

SLAview Manual

SLAview Manual

Table of Contents

Preface	xii
Target audience	xii
Conventions used in this manual	xii
1. Introduction	1
About	1
Main features	1
Minimum requirements	2
Hardware	2
Browser	2
2. Basic concepts	3
SNMP Polling, summarization and graphs	3
Alarms	3
3. Quick startup guide	4
Accessing the WEB interface	4
Configuring SNMP metrics on devices	5
Alarm monitoring	5
4. Telcomanager grapher	7
Period	7
Daily graph	7
Weekly graph	7
Monthly graph	7
Quarterly graph	7
Yearly graph	7
Biennially graph	7
Five years graph	8
Custom graph	8
Features	8
Statistics box	8
Show value	8
Vertical zoom	8
Single curve	8
Relative mode	8
Axis configuration	8
Custom Polling	9
Add to graphset	9
Graph type	9
Save image	9
Aggregated chart	9
Zoom in and zoom out	9
Export	9
Auto refresh	9
Keys	10
5. Historical data	11
Favorites	11
Adding objects to the Favorites	11
Removing objects from the Favorites	11
Dashboards	11
Add new dashboard	11
Add new widget	12
Groups	12
Add groups metadata	13

Link Groups	14
Devices	15
Create Device using Wizard	19
Verifying mapped objects for the device	19
Import devices file	19
Batch operations	20
Add devices metadata	21
Probes	21
Tasks	28
Prerequisites	29
Add probes metadata	29
Reports	29
Templates	29
Variable analysis	31
Top N	32
Syslog	34
Trend Analysis	34
IP Mapping	37
Graph set	37
Definitions	37
Creation	37
Adding graphs	38
Visualizing a Graph set	38
Editing a Graph set	38
Generating graphs for a Graph set	38
Circuit	39
Route history	39
Definitions	39
Creation	40
Visualizing a route test	40
6. Configuration	41
Profiles	41
Definitions	41
Managing profiles	41
Exporting Profiles	48
QoS	49
Definitions	49
Enabling the QoS feature	49
Enabling QoS monitoring on interfaces	49
Collectors	49
Import collectors file	50
Add collectors metadata	50
Objects	51
Importing object files	51
Mappers	51
Cross OID mapping	53
Associating devices to mappers	53
Exporting and importing mappers	53
Maintenance	53
ICMP polling	53
Add ICMP Polling metadata	54
EPM (Extended Processing Module)	54
Probe types	55
Add probe types metadata	56

Rules	56
Creating rules	56
No Response filter	57
Trap Receiver	57
Trap Receiver Configuration	57
Trap Receiver Logic	58
Trap Alarm	58
Trap Receiver Report	58
Trap Receiver Logic Formula	59
Add trap receiver metadata	59
Scripts	60
Creating scripts	60
Executing scripts	63
Collector Script	63
IP mapping Script	67
Mapper Script	67
Provisioning Script	70
Device Credential	71
Add device credential metadata	72
Syslog Filter	73
Add syslog filter metadata	73
7. Tools	75
Discovery	75
MIB Browser	75
External Software	75
Telcomanager Windows Collector	75
Telcomanager Host Agent	76
8. System	77
Access Log	77
User access	77
Simultaneous access	77
Users	77
Editing users	77
Disabling users	78
User Groups	78
User profiles	79
Safe mode log	79
Alarm Console	80
Backup/Restore	80
Local configuration backup	80
Local configuration restore	81
Remote backup	81
Remote restore	82
Restore status	82
Parameters	82
Active directory	82
ALARMmanager	83
Association agents	83
Auto login	84
Backup	84
BGP	84
Capture agent configuration	84
Circuit	85
Cisco WAAS	85

Configuration history	85
Custom Collector	86
Data storage	86
dbn0/Altaia integration	87
Distributed architecture	88
EPM	88
Expiration warning	89
Exporting	89
GIS map	91
Grapher	91
HTTPS Configuration	91
Interface customization	92
IP mapping	92
ICMP	92
Link Group Agent	93
Local preferences	93
Login redirection	94
Log level	94
Logo	94
Object Mapper	94
QoS	94
Redundancy	95
Regional settings	95
Reports	96
Safe mode	97
SMS server	97
SMTP	98
SNMP	99
System Version Check	100
TACACS	100
Telcomanager Host Agent	100
Telcomanager JMX Agent	100
Theme	100
Trap receiver configurations	101
Trend Analysis	101
User access history	101
Web Services	101
MIBs	101
Diagnostics	102
Network information	102
Connectivity tests	102
Packet Capture	102
Objects	102
SNMP verifier	102
Summarizer	102
Storage usage	103
Log files	103
Configuration Logs	104
SLAview Rawdata Consult	104
Timezone	105
Support	105
Open request	105
Check for system updates	105
Remote support tunnel setup	105

About	105
9. ALARMmanager	106
Reports	106
Suppressed reports	106
Consolidated reports	106
Advanced reports	107
Email Template	109
Introduction	109
Customizing the email	109
Alarm urgency level	110
Changing the urgency level priority	110
Adding a new urgency level	110
Add alarm urgency level metadata	110
Alarms	111
Default alarm configuration	111
Behavior change alarm configuration (History Alarms)	113
Syslog alarm configuration	120
Alarm suppression management	120
Add alarms metadata	121
Alarm profiles	121
Add alarm profile metadata	122
Service Alarms	123
Introduction	123
Create a new Service Alarm	123
Formula	124
Console	124
Introduction	124
Console operation	124
10. NOC display	128
NOC display	128
11. MapView	129
Introduction	129
Main features	129
Operation	129
Map navigation	129
Map's alarm filter	129
Object alarm filter	130
Saving the map	130
Toggling the view	130
Grid layout	131
Creating and removing connections	131
Selecting objects	131
Aligning objects	131
Editing map object properties	131
Editing map object text properties	131
Changing the background image	131
Zoom in/out	132
Fit to screen	132
Stretch image	132
Adding text and geometric shapes	132
12. Metadata	133
Introduction	133
Add metadata	133
.....	133

13. License enabled features	134
Redundancy	134
Concepts	134
Enabling the redundancy	134
Distributed architecture	134
Concepts	134
Prerequisites	134
Deployment	135
14. Glossary	136
Abbreviations	136

List of Tables

1. Manual conventions	xii
4.1. Keys	10
5.1. New dashboard form	11
5.2. New widget form	12
5.3. New group form	13
5.4. Metadata fields	13
5.5. New link group form	14
5.6. Metadata fields	15
5.7. New device form	15
5.8. Fields from device file	20
5.9. Metadata fields	21
5.10. Telco ICMP Jitter probe	23
5.11. Telco HTTP probe	23
5.12. Telco DNS probe	24
5.13. Telco SSH probe	24
5.14. Telco TCPConnect probe	25
5.15. Telco Twamp	25
5.16. Cisco IP/SLA Jitter probe	26
5.17. Cisco IP/SLA ICMP Echo probe	27
5.18. Cisco IP/SLA Path Echo probe	27
5.19. Cisco IP/SLA UDP Echo probe	28
5.20. Metadata fields	29
5.21. Template Form	30
5.22. Variable analysis report	31
5.23. Variable analysis reports signaling	32
5.24. Top N report	33
5.25. Syslog report	34
5.26. Trend analysis configuration form	35
5.27. Trend analysis report form	36
5.28. IP Mapping form	37
5.29. Graph set creation	37
5.30. New Circuit Form	39
5.31. Route test creation	40
6.1. Profile form	41
6.2. Summarization variable	44
6.3. Graph	45
6.4. Graph curve	46
6.5. Associate profile form	47
6.6. QoS Wizard form	49
6.7. Collector form	50
6.8. Fields from collectors file	50
6.9. Metadata fields	51
6.10. Mapper form	52
6.11. Metadata fields	54
6.12. Probe type form	55
6.13. Metadata fields	56
6.14. Automatic profile rules	57
6.15. Trap Receiver Configuration	57
6.16. Trap Receiver Logic	58
6.17. Trap Receiver Report	59
6.18. Metadata fields	59

6.19. Wildcard List	71
6.20. Device credential form	72
6.21. Metadata fields	72
6.22. Syslog filter form	73
6.23. Metadata fields	73
7.1. Discovery fields	75
8.1. User form	77
8.2. User form	79
8.3. User form	79
8.4. Safe mode log form	80
8.5. ALARMmanager console columns	80
8.6. FTP server form	81
8.7. S3 server form	81
8.8. Active directory form	82
8.9. ALARMmanager parameters form	83
8.10. Automatic association agent form	83
8.11. BGP form	84
8.12. Capture agent configuration form	85
8.13. Circuit form	85
8.14. Cisco WAAS form	85
8.15. Log history parameters	85
8.16. Custom collector form	86
8.17. Data storage form	86
8.18. dbn0/Altaia integration form	87
8.19. Distributed architecture parameters form	88
8.20. EPM form	88
8.21. Expiration warning form	89
8.22. Syslog protocol	90
8.23. Grapher parameters form	91
8.24. Https parameters form	91
8.25. Device formula name	92
8.26. IP Mapper configuration parameters form	92
8.27. ICMP process parameters form	93
8.28. Local preferences form	93
8.29. Object mapper configuration parameters form	94
8.30. Redundancy activation settings	95
8.31. Redundancy Commutation settings	95
8.32. Regional settings form	95
8.33. Scheduled reports configuration form	96
8.34. FTP Server configuration form	96
8.35. Safe mode form	97
8.36. SMPP server form	97
8.37. SMTP parameters form	98
8.38. TRAP fields	99
8.39. Theme configuration	100
8.40. User access history form	101
8.41. Configurations API form	101
8.42. TRAFip's raw data form	101
8.43. Packet Capture	102
8.44. SLAview Rawdata Consult - Step 1	104
8.45. SLAview Rawdata Consult - Step 2	104
9.1. Suppressed alarms report form	106
9.2. Consolidated alarm report form	106
9.3. Advanced alarm report form	107

9.4. Advanced alarm reports signaling	108
9.5. Email template	109
9.6. Email variables	109
9.7. ALARM urgency level form	110
9.8. Metadata fields	111
9.9. Default alarm form	111
9.10. Behavior change alarm form	114
9.11. Default alarm form	120
9.12. Metadata fields	121
9.13. Alarm profile form	122
9.14. Metadata fields	122
9.15. Service Alarms form	123
9.16. ALARMmanager console	125
12.1. Metadata fields	133
14.1. Abbreviations list	136

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, TCP/IP protocol and SNMP 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

SLAview is a network management system focused on performance analysis.

The main technologies used are SNMP protocol, ICMP protocol, Cisco IP SLA Probes, Telcomanager Software Probes and behavior analysis algorithms.

Main features

- Monitoring of any network device using SNMP v1, v2c and v3 protocols.
- Access to all system features through a web browser.
- Hierarchical views.
- Syslog collection and reporting.
- Multi-tenant platform that provides user environment isolation.
- Formula creation, allowing users to define their own KPIs (Key Performance Indicators).
- Behavior analysis alarms on any monitored KPI.
- Scalable architecture. The system can grow on the number collected elements by the use of remote collectors appliances and on the number of users and reports supported through the deployment of EPMs (Expanded Processing Modules), which are appliances responsible to perform load sharing with the central system.
- High Availability can be provided trough the use of the redundant solution, in which two appliances work in HOT-STANDBY.
- Trend analysis reports.
- All reports can be saved as templates, scheduled and exported in PDF, HTML and CSV format.
- Online SNMP Polling down to 10 second intervals by clicking on any graph.
- Mass graph image export.
- Flexible graph creation.
- Interactive HTML5 grapher, with features like vertical and horizontal zoom, auto-scale and aggregated charts.
- SNMP Object discovery.
- High performance database for historical data storage.
- Top N reports for all monitored elements.
- Advanced alarms reports which allow data aggregation via pivots.
- Polling, consolidation and graph profiles.

- Automatic profile association, easing daily administrative tasks.
- MAP tool named MAPview, with topology mapping features and intuitive user interface navigation.
- ALARMmanager tool, which allows users to configure alarms as a formula with the monitored metrics for each object. The alarms can be visualized on a console or sent by email, SMS and SNMP traps.
- Auto QoS (Quality of Service) agent developed for Cisco Class Based QoS MIB.

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. Basic concepts

SNMP Polling, summarization and graphs

The main technology employed on SLAview system is SNMP (Simple Network Management Protocol) protocol.

SLAview is capable of monitoring any equipment that runs a SNMP agent or even only responds to ping queries.

The SNMP protocol works with the equipment's MIB (Management Information Base). The MIB is a database that can be consulted to provide configuration and performance information. A SNMP agent controls access to the MIB and responds to SNMP queries at this database.

SLAview system has a very flexible polling process. It can map instances of a wide variety of objects in the MIB files, like network interfaces, processors, storage units and many others. The object mappings are defined by the user and we will always refer to them as monitored objects or mapped objects. Once the mappings are performed, the object instances found should be associated to profiles where the OIDs that are used in the polling process were defined.

The system provides profiles, where the user can define summarization formulas based on the OIDs, which are actually the metrics or KPIs that should be monitored.

The graphs are also defined in the profiles and its curves are formulas based on the summarization variables previously defined.

Alarms

Alarms are defined as formulas based on the summarization variables. You can define the formulas freely using regular math infix notation.

Chapter 3. Quick startup guide

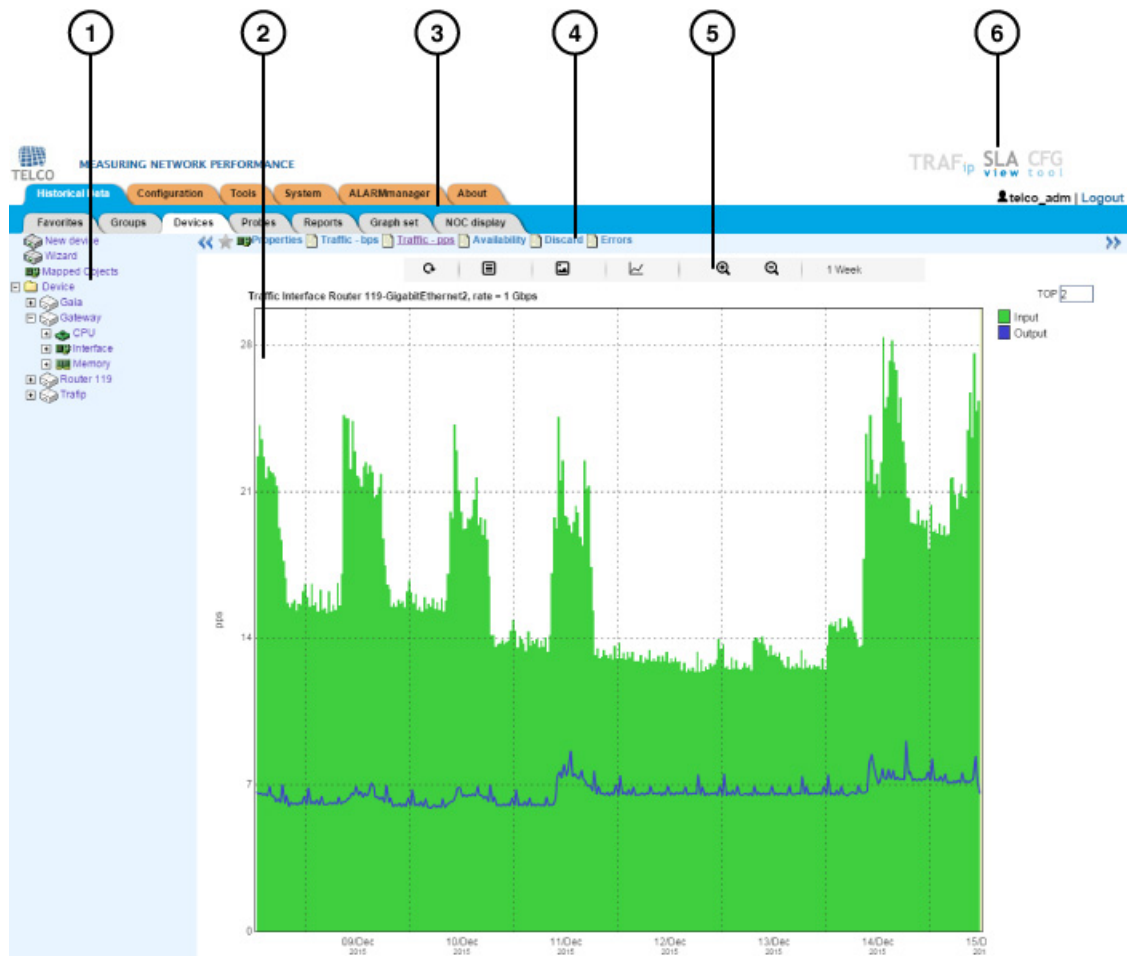
Accessing the WEB interface

Once the SLAview server is accessed typing its IP address in a web browser, choose SLAview system by clicking the SLAview icon located at the up right corner of the window.

The initial access to the system can take place using the user telco_admin and password sysoper. At this point, it is recommended a password change.

If the authentication is successful, the screen below is presented to the user.

The session can be closed at any time by clicking the Logout icon at the up right corner of the window.



SLAview main screen

The main system screen is divided in the following areas:

Area 1: tree menu. Used to navigate through system objects and configuration items.

Area 2: data display. Used to display graphs, reports and configurations forms.

Area 3: main menu. Used to select all system features.

Area 4: graph selection. Used to select object graphs and properties.

Area 5: control panel. Used to access the graph features.

Area 6: header. Used to indicate which user is logged in, logout and switch between TRAFip and SLAview system.

Configuring SNMP metrics on devices

For the successful implementation of this procedure, the network elements that will be used must have an accessible read SNMP community configured.

Procedure 3.1. Configuration steps

1. Select **Historical data** → **Devices** → **New device** and fill the form according to the instructions below:
 - a. Name and management IP address.
 - b. SNMP version and community as configured at the network element.
 - c. At Mapper field, select Interface and also CPU and Memory in case of Cisco equipment.
 - d. Click the Save button.
2. Wait around 5 minutes for the system to discover the network element interfaces, select **Configuration** → **Profiles** → **Mapped object**, click Associate Mapped Object button and fill the form according to the instructions below:
 - a. Select the profile type that matches the interface type that you wish to monitor. Ex: for serial Cisco interfaces select Serial-cisco option.
 - b. Use the filter to select the interfaces. Ex: *Serial*.
 - c. Select Interface at the type field and click the Send button.
 - d. Move the desired interfaces to the right box.
 - e. Use the OID filter 1.3.6.1.2.1.2.2.1.7 = 1, marking the option Use mapped object index. This will filter the *ifAdminStatus up* interfaces.
 - f. Click Send and then Save.
3. Wait about 10 minutes and select **Historical data** → **Devices** → **Device**. Then click on the created device and verify the graphs on monitored interfaces.
4. Repeat the same procedure for CPU and memory objects if you are monitoring a Cisco element. At step 2, the type should be CPU or memory.

Alarm monitoring

Procedure 3.2. Configuration steps

1. Select **ALARMmanager** → **Profiles** → Click the New button.

2. Fill the profile name and choose Mapped Object option at the Object type field.
3. Select the alarms you want to use. Ex: interface down and high bandwidth utilization.
4. Select the objects you want to monitor. Ex: Router1FastEthernet0/1. Now click the Save button.
5. Select **System** → **Users**. Click the New button.
6. Fill the profile name, select the users and then the alarms that those users will be able to receive. Click the Save button to save the changes.

Chapter 4. Telcomanager grapher

When you click on an object icon in the tree menu or click on an object name in the objects configuration list, its graphs are presented in the graph selection area. When you click on an icon at this area, the Telcographer is loaded in the data display area.

The Telcographer is a highly interactive grapher written in HTML5. The functions of this application will be explained below.

Period

The grapher reads its information from the TelcoDatabase, in which all information is stored in a 5 minute period.

The 5 minute period information is available for the full period that is stored for each monitored object.

Daily graph

In this period, the information is presented with the greatest level of detail. The time period is 24 hours. There is 1 sample for each 5 minutes and 288 total samples.

Weekly graph

Each sample is the mean value of 6 5 minute samples, which corresponds to 30 minutes. The time period is 7 days with 336 samples. The maximum curve is obtained by calculating the maximum value from every 6 5 minute samples.

Monthly graph

Each sample is the mean value of 24 5 minute samples, wvvhich corresponds to 2 hours. The time period is 30 days with 360 samples. The maximum curve is obtained by calculating the maximum value from every 24 5 minute samples.

Quarterly graph

Each sample is the mean value of 72 5 minute samples, which corresponds to 6 hours. The time period is 90 days with 360 samples. The maximum curve is obtained by calculating the maximum value from every 72 5 minute samples.

Yearly graph

Each sample is the mean value of 288 5 minute samples, which corresponds to one day. The time period is 364 days with 364 samples. The maximum curve is obtained by calculating the maximum value from every 288 5 minute samples.

Biennially graph

Each sample is the mean value of 576 5 minute samples, which corresponds to two days. The time period is 728 days with 364 samples. The maximum curve is obtained by calculating the maximum value from every 576 5 minute samples.

Five years graph

Each sample is the mean value of 1440 5 minute samples, which corresponds to five days. The time period is 1820 days with 364 samples. The maximum curve is obtained by calculating the maximum value from every 1440 5 minute samples.

Custom graph

You can choose a custom period for your graph. To do it, select the **Custom** period and enter the initial date and time and the final date and time.

Features

The Telcographer has many features that are available at control panel. Some of them can also be accessed by clicking the right mouse button at any point on the graph.

Statistics box

The mouse over action on the curve label will display a statistics box with the following information: maximum, minimum, mean, total value and standard deviation for the curve.

Show value

This feature will cause the mouse pointer to display the x and y axis value for the pointer position.

Vertical zoom

To use this resource, follow the steps below:

1. Select this option on the Options menu at control panel.
2. Press and hold the mouse button on the initial y axis position.
3. While holding the button, move the mouse cursor to the final y axis position and release the mouse button.

Single curve

Select this option on the Options menu at control panel and then click on one of the curves label. This action will cause the graph to show only the selected curve.

Relative mode

Click this option on the popup menu to display each curve sample in the graph relatively to the other curves, which means that for each sample, the sum of the data represents 100%.

This mode only works if all the graph curves are in stack mode.

Axis configuration

Select this option on the Options menu at control panel to open a window where you will be able to select the curves that will be displayed using the left or right x axis scales.

Custom Polling

You will find this option by clicking the right mouse button on the graph. It opens a new browser window, where you will be able to fill a refresh rate and submit the form to start an online polling for the graph.

Add to graphset

Click the right mouse button on the graph and after select this option to open a box where you will be able to associate the graph to a previously created graphset.

Graph type

With the **Graph type** menu at control panel, you can choose the display type of the graph: line, pie or bar.

Save image

Click this option on the graph popup menu option to save the graph as a jpeg image.

Aggregated chart

Select this option on the graph popup menu to open aggregated charts representation of the graph. There are 2 options of charts: pie and bar. Those charts can be filtered by a period of the day. For example, if you open a pie chart from a weekly graph and filter from 10:00h to 17:00h, the pie chart will represent the weekly data only for that period of the day.

Even if you don't enable the filter, you can configure the graph period using the field **Period**. When this field is filled with **1 day**, another field is displayed: **Last hours**. For instance, when this field is filled with 1, it means the graph values are related to the last hour. The maximum value that can be configured in this field is **24**, which represents the last 24 hours.

Tip

You can remove a curve from the graph just by clicking on it in the label.

Zoom in and zoom out

Click this option on the graph popup menu to zoom in and out on the time scale. For example, using it on an annual graph, it is possible zoom in the daily graph for one particular day.

Important

These options are only available at line graphs.

Export

Access this option by clicking the right mouse button on the graph. The graph data can be exported in HTML, CSV or TSV formats.

Auto refresh

Select this option to cause the graph to refresh automatically every 5 minutes. This feature have to be previously enabled at **System** → **Parameters** → **Grapher** , where you can also set the refresh interval.

Tip

The graphs in **Packets/s** (pps) and **Bit/s** (bps) have a curve for no sample applied. So, to check this curve's information, pass the mouse over the label named "**No sample total**".

Keys

Some keys on your keyboard have special functionalities. Check them below and their descriptions.

Table 4.1. Keys

Key	Description
D	Transforms the graph into derivative mode.
I	Indicates detailed information about the graph such as resolution, curves, samples and timestamps.
L	Lists the timestamp and the value of each point from a curve.
N	Changes graph curves format, once all of them are in stack mode.
P	Provides a projection curve considering only the points between the signalized lines. When you move down the mouse, the number of points decrease, otherwise the number of points increase.
R	Adjusts the graph to get the max resolution.
S	Save the graph as a PNG image.
W	Changes the curve configuration to waas accell.
Z	Opens the Projection Violation popup, once the Trend Analysis is enabled.
-	Zoom out.
+	Zoom in.
LEFT	Moves the graph to left.
RIGHT	Moves the graph to right.
*	Graph returns to its normal size.

Tip

You can convert the timestamp to date using the **ts2date** command at CLI.

Chapter 5. 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.

Favorites

Using this feature, each user can configure its objects of interest for fast access.

Adding objects to the Favorites

To add objects to your Favorites, simply click the gold star icon shown as the first element of the graph selection area for the desired object.

Removing objects from the Favorites

To remove objects from your Favorites, simply click the gold star icon shown as the first element of the graph selection area for the desired object.

Dashboards

This tab allows the creation of custom dashboards, offering different types of widgets, containing data of summarization variables or alarms. The widget can be of report, pie chart, bar chart or gauge types.

Each user can only visualize dashboards that were associated with his user profile. Also, is only possible for the user visualize information from objects in groups that were associated with him user profile.

The summarization variable widgets brings a daily, weekly or monthly Top 10 for the choosen variable. That is, the 10 objects which have the highest values for the variable will be displayed. For widgets of this datatype, report, pie chart and bar chart views are available.

The alarm widgets brings the amount of alarmed objects and the total amount of objects associated with the alarm. It is also informed the percentage of alarmed objects. You can filter the alarm in ALARMmanager by clicking the widget. For widgets of this datatype, only the gauge view are available.

Add new dashboard

Access **Historical data** → **Dashboards**. After, click in the **New dashboard** option. Fill the form as detailed below:

Table 5.1. New dashboard form

Field	Description
Name	Dashboard name
Description	Dashboard description
User profiles	User profiles that can visualize the dashboard

Tip

To open a dashboard in a new window, use the icon .


Add new widget

Access any dashboard and then click in the empty widget to create a new widget. Fill the form as detailed below:

Table 5.2. New widget form

Field	Description
Title	Widget title
Object type	Choose if the object type will be Device or Mapped Object
Datatype	Choose if the datatype will be Summarization variable or Alarm
Summarization variable	Choose a summarization variable. This option will be only displayed if the Summarization variable datatype are selected
Alarm	Choose an alarm. This option will be only displayed if the Alarm datatype are selected
Period	Choose the widget period between Daily, Weekly or Monthly. This option is only available if the Summarization variable datatype are selected
Widget type	Choose a widget widget type between Report, Pie chart, Bar chart or Gauge
Width	Choose the widget width

Tip

To edit the widget, click in the icon .

Groups

The groups are used to organize the monitored objects. They are hierarchical and can have as many levels as needed.

Groups can be used to restrict user access to monitored objects. By associating a user profile to a group, the users in the profile are restricted to the objects associated to this group or to the groups beneath it in the hierarchy.

Objects can be associated to groups manually or automatically. When manual association is enabled, the group form will show **Devices** and **Mapped objects** to be associated. Otherwise, the group form will show **Devices** and **Mapped objects** rules to be used as association conditions.

Objects can be removed from group automatically when they don't meet the association rules anymore. This option is only available when the group has auto association enabled.

Important

When the group icon is a yellow folder, this group has no graphs. When the icon is a green folder, there is at least one object with graph in this group.

Procedure 5.1. Configuration steps

1. Select **Historical data** → **Groups** → **Groups** .
2. Click the **New** button to define a new group and fill the form.

Table 5.3. New group form

Field	Description
Name	Define a group name.
Description	Define a group description.
Group summarization	Enables group summarization for this group. If group summarization is enabled for the User, the summarized group graph is displayed.
Automatic association	Select Yes to enable the automatic association of objects to this group considering rules.
Root group	The root group in respect to this one. If no root group is selected, then this group will be a root group in the system.
Automatic removal	Select Yes to enable the automatic removal of objects when they do not meet the association rules anymore. This option is only available when the group has Automatic association enabled.
Devices	Devices that will belong to this group.
Mapped objects	Mapped objects that will belong to this group.
Alarm profiles	Associates the group to an alarm profile. The group can only be associated with an alarm profile if your group summarization is enabled.
User profiles	User profiles to have access to this group.

3. Click the **Save** button.
4. To add more groups below this group, click its group icon on the group tree. Then, click on Subgroups in the graph selection area and repeat the steps above.

Add groups metadata

To access the metadata configuration page, access **Historical Data** → **Groups**, click on **Groups** 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 5.4. 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 a group, access the groups list and click on **Metadata** button beside the group that will be configured.

Then, fill the metadata according to its type.

Link Groups

Link Groups are used to create automatic groups associated to mapped objects representing the connections in the system.

For the set of groups formed by the subgroups belonging to the Link Group's source group, the system will check if there are connections to each other and, if so, will create groups for each side of the connection with the interfaces that represent this connection.

For example: a group 'S', has two subgroups: 'A' and 'B'. 'A' has device 'Da' and 'B' has device 'Db'. Interface 'Ia' belongs to 'Da' and interface 'Ib' belongs do 'Db'. 'Ia' and 'Ib' are connected. A Link Group 'L' is created with source group 'S'. Two groups will be created under 'L': 'A' --> 'B' that has interface 'Ia' and 'B' --> 'A' that has interface 'Ib'.

Visualization is restricted the same way as normal groups.

Procedure 5.2. Configuration steps

1. Select **Historical data** → **Groups**.
2. Click the Link Groups icon to open configuration form.
3. Click the **New** button to define a new link group and fill the new link group form.

Table 5.5. New link group form

Field	Description
Prefix	Prefix to be concatenated to source group name.
Suffix	Suffix to be concatenated to source group name.
Create subgroup	If yes, groups will be created recursively. If no, only the root groups will be created.
Destination group	Group where the link group will be created.
Source group	Group to fetch the connections.
Rules	Rules to filter which interfaces will be considered. Only applied to interface names.

4. Click the **Save** button.
5. The new groups will be created after running the link group agent. The agent execution times can be configured in the system parameters.

Add link groups metadata

To access the metadata configuration page, access **Historical Data** → **Groups**, click on **Link group** 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 5.6. 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 a link group, access the link groups list and click on **Metadata** button beside the group that will be configured.

Then, fill the metadata according to its type.

Devices

A device is any network element that has an IP address and supports the SNMP or ICMP protocols.

To map logical and physical device's objects like interfaces, cpus and so on, the system has a mapper process that periodically runs and performs the mappings (See Mappers configuration section). There is a pre-configured mapper to map device's interfaces that uses the ifDescr OID to perform this task.

Procedure 5.3. Device configuration steps

1. Select **Historical data** → **Devices** → **Device** .
2. Click the **New** button and fill the form below.

Table 5.7. New device form

Field	Description
Name	Device name.
Description	Device description.
Management IP address	Device IP address. This IP address should respond SNMP read queries for SNMP monitoring and ICMP echo requests for ICMP monitoring.

Field	Description
Type	Type of device, the user can use this field to freely categorize all devices configured.
Manufacturer	Name of the device manufacturer.
Latitude	Geographic coordinate, in decimal degrees (DD), used to locate the device on georeferenced maps. Example: -22.9035.
Longitude	Geographic coordinate, in decimal degrees (DD), used to locate the device on georeferenced maps. Example: -43.2096.
SNMP credential	Choose a SNMP credential.
SNMP Version	Choose the SNMP version. Possible values are: SNMP v1 or SNMP v2c Specify an SNMP community SNMP v3 Specify the authentication type and its parameters
SNMP community	Enter the SNMP community.
Use Default SNMP configuration	This option lets you define specific values to be used specifically for this device. The default values are specified at SNMP collector parameters configuration.
Use sysUpTime OID to discard results	Discard the collection if the device is not allowed for more than 5 minutes. Prevents miscalculations.
SNMP Timeout	Time limit in seconds to 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 that will be sent 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.
SNMP window	Number of SNMP packets that will be sent without answer from the device being polled.
SNMP port	The SNMP port.
Agents	This option lets you define one or multiple SNMP agents in the same IP address and different ports. Now you can specify OID masks and SNMP port for this mask.

Field	Description
	<p>This means that the SNMP collector will use the specified UDP port if the OID to be collected on this device matches the specified mask.</p> <p>Example:</p> <ul style="list-style-type: none"> • OID prefix .1.3.4.6.9.9.1.2.* SNMP port: 163 • OID prefix .1.3.4.6.9.9.1.3.* SNMP port: 164
Connection credential	Choose a Connection credential.
Connection protocol	Choose SSH or Telnet .
SSH port	When the Connection protocol is SSH, enter the SSH port. The default value is 22 .
Telnet port	When the Connection protocol is Telnet, enter the Telnet port. The default value is 23 .
User	User to be used to access the device. This string is available as a wildcard %username% for provisioning scripts.
User password	Password to be used to access the device. This string is available as a wildcard %passwd% for provisioning scripts.
Enable secret	Enable password to be used to access the device. This string is available as a wildcard %enable_passwd% for provisioning scripts.
Enable TRAFip collect	Enables the collection by TRAFip.
Netflow exporter ip address	Fill the IP address that the netflow exporter will use to send flows. Next to this field, there is a magnifying glass icon. Click to fill automatically based on Management IP address.
Sampling rate configuration	Can be set manually or based on flow.
Netflow sampling rate	If you are exporting sampled flows, choose whether to consider a manual configured rate or to detect the rate from the flow records.
Enable SLAview collect	Enables the collection by SLAview.
Automatic profile	Select this option to enable the use of this device and its mapped objects on automatic profiles. The association will only occur if the device or its objects match the profile rules. (See Profile configuration section) .
Collect via THA	Select the way THA information should be collected. Local: all THA requests will be sent directly to this device. Therefore Telcomanager Host Agent (THA) must be installed on this device. Gateway: all THA requests will be sent to THA gateway configured at System → Parameters → Telcomanager Host Agent .

Field	Description
	THA gateway will be responsible for collecting information from this device.
Enable configuration management	Enables the configuration management by CFGtool.
Configuration export mode	Select Active to export the device configuration according to the interval configured at System → Parameters → Configuration management . To export configuration using trap filter, select Passive .
Enable CallView collect	Enables the collection by CallView.
Voice profile	Select the voice profile to collect call data.
Enable JMX collect	Select Yes to collect of Java Management Extensions statistics or No to disable it. In order to collect this information, Telcomanager JMX Agent must be configured at System → Parameters → Telcomanager JMX Agent .
Topology mapping method	Select the protocol to be used for topology mapping. Available options are CDP - Cisco Discovery Protocol, LLDP - Link Layer Discovery Protocol or both. Using either method, SLAview uses the SNMP protocol to fetch information from these protocols on the monitored devices MIB tables.
Enable provisioning	Enable provisioning to configure automatically Cisco IP SLA probes, Telcomanager probes and Netflow exportation.
Collector	Device association to a remote collector. This field is available only when the distributed architecture is enabled.
Authentication script	When the Connection protocol is Telnet , you have to select a Login script.
Provisioning script	Fill this option for Netflow provisioning in distributed architecture systems and probes configuration. This script will be used to reconfigure Netflow export to a backup collector if a collector fails.
Polling templates	Choose an ICMP polling template for the device. The polling template lets you configure the specific times to poll the devices and measure their availability.
Device type	Field used to pick an icon to represent the device graphically on Maps. You can choose between: Camera, Firewall, Router, Server, Switch or Wireless. The default device type is Router .

Field	Description
Configuration exporter script	Select configuration exporter scripts.
Domain	Device domain association.
Groups	Click the List button and select the desired groups to place this device in one or more points in the group hierarchy.
Mappers	Select the desired mappers to map objects like interfaces and cpus on this device.(See Mappers configuration section)
Alarm profiles	Associate the device with an alarm profile.

Create Device using Wizard

There is a wizard for device creation that will guide you and validate each step at a time.

1. Select **Historical Data** → **Devices** → **Wizard** .
2. Fill the fields according to the table above.
3. During the creation, you are able to test the equipment connectivity, map the device's object and test mapped objects association to profiles, for instance.
4. After this, you can view and save your new device.

Verifying mapped objects for the device

Click the Mapped objects icon in the tree menu area to see all the mapped objects of the system. Accessing the form of each one, you can enable the trend analysis and enter a description. And besides, you can associate the profile and/or alarm profile.

It is also possible to check the configuration history and delete the object using the **History** and **Delete** buttons.

There is a filter at the top of the page with options to select located and not located objects. Not located items are mapped objects that are not being located by one of the device's mappers. Ex: an interface module that was removed from a router will cause its interfaces to go to not located state.

At the tree menu area, below each device, the system shows its mapped objects. The icons color indicates the following conditions:

- | | |
|-------------------|----------------------------------------------------------|
| Green icon | The object has a profile associated to it. |
| Uncolored icon | The object does not have a profile associated to it. |
| Red blinking icon | The object was not located by the object mapper process. |

Import devices file

To import a file of devices, access **Historical data** → **Devices**.

Click the **Devices** tree menu item.

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

A import devices file has the following fields:

Table 5.8. Fields from device file

Field	Description
Name	Possible characters for name field.
Description	Possible characters for description field (optional).
Management IP address	IP Address. Ex.: 10.0.0.1
SNMP Version	Type 1 for SNMP version 1, 2c for version 2 and 3 for version 3.
SNMP community	Possible characters for snmp community.
Connection protocol	Type SSH or TELNET .
User	Possible characters for name field (optional).
User Password	Possible characters for password field (optional).
Enable Secret	Possible characters for password field (optional).
Enable TRAFip collect	YES to enable and NO to disable the TRAFip collect.
Netflow exporter ip address	IP Adress list separated by comma. Ex.: 10.0.0.1,10.0.0.2
Sampling rate configuration	Enter 0 for manual and 1 for flow.
Netflow sampling rate	Integer value greater than 0.
Enable SLAView collect	YES to enable and NO to disable the SLAview collect.
Automatic profile	Select YES to enable the use of this device and its mapped objects on automatic profiles.
Device Type	Field used to pick an icon to represent the device graphically on Maps. Choice camera, firewall, router, server, switch or wireless.

Batch operations

It's possible to perform some operations for multiple devices at the same time. To do so, you must select one or more devices and use the **Enable** select box right above the device list. The operations available are:

- **TRAFip**: enables TRAFip collect.
- **SLAview**: enables SLAview collect.
- **CFGTool**: enables configuration management.
- **CFGTool Physical Inventory**: enables physical inventory collect.
- **CALLview**: enables CALLView collect.

Add devices metadata

To access the metadata configuration page, access **Historical Data** → **Devices**, click on **Device** 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 5.9. 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 device, access the devices list and click on **Metadata** button beside the device that will be configured.

Then, fill the metadata according to its type.

Important

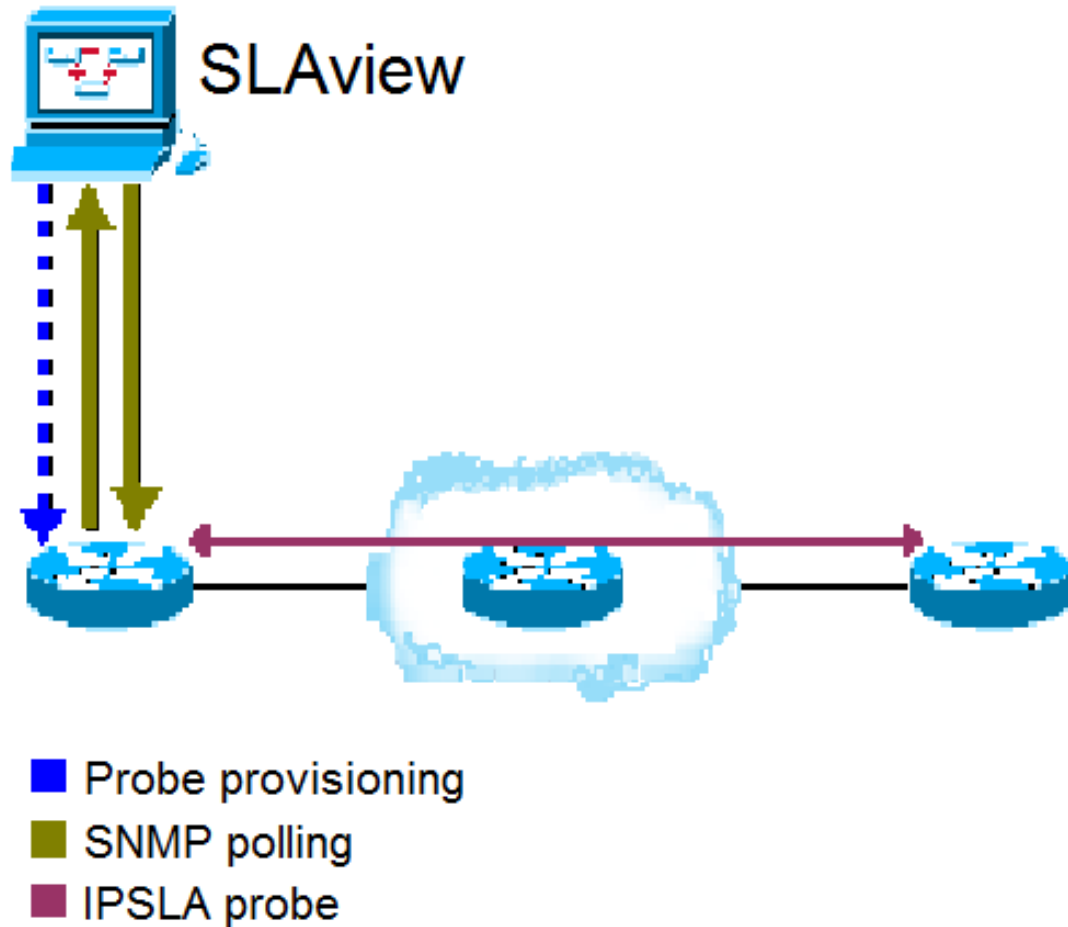
If the device icon is red, it means all its exports IP's are down.

Probes

Probes are active agents that perform performance measurements in the network. Many vendors support this type of agent, like Cisco IP SLA probes, Juniper real-time performance (RTM) probes, Telcomanager probes and many others.

Probes are much alike mapped objects like interfaces and CPUs. The difference from those is that SLAview is able to configure these agents on the network devices, by executing configuration scripts written by the user. This can be done for any kind of device that supports SSH or TELNET protocols to perform configuration.

The figure below depicts the interaction between SLAview and the probes.



IPSLA probe provisioning

The system executes the following steps to bring up a probe:

Procedure 5.4. SLAview probe provisioning steps

1. SLAview configures a probe in a network element using a script template or a new script written by you.
2. SLAview identifies the configured probe using a probe mapper that was associated to the network element being configured.
3. The network element performs the probe performance measurements in the network.
4. SLAview collects SNMP OIDs according to the profile configured for the probe.

Tip

If your area is responsible to configure the probes on the network, but you still need to collect the measurements using SLAview, you can treat a probe just like another mapped object. If it is a Cisco probe, all you have to do is to associate the Cisco mapper to the device where the probes are already configured and then associate the correct profile to monitor the probes that will be mapped.

New probes can be created. There is a wizard for probe creation that will guide you and validate each step of the creation.

Procedure 5.5. Configuring pre-existing probes

1. Select **Historical Data** → **Probes** → **Wizard** .
2. Fill the form according to the instructions below for each probe type. Each provisioning script belongs to one probe type. If you choose to run your script during the wizard, the probe will be created in the system and you will be asked to associate profiles to it.

Table 5.10. Telco ICMP Jitter probe

Field	Description
Name	Probe name.
Device	Select the device where the probe will be configured. Notice that the device should have been previously added to the system.
Probe type	Select probe Telco/ICMP Jitter .
Destination IP address	Probe destination IP.
High latency discard (packets)	How many high packets will be discarded from the statistics.
Low latency discard (packets)	How many low packets will be discarded from the statistics.
Number of packets	Number of measurement packets to be sent out by the probe.
Packet interval (ms)	Interval between measurement packets.
Packet size (bytes)	Size of the measurement packet.
Provisioning script	Select the script Probe Telco ICMP Jitter .
Probe removal script	Choose a script to remove the probe from the device.

Metrics provided by this probe:

- Round-trip latency.
- Round-trip jitter.
- Round-trip packet loss.

Table 5.11. Telco HTTP probe

Field	Description
Name	Probe name.
Device	Select the device where the probe will be configured. Notice that the device should have been previously added to the system.
Probe type	Select probe Telco/HTTP .
URL	Fill the URL to be tested.

Field	Description
Provisioning script	Select the script Probe Telco HTTP .
Probe removal script	Choose a script to remove the probe from the device.

Metrics provided by this probe:

- HTTP round trip latency.
- Availability.

Table 5.12. Telco DNS probe

Field	Description
Name	Probe name.
Device	Select the device where the probe will be configured. Notice that the device should have been previously added to the system.
Probe type	Select probe Telco/DNS .
Destination IP	Probe destination IP.
URL	Fill the URL to be translated.
Provisioning script	Select the script Probe Telco DNS .
Probe removal script	Choose a script to remove the probe from the device.

Metrics provided by this probe:

- DNS round-trip latency answer.
- Availability.

Table 5.13. Telco SSH probe

Field	Description
Name	Probe name.
Device	Select the device where the probe will be configured. Notice that the device should have been previously added to the system.
Probe type	Select probe Telco/SSH .
Destination IP	Probe destination IP.
Port	TCP Port where the SSH service is running.
Provisioning script	Select the script Probe Telco SSH .
Probe removal script	Choose a script to remove the probe from the device.

Metrics provided by this probe:

- Round-trip SSH answer latency.

- Availability.

Table 5.14. Telco TCPConnect probe

Field	Description
Name	Probe name.
Device	Select the device where the probe will be configured. Notice that the device should have been previously added to the system.
Probe type	Select probe Telco/TCPConnect .
Destination IP	Probe destination IP.
Port	TCP port where the service is running.
Provisioning script	Select the script Probe Telco TCPConnect .
Probe removal script	Choose a script to remove the probe from the device.

Metrics provided by this probe:

- Round-trip answer latency for the TCP connection.
- Availability.

Table 5.15. Telco Twamp

Field	Description
Name	Probe name.
Device	Select the device where the probe will be configured. Notice that the device should have been previously added to the system.
Probe type	Select probe Telco/Twamp .
Twamp light mode	Select Yes to enable TWAMP light mode.
Destination IP address	Probe destination IP.
Number of packets	Number of measurement packets to be sent out by the probe.
Twamp interval (ms)	Sending interval.
Twamp payload (bytes)	Payload, in bytes.
Twamp port	Responder port. The default value is 862 .
Provisioning script	Select the script Probe Telco TWAMP .
Probe removal script	Choose a script to remove the probe from the device.

Metrics provided by this probe:

- Round-trip time
- Send time

- Receive time
- Process time

Table 5.16. Cisco IP/SLA Jitter probe

Field	Description
Name	Probe name.
Device	Select the device where the probe will be configured. Notice that the device should have been previously added to the system.
Probe type	Select probe SLA/Jitter .
Destination IP address	IP address of a target Cisco device that supports IP SLA responder feature.
Destination UDP port	Destination UDP port for the measurement packet.
Initial interval (s)	Initial interval that the Cisco device will wait to start the probe after booting. The use of this parameter is recommended to avoid the probes to run at the same time.
Interval between packets (ms)	Interval between measurement packets.
Number of packets	Number of measurement packets to be sent each time the probe runs.
Origin IP address	IP address to be used as the origin IP for the measurement packets.
Origin UDP port	Origin UDP port of the measurement packets.
Packet size (bytes)	Size of each measurement packet.
TAG	Choose a tag.
Type of service (ToS)	ToS field to be set in the measurement packets.
VRF	Text identifying a VRF. When this parameter is used, the measurement packets will go through the VRF specified.
Provisioning script	Select the script IP/SLA Jitter [ip sla monitor rtr] depending of the devices IP SLA syntax.'
Probe removal script	Choose a script to remove the probe from the device.

Metrics provided by this probe:

- One-way and round-trip latency.
- One-way and round-trip jitter.
- One-way and round-trip packet loss.
- Availability.

Tip

this probe requires the target device to be a Cisco router that supports IP SLA responder feature. To enable the feature, just type the command **ip sla responder** or **rtr responder** in the Cisco's device command line interface.

Table 5.17. Cisco IP/SLA ICMP Echo probe

Field	Description
Name	Probe name.
Device	Select the device where the probe will be configured. Notice that the device should have been previously added to the system.
Probe type	Select probe SLA/ICMP Echo .
Destination IP address	IP address of a target Cisco device that supports IP SLA responder feature.
Origin IP address	IP address to be used as the origin IP for the measurement packets.
Provisioning script	Select the script Probe IP/SLA ICMP Echo [ip sla monitor rtr] depending of the devices IP SLA syntax.'
Probe removal script	Choose a script to remove the probe from the device.

Metrics provided by this probe:

- Round-trip latency.
- Availability.

Table 5.18. Cisco IP/SLA Path Echo probe

Field	Description
Name	Probe name.
Device	Select the device where the probe will be configured. Notice that the device should have been previously added to the system.
Probe type	Select probe SLA/Path Echo .
Destination IP address	IP address of a target Cisco device that supports IP SLA responder feature.
Origin IP address	IP address to be used as the origin IP for the measurement packets.
Provisioning script	Select the script Probe IP/SLA Path Echo [ip sla monitor rtr] depending of the devices IP SLA syntax.'
Probe removal script	Choose a script to remove the probe from the device.

Metrics provided by this probe:

- Round-trip latency.

Table 5.19. Cisco IP/SLA UDP Echo probe

Field	Description
Name	Probe name.
Device	Select the device where the probe will be configured. Notice that the device should have been previously added to the system.
Probe type	Select probe SLA/UDP Echo .
Destination IP address	IP address of the target device.
Destination UDP port	Destination UDP port for the measurement packet.
Origin IP address	IP address to be used as the origin IP for the measurement packets.
Origin UDP port	Origin UDP port of the measurement packets.
Provisioning script	Select the script Probe IP/SLA UDP Echo [ip sla monitor rtr] depending of the devices IP SLA syntax.'
Probe removal script	Choose a script to remove the probe from the device.

Metrics provided by this probe:

- Round-trip latency.
 - Availability.
3. Select **Configuration** → **Profiles** → **Mapped object** and click the **Associate Mapped Object** button to associate the probe created to the adequate profile. Ex: for Telco-DNS probes, use Software/DNS profile and for IP/SLA UDP Jitter probe use SLA/Jitter profile.

Tasks

The task list shows informations about the probe provisioning.

The tasks will be displayed according to the date and time of execution.

Using the **Script** button, it's possible to obtain more specific information about the script. For instance, the script, its name and its execution mode.

The **Show** button provides provisioning details like the status and the device. The provisioning result can be obtained by clicking the **Show** button again.

The tasks can be deleted at any time with the **Delete** button.

Prerequisites

- The device where the probes will be configured must have a CLI (command line interface) accessible through the SSH or telnet protocols.
- The measurement agent must have its performance variables available via SNMP protocol.
- The agent MIB must have an OID whose values are unique and identify each probe instance. For example, the probe name.
- The above OID must be configurable through the device's command line interface, so the created mapper is able to match the mapped probe with what was provisioned.

Add probes metadata

To access the metadata configuration page, access **Historical Data** → **Probes**, click on **Mapper** 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 5.20. 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 probe, access the probes list and click on **Metadata** button beside the probe that will be configured.

Then, fill the metadata according to its type.

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.

- Fill the fields below:

Table 5.21. 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.

- 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

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

Variable analysis

The variable analysis report provides a consolidated statistic for any variable configured in the system.

Tip

To know how to create a variable, check the section **Summarization variables**.

Creating a new report

1. Access **Historical Data** → **Reports** → **Variable analysis** .
2. Choose **New device report** or **New mapped object report** to have a device profile report or a mapped object profile report.
3. Select the desired profiles and then click on the desired variables for each function (Max, Min, Average, Sum, Standard deviation, Percentage of limit and Percentile).
4. Fill the form:

Table 5.22. Variable analysis report

Field	Description
Generate report Save template	Choose Generate report for a one time report or Save template to save the report as a template
Object filter	Filter by Object.
IfAlias filter	Filter by the IfAlias SNMP OID in case of mapped object reports.

Field	Description
Show group path	Enable this option to display the associated group on report.
Start time	Start time for data selection.
End time	End time for data selection.
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.
Output format	Option available only for non-template reports. Once the report becomes a template, this option is ignored.
Excluded range	Add a signaling to ignore variable with a value range.
Variable pattern replace	Add labels to variables.
Signaling	Add a signaling to color a cell.
Groups	Use the available buttons to add or remove groups from the list. The list will filter objects below the selected groups in the group hierarchy.
Consolidate results by groups	Check this option to summarize the results by the groups.

Signaling

The signaling option is used to color the advanced Top N report cells.

When you use a signaling in a report, the report cells will be colored according to the thresholds configured.

Go to **Historical Data** → **Reports** → **Variable analysis** → **Signaling** and click the New button to create a new report signaling.

Table 5.23. Variable analysis reports signaling

Field	Description
Name	Signaling name.
Description	Description field.
Signaling levels	Fill the levels for signaling. Example: <ul style="list-style-type: none"> • 40.00<=critical<=100.00 color red • 20.00<=medium<40.00 color blue • 5.00<=low<20.00 color gray

Top N

Definitions

Top N reports provide a consolidated statistic for any metric configured in the system.

A user will only be able to visualize statistics for the objects it has access to.

Launch a new report

1. Access **Historical data** → **Reports** → **Top N** .
2. Choose **Device** or **Mapped Object** to have a device profile report or a mapped object profile report.
3. Choose the desired profile and then click on the desired metric within that profile.
4. Fill the form:

Table 5.24. Top N report

Field	Description
Generate report Save template	Choose Generate report for a one time report or Save template to save the report as a template
Analyzed object	Automatically filled with selected profile type.
Analyzed variable	Automatically filled with the selected variable name.
Object filter	Filter by Object.
Manufacturer	Filter by objects manufacturer.
Manufacturer Type	Filter by objects manufacturer type.
IfAlias filter	Filter by the ifAlias SNMP OID in case of interface reports.
Start time	Start time for data selection.
End time	End time for data selection.
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.
All profiles	Search that metric for all objects that are being monitored by it, not only for this profile.
Use percentile	Use percentile to compute report results.
Show bandwidth usage percentage	Shows the bandwidth utilization as a percentage.
Output format	Option available only for non-template reports. Once the report becomes a template, this option is ignored.
Groups	Use the available buttons to add or remove groups from the list. The list will filter objects below the selected groups in the group hierarchy.
Consolidate results by groups	Check this option to summarize the results by the groups.
Show group path	Enable this option to display the associated group on report.

Syslog

Definitions

You can configure any device to send syslog messages to SLAview.

The messages are received at UDP port 514.

The syslog messages will be stored and deleted based on the syslog storage configuration.

Launch a new report

1. Access **Historical data** → **Reports** → **Syslog** → **New report** .
2. Fill the form:

Table 5.25. Syslog report

Field	Description
Begin	Enter the initial period time in the format dd/mm/yyyy.
End	Enter the final period time in the format dd/mm/yyyy.
Message	Filter the syslog message. Leave blank to have all messages.
Priority	Select the message priority. Leave the 0 to have all priorities.
Level	Select the syslog message level. Choose All to have all the messages.
Number of lines	Choose a limit to the report output: 10000 or Unlimited . If you select Unlimited , the report must be generated in CSV format. Option available only for non-template reports. Once the report becomes a template, this option is ignored.
Output format	Choose the report format. Option available only for non-template reports. Once the report becomes a template, this option is ignored.
Filters	Filter the Syslog messages by the host Name , Management IP address or metadata . At least one field must be filled and use Regular Expressions to filter the objects.

3. Click the Send button.

Trend Analysis

Once this feature is enabled, the system is able to predict the behavior for any graph curve and inform a violation date for a given threshold or given the date, inform curve value.

Configuration

Access **System** → **Parameters** → **Trend analysis**

Table 5.26. Trend analysis configuration form

Field	Description
Degree of freedom	The polynomial order to be used. Currently only first degree polynomials are supported.
Sampling	Configure the sampling for day, week or month granularity for the trend analysis process.
History	Configure the number of samples that will be analyzed. Ex: If you choose the value 6 for history and week for sampling, the system will analyse 6 weeks back to predict the trend.
Interval	If All day option is marked, this field is ignored, otherwise the analysis will consider only the configured range for each day.

Enabling projection for a graph curve

1. Access **Configuration** → **Profiles** → **Mapped Object|Device** .
2. Click the Graph button for the desired profile.
3. Click the Curve Edit button for the desired graph.
4. Click the Edit button for the desired curve.
5. Click **Yes** at the **Enable trend analysis** select box and choose **Standard configuration** or **customize configurations** for that curve.

Important

The Trend Analysis reports will be available one day after enabling the feature, since the trend analysis process runs on a daily basis.

Graphical reports

1. Access the graph that contains a curve configured for projection, right click on it and select the **Projection violation** option.
2. Select the desired curve in the popup box, insert a value for it and click OK to have the growth rate and violation date.

Launch a new report

1. Access **Historical data** → **Reports** → **Trend analysis** → **New report** .
2. Fill the form:

Table 5.27. Trend analysis report form

Field	Description
Object type	Select the object type.
Profile	Select the object profile.
Curve	Select the graph curve.
Output format	Option available only for non-template reports. Once the report becomes a template, this option is ignored.
Limit violation Estimate	<p>Limit violation If you choose this option, you will have to select one of the modes: Rate or Object limit. By choosing Rate, you will enter a integer value and its unit is bits per second (bps). The result is the date when the Rates average exceeds the value you filled. By choosing Object limit, you will enter a integer value between 0 and 100 and its unit is %. The result is the date when the Rates average exceeds the value of the percentage limit you filled. For instance, you can discover when the speed of an interface will burst.</p> <p>Estimate If you choose this option, you will enter a date and a time. The result is the curve value at that moment.</p>
Filter	Use Regular Expressions to filter objects.
Filter by device	Select the devices to be analyzed. If you do not select any device, all will be considered.
Filter by group	Select the groups to be analyzed. If you do not select any group, all will be considered.
Data input	It is possible to apply an operation (Addition or Subtraction) to perform on curve value to calculate the trend. You can also choose the data input type (Absolute or Relative [%]). Just to

Field	Description
	select the desired options and enter the value, in bits/s.

3. After filling the form, click **Send** to launch the report.

IP Mapping

The IP Mapper is an mapping agent for IP addresses and names. The user should configure one mapping script and the agent execution interval (in minutes). The script can be configured accessing the option **IP mapping** in **Configuration** → **Scripts**. The IP Mapper need be enabled in **System** → **Parameters** → **IP Mapping** where is also possible configure the execution interval and the maximum storage period.

To visualize the mapped IP addresses and names, access **Historical Data** → **Reports** → **IP Mapping** .

Table 5.28. IP Mapping form

Field	Description
Filter by name	Fill to filter by name.
Filter by ip	Fill to filter by IP address.
Filter by mapping time	Select to use filters by initial and final mapping time.
Initial mapping time	Fill with the desired initial mapping time.
Final mapping time	Fill with the desired final mapping time.

Graph set

The graphset is a graphical report where you can visualize multiple graphs in a grid at the data display area.

Definitions

Operator and **Configurator** users are only able to manage their own graphsets.

Administrator users are able to visualize, edit and delete all graph sets, but cannot create a graph set for a specific user.

Creation

Access the path **Historical data** → **Graph set** → **New graph set** .

Table 5.29. Graph set creation

Field	Description
Name	Graph set name.
Description	Description about the graph set.
Time between slides	Time in seconds to switch slides used in NOC display.
Display in NOC	Select Yes and the graph set will be available in NOC display.

Field	Description
Save at	Path to save an image of the graph set. Example: C:\Users\Telco\Images
Dimensions	Dimensions of saved image.

Adding graphs

1. Access any graph;
2. Click the right mouse button on the graph;
3. Access the option **Add to graph set** on the popup menu and select the desired graph set.

There is another way to add graphs to the graph set. It makes possible to add pie and/or bar charts. Check the procedure below:

1. Access the graph set;
2. Click on + symbol;
3. Fill the fields (object type, objects, graphs, graph type and period);
4. Click on **Insert graph**.

Tip

To desassociate a graph, just click on **X** by his side.


Visualizing a Graph set

1. Access the path **Historical data** → **Graph set**
2. Click on the icon for the desired Graph set, that it's on the tree menu.

Editing a Graph set

1. Click on **Historical data** → **Graph set**.
2. Choose one of the following buttons:
 - **Dependencies** to view and delete graphs from a graph set.
 - **Edit** to change the name and description fields from the Graph set.
 - **Delete** to erase the graph set.

Generating graphs for a Graph set

1. Access the graph set;
2. Click on  symbol;

3. Choose one of the following options:
 - **View graphs** to set an initial time for the graphs displayed on screen.
 - **Save images** to generate and save each graph as one PNG image.
4. Fill the fields:
 - **From:** Initial time of the graph;
 - **Save at:** Path to save an image of the graph set. Example: C:\Users\Telco\Images;
 - **Dimensions:** Dimensions of the image to be saved.
5. Click on **Generate graphs** button.

Circuit

A circuit is a connection between two interfaces of two devices.

Procedure 5.6. Circuit configuration steps

1. Select **Historical data** → **Circuit** → **Circuit** .
2. Click the **New** button and fill the form below.

Table 5.30. New Circuit Form

Field	Description
Name	Circuit Name.
Device A	Device name A.
Mapper A	Mapper Name A.
Interface A	Interface Name A.
Device B	Device name B.
Mapper B	Name of Mapper B.
Interface B	Interface Name B.
Metadata Name	This field is only available if metadata already exists.

Circuits can also be discovered automatically by the system through the CDP and LLDP protocols.

Every circuit is represented on maps which its edges are part.

Route history

Definitions

The Route history allows the configuration of traceroute automatic tests. The user should configure the name of the test, a IP address or hostname and the interval of the test. (At least 5 minutes).

Creation

Access the path **Historical data** → **Route history** → **New route test** .

Table 5.31. Route test creation

Field	Description
Name	Route test name
Host	IP address or hostname.
Interval	Test execution interval, in minutes.

Visualizing a route test

1. Access the path **Historical data** → **Route history** → **List of route tests** .
2. Click on **Details** to display all test executions.
3. Click on **Show** to open the information about the test execution.

You can also visualize the tests information through graphs. Just click on (View graphs). Each graph represents one hop, informing the average latency obtained for the hop in each test execution.

Chapter 6. Configuration

Profiles

Definitions

SLAview profiles were designed to let the user specify which information should be collected and how that information should be processed by the system. Then the profiles can be used for a group of devices or mapped objects.

Profiles allows you to specify collect variables, collect variables based on formulas, which are called summarization variables, and graphs, which contains curves that are formulas based on summarization variables.

Once the profiles are configured, they can then be associated to the devices or mapped objects present in the system. This association can be manual or automatic.

Keep in mind that SLAview already has pre-configured profiles for the most common network monitoring scenarios.

Profile types

SLAview supports 2 profile types, which are device profiles and mapped object profiles. The main difference between these two types is the way the SNMP collector will process the collect variables configured for each type.

Types

Device profiles

The system will collect exactly the specified OID. Example: if you want to collect the sysUpTime OID from a device, then you should configure the OID 1.3.6.1.2.1.1.3.0, NOT 1.3.6.1.2.1.1.3. This means that SLAview will collect instance 0 of the sysUpTime OID.

Mapped object profiles

Slaview maps the instance of the object that should be collected, thus when the SNMP polling takes place, the instance value is appended to the OID. Example: to collect the ifInOctets OID for an interface, you should configure only the OID 1.3.6.1.2.1.2.2.1.10.

Managing profiles

Profiles

- **Create a profile**

Click the New button on the profile configuration screen and specify the parameters below:

Table 6.1. Profile form

Field	Description
Name	Profile name.

Field	Description
Automatic Association	Select Yes if the objects should be automatically associated to the profile. In that case, the appropriate rules should be selected.
Automatic removal	Select Yes if the objects should be automatically removed from the profile. An object will be automatically removed when the profile rules are no longer satisfied.
Collect variables	Enter the collect variables that will be at this profile. You can set them manually (SNMP), use a script (Telco Script), use predefined statistics (ICMP) or use an agent installed on a Windows (THA).
Summarization variables	A summarization variable is defined only once and it can be used one time in each profile. This behavior allows for the definition of different formulas for the same summarization variable. For example, the CPU Utilization variable can be defined on a profile named Cisco with a different formula than on a profile named Extreme .
Graphs	The graph configuration is extremely flexible. Each graph curve is a formula based on summarization variables and a graph can have many curves.

Important

The profile collect variables can be changed at any time, but the removal of one of them will also cause a cascade removal of the summarization variables and graph curves related to that collect variable for the profile and loss of historical data from the removed variables.

Important

When a profile's text is red in the list, it means there is no SNMP response.

Managing collect variables

To access the already existing collect variables, click on Collect button at the profile configuration screen.

You can create a new collect variable clicking on New button.

Tip

Remember that it's also possible to create collect variables using the profile's form.

The variables can be edited using the Edit button and it can be deleted using the Delete.

1. SNMP Collect

- a. Select **SNMP** option;
- b. Set the fields **Name** and **OIDs**. You can fill these fields manually or use the MIB Browser tool (follow the steps below).
 - i. Click the Find OID button to call the MIB Browser tool.

- ii. Choose the desired MIB and click the Select button.
 - iii. Select the desired OID on the MIB navigation tree.
 - iv. Click the OID and, in case you want to test it against a pre-configured device, select the device on the list at the MIB Tester field and click the SNMP WALK button.
 - v. Click the Insert button to transport the data from the selected OID to the OID fields.
- c. Finally, click the Add button in the main window to confirm the operation and the SNMP variable will be added to the profile.

2. Telco Script Collect

- a. Select **Telco Script** option;
- b. Fill the field **Name**;
- c. Choose the desired collector script. To create one, go to **Configuration** → **Scripts**.
- d. Finally, click the Add button to confirm the operation.

3. ICMP Collect

- a. Select **ICMP** option;
- b. Fill the field **Name**;
- c. Choose the desired option: **Jitter**, **Latency** or **Packet drop**;
- d. Finally, click the Add button to confirm the operation.

Tip

To configure the packets, refer to **System** → **Params** → **ICMP** .

4. THA Collect

- a. Select **THA** option;
- b. Fill the field **Name**;
- c. Choose the desired option: **Service status**, **Performance counter** or **SQL counter**;
- d. If you select **Performance counter** or **SQL counter**, fill the counter name;
- e. Fill the service name;
- f. Finally, click the Add button to confirm the operation.

Important

This type of collect only will work in devices which have the Telcomanager Windows Agent installed.

5. OID wildcards

This tool enables the SNMP collector to perform a SNMP_WALK operation on the OID and the result of collect becomes the result of operation.

Check below the currently supported wildcards. All of them, with the exception of %INDEX% and %METADATA_<NAME>%, should be appended to the end of the OID.

Wildcards

%INDEX_WALK_MAX %	This wildcard will fetch the maximum value returned on SNMP_WALK operation.
%INDEX_WALK_MIN%	This wildcard will fetch the minimum value returned on SNMP_WALK operation.
%INDEX_WALK_SUM %	This wildcard will provide the sum of values returned on SNMP_WALK operation.
%INDEX_WALK_AVG %	This wildcard will provide the average of values returned on SNMP_WALK operation.
%INDEX_WALK_COUNT %	This wildcard will provide the quantity of values returned on SNMP_WALK operation.
%INDEX_WALK_LAST %	This wildcard will fetch the value of the penultimate index returned. This is useful for MIBs that return a history of the N last collected values.
%INDEX%	This wildcard can be used at any position in the OID. It will cause the SNMP collector to replace OID index at that position instead of appending the index at the end of the OID.
%METADATA_<NAME> %	This wildcard can be used at any position in the OID. The SNMP collector takes the value of the metadata and replaces it in the wildcard. Where NAME is the name of the metadata.

Summarization variables

To access the already existing summarization variables, click on Summarization variables button at the profile configuration screen.

You can create a new summarization variable clicking on New button.

Tip

Remember that it's also possible to create summarization variables using the profile's form.

The variables can be edited using the Edit button and it can be deleted using the Delete.

1. Create summarization variables

Table 6.2. Summarization variable

Field	Description
Name	Define the variable name.

Field	Description
Unit	Choose a unit. Example: pps, bps, volts.
Percent	Field used for report formatting. Select it for variables that return percentage values.
Per second	Field used for report formatting. Fill this box for variables that return rate values, like traffic for example.

Important

Don't forget to click on **Add** button!

2. Summarization variable formula

At this point, you will be able to define formulas in infix notation using the collect variables configured on the profile.

Select the collect variables and enter the functions to build the formula and click on **Add** button.

- **Definitions**

The [delta_ts] variable represents the time period between each SNMP polling, which is fixed on 300 seconds.

The [delta] function is applied to an OID to perform the difference between the value collected now and the previous collected value.

These [delta_ts] and [delta] fields are used when a variable should be expressed as a rate, like for example, the input traffic on a network interface, for which we have the following formula:

```
((delta("ifHCInOctets") * 8) / $delta_ts$)
```

The [prev] function retrieves the previous value collected for the OID. The following formula demonstrates the utilization of this function:

```
(prev("ifHCInOctets") * 8)
```

In another example, the interface availability is expressed as a percentage value:

```
if(("ifOperStatus" == 1),100,0)
```

On the above formula, if the ifOperStatus variable is equal to 1, the formula will return 100, otherwise, it will return 0.

After you finish editing the formula, click the Save button.

Graphs

1. Create graphs

Table 6.3. Graph

Field	Description
Name	Description that will appear at the graph selection area.

Field	Description
Title	Description that will appear above the graph.
Unit	Description for the y axis of the graph.

Important

Don't forget to click on **Add** button!

2. Create graph curves

After adding a graph to the profile, it will be shown on the form a new section to create the curves for the graphs.

You can add as many graphs you want and you will can configure the curves for each one of them.

- **Table 6.4. Graph curve**

Field	Description
Label	Curve name.
Line type	Line types 1, 2 and 3 have different thickness. Area will fill the area below the curve and Stack will stack the curves.
Color	Curve color.
Plot maximum curve	The maximum curve is plotted at the week, month and year graphs. To plot the maximum curve always, the system considers the minimum resolution data available, which is always the 5 minute data.
Enable trend analysis	Trend analysis default parameters. Refer on trend analysis section for hints on how to configure these parameters.
Formula	Formula in regular infix notation based on summarization variables.

Important

Don't forget to click on **Add** and **Save** buttons!

Objects association

- **Associate objects to profiles**

SLAview supports two profile association methods, which are manual and automatic association. For the last case, it is necessary to create association rules.

Manual profile association

1. Click the Associate (Mapped Object | Device) button on the profile configuration screen and fill the form:

Table 6.5. Associate profile form

Field	Description
Profile	Select the profile on which you wish to associate objects.
Filter	You can provide a string to filter the objects. You have to use Regular Expressions to filter.
Group path filter	You can provide a group path to filter objects associated to the group.
Type	Select the mapped object type. If this is a device profile, this field is not present.

2. Click the Send button
3. The available objects will appear, then move the desired objects to the right box.

Make use of the OID filter if you want to filter an SNMP condition. For example, use the expression `1.3.6.1.2.1.2.2.1.7 = 1` and select the **Use mapped object index** option to filter interfaces with `ifAdminStatus up`.

4. Click the Send button.
5. SLAview will test the results for the filtered objects against all the profile OIDs. If you click the Save now, only the objects that responded to all profiles OIDs will be associated. You can select the **Force association** option for the objects that had errors responding to the profile, so they will also be associated.

Important

You should only use the **Force association** with caution, because SLAview will try to collect OIDs on objects that do not respond to them, which can lead to collect errors.

Tip

Use the **Force association** option only when you know that the object will start responding to the OIDs in a short period of time. Otherwise, create another profile without the faulty OIDs and use that profile on the objects.

Automatic profile association

This process enables operators to easily integrate network elements to SLAview, without having to worry about configuring all the profile associations.

The automatic association process runs every day on two configured hours that can be adjusted at **System** → **Parameters** → **Association agents** → **Automatic profile** .

Procedure 6.1. Create rules

- Create new rules to use on profiles.

Procedure 6.2. Use rules on profiles

1. Click the Edit button for the profile at the profile configuration screen.

2. Select **Yes** on the **Automatic association** select box.
3. Move the rules from the left box to the right box.
4. Click the Save button.

Important

All rules are connected by an AND operator. So, for an object to be associated to a profile, it must abide to all profile rules.

Procedure 6.3. Test the rules

1. Click the Agent button at the profile configuration screen for the desired profile.
2. Fill the form according to the devices against which you wish to test.
3. Click the Send to start the association agent on-demand.
4. Check the agent log file at **System** → **Diagnostics** → **Log Files** → **profiled.log** , to see if the agent is finished.
5. Click the Dependences button for the profile to check if the Rule and SNMP polling tests are ok for the profile objects.
6. If you have errors for the SNMP column, click the Diagnostic button to check what OIDs have errors.

Important

If the object does not match the profile rules, it will not appear at this point because it was not associated to the profile.

System behaviors related to Automatic profiles

- The lack of SNMP response for any profile OID on a object at the first test will avoid the SNMP polling on that object until the object responds for that OID on the next test. The graphs for that object will indicate the failure.
- If an object stops responding for an OID during normal system operation, the OIDs that responded will continue to be collected and the failure will be indicated at the object's graphs.
- If during normal system operation an object fails for a rule, the SNMP polling for that object will be interrupted.

Exporting Profiles

The profile export tool enables the user to export all profile configurations from SLAview to a file and then import back the configurations. This feature is very useful to import predefined profiles available from Telcomanager consultants team.

1. Click **Configuration** → **Profiles** → **Show** .
2. Click on **Export** button.

Tip

You can export all your profiles to an unique file using the **Export all** button.

QoS

Definitions

The QoS monitoring module was specifically developed to work with devices that support the CLASS-BASED-QoS MIB from Cisco System, therefore it will only work for Cisco devices that support that MIB.

QoS can be monitored on other systems, but they will have to be mapped through the SLAview generic mapper.

Using a specific mapping agent, SLAview is able to identify all QoS policies applied for an interface, create the appropriate profiles to monitor those policies and perform profile association.

Enabling the QoS feature

- Access **System** → **Parameters** → **QoS** and enable the QoS Cisco Profile, so SLAview will be enabled to create the QoS profiles automatically.

Enabling QoS monitoring on interfaces

1. Access **Configuration** → **QoS** and create a new **QoS** clicking the New button.
2. Select the desired interfaces/rules and monitorings and click the Save button.

Table 6.6. QoS Wizard form

Field	Description
Name	Name to identify a QoS Wizard.
Automatic association	Select Yes if the interfaces should be automatically associated to the profile. In that case, the appropriate rules should be selected. Otherwise , select the interfaces to be monitored.
Monitoration	Select QoS monitors.

The Automatic association agent for QoS profiles runs every day on two configured hours that can be adjusted at **System** → **Parameters** → **Association agents** → **Automatic association agent for QoS profiles** .

The next time the Cisco Policy Mapper process and the Cisco auto QoS Profile processes run, they will search for QoS policies on the interfaces and try to create the monitorings respectively.

This feature collects information about bandwidth limit and it is shown on graph, if there is configured class.

Important

The mentioned processes run every hour.

Collectors

This section should be used if you are deploying the system in distributed architecture mode.

For more details on distributed architecture deployment, refer to distributed architecture parameters section.

Table 6.7. Collector form

Field	Description
Name	Name to identify a collector appliance.
Key	Fill a string key. This string should match the collector key field at the System → Parameters → Distributed architecture menu in the collector appliance.
IP address	IP address that the collector will use to access the central appliance.
Exporter IP/Mask	IP address used by the collector to receive flows from routers. This IP address is used in case you want the system to continue to receive flows if a collector appliance crashes.
Password	This password should match the password field at the System → Parameters → Distributed architecture menu in the collector appliance..
Backup collector	Collector that will be the backup for this collector in case of failure.
Devices	Devices that this collector will collect.

Import collectors file

To import a file of collectors, access **Configuration** → **Collectors**.

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

A import devices file has the following fields:

Table 6.8. Fields from collectors file

Field	Description
Name	Possible characters for name field.
Key	Alphanumeric characters.
IP Address	IP Address. Ex.: 10.0.0.1
Password	Possible characters for password field.

Add collectors metadata

To access the metadata configuration page, access **Configuration** → **Collectors** 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 6.9. 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 collector, access the collectors list and click on **Metadata** button beside the collector that will be configured.

Then, fill the metadata according to its type.

Objects

In this section you can access and edit the already configured objects and create new ones.

For some object types, you have the option to upload a configuration file. This means you can configure more than one object at once.

Importing object files

1. Access **Configuration** → **Objects** and click the Import button for the desired object type.
2. Upload the formatted file according to the instructions on screen.
3. Click the Add button.
4. Adjust the configurations and click the Save button.

Mappers

Mappers are used to discover objects related to a device using the SNMP protocol or a Telco script. Examples of those objects are: network interfaces, processors, memory banks, storage units, probes and so on.

Mappers can have Devices automatically associated to them, considering Rules that must be set as conditions.

Procedure 6.4. Creating a mapper

1. Select **Configuration** → **Mappers**.
2. Click the New item button and fill the form as detailed below:

Table 6.10. Mapper form

Field	Description
Name	Mapper name
Icon	Image that will be exhibited next to the objects discovered by this mapper at the tree menu. See step 3 for instructions on customizing this image.
Type	Choose SNMP , Telco Script , Process or Windows service .
Script	Select the script. Create one in Scripts section
Automatic removal	If you want the objects mapped by this mapper to be removed after a certain number of consecutive days in which they are missing, select Yes and fill the number of days.
Include prefix	Include the mapper name as a prefix for objects discovered by this mapper.
OID instance used as object name	Mark this option if instead of populating the object name with the OID value, the mapper should populate it with the OID instance. This option should be used for objects that do not have an OID whose values can represent them. So you can use a statistics OID and map the object instances with this option.
Network interface	Mark this option if the objects that will be discovered are network interfaces. This will cause the mapper to fetch interface properties like ifAlias and ifSpeed.
Probe	Mark this option if this mapper is meant to discover probes, so the probes will also be exhibited at Historical Data → Probes menu.
Name	Name of the OID to be used for mapping objects.
OID	OID that will be used.
MIB	OID MIB.
Filter by SNMP collect	Filtering by SNMP collect response.
Devices association	Enable automatic device association to this mapper considering Rules. When enabled the form will show auto removal option that will remove the associated devices when the conditions are not met anymore
Devices	Select the devices that will be associated to the mapper. If you select Process as mapper type, once you have moved the object from the left to the right box, click on it and then click on List process . After this, select the desired processes.

Tip

Under the section Mapping Setup, you should specify an OID (Object Identifier) from a device MIB (Management Information Base) where the system can find unique instance names as the returned values, so the objects can be identified. This OID can be loaded using the MIB Browse tool by clicking the Search OID button.

Use the Find OID button to browse the MIB and fill the last three form fields.

3. Configure the mapper icons.
 - a. Select the **Configuration** → **Mappers** menu and click the Change icons button.
 - b. Click the New icon button.
 - c. Fill the mapper name and upload a icon for each object condition.
 - d. Click the Send button.

Cross OID mapping

This feature allows you to create a mapper specifying 2 OIDs. The mapper will then find the values of the first OID and use then as indexes to find a value in the second OID.

So the mapper will map the index of the first OID with the value of the second OID.

This mapper can be used, for example, to map Cisco CPUs, where you can specify the following OIDs:

```
1.3.6.1.4.1.9.9.109.1.1.1.1.2;1.3.6.1.2.1.47.1.1.1.1.7
```

The first OID is the cpmCPUTotalPhysicalIndex from the CISCO-PROCESS-MIB and the second is the entPhysicalName from the ENTITY-MIB, where you can find the name of each CPU.

Associating devices to mappers

After configuring a new mapper, you should associate it to the devices where the objects should be discovered. This association can be done at each device configuration or by clicking the Devices association button at the mappers list.

Exporting and importing mappers

The **Export** button exports all mapper configuration to a file. To import back the configuration, you can use the **Import** button and then download this file.

Maintenance

You can create a maintenance to suppress ICMP alarms during maintenance windows in your infrastructure.

ICMP polling

SLAview ICMP polling interval is flexible and configured through the ICMP polling templates.

Procedure 6.5. Activating device polling

1. Associate the device to an alarm profile that has the **Not responding ICMP** alarm. (see **Historical data** → **ALARMmanager** → **Profiles**) .
2. Go to **Configuration** → **ICMP Polling** and create a new polling template where you will:
 - Define the days and hours of the week for the polling.
 - Define the polling interval.
 - Associate the devices that will use this template.

Add ICMP Polling metadata

To access the metadata configuration page, access **Configuration** → **ICMP polling** 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 6.11. 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 ICMP polling, access the ICMP polling templates list and click on **Metadata** button beside the template that will be configured.

Then, fill the metadata according to its type.

EPM (Extended Processing Module)

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

It needs to be enabled at **System** → **Parameters** → **EPM** .

EPM is a scalable solution for the amount of users accessing the system by the web interface, visualizing graphics e summarized data reports. The summarized data are replicated to the EPM machines making data access faster and data redundant.

1. Click **Configuration** → **EPM**.
2. Click New to create a new EPM entry.
3. Fill the name and IP adress fields.
4. Set administrative status.
5. Click Save.

Probe types

The probe type object is intended to define the fields that will be provisioned on the remote device and also available in the probe configuration form.

Procedure 6.6. Configuring new probe types

1. Select **Configuration** → **Probe types**. Click the new button to define a new type.
2. Fill the form according to the instructions below:

Table 6.12. Probe type form

Field	Description
Name	Probe type name. Ex: Cisco/IP SLA jitter
Description	Descriptive text.
Attributes	<p>Click the Add button for each attribute necessary to configure this probe. Ex: destination IP, number of packets...</p> <p>Name Text identifying the attribute. Ex: destination IP</p> <p>Provisioning Code Text to be used in the provisioning scripts. Ex: ip_dst</p>

3. **Create a mapper to map the probe objects**
 - Select **Configuration** → **Mappers** and configure the mapper with and OID that is unique and select and fill the **Probe** field. Ex: for Telco Probes the OID used is tmTAPName, which represents the probe name.
4. **Associate the new mapper to the device**
 - a. When you are creating the new mapper at **Configuration** → **Mappers**, configure **Devices association** according to your necessity. You can enable the Automatic Association and Automatic Removal or select specific devices.
 - b. To check the association, click Dependencies at **Configuration** → **Mappers**.

- c. Now, when a new probe is provisioned in associated devices, the system will discover them.
5. **Create a provisioning script**
 - Select **Configuration** → **Scripts**. Click the New button and create a script for the new probe type using the attributes defined on step 2 (see provisioning scripts syntax).
 6. **Create a new profile**
 - a. Select **Historical data** → **Probes** → **Wizard** and create a new probe using the probe type created.
 - b. Associate the profile to the probe at **Historical data** → **Profiles** → **Mapped object** , Associate mapped object button.

Add probe types metadata

To access the metadata configuration page, access **Configuration** → **Probe types** 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 6.13. 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 probe type, access the probe types list and click on **Metadata** button beside the probe type that will be configured.

Then, fill the metadata according to its type.

Rules

Creating rules

1. Select **Configurations** → **Rules** and select the kind of rule at left, if it's Device, Mapped object or Groups.

- Click the New button to create a new rule and fill the form:

Table 6.14. Automatic profile rules

Field	Description
Name	Rule name.
Description	Rule description
Database field filter	Filter based on database fields. For instance, the Name field is the object name and the Mapper field (only for mapped object rules) is the mapper name.
Metadata field filter	Filter based on metadata fields. Choose the device metadata (for device rules) or the mapped object metadata (for mapped object rules).
Filter by SNMP collect	Filter based on OIDs that will be polled when the rules are tested. Select the option Use mapped object index when using OIDs that should be tested against mapped objects, like, for example, ifConnectorPresent.

No Response filter

The 'No Response' filter, that is located in 'Filter by SNMP collect', consists in validate a object in case it returns a specific error message.

To use it, you must choose the 'No Response' operator in the filter. In the 'value' field you have to use one of this values:

- \$nosuchobject\$ - It's used to validate 'No such object' response from an object.
- \$nosuchinstance\$ - It's used to validate 'No such instance' response from an object.

Trap Receiver

SLAview is able to receive, parse and generate alarms on ALARMmanager based on SNMPv1 and V2 traps.

This module is composed by trap receiver, trap logic, trap alarm and a received trap report.

A trap is identified by its OID. When a trap is received and if there is a trap receiver created using the same OID, the trap receiver's logics will be evaluated to decide if it is necessary generate an alarm occurrence. This occurrence will only be generated if there is an alarm using the trap receiver's logics.

Trap Receiver Configuration

Select **Configuration** → **Trap receiver**. Click the New to create a new trap receiver.

Table 6.15. Trap Receiver Configuration

Column	Description
Name	Name of the trap receiver.

Column	Description
Description	Description about the trap receiver.
OID	OID to identify the trap. You can click the OID Search to navigate through the MIB browser.
MIB	MIB that holds the OID.
Identify device by source	Choose if the device that generated the trap will be identified by source (IP address) or not. If not, you must choose an OID to associate to a devices field.'
Device identification - OID	OID to identify the device.
Device identification - Field	Field to identify the device.

Click **Save** to create the trap receiver.

Important

The trap may take about 5 minutes to be recognized. It happens because this is the time the system needs to update the new configuration.

Trap Receiver Logic

Trap receivers may have as many logics as you associate to it. Each logic may be associated to an alarm (see ALARMmanager section), to arm or disarm it.

Select **Configuration** → **Trap receiver**.

Click logics to list the logics from one trap receiver in the list.

Click New to create a new logic.

Table 6.16. Trap Receiver Logic

Column	Description
Name	Name of the logic.
Description	Description about the logic.
Formula	Refer to alarm formula.
Object type	Choose Device or Mapped Object. If Mapped Object is selected, you have to select a mapper, an OID and a Field to identify the object.
Mapper	Mapper to identify the mapped object.
OID	OID to identify the mapped object.
Field	Field to identify the object.

Trap Alarm

Refer to ALARMmanager alarms.

Trap Receiver Report

This report lists informations about all the traps received by the system, using filters to generate the content.

Table 6.17. Trap Receiver Report

Column	Description
Begin	Trap received starting from begin.
End	Trap received up to end.
Source	Source of the traps. By IP or hostname.
Varbind	Trap varbind.
Output format	HTML or CSV.
Number of lines	Number of lines in report.

Trap Receiver Logic Formula

The expressions in the **Logic Formula** field are written in regular infix notation.

You should construct the formulas using the following rules:

- Use round brackets "(" for operator precedence.
- Use the AND and OR logical operators.
- Use the ==,<,>,<=,>= comparison operators.

Procedure 6.7. Formula input

1. Select a varbind above the formula box and click Add the transport it to the box.
2. Edit the formula in the formula box to form the desired expression.

Add trap receiver metadata

To access the metadata configuration page, access **Configuration** → **Trap Receiver** 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 6.18. 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 trap receiver, access the trap receiver list and click on **Metadata** button beside the trap receiver that will be configured.

Then, fill the metadata according to its type.

Scripts

You can create and execute scripts of the following types: **Mapper**, **Collector**, **Provisioning** and **IP mapping**.

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.
- **tmlBGP.addToBlackHole**: Adds the subnet to the blackhole.
- **tmlBGP.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.

Collector Script

Create a Collector Script to perform a Telco Script Collect.

This type of script provides you a way to manipulate your collect results.

The collector script can be executed in the **Simple** or **Advanced** mode. You can change this mode in the upper right-hand corner of the screen.

Advanced mode

In this mode, the device and its mapped objects data can be collected in a unique execution. In order to do it, the collect scripts have to return a table and it has to follow the structure:

- First level: Use **'dev'** for device collect variables and use **'mobj'** for mapped object collect variables.
- Second level: Mapper name. This level is only necessary when the first level is **'mobj'**.
- Third level: Mapped object ifDescr. This level is only necessary when the first level is **'mobj'**.
- Fourth level: Collect variable name.

So, the table follows the model:

```
result = {}
result['dev'] = {}
result['dev']['Total storage'] = storageTotal
result['dev']['Available storage'] = storageAvailable

result['mobj'] = {}
result['mobj']['Interface'] = {}
result['mobj']['Interface']['net0'] = {}
result['mobj']['Interface']['net0']['ifSpeed TCS'] = speed
```

```
-- "Total storage", "Available storage" and "ifSpeed TCS" are
   the collect variable names
-- "Interface" is the mapper name
-- "net0" is the mapped object ifDescr
```

Check the example below:

```
----- begin script -----

h = params['ipaddr']
c = params['snmp']['community']
v = params['snmp']['version']

mobjs = params['mobj']
-- mobjs = { [mapper] = { [name] = { ['ifindex'] = ifIndex,
  ['description'] = ifAlias } } }

t = tmlSnmp.snmpGet(h,c,v,{[1] = '1.3.6.1.2.1.1.5.0'})

ret ={}
ret['dev'] = {'sysName' = t['1.3.6.1.2.1.1.5.0']}

t = tmlSnmp.snmpWalk(h,c,v,{[1] = '1.3.6.1.2.1.2.2.1.2',
  [2] = '1.3.6.1.2.1.2.2.1.5'})

descr = t['1.3.6.1.2.1.2.2.1.2']
speed = t['1.3.6.1.2.1.2.2.1.5']

ret['mobj'] = {'Interface' = {}}

for key,value in pairs(descr) do
  ret['mobj']['Interface'][value] = { ['ifDescr'] = value,
  ['ifSpeed'] = speed[key] }
end

return ret

----- end script -----
```

Simple mode

In this mode, the collect scripts have to return a value.

Take the following examples to create your Collector scripts using Lua Scripting Language:

```
----- begin script -----

srcaddr=nil
```

```

timeout=3000

n = tmlPing.pingNew({srcaddr=srcaddr,timeout=timeout,details=false})

-- 'details' is an optional parameter

p = n:run({{ipaddr='10.0.0.99',nbpkts=10,interval=10,pktsize=64}})

tmlDebug.vardump(p)

t = tmlSnmp.snmpGet('10.0.0.99','public','v2c',
  {[1] = '1.3.6.1.2.1.1.3.0'})

-- Values will be stored in t['1.3.6.1.2.1.1.3.0']

return t['1.3.6.1.2.1.1.3.0']

----- end script -----

----- begin script -----

db = tmlMsSql.msSqlNew({host=%HOST%,user=%USER%,passwd=%PASSWORD%,
  dbname=%DBNAME%})
rows = db.query(db, %QUERY%)

for i,row in pairs(rows) do
  value = row[%COL_NAME%]
done

-- DBNAME, QUERY and COL_NAME are strings

----- end script -----

----- begin script -----

t = tmlSnmp.snmpWalk('10.0.0.99','public','v2c',
  {[1] = '1.3.6.1.2.1.2.2.1.2'})

str=""

val = t['1.3.6.1.2.1.2.2.1.2']

for key,value in pairs(val) do
  str = str .. value .. "\n"
end

tmlDebug.vardump(val)

return str

```

```
-- Each value is table with the returned index and its
value ( ['idx'] = ['value'] )
```

```
----- end script -----
```

Check below the previous example using parameters:

```
----- begin script -----
```

```
h = params['ipaddr']
c = params['snmp']['community']
v = params['snmp']['version']

t = tmlSnmp.snmpWalk(h,c,v,{[1] = '1.3.6.1.2.1.2.2.1.2'})

str=""

val = t['1.3.6.1.2.1.2.2.1.2']

for key,value in pairs(val) do
    str = str .. value .. "\n"
end

tmlDebug vardump(val)

return str

-- Each value is table with the returned index and its
value ( ['idx'] = ['value'] )
```

```
----- end script -----
```

```
----- begin script -----
```

```
h = params['ipaddr']
c = params['snmp']['community']
v = params['snmp']['version']
timeout = params['snmp']['timeout']
retries = params['snmp']['retries']
mpp = params['snmp']['max_per_packet']
mpps = params['snmp']['max_pps']
w = params['snmp']['window']
port = params['snmp']['port']

t = tmlSnmp.snmpGet2({host = h,community = c,
version = c, timeout = timeout,retries = retries,
max_pps = mpp, max_per_packet = mpps, window = w,
port = port},{[1] = '1.3.6.1.2.1.1.3.0'})
```

```
tmlDebug vardump(t['1.3.6.1.2.1.1.3.0'])

return t['1.3.6.1.2.1.1.3.0']
```

```
----- end script -----
```

IP mapping Script

Create a custom script that will be used by the **IP Mapper** to associate names with IP addresses.

The script has to return a table. Each entry in this table is formed by other table, which has to have the following entries:

- name
- ipaddr

Important

All returned fields may be string.

Take the following example to create your IP mapping script using Lua Scripting Language:

```
----- begin script -----
```

```
r = {}

r[1] = {['name'] = 'name1', ['ipaddr'] = 'ipaddr1'}
r[2] = {['name'] = 'name2', ['ipaddr'] = 'ipaddr2'}
r[3] = {['name'] = 'name3', ['ipaddr'] = 'ipaddr3'}

return r
```

```
----- end script -----
```

Mapper Script

Create a custom script, associate it to a Mapper and map a device.

The script has to return a table. Each entry in this table is formed by other table, which has to have the following entries:

- name
- description
- version
- index

Important

All returned fields may be string.

Take the following examples to create your mapper scripts using Lua Scripting Language:

```
----- begin script -----
r = {}

t = tmlSnmp.snmpWalk('10.0.0.1','erlang2','v2c',
{[1] = '1.3.6.1.2.1.2.2.1.2', [2] = '1.3.6.1.2.1.2.2.1.5',
 [3] = '1.3.6.1.2.1.2.2.1.3', [4] = '1.3.6.1.2.1.31.1.1.1.18'})

ifDescr = t['1.3.6.1.2.1.2.2.1.2']
ifSpeed = t['1.3.6.1.2.1.2.2.1.5']
ifType = t['1.3.6.1.2.1.2.2.1.3']
ifAlias = t['1.3.6.1.2.1.31.1.1.1.18']

for key,value in pairs(ifDescr) do
  r[key] = {'name' = value,['description'] = value,
  ['version'] = '1',['index'] = key, ['alias'] = ifAlias[key],
  ['iftype'] = ifType[key], ['speed'] = ifSpeed[key]}
end

tmlDebug.vardump(ifDescr)

return r

----- end script -----
```

Check below the previous example using parameters:

```
----- begin script -----

h = params['ipaddr']
c = params['snmp']['community']
v = params['snmp']['version']
r = {}

t = tmlSnmp.snmpWalk(h,c,v,{[1] = '1.3.6.1.2.1.2.2.1.2',
 [2] = '1.3.6.1.2.1.2.2.1.5', [3] = '1.3.6.1.2.1.2.2.1.3',
 [4] = '1.3.6.1.2.1.31.1.1.1.18'})

ifDescr = t['1.3.6.1.2.1.2.2.1.2']
ifSpeed = t['1.3.6.1.2.1.2.2.1.5']
ifType = t['1.3.6.1.2.1.2.2.1.3']
ifAlias = t['1.3.6.1.2.1.31.1.1.1.18']

for key,value in pairs(ifDescr) do
```



```

r[key] = {'name' = value, ['description'] = value,
 ['version'] = '1', ['index'] = key, ['alias'] = ifAlias[key],
 ['iftype'] = ifType[key], ['speed'] = ifSpeed[key]}
end

```

```

tmlDebug.vardump(ifDescr)

```

```

return r

```

```

----- end script -----

```

Check more examples:

```

----- begin script -----

```

```

h = params['ipaddr']
c = params['snmp']['community']
v = params['snmp']['version']
timeout = params['snmp']['timeout']
retries = params['snmp']['retries']
mpp = params['snmp']['max_per_packet']
mpps = params['snmp']['max_pps']
w = params['snmp']['window']
port = params['snmp']['port']

r = {}
t = tmlSnmp.snmpWalk2({host = h, community = c,
 version = v, timeout = timeout, retries = retries,
 max_pps = mpps, max_per_packet = mpp, window = w,
 port = port}, { [1] = '1.3.6.1.2.1.2.2.1.2',
 [2] = '1.3.6.1.2.1.2.2.1.5', [3] = '1.3.6.1.2.1.2.2.1.3',
 [4] = '1.3.6.1.2.1.31.1.1.1.18'})

ifDescr = t['1.3.6.1.2.1.2.2.1.2']
ifSpeed = t['1.3.6.1.2.1.2.2.1.5']
ifType = t['1.3.6.1.2.1.2.2.1.3']
ifAlias = t['1.3.6.1.2.1.31.1.1.1.18']

```

```

for key,value in pairs(ifDescr) do
  r[key] = {'name' = value, ['description'] = value,
 ['version'] = '1', ['index'] = key, ['alias'] = ifAlias[key],
 ['iftype'] = ifType[key], ['speed'] = ifSpeed[key]}
end

```

```

tmlDebug.vardump(t['1.3.6.1.2.1.2.2.1.2'])

```

```

return r

```

```

----- end script -----

```

```

----- begin script -----

h = params['ipaddr']
c = params['snmp']['community']
v = params['snmp']['version']

r = {}

t = {'ip' = h, 'community' = c, 'snmpversion' = v}
map = tmlUtils.processMapper(t)

for k,v in pairs(map) do
    tmlDebug vardump(v)
end

return map

----- end script -----

```

Provisioning Script

The provisioning script performs a sequence of requests and expected replies with the device.

This type of script can be written on 3 modes: **Text**, **Lua** and **Send/Expect**.

Text Mode

In this mode, the script will be basically composed of all commands that are executed on a device.

Lua Mode

In this mode, it is possible to customize the provisioning.

It provides the variable **params['connection']** to be used to communicate with the device being provisioned.

Send/Expect Mode

This is widely used mode in provisioning.

Check below the script Probe IP/SLA ICMP Echo [ip sla monitor] written using this mode followed by its description.

```

send: enable
expect: pass
send: %enable_passwd%
expect: #
send: configure terminal
expect: (config)

```

```

send: ip sla monitor %probe_index%
abort: invalid;#
send: type echo protocol ipIcmpEcho $ip_destination$ source-ipaddr $ip_source$
abort: incomplete;#
send: tag %probe_name%
expect: #
send: frequency 300
expect: #
send: exit
expect: (config)
send: ip sla monitor schedule %probe_index% life forever start-time now
expect: #
send:exit

```

- The **send** fields are commands to be executed in the devices.
- The **expect** fields are strings expected from the devices.
- The **abort** fields are used to insert a string that will cause the script finalization if received from the device. The text inserted after the ; character will work the same way the expect field.
- The fields enclosed with the \$ character are fetched from the database based on the provisioning codes used to configure probe types. They are only used in probe creation.
- The fields enclosed with the % character are special wildcards. The supported wildcards are listed in the next section.

Wildcards

Table 6.19. 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.
%probe_index%	Snmp index from the probe
%probe_name%	Name field from the probe configuration form.
%collector_ip%	IP address of the new collector when the current collector is down in distributed architecture.
%current_collector_ip%	IP address of the current collector in distributed architecture.

Device Credential

Many devices use the same SNMP and Connection configuration.

It's possible to create a credential for these configuration parameters and then associate it to the devices that have the same configuration.

To create a new credential, access **Configuration** → **Device Credential** → **New device credential** or **Configuration** → **Device Credential** → **Device Credential** and click on **New** button.

Table 6.20. Device credential form

Field	Description
Name	Define the credential name.
Protocol	Choose SNMP , SSH or Telnet .
SNMP Version	Choose the SNMP version. Possible values are: SNMP v1 or SNMP v2c Specify an SNMP community SNMP v3 Specify the authentication type and its parameters
SNMP community	Enter the SNMP community.
SSH port	Enter the SSH port. The default value is 22 .
Telnet port	Enter the Telnet port. The default value is 23 .
User	User to be used to access the device. This string is available as a wildcard %username% for provisioning scripts.
User password	Password to be used to access the device. This string is available as a wildcard %passwd% for provisioning scripts.
Enable secret	Enable password to be used to access the device. This string is available as a wildcard %enable_passwd% for provisioning scripts.
Devices	Associate the devices that will use the credential.

Add device credential metadata

To access the metadata configuration page, access **Configuration** → **Device credential**, click on **Device credential** 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 6.21. Metadata fields

Field	Description
Name	Enter the metadata name.
Description	Describe the metadata (optional).

Field	Description
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 device credential, access the device credential list and click on **Metadata** button beside the credential that will be configured.

Then, fill the metadata according to its type.

Syslog Filter

The syslog filters can be used as Activation rules in **Syslog alarms**.

To create a new Syslog filter, access **Configuration** → **Syslog filter** → **New syslog filter** or **Configuration** → **Syslog filter** → **Syslog filter** and click on **New** button.

Table 6.22. Syslog filter form

Field	Description
Name	Enter the filter name.
Description	Enter the filter description.
Facility	Define the Syslog Facility.
Severity	Define the Syslog Severity.
Message	Define the Syslog Message.

Add syslog filter metadata

To access the metadata configuration page, access **Configuration** → **Syslog filter**, click on **Syslog filter** 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 6.23. Metadata fields

Field	Description
Name	Enter the metadata name.
Description	Describe the metadata (optional).
Datatype	Choose the metadata type: Text , Integer or Enum (Enumerate).

Field	Description
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 syslog filter, access the syslog filter list and click on **Metadata** button beside the filter that will be configured.

Then, fill the metadata according to its type.

Chapter 7. Tools

Discovery

The discovery feature is used to discover every host in a network. Click **New** button to use this function.

Table 7.1. Discovery fields

Field	Description
Generate report Save template	Choose Generate report for a one time report or Save template to save the report as a template.
Send e-mail with unregistered ips	Once Save Template and Schedule Template are selected, this field will be available in the form. Select it to send emails to the template owner if the report discovers any hosts not registered in the tool.
IP/Mask	Fill the IP/Mask.
IP address list excluded from the analysis	Enter a list of IPs, separating them by comma (,).
Group IPs from the same host	Select the option Yes to display the IPs that belong to the discovered device.

Tip

If **Send e-mail with unregistered ips** is selected, 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.

Click **Send** button to start the discovery function.

When the process is finished, is possible to add any of the discovered hosts as a device. You can select individually, use the **All** button to select all of them at one time or use the **All SNMP** button to select only those who have SNMP response according to SNMP credentials.

After this, click on **Select** button, fill the fields and click on **Add**.

MIB Browser

You can explore all the MIBs installed in the system using MIB browser. Those elements are listed on the screen with filters applied.

If you want to explore a MIB, click the Select button in the right side.

External Software

Telcomanager Windows Collector

Download the executable **Telcomanager Windows Collector** to install the Netflow collector for Windows.

It replicates all the Netflow packets received by a Windows machine to a TRAFip appliance.

Telcomanager Host Agent

Download the executable **Telcomanager Host Agent** (THA) to install it on Windows.

This agent collects information about the running processes. It will be necessary to use THA collect.

Chapter 8. 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 8.1. 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 .

Field	Description
SMS	Celular phone number to send alarms using the SMPP protocol or celular@teste.com to send short emails with alarms. The system can also send SMSs through the integration with a web portal. To configure the SMS Server access System → Parameters → SMS Server
Safe mode permission	This option is only available to Administrator users. Select Yes so the user will can enable the safe mode at System → Parameters → Safe mode . Only one user will have this power.
Enable Favorites	Enable Favorites feature.
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 .
Hide objects with no profile	Hide mapped objects that are not associated to a profile to the user.
Enable advanced alarm report	Enable advanced alarm reports to that user.
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.

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 8.1. Managing user groups

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

Table 8.2. User form

Field	Description
Name	User group name.
Description	User group 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 8.2. Managing user profiles

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

Table 8.3. 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.
Groups	Select the groups that the profile users will be able to access.
Layer	Select the layers that the profile users will be able to access in FRONTlayer system.
Service alarms	Associate service alarms to this profile.

Safe mode log

Through this log, it is possible to discover when and which user enabled or disabled the safe mode at **System** → **Parameters** → **Safe mode** .

Table 8.4. Safe mode log form

Field	Description
Initial date	Enter the initial period time in the format dd/mm/yyyy.
Final date	Enter the final period time in the format dd/mm/yyyy.
User	Filter the user that changed the safe mode status.

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 8.5. 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.
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 8.6. FTP server form

Field	Description
IP version	Select IPv4 or IPv6.
Backup Server	IP address of the backup server.
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 8.7. 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.

Field	Description
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 8.8. 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 8.9. 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 8.10. Automatic association agent form

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

Automatic alarm profile

Set two moments within the day to execute the automatic alarm profile association.

Automatic association agent for groups

Define the time to start the automatic association for groups.

Automatic association agent for mappers

Define the time to start the automatic association for mappers

Automatic association agent for QoS profiles

Define the time to start the automatic association for QoS profiles.

Automatic profile

Set two moments within the day to execute the automatic profile association agent.

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 8.11. 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 8.12. 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 8.13. 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 8.14. 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 8.15. 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 .
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.

Field	Description
Maximum summarization statistics storage period	This is related only to the summarization processes. This statistic can be checked at System → Diagnostics → Summarizer .

Custom Collector

Set the allowed number of simultaneous collects.

Table 8.16. Custom collector form

Field	Description
Maximum number of simultaneous collects	Choose a integer smaller than or equal to 50. The default is 10 .

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 8.17. 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

Field	Description
	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.
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 8.18. dbn0/Altaia integration form

Field	Description
Enable dbn0/Altaia integration	Choose Yes or No .
Server IP Address	Enter the server IP address.

Field	Description
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 8.19. 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 8.20. EPM form

Field	Description
Enable EPM	Select this option if you deserve to enable this module of the monitoring solution.

Field	Description
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 8.21. Expiration warning form

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

Exporting

Syslog

Syslog is a monitoring mechanism that sends messages when specific events are triggered. These messages are composed, basically, of ip address, timestamp and the log message.

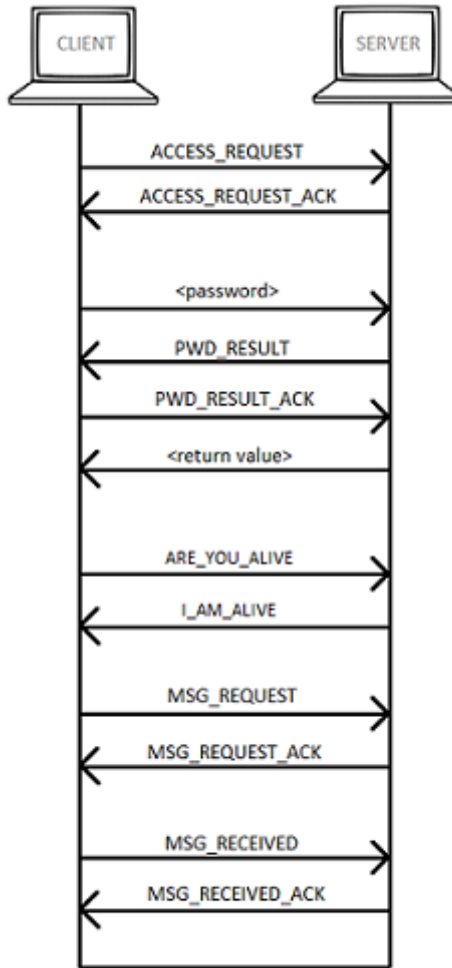
This mechanism offers more detailed information when compared to SNMP traps due to the fact that it sends messages by each device.

TRAFip has a exporter agent which sends these Syslog messages from the associated devices.

It's required to have a communication between the host that will receive the Syslog messages and the TRAFip. To configure which hosts will be enabled to access the Syslog export, click on **Add** button and specify the host and the password.

In **Filter by source**, you will configure the devices to be heard, it means they will send Syslog messages. To enable a device, transport it to the right side of the box using the '>>>' button.

The following image illustrates the communication protocol between client and server:



Syslog protocol

Table 8.22. Syslog protocol

Message	Description
ACCESS_REQUEST	Access request sent to server.
ACCESS_REQUEST_ACK	Server confirms the message sent by client was received.
<password>	It is the password set by you in Password field at System → Parameters → Exporting → Syslog form.
PWD_RESULT	Password authentication.
PWD_RESULT_ACK	Server confirms the message sent by client was received.
<return value>	It is the authentication return value. If the host is authenticated, return 1. Otherwise, the connection is closed.

Message	Description
ARE_YOU_ALIVE	Checks if the exporter agent is active and running.
I_AM_ALIVE	Confirms the exporter agent is active and running.
MSG_REQUEST	Client requests to server to send the messages.
MSG_REQUEST_ACK	Server confirms the message sent by client was received.
MSG_RECEIVED	Client confirms the messages were received.
MSG_RECEIVED_ACK	Server confirms the message sent by client was received.

GIS map

It's necessary to register the **MapQuest AppKey** to visualize a georeferenced map on Mapview.

To choose the plan that best meets your needs access <https://developer.mapquest.com/plans> .

Grapher

Adjust the grapher parameters.

Table 8.23. 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 8.24. 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.

Interface customization

You can customize how the devices will be displayed on **Historical Data** → **Devices** → **Device** tree menu.

To do this, just fill the **Device formula name** field with what you desire to be shown on menu.

The formula has special tags which use the device information. Here they are:

Table 8.25. Device formula name

Tag	Description
%n	Refers to device name .
%a	Refers to device management IP address .
%t	Refers to device type .
%m	Refers to device manufacturer .
%d	Refers to device type (Camera, Firewall, Router, Server, Switch or Wireless).

In the **List interfaces by** field you can select the **Description** option to display the objects mapped by the object name or select **Label** to display them with a specific name.

The assignment of the **Label** is done manually.

Access **Chosen device** → **Chosen Mapped object** → **Properties** to fill the **Label** field with the name that will represent the object.

This **Label** must have a unique key.

IP mapping

For more details about IP mapping, refer to IP Mapper section.

Table 8.26. IP Mapper configuration parameters form

Field	Description
Enable IP Mapping	Once Yes is selected, the IP mapping agent will be enabled. Otherwise, it will not execute.
Execution Interval	Set the interval between mapper executions.
Configuration history storage period	Set the period for storing the history of IPs and names associations performed by the mapper.

ICMP

ICMP polling process configuration. The process responsible for ICMP polling is the ICMPAgent

The ICMP polling runs every minute, but to avoid unnecessary pollings, the system has a damping process that causes the polling frequency to decrease with time and it will go back to normal if the element starts responding again.

Table 8.27. ICMP process parameters form

Field	Description
Number of failures to start damping	After this number of consecutive failures, the damping process will start.
Interval increase after each failure	After the device is placed in damping mode, this number is added to the number of intervals between polling each time the device is polled.
Maximum interval allowed in damping	This is the maximum number of times that the ICMPAgent will skip this device polling, even in damping mode. When this condition is reached, the ICMPAgent will generate an occurrence for the alarm Maximum damping reached each minute and for each device.
ICMP timeout	Timeout for the ICMP polling.
ICMP test	Choose Yes for host up and down tests.
Retry ICMP test	Choose Yes to do new ICMP tests in devices which failed in the first ICMP test.
TCP test on port 23	Choose Yes to test TCP connection on port 23. If the ICMP test is enabled, this test will be done only in the devices which failed in the first ICMP test.
Extended test	Associate a device metadata containing others IP addresses to be tested for a same device.
Number of packets	Define the number of packets to be sent in ICMP collect. The maximum value is 10 .
Packet size	Define the size of the packets to be sent.
Interval between packets	Define the interval, in milliseconds, between the packets.
Number of simultaneous tests	Define how many tests can be executed at the same time. Fill 0 (zero) to run all the tests simultaneously.

For more information on the ICMP process configuration, refer to ICMP configuration section

Important

At least one of the tests (**ICMP test** or **TCP test on port 23**) must be enabled.

Link Group Agent

This setting will let you choose two execution times within the day to execute the link group agent.

Local preferences

Table 8.28. 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 .

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

Object Mapper

For more details about object mapping, refer to mapper configuration section.

Table 8.29. Object mapper configuration parameters form

Field	Description
Execution Interval	Set the interval between mapper executions.
Configuration history storage period	Set the period for storing logs from configurations performed by the mapper.
Simultaneous TCS mappers limit	Define the maximum number of simultaneous TCS mapper executions. Fill with a value between 1 and 200 . The misconfiguration of this parameter can affect the system performance, so be careful!
Number of simultaneous collect	Define the limit of simultaneous SNMP jobs to run. The misconfiguration of this parameter can affect the system performance, so be careful!
Number of simultaneous processes	Define the limit of simultaneous mapper processes to run. The misconfiguration of this parameter can affect the system performance, so be careful!
Number of devices for each process	Define the limit of simultaneous devices for each process. The misconfiguration of this parameter can affect the system performance, so be careful!

QoS

Select **Yes** to enable the ciscoPolicyMapper and qos_d processes. You also need to select the time these processes will run.

The CiscoPolicyMapper process will fetch all QoS policies on the cisco network devices. The devices need to support the CLASS-BASED-QOS-MIB and the policies must be configured at the interfaces. Refer to QoS.

The qos_d process will work with the results of the ciscoPolicyMapper process to create the SLAview profiles needed to view the qos statistics.

Redundancy

This section is used to specify the redundancy setting.

Activation

Table 8.30. 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.
Prefered state	Select Master or Slave .

Refer to redundancy section for details on enabling this feature.

Commuation

Table 8.31. Redundancy Commuation settings

Field	Description
Commuation 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 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 8.32. 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.

Field	Description
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.

Report alarm plus aggregation time

This section corresponds to advanced alarm reports.

Visualize the start aggregation time and configure the start time and the end time of the periods.

For further information about this aggregation, refer to Data aggregation section.

Important

By changing this parameters, the start aggregation time will be reset.

Scheduled Reports

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

Table 8.33. 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 8.34. 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.
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**.

Safe mode

By enabling this mode, the users will not be able to change the system. Thus, in safe mode, it will not be possible to create, edit or remove objects, execute reports, scripts and manual association agents (Mappers, SLAview profiles, Alarm profiles and Groups) and generate backup files.

Furthermore, some tabs will not be displayed anymore. These are:

- **Historical Data** → **Reports**;
- **Historical Data** → **Probes**;
- **Configuration** → **QoS**;
- **Configuration** → **Maintenance**;
- **Configuration** → **ICMP Polling**;
- **Configuration** → **Probe types**;
- **Configuration** → **Trap receiver**;
- **Configuration** → **Rules**;
- **Tools** → **Discovery**;
- **System** → **MIBs**;
- **ALARMmanager** → **Reports**.

Table 8.35. Safe mode form

Field	Description
Enable	Select Yes to enable the safe mode and block changes in the system.

Important

The permission to change this parameter must be enabled at user form.

SMS server

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

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

Table 8.36. SMPP server form

Field	Description
SMS Protocol	Choose the SMPP option.
Host	SMPP host.

Field	Description
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 8.37. 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

Use sysUpTime OID to discard results	If you mark this option, the MIBget process will fetch the sysUpTime.0 instance for the device and discard all results if the return value for this OID is less than 300 seconds. This condition will be considered a reboot on the device and the SNMP counters could be invalid.
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 8.38. TRAP fields

Field	Description
Trap forwarding hosts	IP addresses of the hosts. Ex: 10.0.0.1,10.0.0.2.

Field	Description
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 8.39. 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.

Trap receiver configurations

Enter the port the sensor will listen on for SNMP traps. The default port is **162**.

Trend Analysis

Trend analysis default parameters. Refer to trend analysis section for hints on how to configure these parameters.

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 8.40. 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 8.41. 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 8.42. TRAFip's raw data form

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

MIBs

Select **System** → **MIBs**. In this section you can upload MIB files and verify errors on them.

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 8.43. 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.

SNMP verifier

Use this menu to start the SNMP diagnostics against all devices configured in SLAview.

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.
ICMPAgent.log	ICMP polling process logs.
LinkCacheBuilder.log	Logs from the process that creates the automatic connection in the MAPview application.
mibcache.log	Logs about the MIB compilation process.
MIBget.log	SNMP polling process logs.
ObjectMapper.log	SNMP object mapping process logs.
qos_d.log	Logs from the Cisco auto qos profile configuration process.

SLaSumCaching.log	Logs from SLAview summarization process.
SLAdiscover.log	Logs from the process that maps the network connections via SNMP for the MAPview application.
telco_logrotate.log	Lgs from the log rotating process.
ALARMaction.log	Logs from the process that sends alarms via traps, emails and sms notifications.
ALARMDaemon.log	Logs from the process that processes occurrences and generates alarms.
ciscoPolicyMapper.log	Logs from the process that maps QoS policies for interfaces in the Cisco Class Based QoS MIB.
dbsync.log	Logs from the database synchronization process for redundant environments.
Standyd.log	Logs from the process that controls the redundancy states between the master and backup appliances.
tmsync.log	Logs from the process data synchronization process from master to backup appliances in redundant environments.
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** .

SLAview Rawdata Consult

Allow users access exactly the values collected by the SLAview SNMP collector.

Table 8.44. SLAview Rawdata Consult - Step 1

Column	Description
Object type	Choose Device or Mapped Object.
Name	Object name.

Click **Filter** to apply the filter.

Table 8.45. SLAview Rawdata Consult - Step 2

Column	Description
Object	Select filtered object.
Start time	Minimum collect time.
End time	Maximum collect time.

Click **Generate report**.

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 9. 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 9.1. 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 9.2. 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.

Advanced reports

This report provides flexible data visualization in different formats, using pivoting technology.

Important

This report is processed on a daily basis, so when you run the report, the current day data will not be available.

Table 9.3. Advanced alarm report form

Field	Description
Action	Alarm action.
Start time	Initial day. This filter will work on the alarm start time.
End time	Final day. This filter will work on the alarm end time.
Exclude weekends	Exclude weekend periods from the report data.
Type	Object type.
Manufacturer	Filter by objects manufacturer. You have to use Regular Expressions to filter.'
Manufacturer Type	Filter by objects manufacturer type. You have to use Regular Expressions to filter.'
All day	Check Yes to have all day long aggregated data or check No to have data aggregated in the two time periods configured on System → Parameters → Reports → Report alarm plus aggregation time . Ex.: 9 a.m. to 12 p.m. and 13 p.m. to 18 p.m.
All objects	Check Yes to include all objects or check No to include only alarmed objects.

Field	Description
Output format	Select HTML, PDF or CSV format. Option available only for non-template reports. Once the report becomes a template, this option is ignored.
Alarms	Select the alarms for the report.
Groups	This field can be used to filter objects associated to some root groups.
Column headers	Select the items that will be placed at the report columns.
Line headers	Select the items that will be placed at the report lines.
Data aggregation	Refer to Data aggregation section.

Data aggregation

The data aggregation field is used to define the report data cells. The available field are:

- Functions: function to be applied to the data. The available function are:

Availability	Percentage of time while the alarm was not active.
Frequency	Percentage of time while the alarm was active.
Sum	Summation to be applied to the alarm periods.
Average	Average to be applied to the alarm periods.
Count	Number of alarm occurrences.
Maximum	Maximum alarm occurrence time.
Minimum	Minimum alarm occurrence time.

- Element: Data to apply the function.
- Alarm signaling: definition of thresholds for cell coloring. Refer to advanced report signaling section.

Signaling

The alarm signaling option is used to color the advanced alarm report cells.

When you use a signaling in a report, the report cells will be colored according to the thresholds configured.

Go to **ALARMmanager** → **Reports** → **Advanced report** → **Alarm Signaling** and click the New button to create a new report signaling.

Table 9.4. Advanced alarm reports signaling

Field	Description
Name	Signaling name.
Description	Description field.
Signaling levels	Fill the levels for signaling. Example:

Field	Description
	<ul style="list-style-type: none"> • 40.00<=critical<=100.00 color red • 20.00<=medium<40.00 color blue • 5.00<=low<20.00 color gray

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 9.5. 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 9.6. 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.
\$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 9.7. 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.
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 9.8. 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 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

Default alarm configuration

This type of alarm is used for imediate traffic analysis, when there are known conditions for which it is possible to define a formula. Use this alarm to keep control over boundary conditions that need treatment when detected.

Table 9.9. Default alarm form

Field	Description
Name	Descriptive text for the alarm. Ex.: high traffic, no HTTP traffic.
Object type	Choose the desired type of object to alarm: Device , Mapped object or Groups .
Alarm type	Choose Default .
Formula	Refer to Default alarms formula section.
Summarization variable	Select the desired summarization variable and click on the Add variable button to transport it to the formula box.
Varbind	A free text field that can be used to recognize the alarms that are forwarded as traps.
Mail	Refer to Actions section.
Mobile	Refer to Actions section.
Trap	Refer to Actions section.
Provisioning	Refer to Actions section.
Provisioning script	Select a provisioning script to be executed.
Mail delay	Refer to Actions section.
Mobile delay	Refer to Actions section.
Trap delay	Refer to Actions section.

Field	Description
Provisioning delay	Refer to Actions section.
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 sms for suppressed alarms	If the option No is selected, the sms will be sent and the suppressed condition will be indicated in the sms. The Yes option will prevent the sms 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.
Disable provisioning for suppressed alarm	The Yes option will prevent the script from being executed when the alarm is suppressed.
Consecutive occurrences to activate	Choose the number of consecutive occurrences of the alarm formula that should trigger the alarm. Not used by Trap alarms.
Consecutive non-occurrences to deactivate	Choose the number of consecutive non-occurrences of the alarm formula that should disarm the alarm. Not used by Trap alarms.
Urgency level	Select an alarm urgency level for the alarm.
Alarm profiles	Select the alarm profiles this alarm should belong to.

Default alarms formula

The expressions in the **Formula** field are written in regular infix notation.

You should construct the formulas using the following rules:

- Use round brackets "()" for operator precedence.
- Use the AND,OR, and NOT logical operators.
- Use the ==,<,>,<=,>= comparison operators.
- Use the *,-,+ and / symbols to perform these operations.

Procedure 9.1. Formula input

1. Select the variables and click on the Add variable button to transport them to the formula box.
2. Edit the formula in the formula box to form the desired expression.

If you wish to define when an alarm occurrence should be generated you can use the variables **weekday** and **time** with the operators defined. The values for **weekday** have to be between 1 (sunday) and 7 (saturday). For the variable **time**, you should use HH:MM.

Check the following example:

```
(( "Input traffic"/"Speed")>=0.9) or (( "Output traffic"/"Speed")>=0.9)
```

```
and (weekday > 1 and weekday < 7 and time > 09:00)
```

The previous alarm will be triggered if the input or output traffic raises above 90% utilization and the weekday is between sunday and saturday after 09:00 a.m..

You can also reference device or mapped object metadatas in the alarm formula, according to the object type of the alarm.

The syntax is: **this.object.metadata("<metadata_name>")**.

Look at the following example:

```
"Packet loss" > this.object.metadata("Packet loss limit")
```

Assume that the formula shown above was configured for an alarm with **Device** as object type. The configured value of the device metadata "Packet loss limit" for a device X is 5 and for a device Y is 10. This way, if the packet loss of the device X is greater than 5, the alarm will be triggered. Similarly, if the packet loss of the device Y is greater than 10, the alarm will be activated for this object.

Group alarms formula

The formulas of the group alarms follow the same notation and rules described in the previous section. The only change is the need to use an object type prefix before the variable name. If the variable is of Device type, you must use the prefix "D:" before the variable name, if the type is Mapped Object, you must use the prefix "M:" before the variable name.

Procedure 9.2. Formula input

1. Select the variables and click on the Add variable button to transport them to the formula box.
2. Edit the formula in the formula box to form the desired expression.

Example 1:

```
(( "M:Input traffic" / "M:Speed" ) >= 0.9) or (( "M:Output traffic" / "M:Speed" ) >= 0.9)
```

The previous alarm will be triggered if the input or output traffic raises above 90% utilization.

Example 2:

```
("D:CPU Utilization" > 75)
```

The previous alarm will be triggered if the CPU utilization raises above 75%.

Important

To be able to use alarms for a group, it is necessary enable the group summarization for it.

Behavior change alarm configuration (History Alarms)

Behavior change alarms are used for KPIs (Key Performance Indicators) for which it is possible to establish a behavior. This feature's principle of operation is to establish this behavior for each hour of the day and

if the analyzed KPI suffers a sudden behavior change for the current hour, the system will alarm this condition.

What you should keep in mind is that some variables are not suitable for this type of analysis. For example, interface traffic for interfaces where the traffic is sporadic.

So you should use this feature for variables where the behavior is **predictable**.

Good examples of this feature's uses are:

- Network interfaces with high volume of traffic.
- Cpu usage for routers with significant load.
- Number of connection on a web server with significant load.

Bad examples of this feature's uses are:

- Network or server errors in general.
- Network interfaces with low or unpredictable volum of traffic.

Configuration

This alarm is based on a trend analysis which is performed over a time period configured by the user for each alarm. The alarm is always applied on a summarization variable and has a tolerance factor that will help to fine tune it.

Table 9.10. Behavior change alarm form

Field	Description
Name	Descriptive text for the alarm. Ex.: high traffic, no HTTP traffic.
Object type	Choose the desired type of object to alarm: Device , Mapped object or Groups .
Alarm type	Choose History.
Variable	Select the summarization variable and click on Add variable button.
Activation time formula	Refer to Activation alarm formulas section.
Minimum history (days)	Minimum historical data needed to build the trend analysis. So if you start to monitor an interface, the behavior change alarms will start to work after that period. Recomendated value is 7 days.
Maximum history (days)	Maximum historical data that will be used to build the trend analysis. Recomendated value is 30 days.
Number of consecutive violations (days)	Refer to number of consecutive violations section.
Upper tolerance factor	This factor is measured in amount of standard deviation and it is used to compare the expected value with the actual value. Refer to Tolerance factor.
Lower tolerance factor	This factor is measured in amount of standard deviation and it is used to compare the expected

Field	Description
	value with the actual value. Refer to Tolerance factor.
Alarm period (minutes)	Refer to Alarm period section.
Trigger mode	Defines which tolerance factors will be considered to trigger the alarm. Choose between Both , Upper or Lower .
Protection value (%)	Considers a minimum value for the threshold that is added to the expected values.
Mean value projection	Select Yes to calculate the projection of the maximum and minimum values based on the average value.
Disable negative trends	Select Yes to not consider negative trends for the projection.
Alarm period (minutes)	Refer to Alarm period section.
Mail	Refer to Actions section.
Mobile	Refer to Actions section.
Trap	Refer to Actions section.
Provisioning	Refer to Actions section.
Mail delay	Refer to Actions section.
Mobile delay	Refer to Actions section.
Trap delay	Refer to Actions section.
Provisioning delay	Refer to Actions section.
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.
Disable sms for suppressed alarms	If the option "No" is selected, the sms will be sent and the suppressed condition will be indicated in the sms. The "Yes" option will prevent the sms from being sent.
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 provisioning for suppressed alarm	The Yes option will prevent the script from being executed when the alarm is suppressed.
Consecutive occurrences to activate	Choose the number of consecutive occurrences of the alarm formula that should trigger the alarm. Not used by Trap alarms.
Consecutive non-occurrences to deactivate	Choose the number of consecutive non-occurrences of the alarm formula that should disarm the alarm. Not used by Trap alarms.
Urgency level	Select a level for the alarm.
Alarm profile	Select the alarm profiles this alarm should belong to.

Activation time formulas

This field is used only for history alarms. It defines when an alarm occurrence should be generated.

The variables used are **weekday**, **time**, **everyday** and **everytime**.

To trigger the alarm every day, use **everyday**. To trigger the alarm every time of the day, use **everytime**.

If you wish to define when an alarm occurrence should be generated you can use the variables **weekday** and **time** with the operators defined. The values for **weekday** have to be between 1 (sunday) and 7 (saturday). For the variable **time**, you should use HH:MM.

Example:

1. Fill **Variable** field with: "Input traffic"
2. Fill **Varbind** field with: > 300000
3. Fill **Activation time formula** field with: weekday > 1 and weekday < 7 and time > 09:00

This alarm will be triggered if input traffic raises above 300000 bps and weekday is between sunday and saturday after 09:00 a.m..

Number of consecutive violations

The violated samples will only be considered if they happen consecutively and the number of violations is above the specified parameter, otherwise they will be discarded in the behavior computation.

For example, suppose you have a behavior change alarm for an interface traffic and at some point the expected traffic was 500MB +- 300MB and the detected traffic was 3GB. This sample will not be used in the behavior computation and the expected traffic for the next day will still be 500MB. This sample will only be used if there are N violated samples consecutively, which characterizes a new behavior.

Tolerance factor

This factor is measured in amount of standard deviation and it is used to compare the expected value with the actual value.

The following calculation will be performed to determine if the observed value represents a behavior change:

```
IF (AV < (EV - (N * SD)) OR AV > (EV + (N * SD)))  
THEN trigger the behavior change alarm.
```

Where

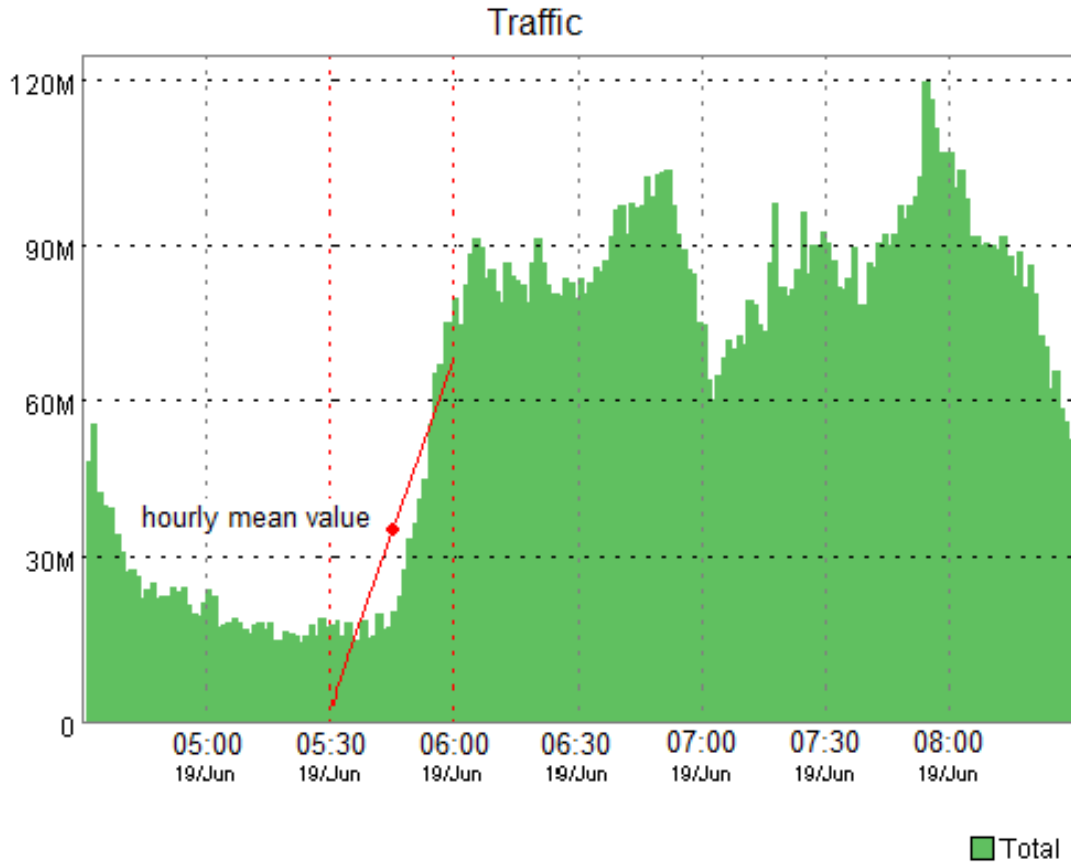
N is the tolerance factor

SD is the standard deviation for the curve

AV is the current half hour average value

EV is the current half hour expected average value

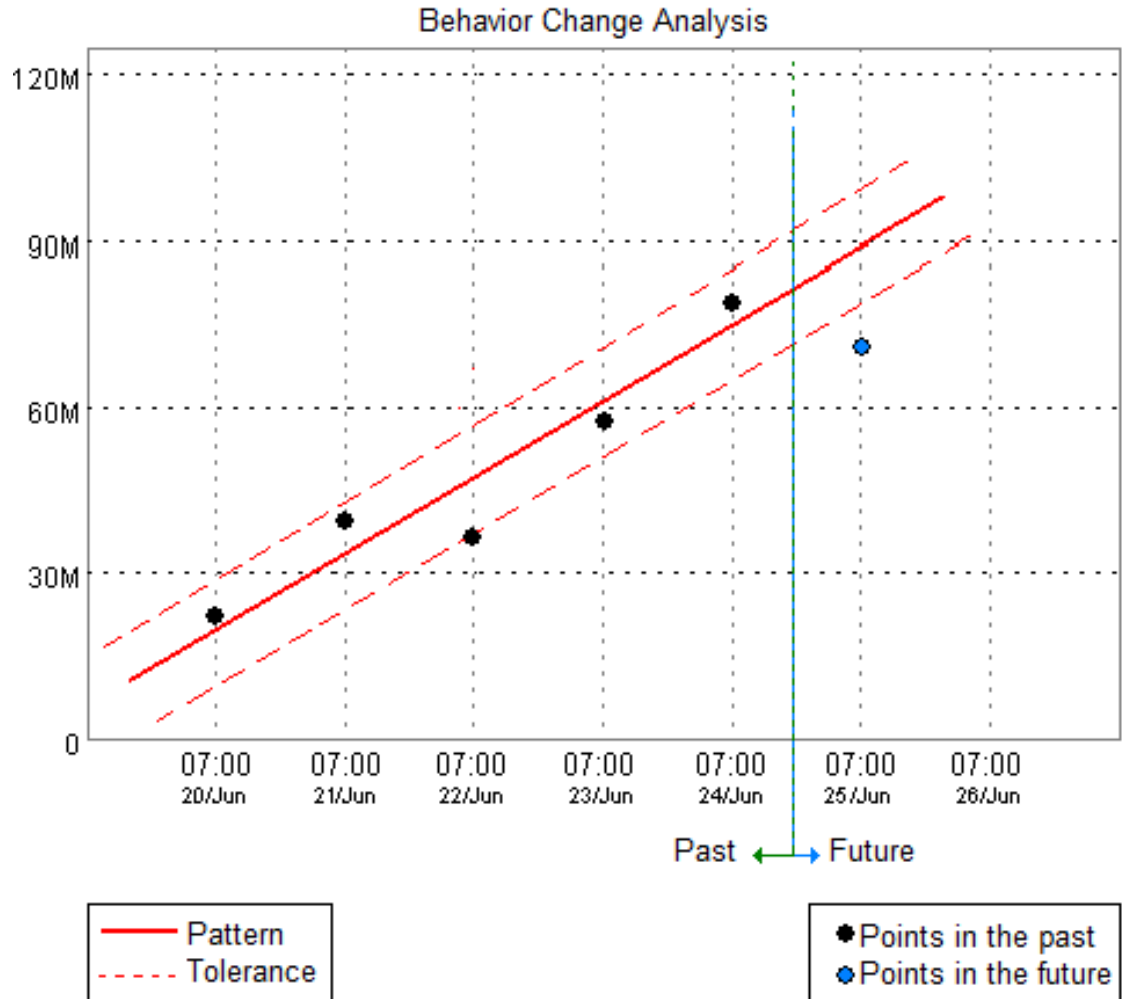
As shown in the graph below, the system calculates the mean value for each hour of the day.



Behavior change mean value

As soon as SLAview has all the values available to calculate the mean value for the current half hour, this value is calculated and compared to the expected value as described previously.

In the next image, you can see the algorithm SLAview uses to estimate the future values for each half hour of the day. It basically performs an approximation to a first degree function using the variable history and if the future actual values fall beyond this function considering the tolerance factor, the alarm will turn on.



Behavior change trend analysis

Alarm period

SLAview will display a sample every 30 minutes or every 5 minutes.

When the alarm period is set as 5 minutes, the system will show the average value for each 5 minutes and compare with the expected value, but it won't save if there is a behavior change.

When the alarm period is set as 30 minutes, the system will show the average value for each half hour and determine if the observed value represents a behavior change.

Actions

Each time the SLAview system processes a 5 minute SNMP polling, all alarm formulas are evaluated and if they return true, occurrences are generated. The alarm will fire for an alarm condition only if the number of consecutive occurrences threshold is surpassed.

The exception of the above behavior is the ICMP polling, where the polling can take place every minute.

When you mark an action for an alarm, you have to fill some fields:

Action fields

Consecutive occurrences to activate	This represents the number of consecutive times a threshold is crossed.
Consecutive non-occurrences to deactivate	This represents the number of consecutive times a threshold is not crossed.

Action types

Mail	Email will be sent to users. The SLAview SMTP server should be configured and also each user email at the user configuration form. The email will be sent after the number of minutes defined in the field Mail delay , starting from the activation time.
Mail	Email will be sent to users. The SMTP server should be configured and also each user email at the user configuration form. The email will be sent after the number of seconds defined in the field Mail delay , starting from the activation time.
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. The message will be sent after the number of seconds defined in the field Mobile delay , starting from the activation time.
Trap	A trap will be sent for each alarm. The trap should be interpreted using the TELCOMANAGER-ALARMMANAGER-MIB.my MIB, which is available at the SLAview mib list. You should also configure the server to send the traps at System → Parameters → SNMP → SNMP trap . The email will be sent after the number of minutes defined in the field Trap delay , starting from the activation time.
Provisioning	A provisioning script will be executed once the alarm is activated. The execution will start after the number of minutes defined in the field Provisioning delay , starting from the activation time.

Behavior change alarm graphs

Once you configure a new behavior change alarm, a new graph icon with the label **Behavior change**, will be available for all objects that are associated to that alarm.

This graph is available for each alarm configured for that object and contains three curves. One curve is the mean values for the summarization variables and the other two curves are the upper and lower limits considered for alarm occurrences generation.

Syslog alarm configuration

Table 9.11. Default alarm form

Field	Description
Name	Descriptive text for the alarm.
Alarm type	Choose Syslog .
Mail	Refer to Actions section.
Mobile	Refer to Actions section.
Trap	Refer to Actions section.
Provisioning	Refer to Actions section.
Provisioning script	Select a provisioning script to be executed.
Mail delay	Refer to Actions section.
Mobile delay	Refer to Actions section.
Trap delay	Refer to Actions section.
Provisioning delay	Refer to Actions section.
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 sms for suppressed alarms	If the option No is selected, the sms will be sent and the suppressed condition will be indicated in the sms. The Yes option will prevent the sms 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.
Disable provisioning for suppressed alarm	The Yes option will prevent the script from being executed when the alarm is suppressed.
Urgency level	Select an alarm urgency level for the alarm.
Activation syslog filter	Select an syslog filter to activate the alarm.
Deactivate by	Choose between Syslog and Time .
Deactivation time	Enter the time to deactivate the alarm.
Deactivation syslog filter	Select an syslog filter to deactivate the alarm.
Device alarm profiles	Select the alarm profiles this alarm should belong to.

Alarm suppression management

At this section you will learn how to manage all the alarm/object tuples that your user has access to.

To suppress, follow the procedure below:

1. Go to **ALARMmanager** → **Alarms** tab and click the Suppressed alarms button.

2. Fill the filter fields at this form to select the desired alarms/objects and click the Filter button.
3. Select the alarms/objects on the list
4. Fill the Suppression reason text field, if desired.
5. Click the Save button to suppress the alarms/objects selected.

To unsuppress the alarms, follow the same procedure, but deselect the desired alarms/objects.

Important

Notice that if the alarm is already suppressed, it won't be suppressed again and the same happens for the un-suppression action.

Important

In Mapview, check the option "Consider suppressed" to show their alarm colors on the map. If a suppressed alarm is inactive for a moment and then it becomes active again, it is marked as suppressed.

Add alarms metadata

To access the metadata configuration page, access **ALARMmanager** → **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 9.12. 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.

Alarm profiles can be automated by using the same rules used for summarization profiles. Configure when in **System** → **Parameters** → **Association agents** → **Association agents** .

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

Table 9.13. Alarm profile form

Field	Description
Name	Define a name for the alarm profile.
Object type	Choose the object type according to the object that should be monitored: Device or Mapped Object .
Object association type	Choose Manual to associate manually or Automatic to use a rule to associate.
Device alarm	This field is only shown when the Object type is Device. Select the desired alarms for this profile.
Mapped object alarm	This field is only shown when the Object type is Mapped Object. Select the desired alarms for this profile.
Devices	This field is only shown when the Object type is Device and the Object association type is Manual. Select the desired devices for this profile.
Mapped objects	This field is only shown when the Object type is Mapped object and the Object association type is Manual. Select the desired mapped objects for this profile.
Association rule	This field is only shown when the Object association type is Automatic. Select the rules used to associate the objects that should be monitored.

Important

When an object or an alarm is associated to an alarm profile, the system checks if the alarms are compatible to the objects. If they are not compatible, the configuration is not allowed. An object is compatible to an alarm if it has all summarization variables of the alarm formula.

Add alarm profile metadata

To access the metadata configuration page, access **ALARMmanager** → **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 9.14. Metadata fields

Field	Description
Name	Enter the metadata name.
Description	Describe the metadata (optional).

Field	Description
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.

Service Alarms

Introduction

The Service Alarms feature allows to join alarms from different objects in a single formula. Now Trafip can alarm under more sophisticated conditions.

You'll be able to create for example the following alarms:

- An alarm that is active when a WAN link has a high latency and also has a low traffic.
- An alarm to tell you when either the primary and backup links of a location will fail.

Create a new Service Alarm

1. Select **ALARMmanager** → **Service Alarms**. Click the new button to define a new type.
2. Fill the form according to the instructions below:

Table 9.15. Service Alarms form

Field	Description
Name	Service Alarm name.
Varbind	Varbind of a trap to be sent when the alarm become active.
Formula	Service Alarm formula. The formula is built using the following Fields: Object, Name and Alarm. Refer on Service Alarm Formula section.
Object	Type of object the Service Alarm is related to. It's used to build the formula.
Name	Name of the object chosen at "Object" field. It's used to build the formula.
Alarm	Alarm that will be associated to the object chosen at "Object" and "Name" fields. To learn about alarms read: AlarmManager Alarms section.
Mail	An e-mail will be sent to the users.
Email delay	Delay in minutes to send an e-mail to the users.

Field	Description
Mobile	A SMS and/or a Telegram message will be sent to the users.
Mobile delay	Delay in minutes to send a SMS and/or Telegram message to the users.
Trap	A Trap will be sent when the alarm become active.
Trap delay	Delay in minutes to send a Trap.
Urgency level	Choose the alarm urgency level.

Formula

In the formulas you can use the OR,AND,NOT and XOR logical operators to build more complex formulas.

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.
- User groups to receive alarms.
- Graphical interface to create custom alarms and formulas.
- 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.

Access control

Each user will receive alarms about objects according to its associations to the group hierarchy and to the alarms configured to it at the user profile.

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.

You can configure the columns at **System** → **Users** → **Alarm console** .

The console has the following columns:

Table 9.16. ALARMmanager console

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	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 Unacknowledged alarm option from the menu.

Alarm Suppression

The alarm suppression mechanism allows you to suppress any alarm/object tuple, providing that the alarm is already configured for that object. The suppression will either disable emails, short messages and traps

for that alarm/object or indicate this condition at the emails, short messages and traps. You can set the desired behavior by setting this field at alarm configuration.

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

You can manage the alarm/object suppression list globally at **ALARMmanager** → **Alarms** → **Suppressed alarms** .

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 them 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.

Check this section for instructions on how to use this filter.

Locating object on maps

Select any alarm line on the console and then click the Locate on MapView button to open the map that contains that alarmed object.

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 10. NOC display

NOC display

The NOC display mode is a view of the Graph sets. This display automatically switches between all user's enabled graph sets after a period previously configured in each graph set.

This feature is useful when the operator must constantly check all graphs on the graph set.

Chapter 11. MapView

Introduction

The Mapview application works along with SLAview and plots a graphical representation of the SLAview groups structure.

Mapview maps are hierarchical, just like the SLAview. Also, subgroups or devices inside groups are represented as graphical icons and change colors based on alarms.

Mapview also plots connections between these elements, identifying the connections based on CDP (Cisco Discovery Protocol) SNMP tables, LLDP (Link Layer Discovery Protocol) SNMP tables and IP SNMP tables, where interfaces in the same 30 bits subnets are considered linked to each other.

Main features

- HTML5 applet graphical interface.
- Hierarchical network topology.
- Easy mouse navigation and interaction throughout the maps, with drill down navigation.
- The integration to ALARMmanager allows for alarm filtering by clicking on any map object, enabling problem isolation.
- The same network element can be associated to multiple maps, enabling different topological views of the network.
- User based access control.
- Configurable background image.
- Automatic link connection between network elements.
- Editable size and positions for each map element.
- Georeferenced maps view.

Operation

Map navigation

Mapview maps reflects the hierarchical group structure from SLAview system. You can navigate through that hierarchy by clicking at each map icon with the right mouse button and opening it.

You can also navigate in the link hierarchy by clicking at the map links with the right mouse button.

Map's alarm filter

This filter can be triggered from any map. It is located below the map's color labels.

To use this filter you must follow the steps below:

1. Select the **Show** button next to **Filter** located at the bottom of any map. At this point, the Alarm Filter window will appear.
2. Select the alarms you want to filter and place them at the right box at the Alarm Filter window.
3. Select the **Include alarms** option to have those alarms shown at the map or the **Exclude alarms** option to exclude them from the map.
4. Click the **OK** button to have this filter applied to the map in question.

To disable this filter, click the **Clear filter** button.

Object alarm filter

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

Using right mouse button on a Mapview object, you will be able to select the **Filter alarms on ALARMmanager** to have only those object's alarms at the alarm console or **Filter alarms out of ALARMmanager** to exclude those object's alarms from the alarm console.

Tip

The object alarm filter can work together with map's alarm filter. This tool is very useful when you need to check alarms from a specific device or group excluding alarms from objects related to them hierarchically, for instance. In that case, the alarm console will display **Filter enabled**.

Saving the map

You can save the following map attributes:

- Position and size of each map object.
- Font position and size for each map object.
- Map window size.

To perform that operation click at **File** → **Save Map**.

Toggling the view

It's possible to visualize a georeferenced map using the **Visualization** → **Toggle to GIS view** menu or the shortcut **T**. In this view mode, the objects are displayed according to their latitudes and longitudes.

In the case of devices, the geographic location is set in fields **Latitude** and **Longitude** on their own forms. The device groups are displayed based on an average of all devices in group.

You can return to default view using the **Visualization** → **Toggle to image view** menu or the shortcut **T** again.

Important

To visualize the maps using this view, it is necessary to register a key provided by MapQuest. Register this key in **System** → **Parameters** → **GIS map**.

Grid layout

To layout the map elements, click the **Tools** → **Grid layout** menu.

Creating and removing connections

To create a connection between two map objects, click on two map objects with the SHIFT key pressed and click the **Edit** → **Create links** menu.

To remove the connection, select two objects and click the **Edit** → **Remove links** menu.

Selecting objects

You can select an object by clicking on it.

To select all objects simultaneously, click the **Edit** → **Select all** menu or use the shortcut **A**.

Aligning objects

You can automatically align pre-selected objects by clicking on the **Tools** menu and choosing the desired alignment.

Editing map object properties

To increase an object size, select it and click on **Edit** → **Increase object size** or use the shortcut **P**. To decrease it, click on **Edit** → **Decrease object size** or use the shortcut **M**.

To return to the standard icon size, click the **Edit** → **Original size** menu. Be careful using this option, because the object text size will be changed too.

To edit various objects simultaneously, drag the mouse around them and, then, choose one of the options above. To save the changes, you have to save the map.

Editing map object text properties

To increase the font size of an object, select it and click on **Edit** → **Increase font size** or use the shortcut **F**. To decrease it, click on **Edit** → **Decrease font size** or use the shortcut **N**.

To return to the standard text object size, click the **Edit** → **Original size** menu. Be careful using this option, because the icon size will be changed too.

By default, the text is shown above the object, but you can edit this position using the **Text** menu. Choose one of the options: **Up**, **Down** or **Right** and save the map.

Changing the background image

To open the Image manager, click on **Edit** → **Map images**.

To upload a new image in the system, fill the **File Name**, choose the file and click on **Add** button.

You can visualize it using the **Visualize** button and remove it using the **Delete** button.

To define the background image for the map, select the image and close the popup.

Tip

Don't forget that it is necessary to save the map. Do it clicking on **File** → **Save Map**.

Zoom in/out

Click the right mouse button in the map area to select **Zoom in/Zoom out** options. The **Initial State** option takes back to the initial zoom level.

You can also use the **Visualization** menu to select these options.

Fit to screen

Click the right mouse button in an empty map area to select **Fit to screen** or use the **W** shortcut.

This feature is also accessible through the **Visualization** menu.

Stretch image

Using the **Visualization** → **Stretch image** menu or the shortcut **B**, it is possible to stretch the MAPview background image size to the window size.

You can return to default mode, where the background image size does not change, using the **Visualization** → **Keep image size** menu or the shortcut **B** again.

Adding text and geometric shapes

Through icons in the Mapview menu, you can add pre-defined texts and geometric shapes to the map. The available geometric shapes are quadrilaterals, circles and ellipses.

You can choose different properties for geometric shapes, such as: text, width, height, diameter, stroke width, font size, color, and fill. The properties of the object can be edited at any time by clicking on it with the right mouse button and choosing **Properties**. To save the added objects, you need to save the map on **File** → **Save Map**.

Chapter 12. Metadata

Introduction

The Metadata application works along with the system objects.

Objects can be associated with a **Metadata** during their creation or editing.

Add metadata

To access the metadata configuration page, access the object configuration and click on **Interface groups** 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 12.1. Metadata fields

Field	Description
Name	Enter the metadata name.
Description	Describe the metadata (optional).
Datatype	Choose the metadata type: Text , Integer or Enum .
Values	This field is only available when the Datatype is Enum . Enter a list of values, separating them by semicolon (;).
Required field	Select YES to be required the filling the metadata field when an object is created or edited.
Show in object list	Select YES to display the metadata on the object configuration screen.

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

Chapter 13. 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 14. Glossary

Abbreviations

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

Table 14.1. 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.