Start process from occupation at %	When this value is reached, the agent will be executed. Fill with a value between 1 and 85 .
Execution type	Choose if the agent will run at each Time interval or in a Time schedule .
Execution time interval (minutes)	Define the time interval, in minutes, to the agent be executed. The minimum value is 10 .
Scheduled report time	Define the time when the agent execution will start.
SYSLOG storage	Storage dedicated to SYSLOG raw files.
Scheduled reports	Storage dedicated to scheduled report files.
Trap receiver storage	Storage dedicated to trap receiver files.
Capture files storage	Storage dedicated to capture files.
Clean historical data	Enables deletion of old historical data.
Clean alarms	Enables deletion of old alarm history.
TRAFip raw data storage	Storage area dedicated to TRAFip raw flow files. This storage usually grows a lot faster than the summarized data. If you configure it with the same size of the summarized data, you will typically end up with 10 times less historical data.
TRAFip summarized data storage	Storage dedicated to TRAFip processed data or TDB - Telco Database. This data is used for graphs and Top N reports.

Field	Description
TRAFip summarization remote files	Storage dedicated to TRAFip processed data files sent from collectors on distributed architecture environment.
TRAFip behavior change data	Storage dedicated to TRAFip behavior change files, for instance, history alarms data.
SLAview raw data storage	Storage dedicated to SLAview raw files. This is in general the collected SNMP OIDs.
SLAview summarized data storage	Storage dedicated to SLAview processed data. This data is used for graphs and reports.
SLAview summarization remote files	Storage dedicated to SLAview processed data files sent from collectors on distributed architecture environment.
SLAview behavior change data	Storage dedicated to SLAview behavior change files, for instance, history alarms data.
CFGtool versions data	Storage dedicated to device configuration files. Even when this value is reached, the version data of devices with just one version will not be excluded.

When the fields **Raw data (MB)** and **Summarized data (MB)** are filled with '0' (zero), it means the system is distributing automatically the **Available distribution space** between the **TRAFip raw data storage**, **SLAview raw data storage**, **TRAFip summarized data storage** and **SLAview summarized data storage**.

You are able to set manually these values, but don't forget the raw data storage usually grows a lot faster than the summarized data. To redistribute the storages, divide the **Available distribution space** by four and you will have each storage size value.

Caution

If you reduce the storage space of any of these areas, the next time the garbage collector process runs, it will clear the data to adequate the storage space.

dbn0/Altaia integration

Altaia is a performance and QoS management platform. Fill the fields in the form and configure the dbn0/Altaia integration.

Table 5.16. dbn0/Altaia integration form

Field	Description
Enable dbn0/Altaia integration	Choose Yes or No .
Server IP Address	Enter the server IP address.
Directory to send the file	Enter the directory.
Server user	Enter the server.
User Password	Enter the user password.
5 minutes steps	Enter a number.
5 minutes delay	Enter a integer equal to or greater than 2.

Distributed architecture

These parameters should be used if you wish to run the system on distributed architecture mode.

For more details about distributed architecture's concepts and prerequisites, refer on distributed architecture feature section.

Table 5.17. Distributed architecture parameters form

Field	Description
Maximum number of consecutive collector fails	This number represents how many times the central node will wait for the processed files from a collector node until this node is considered down. This check is performed every 5 minutes by the sum-control processes for TRAFip and SLAview systems. After a collector is set to down by the central node, the backup collector, if set, will take on the faulty collector operations.
Enable Distributed Architecture	Select this option if this appliance will be part of a distributed architecture system.
Is collector?	Mark Yes at this option if this appliance will take a collector role on the system. Otherwise this appliance will be considered a central node.
Collector key	Fill with a string to identify this collector on the central node.
IP version	Select IPv4 or IPv6.
Central Storage IP	Fill with the IP address of the appliance to be used as a central node.
Password	Password used for authentication.

EPM

EPM (Extended Processing Module) is another appliance in addition to the already installed one in the client. It is an extended module of the monitoring solution.

Table 5.18. EPM form

Field	Description
Enable EPM	Select this option if you deserve to enable this module of the monitoring solution.
Is EPM?	Mark Yes at this option if this appliance will be used as EPM.

Important

By changing this setting you'll lost all your historical data, so be careful!

Expiration warning

Set when you will be informed about the license expiration date.

Table 5.19. Expiration warning form

Field	Description
Warn expiration lasting	Define the number of days between 10 and 30.

Grapher

Adjust the grapher parameters.

Table 5.20. Grapher parameters form

Field	Description
Enable Derivative Graph as Default	On standard mode, graphs points are connected using linear interpolation. On derivative mode, the piecewise interpolation is used.
Enable auto-refresh	Select this option to have all graphs automatically refreshed. You can also enable this option at runtime for each graph.
Exclude weekends	Enabling this option, the weekend days will be shown in brighter colours on the graphs.
Auto-refresh interval	Interval between refreshes.
Business hours	This option enables modifications in the graphs according the business hours period defined at Local preferences. Choose between No action , Highlight business hours or Show business hours only .

HTTPS Configuration

Configure the HTTPS (HyperText Transfer Protocol Secure) mode.

Table 5.21. Https parameters form

Field	Description
Enable https	Choose Yes and the server will restart in https mode.
Certified	Select the https certified. The file must have the .pem extension and must be signed by a CA (Certification Authority) to be valid.

Local preferences

Table 5.22. Local preferences form

Field	Description
PDF page size	Page size to be used for PDF reports.
Search limit	Fill with a positive integer to limit your researches. The default number is 2500 .
Business hours first period	Set the start time and the end time for the business hours first period.

Field	Description
Business hours second period	Set the start time and the end time for the business hours second period.

Login redirection

Fill the **Destination page after login** field to be redirected to another system after login. On the redirected system, you will be able to access all TRAFip/SLAview objects without authentication.

Log level

Choose the ALARMDaemon level: **Low**, **Medium** or **High**.

This level will determine the amount of details in alarm log.

Logo

Pick an image file from your Desktop and upload it, so the image will be displayed at the top right corner.

Remember the image must be of fixed height of 43 pixels and variable width from 20 to 200 pixels.

Redundancy

This section is used to specify the redundancy setting.

Activation

Table 5.23. Redundancy activation settings

Field	Description
Enable redundancy	Choose Yes.
Local IP Synchronization	Fill with the IP address configured for the interface directly connected to the other appliance.
Remote IP synchronization	Fill with the IP address configured for the remote appliance.
Max history size	Configure the max history size in MB. The minimal historic size is 16MB.
Preferred state	Select Master or Slave .

Refer to redundancy section for details on enabling this feature.

Commutation

Table 5.24. Redundancy Commutation settings

Field	Description
Commutation interfaces	Add the interfaces that will share IP addresses between the two appliances. Use the Add button to add multiple interfaces. At least one interface

Field	Description
	must be reserved to have an exclusive IP address for management purposes. One interface must be used for the back-to-back connection and the others can be used to share IPs.

Regional settings

Table 5.25. Regional settings form

Field	Description
Decimal separator	Decimal separator to be used for system reports.
System Language	Choose the default system language. Each user can define its own language settings under user configuration.
Number of decimals in export files	Configuration used to format number fields on exported reports.
Csv file separator	Separator to CSV reports.

Reports

This section shows how to make advanced configurations for reports.

Scheduled Reports

You have the option to schedule your reports. In this section, configure this mode.

Table 5.26. Scheduled reports configuration form

Field	Description
Refresh time of the wait page (seconds)	Enter a integer number.
Max Time of Execution (minutes)	Enter a integer number.
Max Simultaneous Processes	Enter a integer number.
Email subject prefix	Define the default email subject prefix.
Hostname for link in email	Configure the email hostname.

You can also send scheduled reports to FTP server. Fill the following form to register this server:

Table 5.27. FTP Server configuration form

Field	Description
Server	IP address of the FTP server.
Directory	FTP server directory.
User	User to authenticate on the FTP server.
Password	TCP port to connect to the FTP serve.
Port	TCP Port to connect to the FTP serve.

Field	Description
Storage limit (MB)	Set the maximum size that can be occupied by reports.

To send report to the FTP server, access the template that you want send and select the **Schedule template** option followed by choose **yes** in the **Send report to FTP server field**.

SMS server

SMPP(Short message peer-to-peer protocol) method

Use this method if your mobile operator provides a SMPP account.

Table 5.28. SMPP server form

Field	Description
SMS Protocol	Choose the SMPP option.
Host	SMPP host.
Port	SMPP port.
System ID	SMPP system ID.
System Type	SMPP system type.
Password	SMPP password.
URL	Refer to URL section.
Origin phone number	phone number that will be displayed as the caller on SMS messages.

SMSs can be sent using two distinct methods. Both configured through this form.

URL(Uniform Resource Locator) method

This method should be used if you have a http gateway.

SLAview will perform an http GET operation using the provided URL.

You should use the \$CELLPHONE\$ and \$MSG\$ wildcards in the URL.

The \$CELLPHONE\$ wildcard will be replaced by the SMS field that you filled in the user configuration form.

The \$MSG\$ wildcard will be replaced by the alarm message, which contains the following information:

- Alarm name.
- Alarm urgency level.
- Alarm state.
- Date and time that the alarm switched to that state.
- Alarm varbind.

SMTP

Fill this form with the SMTP parameters to send emails.

Table 5.29. SMTP parameters form

Field	Description
SMTP Server	Configure the SMTP Server. The port used by the SMTP server can be changed in this field. Follow the example: smtp.server.com:port
SMTP user	Enter the email.
SMTP password	Enter the user password. If the SMTP server does not require authentication this field should be left blank.
SMTP from	Set a sender for the email.

You can verify SMTP configuration before saving: click on **SMTP test** and enter the email address for test.

SNMP

SNMP Collector

These parameters will be used for all processes that perform SNMP polling. These are the default configurations, but they can be fine tuned at the device level.

For a reference of all system processes, go to the log files section.

SNMP parameters

SNMP Timeout	Time limit in seconds that the collector will wait for a SNMP reply packet. Value range: 1-10.
SNMP Retries	Number of retries that will be issued to the device if it does not respond to a SNMP query. Value range: 1-10.
Number of OIDs per packet	Number of OIDs the collector will send in each SNMP packet. Value range: 1-100.
Maximum packet rate (pps)	Maximum number of packets per second that a SNMP collector will send for each device.
Maximum global packet rate (pps)	Global limit for the number of packets sent per second. Considers all registered devices. Fill 0 for no limit.
SNMP window	Number of SNMP packets that will be sent without answer from the device being polled.
SNMP port	Default TCP port to connect to the SNMP agent
Ignore interfaces	Fill the expression to ignore these interfaces.
High counter interfaces	Fill the expression to use the high counter OIDs (ifHCInOctets and ifHCOutOctets) on these interfaces.

SecRate Interfaces

Fill the expression to use the sec rate OIDs (IfHCIn1SecRate and IfHCOut1SecRate) on these interfaces.

SNMP Trap

Fill the fields below to specify the hosts that will receive traps. This traps can be alarms from ALARMmanager or self generated traps from TELCOMANAGER MIBS.

Table 5.30. TRAP fields

Field	Description
Trap forwarding hosts	IP addresses of the hosts. Ex: 10.0.0.1,10.0.0.2.
Trap Communities	SNMP communities of the trap hosts.

System Version Check

Every day between 2 a.m. and 3 a.m., the system version check verifies if there is a new available build version. Once this is true, the user will be informed.

TACACS

Enables TACACS+ authentication method. Two servers can be configured for redundancy.

The username and password for each user should be configured in the system exactly like the TACACS (Terminal Access Controller Access-Control System) server.

When this method is enabled, there isn't local authentication, it means **Operator** and **Configurator** users can only log in using TACACS.

Important

The **Administrator** user can choose to log locally or not, however, it's recommended to always have a **administrator** user with **Local authentication** enabled, when there is a external access control.

Telcomanager Host Agent

Fill this form with IP address and port of Telcomanager Host Agent server. This address will be used to collect information from all devices configured to use THA Gateway mode. By default, THA uses port 8888.

Important

In order to collect information remotely on Active Directory (AD), the following services must be running on the remote machines:

- Remote Procedure Call (RPC)
- Remote Registry

Telcomanager JMX Agent

Fill this form with IP address and port of Telcomanager JMX Agent server. This address will be used to collect information from all devices configured to collect JMX statistics.

Theme

In this section, you can set the Default system theme.

Table 5.31. Theme configuration

Field	Description
Default theme	Choose the default system theme: Dark, Green & Yellow, Red & white or Telcomanager .

Tip

Notice that each user can define his own theme in user configuration.

Threat Analysis

In this section, you will configure if you desire to use TRAFip to detect suspect traffic or to use the threat analysis module, TRAFwatcher.

Table 5.32. Threat analysis configuration

Field	Description
Time window to discard flows (sec)	It is the time limit, in seconds, to accumulate traffic. It means this limit defines when the analysis will occur. In the case, only it will be considered the data with the time difference between the first and last one within this limit.
Minimum percentage for traffic characterization	When in distributed architecture, the traffic can be characterized as suspect on collectors when only a percentage of the total thresholds is reached. Define this minimum percentage using this field.
Tolerance for time difference between local system time and flow exporter time	Define the tolerance time, in seconds, to consider a flow is within the analysed period so it will not be discarded. The minimum value is 60 .
Maximum suspect traffic events storage period (days)	Set the maximum period, in days, to store the suspect traffic events.
Interval to run blackhole disable script (min)	Period, in minutes, in which an IP address will be in blackhole before a removal script disables it.
Maximum alarmed IPs allowed	Set a limit of alarmed IPs. When this value is exceeded, it means that the Threat Profile is badly configured for the subnet with a lot of alarmed IPs. So, a Warning is displayed next to the Logo. This parameter preserves the system performance.
Number of threats to show	Define the number of threats to be displayed on Control Panel.
Maximum blackhole IPs storage period (min)	Set the maximum period, in minutes, to store the blackhole IPs.

Important

It is necessary to enable the threat analysis in the desired subnet form.

User access history

There is a tool that offers a daily summarized report containing user access logs. For further information about it, refer to Access log section.

Configure this user access history storage period.

Table 5.33. User access history form

Field	Description
Maximum user access log storage period (months)	Enter a integer smaller than or equal to 36. The default is 12 , that is, 1 year.

Web Services

Configurations API

Table 5.34. Configurations API form

Field	Description
Hosts with access granted to the configurations API	Configure the hosts that are allowed to access the API configurations.
Username used by configurations API	Enter the username.

TRAFip's raw data

Configure the access to TRAFip's raw data.

Table 5.35. TRAFip's raw data form

Field	Description
IP used to access	Enter the IP.
Password	Enter the password.

Diagnostics

Network information

Displays system date and time, network interfaces information and default gateway.

Connectivity tests

Tests like ping, nslookup and traceroute to test the connectivity between the appliance and network elements.

Packet Capture

Using this tool, you can analyze the packets passing through the appliance interfaces.

Click **System** → **Diagnostics** → **Packet capture** .

Click on New button.

Table 5.36. Packet Capture

Column	Description
Network interface card	Choose the interface to analyze.
Maximum file size	Choose the maximum file size where the result of the analysis will be written.
Maximum number of packets	Fill the maximum number of packets to analyze. Fill 0 for no limit.
Port	Filter ports to analyze. Type * for every port or comma separated values.
Exclude Port	Exclude ports to analyze. Type * for every port or comma separated values.
Host	Choose one host to filter or select All for every host.

Click Send to start the capture and then Back to back to the list of capture files.

If you wish to stop the capture, click Stop. A Download button will show up and you can download the capture file.

Objects

Displays the number of objects and profiles configured.

Summarizer

This section displays the time that the summarizer process took to run for the last day.

When deploying the system in distributed architecture, the time to send the summarized files from all collectors is also displayed.

Important

The summarization process runs every five minutes, so the time to run the process should be below 5 minutes for good system performance.

Storage usage

Displays information about storage areas usage.

System registries	Logs from the operating system.
SLAview registries	SLAview logs.
TRAFip registries	TRAFip logs.
SLAview TDB database	Storage usage for the SLAview Telco database, which is used to hold SLAview summarized data.

TRAFip TDB database	Storage usage for the TRAFip Telco database, which is used to hold TRAFip summarized data.
TRAFip raw data	Storage used for the TRAFip raw data.
SLAview raw data	Storage used for the SLAview raw data.
Data details	raw data storage by day for the system you are currently logged in.

Log files

In this area, you can visualize the system log files. Below a list of available files.

LOG Files

createMark.log	Logs from to the version update process.
backupgen.log	Daily configuration backup process logs.
dbackupArchive.log	Logs from the remote backup process.
Gc*	Logs from the garbage collector process.

Configuration Logs

This option contains a form where you can display system configuration logs.

These logs are kept for a period defined at **System** → **Parameters** → **Configuration history** → **Maximum configuration data storage period** .

Timezone

This menu is used to set the correct timezone for the server. You can select one of the pre-defined time zones or to upload a new one.

This procedure is usually necessary if there are daylight savings date modifications.

Support

Open request

Click on **Open request** button to be redirected to Telcomanager's technical support webpage.

Important

You should have access to the Internet.

Check for system updates

Click on **Check for system updates** button to check if there are available patches or updates.

Important

You should have access to the Internet.

Remote support tunnel setup

This option can be used to establish a secure connection to the Telcomanager internet support servers.

Once the connection is established, you can contact the Telcomanager support team with the service code used.

Tip

If your service code does not work, try to enter a different value.

About

This section lists the currently installed version and the licensed options.

You can also check the number of existent devices, the historical data series and the limit bits/s or flow/s.

Chapter 6. License enabled features

Redundancy

The redundant solution enables you to deploy two **identical** appliances working on HOT-STANDBY mode.

Important

This functionality will only work if both appliances have the same version.

Tip

It's recommended that the appliances have the same hardware configuration. In case it's different, the system will display a warning.

Concepts

- When this feature is enabled, the system works with two identical machines in HOT-STANDBY performing data synchronization and watching each other states at all times.
- A communication protocol runs between the two servers and if a failure is detected in one of the servers, the other will act as the ACTIVE server - if it is not already - and the tmTSRedundancyStateChangeTrap trap will be sent. This trap is documented at TELCOMANAGER-TELCOSYSTEM-MIB mib.
- Both appliances share one IP address, that is used to send flows from the routers. This IP address is active only on the ACTIVE server and when they switch states, the MAC address of that interface will also migrate to the new ACTIVE server.

Enabling the redundancy

1. Using two identical Telcomanager appliances with the redundancy license option enabled, connect them back-to-back using the same interface at each appliance and configure a non-valid IP network between those interface using the CLI (command line interface) on each appliance.
2. At the CLI, configure the IP address that will be shared between the two servers only at the ACTIVE server.
3. Go to **System** → **Parameters** → **Redundancy** menu and fill the form on both appliances.
4. Wait around 20 minutes and verify the state of each server at **System** → **Diagnostics** → **Network information** .

Distributed architecture

Concepts

The distributed architecture should be used to scale in terms of the system capacity to collect ip flows and SNMP data and to process the raw data, since those tasks are delegated to collector appliances.

Prerequisites

- All machines involved must have SNMP access to all devices to be monitored.

- The ip flows should be exported to the collector appliances.
- There should be enough bandwidth to transfer the summarization files between collector appliances and the central appliance. Keep in mind that one collector requires around 64 Kbps of bandwidth to monitor 1000 interfaces with 10 summarization variables in each interface.
- TCP ports 22 and 3306 must be available between collector and central appliances. Port 22 is used to transfer files in the SSH protocol and 3306 is used to issue database queries from collector to central appliance.

Deployment

1. At the central appliance, go to **System** → **Parameters** → **Distributed architecture** and fill the form accordingly.
2. At the collector appliances, go to **System** → **Parameters** → **Distributed architecture** and fill the form accordingly.
3. At the central appliance, go to **Configuration** → **Collectors** and fill the form accordingly.
4. Wait around 20 minutes and go to **Configuration** → **Collectors** menu to check if the collectors are listed in the **ON** status.

Chapter 7. Glossary

Abbreviations

This section shows the abbreviations you will find in this manual.

Table 7.1. Abbreviations list

Abbreviation	Description
AD	Active Directory.
API	Application Programming Interface.
AS	Autonomous system.
ASN	Autonomous system number.
Avg	Average.
CDP	Cisco Discovery Protocol.
CLI	Command Line Interface.
CNT	It is an analysis type of traffic profile: Content.
CPU	Central Processing Unit.
DNS	Domain Name System.
DoS	Denial of service.
DST	It is an analysis type of traffic profile: Distribution.
Enum	Enumerate.
EPM	Expanded Processing Module. It is an extended module of SLAview.
FTP	File Transfer Protocol.
GB	Gigabyte.
GIS	Geographic Information System.
HTTP	Hypertext Transfer Protocol.
HTTPS	Hypertext Transfer Protocol Secure.
ICMP	Internet Control Message Protocol.
IETF	Internet Engineering Task Force.
IP	Internet Protocol.
IPFIX	IP Flow Information Export.
IPv4	Internet Protocol version 4. It uses 32-bit addresses.
IPv6	Internet Protocol version 6. It uses 128-bit addresses.
ISP	Internet Service Provider.
Kb	Kilobit.
KPI	Key Performance Indicator.
LAN	Local Area Network.
LLDP	Link Layer Discovery Protocol.

Abbreviation	Description
Max	Maximum.
Mb	Megabt.
MIB	Management Information Base.
Min	Minimum.
MPLS	Multi-Protocol Label Switching.
MTX	It is an analysis type of traffic profile: Matrix.
NaN	When a value is Not A Number.
NTP	Network Time Protocol.
OID	Object Identifier.
QoS	Quality of Service.
RFC	Request for Comments.
RFI	Repeated Flow Interface.
SMS	Short Message Service.
SMPP	Short Message Peer-to-Peer.
SMTP	Simple Mail Transfer Protocol.
SNMP	Simple Network Management Protocol.
SSH	Secure Shell.
TACACS	Terminal Access Controller Access-Control System.
TCP	Transmission Control Protocol.
TCS	Telcomanager Custom Script.
THA	Telcomanager Host Agent.
ToS	Type of Services.
TSA	Telcomanager Windows Security Agent.
UDP	User Datagram Protocol.
URL	Uniform Resource Locator.
WAAS	Wide Area Augmentation System.
WAN	Wide Area Network.