



Visualizer

Guide

Copyright© Version 1.0 bintec elmeg GmbH

Legal Notice

Warranty

This publication is subject to change.

bintec elmeg GmbH offers no warranty whatsoever for information contained in this manual.

bintec elmeg GmbH is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

Chapter 1	Installing Teldat Visualizer	1
1.1	Installation	1
1.2	Initial configuration - Wizard	2
1.2.1	Mode, Hostname, DNS and NTP	3
1.2.2	Configuring NTP and the management network.	3
1.2.3	Configuring the synch network	4
1.2.4	Configuring cluster and external services	4
1.2.5	First connection to the web application	5
Chapter 2	Licenses.	6
Chapter 3	User Management	8
3.1	User setup.	9
Chapter 4	Sensors	11
4.1	Sensors: menu and options	11
4.2	Adding a sensor	11
4.3	Adding a domain	12
4.4	Editing a domain	13
Chapter 5	Viewing data	14
5.1	Traffic: menu and options	14
5.1.1	Options available in the Traffic section submenu	14
5.1.2	Screen body: filtering by time range, attribute tabs and views.	15
5.1.3	Summary, browser and data table	16
5.2	Filter events	16
5.2.1	Custom time filter	16
5.3	Views: multiple options to display data	18
5.3.1	Tops	19
5.3.2	Raw.	19
5.3.3	Compare	20
5.3.4	Unique	20
5.4	Types of aggregation	21
5.5	Granularity.	21
5.6	Types of charts	22
5.7	Options	25

5.8	Attributes: tabs and columns	27
Chapter 6	Dashboards	29
6.1	Dashboard Options	29
6.1.1	Editing and cloning available dashboards	30
6.1.2	Add dashboard	31
6.1.3	Import dashboard	31
6.1.4	Adding a widget: customizing dashboards	31
6.1.5	Time machine	33
6.1.6	Cloning, editing, reloading and deleting widgets from the dashboard.	33
Chapter 7	Updating a cluster	35
7.1	Updating from a remote repository	35
7.2	Updating from ISO (offline mode)	35
Chapter 8	Client Proxy	37
8.1	Introduction	37
8.2	Installation	37
8.3	Register	38
8.4	Managing the sensors	38
8.5	Updating	39

Chapter 1 Installing Teldat Visualizer

This chapter describes how to install Teldat Visualizer Enterprise. In the remainder of this document, we will use the term manager to refer to the machine where Teldat Visualizer is to be installed.

1.1 Installation

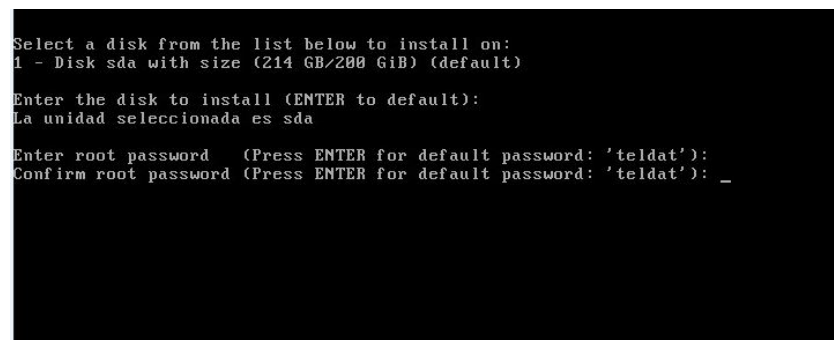
In order to install the manager, the user will have an ISO image with which to boot the machine where the software is going to be installed.

When the installation wizard is started, the following menu appears:



Select "Install Teldat Visualizer" to start the installation.

After a few seconds, another menu will appear that looks like this:



Here, the installer will ask us to select the disk we want to install the software on.



Note

The installer will format the selected disk.

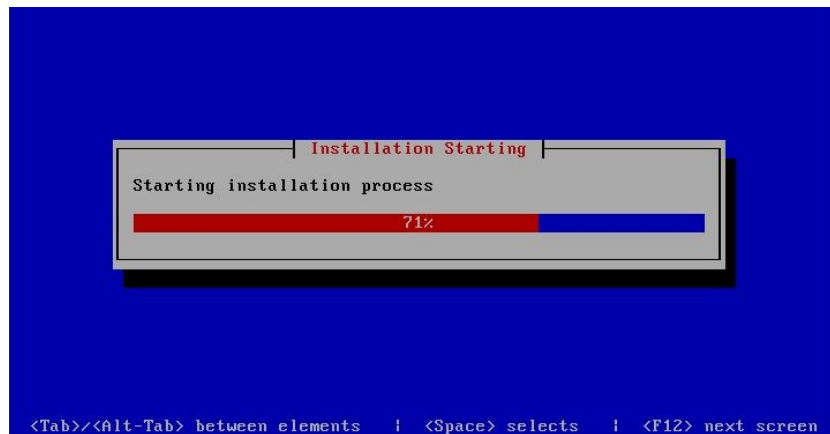
We will also be asked to set a root user password for the system.



Note

The default root password is "teldat".

After this, the software installation packages will download to the hard drive.



Wait until the installation has completely finished (the progress bar should reach 100%).

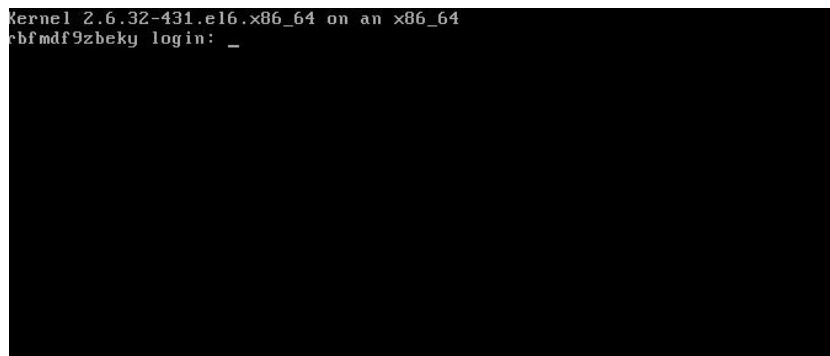
After the installation has finished, the system reboots. During this first reboot, the system performs a series of actions to configure for the first time.



Note

This may take several minutes.

We can start using it when we see the following image in the terminal:



Note

The default username and password are “root” and “teldat”.

1.2 Initial configuration - Wizard

After logging on to the manager, run the **rb_sysconf** command to perform the initial configuration.

These are the options you will find in the main screen of this menu:

- (a) **System Configuration**: allows us to configure the manager’s hostname, IP address, time zone and status.
- (b) **Network Configuration**: allows us to create network bonds and segments, and configure DNS, route and IPMI settings. At least two network interfaces are needed to form a cluster, one for management and another for communication between cluster nodes. For single node installations, only one network interface for management is necessary.
- (c) **Passwords**: access this option if you want to change the system user passwords.
- (d) **w) start simple wizard**: starts a wizard that provides a quick and easy way to install and configure the manager.
- (e) **q) quit**: takes us back to the main system configuration screen.

```

1) System configuration
2) Network configuration
3) Passwords

w) start simple wizard
q) quit

-----
Selection: _
time: 2017/03/30 11:10

```

We can perform the installation automatically with the **w) start simple wizard**.

There are a number of default options available (shown in brackets). To accept them, simply press **Enter**. You can always change them manually, at any time, during the installation process.

1.2.1 Mode, Hostname, DNS and NTP

- Insert Hostname [rbmanager]. The default option is rbmanager. This is a clear and simple name used to identify the manager and its position within a cluster.
- Insert domain: [redborder.cluster]. Default domain.
- Insert DNS Primary. Defined by default. The user can change it to indicate the server that provides DNS services to his/her network and with which the manager is associated.
- Insert DNS Secondary (optional). Option to indicate a secondary DNS. We recommend entering an alternative DNS that replaces the primary one should the server fail.



Note

Different names should be used for each of the managers joining the cluster.

Once these values have been entered, the system will display the following message in green to confirm the changes have been successfully applied: DNS and domain settings applied successfully.

```

1) System configuration
2) Network configuration
3) Passwords

w) start simple wizard
q) quit

-----
Selection: w
time: 2017/03/30 11:19

Selected Mode: cluster
Insert Hostname [rbmanager]: visualizer01
Insert Domain: [redborder.cluster] teldat.cluster
Insert Primary DNS: 10.0.70.5
Insert Secondary DNS (optional):
DNS and domain settings applied successfully

```

1.2.2 Configuring NTP and the management network

The next step is to specify the time server: **NTP server [pool.ntp.org]**: If there is an NTP server in your network that you would like to use, you must enter it here or a default one will be assigned.

If you are only going to deploy one manager, you will need one network interface. If, on the other hand, you are going to deploy a cluster with multiple managers, two network interfaces will need to be reserved:

- One for the management network (Management IP address)
- Another for the synch network (Sync IP address)

You need to configure network bonding on each of these interfaces.

The bonding management configuration requests the following data:

- Insert management IP address:
- Insert management Netmask
- Insert default gateway for this management interface (Y/n)
- Insert a route for this bonding (y/N)? : Option to insert a static route.

Once these values have been entered, the system confirms that the bonding was successfully created.

```

3) Passwords

                                w) start simple wizard
                                q) quit

-----
                                time: 2017/03/30 11:19

Selection: w

Selected Mode: cluster
Insert Hostname [rbmanager1]: visualizer01
Insert Domain: [redborder.cluster] teldat.cluster
Insert Primary DNS: 10.0.70.5
Insert Secondary DNS (optional):
DNS and domain settings applied successfully

NTP server [pool.ntp.org]:
Insert management IP address: 10.0.150.164
Insert management Netmask [255.255.255.0]:
Insert default gateway for this management interface (Y/n)? :
Insert default gateway [10.0.150.1]:
Insert a route for this bonding (y/N)? :
Bonding 0 created successfully

```

1.2.3 Configuring the synch network

If we have configured two network interfaces for the machine, we will have to configure bonding for the synch network.

```

-----
                                time: 2017/03/30 11:19

Selection: w

Selected Mode: cluster
Insert Hostname [rbmanager1]: visualizer01
Insert Domain: [redborder.cluster] teldat.cluster
Insert Primary DNS: 10.0.70.5
Insert Secondary DNS (optional):
DNS and domain settings applied successfully

NTP server [pool.ntp.org]:
Insert management IP address: 10.0.150.164
Insert management Netmask [255.255.255.0]:
Insert default gateway for this management interface (Y/n)? :
Insert default gateway [10.0.150.1]:
Insert a route for this bonding (y/N)? :
Bonding 0 created successfully

Insert sync IP address: 10.0.151.164
Insert sync Netmask [255.255.255.0]:
Insert a route for this bonding (y/N)? :
Bonding 1 created successfully

Would you like to join to another cluster? (y/N) _

```



Note

This part will not be displayed if there is only one network interface configured on the machine.

1.2.4 Configuring cluster and external services

Lastly, we must enter a series of configuration values to create a multi-manager cluster and configure services outside the manager. In the case of on-premise installations, we recommend leaving the default values.

```
Insert Primary DNS: 10.0.70.5
Insert Secondary DNS (optional):
DNS and domain settings applied successfully

NTP server [pool.ntp.org]:
Insert management IP address: 10.0.150.164
Insert management Netmask [255.255.255.0]:
Insert default gateway for this management interface (Y/n)? :
Insert default gateway [10.0.150.1]:
Insert a route for this bonding (y/N)? :
Bonding 0 created successfully

Insert sync IP address: 10.0.151.164
Insert sync Netmask [255.255.255.0]:
Insert a route for this bonding (y/N)? :
Bonding 1 created successfully

Would you like to join to another cluster? (y/N)

Cluster domain name [teldat.cluster] :
Would you like to use remote S3 storage? (y/N)
Would you like to use remote memcached? (y/N)
Would you like to use remote postgresql database? (y/N)

Are you sure you want to apply this configuration ? (y/N) _
```

Once finished, accept and the configuration process will start.



Note

This process may take several minutes/hours to complete, depending on the capacity of the manager being installed. This is mainly because the first installation requires feeding the database with a large number of initial values. However, in successive updates, this will no longer be necessary.

1.2.5 First connection to the web application

Once the software has been installed and configured, you can access the web application by connecting to the <https://IP-de-gestion> URL using a browser and entering the default username (admin) and password (bintec123). For the console connection, you can either do it directly through the console (tty) or remotely (ssh) using the root user and the password that you set during the initial installation. Default is bintec.

This chapter describes how to license a bintec elmeg GmbH Visualizer manager.

Create a new flow sensor

Product type

Teldat-M1

* Name

* Serial Number

SNMP Community (optional)

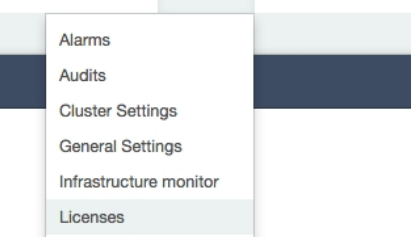
XXXXXXXX

License

There are no available licenses. Add or request a new license.

Save

Cancel



The screenshot shows the Sensu web interface. The top navigation bar includes a search icon, 'Sensors', 'Tools' (with a dropdown arrow), and 'Administrator' (with a user icon). The 'Tools' dropdown menu is open, displaying a list of options: 'Alarms', 'Audits', 'Cluster Settings', 'General Settings', 'Infrastructure monitor', 'Licenses' (highlighted), 'Lookup Sources', 'Objects', 'Overlay Maps', 'Platform Alerts', 'Rule Versions', 'Users', and 'Worker & Job Queue'.

Licenses Request licenses Upload licenses

Resume

Active licenses	Total Dtypes/day	Expire date	Cluster (USD)
0	0 Dtype	Expired	7524(25k) - 4752 - 4415 - 6185 - 6185(9750k)

Dtype consumption today (from 00:00 to 00:00 UTC)

Dtype	Consumption
Dtype	0

Product Type **In Use** **Limit**

No system licenses

Licenses

ID	Date	Dtype/day	Expire date	Status
No system licenses				

To obtain a license, click on the "Request license" button. A form will appear for the user to indicate how many MB will be consumed each day and the maximum number of each type of sensor.

Request License

* Name

Teladat

* Email

admin@networkcloudmanager.com

It will be used to send the license

* MB/day

0

* Atlas-60 Sensors

0

* Teladat-V Sensors

0

* Teladat-M1 Sensors

0

* Teladat-IM8 Sensors

0

* H2-Auto-Plus Sensors

0

* Atlas-i70 Sensors

0

* H2-Rail Sensors

0

* H2-Auto Sensors

0

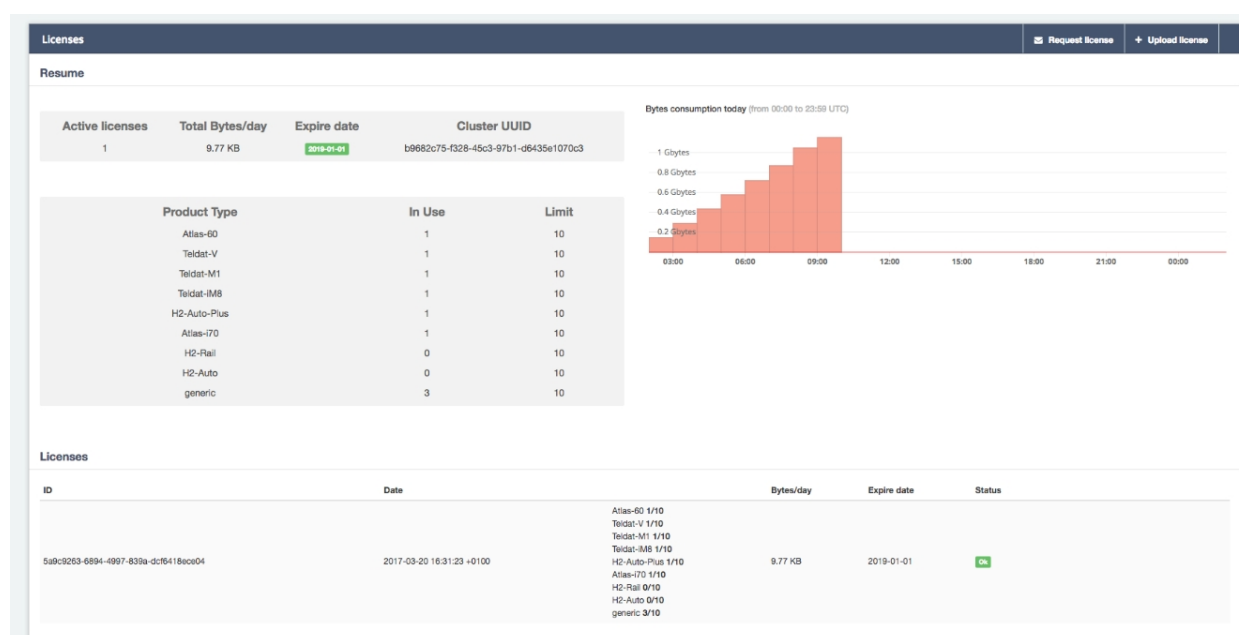
* generic Sensors

0

Once we have the license file (extension .lic), click the "Upload license" button to upload it to the manager.

From now on, the loaded license will appear in the licenses window.

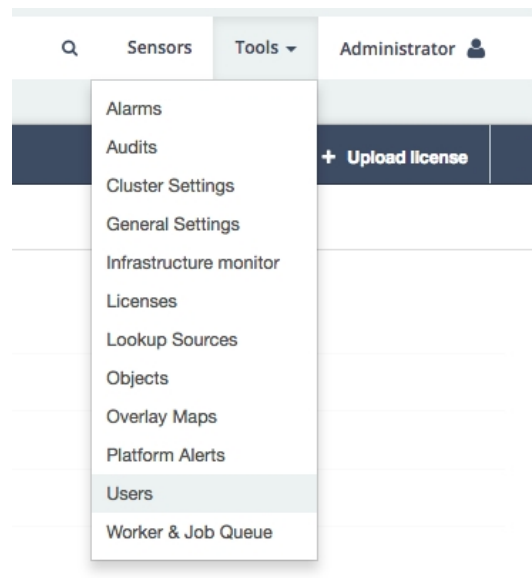
Here we can see all the loaded and active licenses, the number of bytes consumed per day, and the sensor limit for each type of sensor that we can use.









An important piece of information included in the licenses window is the number of daily bytes consumed for the current day. If we exceed this value, events for the associated sensors will no longer be processed.

Chapter 3 User Management

Registering and changing user data, changing user permissions and creating new user accounts is possible from the user management interface, accessed via **Tools # Users**.



If you need to find a specific user, you can enter their data in the search engine or browse the alphabetical listing of registered users.

User Settings									+ New User
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z <u>All</u>									Search
	Enabled	Name	E-mail	Admin	Top Domain	Login Count	Login IP	Last Login Time	
A	<input checked="" type="checkbox"/>	Administrator	admin@networkcloudmanager.com	★	root	10	10.0.30.191	2017/03/31 at 10:55	 
U	<input checked="" type="checkbox"/>	user1	user1@redborder.com	★	root	2	10.0.30.191	2017/03/30 at 17:25	 
	<input checked="" type="checkbox"/>	user2	user2@redborder.com		root	1	10.0.30.191	2017/03/30 at 17:25	 

Only those holding the **Domain Administrator** role can manage users in their domain. The remaining users can view different parts of the platform, but cannot change its content (except for their own user profile).

In addition to domain administrators, there is also a Super Administrator user. This user can manage all the users registered on the platform.

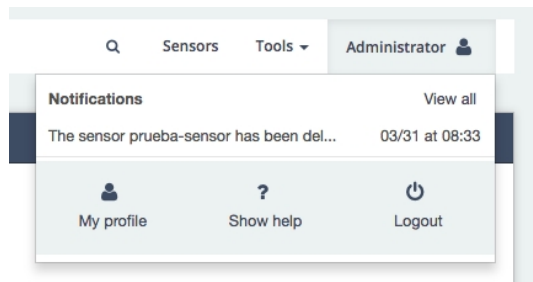
A user is only a **Super Administrator** if it is an Administrator and its Top Domain is root.

In the body of this window, we find a list of all the users registered on the redborder platform, with each user's email address, top domain (maximum access level), login count, IP address and last login.

We can also find two buttons on each user line:

- User setup button
- User delete button

Another way to access our user profile setup menu directly is by clicking on the username that appears in the upper toolbar, and then clicking on **My profile**.



We can also find the help (**Show help**) and logout (**Logout**) buttons in this area. In addition, we will see notifications related to the user's activity.

3.1 User setup

We can click on a user's setup button to change the following data and display a summary of their status and activity within the platform.

User Settings

Name: user1
Login/Username: user1
Email: user1@redborder.com

Top Domain: root

Administrator: ☒

Other actions:
 Edit password
 Recreate API Access Key
 Copy API Key to clipboard

Personalization

User home page: Overview
 (Select the default home page you would like to see)

Items per page: 25
 (Select the default amount of events to list per page view)

Base letter size: Medium

Stats

Login Count:	2	Notes Count:	0
Last Login:	Thu Mar, 2017 05:24 PM	Dashboard created:	1
Current Login IP:	10.0.30.191	Reports created:	0
Last Login IP:	10.0.30.191		

Update **Cancel**

The following sections can be found in the user setup menu:

- Main menu

Administrator: By enabling this, we turn the user into a Domain Administrator under "Top Domain".

Name

Login/Username

Email

Top Domain: The highest domain the user can access. The highest level domain is **root**.

Other actions: There are three buttons to carry out the following actions:

Edit password: Change the user password.

Recreate API Access Key: Create a new API Rest access key.

Copy API Key to clipboard: Copy the API Rest access key.

- Customization menu

User home page: Homepage that should appear after user login.

Items per page: Number of default events displayed in the data display sections.

Better letter size: Font size.

- **Stats menu:** Shows the user's usage statistics.



Note

Entering our password is necessary whenever we want to change our own user account to apply the changes.

Chapter 4 Sensors

This chapter explains how to add new sensors and domains to the redborder manager.

The **Sensors** section can be found in the upper right margin of the header menu, next to the **Tools** section and the user area.



4.1 Sensors: menu and options

This section briefly explains the **Sensors** menu and its corresponding options:

- **Section submenu:** here you will find the available options when it comes to configuring and managing sensors.

Options

+Add sensor

+Add domain

View

- **Main area:** the information shown in this area will depend on the type of view selected in **View**. Three different views are available to display the organization of the sensors registered in the manager:

Tree: list showing network infrastructure according to hierarchical levels and dependency between the elements composing it.

There are two icons next to each element to allow you to edit and delete them. This is the default view.

Client Proxies: alphabetical list of client proxies

Flow sensors: alphabetical list of flow sensors.



Note

Each view has its own option menu and provides different possibilities for creating and editing sensors or domains.

4.2 Adding a sensor

To add a sensor, select **+Add Sensor**. The drop-down menu shows the different types of sensors that you can add to the tree. Select the type of sensor you want from the drop-down menu and then enter the required information.

Both the sensor type and serial number must be selected to register bintec elmeg GmbH sensors. If the sensor is not a bintec elmeg GmbH sensor, a generic sensor must be selected and the sensor IP address/network used to identify it.

Create a new flow sensor

Product type

TelDat-M1

* Name

* Serial Number

SNMP Community (optional)

XXXXXXXX

License

f85e1627-c404-418b-b692-75bfb9bb5cf7 - 2017-04-29

Save

Cancel



Note

As soon as a sensor is created in the manager, it is placed as root (above domain level) by default.

The user can organize his/her sensor infrastructure at any time by dragging and dropping a sensor into the desired level.

A sensor automatically inherits properties from the root domain.

4.3 Adding a domain

To add a domain, select **+Add Domain** located in the upper right submenu, choose the type of domain you want to add and then fill in the required fields (these will vary according to the type of domain you are going to create).

+ Add Domain

Service Provider

Organization

Market

Deployment

Namespace

Campus

Building


Create a new Organization

* Name

Location

Mapa

Search Box



Save

Cancel

4.4 Editing a domain

To access the domain editing features, click on the "Edit" icon (to the right of a domain from the tree view) and select the **Edit** option.

The following data that can be edited in a domain. The fields displayed will differ depending on the type of domain selected:

- **General:** Shows general sensor information. Name (not editable), domain type and description.
- **Namespace Rules:** Allows you to add domain-level rules.
- **Servers:** Here, the user can define Syslog and Proxy server settings. The values displayed are those inherited by default. Overwrite them if necessary.
- **Location:** Locates a sensor/domain on a world map.

Visualizer

13

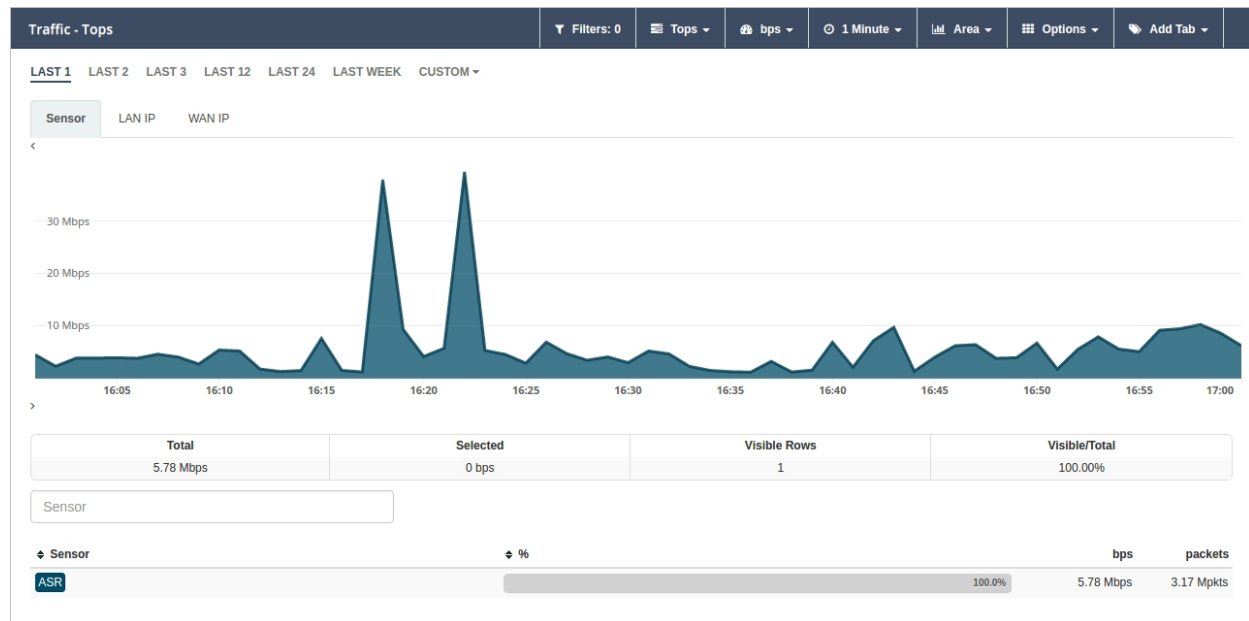
Chapter 5 Viewing data

Here, the user can display, analyze and manage the events collected.

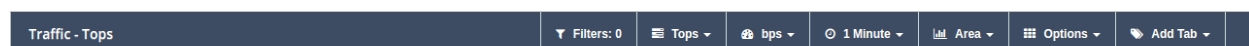
5.1 Traffic: menu and options

The analysis area on the left of the menu bar has various sections corresponding to the different Apps integrated in the platform.

Below, we see the different data display options, graph types, granularity (the frequency with which events are added) and dimensions that can be combined to obtain a fully customized network traffic viewer.



5.1.1 Options available in the Traffic section submenu



- **Filters:** Allow the user to isolate a portion of data for greater detail. In this tab, the user can see how many filters have been applied and perform the following actions on them:

Create an advanced filter (**Advanced Search**)

Create an alarm based on applied filter criteria (**Create an alarm**)

Create a widget based on applied filters and include it in a dashboard or report (**Create a widget on**)

- **Views:** offers different options when it comes to displaying information. They will be explained further on.
- **Aggregation:** these are the different values or units of measurement that can be used to display data. For example, flows per second, (flows/s) or bytes per second (bps).
- **Granularity:** indicates the level of temporal detail with which it is possible to display data. The minimum granularity is one minute.
- **Chart type:** shows the various chart types that can be used to display data. The options available vary depending on which view is selected. These are:

Area

Stacked

Line

Bars

SBars

- **Options:** here, the user can perform different actions to manage the data being displayed in this section. The options vary depending on which view is selected.

Show total (**Show Total**)

Export to CSV (**Export to CSV**)

Time machine (**Time Machine**)

Save tabs as default (**Save tabs as default**)

Sort aggregations (**Sort Aggregations**)

Sort columns (**Sort columns**)

- **Attributes:** The events received by the manager are made up of “column:value” pairs. The values under each column are event-specific data, meaning they provide real information. These are called “attributes”

Attributes can be displayed as tabs or columns (**Add tabs/Columns**) depending on the view that we are querying.



Note

Throughout this document, the column concept is referred to as “Attribute” or “Dimension”.

5.1.2 Screen body: filtering by time range, attribute tabs and views.

Filtering by time range: direct access to events filtered on the basis of a time period.

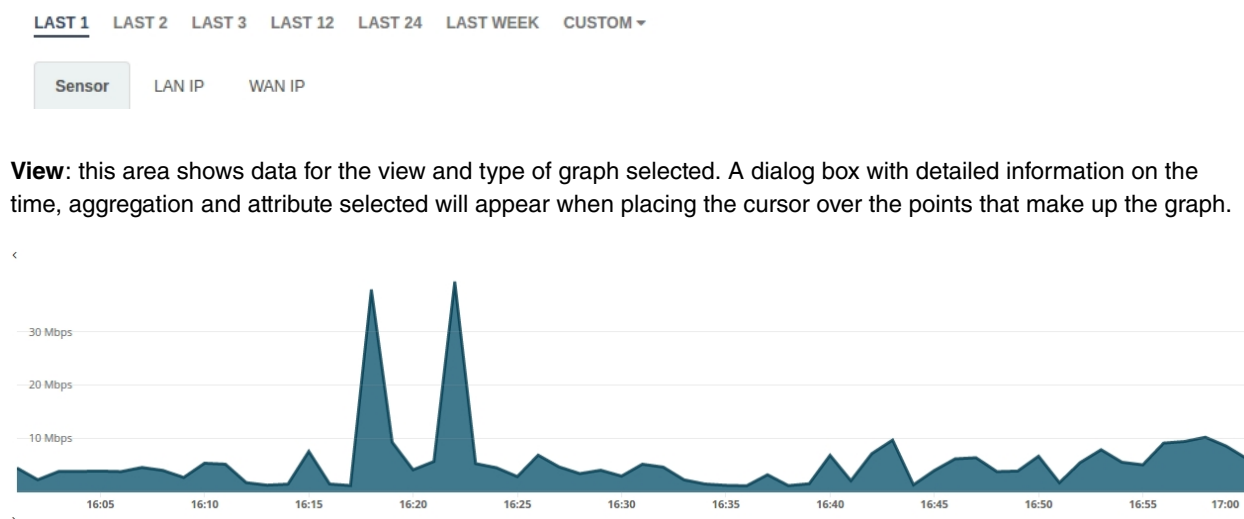
Selecting a range of dates different from the one provided by default is possible. The user can choose the time period that best adapts to his/her needs using the **Custom** option. The steps that must be followed to set a customized time filter are included further on.

Attribute tabs: they classify traffic information based on attributes. By surfing through each tab, we can gather detailed information on the values associated with the attributes we have selected.



Note

The user can always modify the order in which tabs are shown. To do so, he/she must drag the tab to the desired position and release it.



View: this area shows data for the view and type of graph selected. A dialog box with detailed information on the time, aggregation and attribute selected will appear when placing the cursor over the points that make up the graph.

- Time range filtering
- Filter Zoom
- Custom filter
- Advanced search
- Attribute filtering

Time range filtering

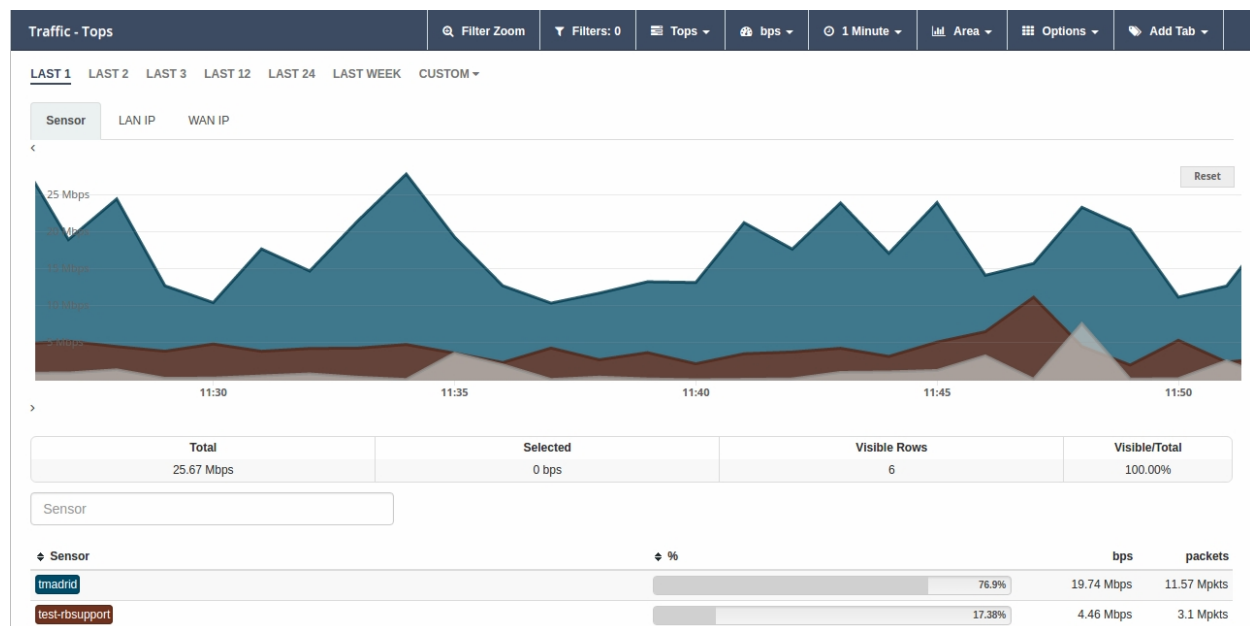
A very quick and easy way to display the events that correspond to a certain period of time is to select some of the options available in the time range filtering tabs:

LAST 1 LAST 2 LAST 3 LAST 12 LAST 24 LAST WEEK CUSTOM ▾

Filter Zoom

The user can manually select a time lapse. This filter is useful to study an event in greater detail. To do so, click on any given point in the graph, drag it to the desired instant and release it. The image displayed will shift to display that time range and the table underneath will only show information relative to it.

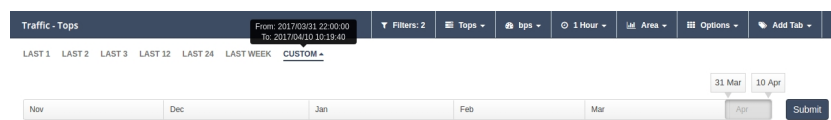
The **Filter Zoom** option will appear as checked in the submenu.



Custom filter

The **Custom** tab of the time range filtering option allows for customized filtering. A start date and an end date can be set just by dragging the mouse over the time bar.

Click on **Submit** to enable this filter.



Advanced Search

When you click on the **Filters** tab, a submenu appears with the **Advanced Search** option.

Since the user sets the search and filtering conditions, this option allows for much greater detail.

Advanced Search

Save Current Filter

View Saved Filters

☒ Choose a query... contains Enter search value

☒ Choose a query... contains Enter search value

Submit Search

Cancel

Filter Selected

There are two ways in which an attribute value can be turned into a filter:

- (a) **Browser**: insert the attribute value you want to search for and click on **Enter**.

A filter with the selected value will be automatically created. You can include as many filters as searches performed. You may also delete a filter from the “Filters” option.

- (a) **Select table rows**: you can select one or more table rows simply by clicking on them. The rows selected will appear highlighted in yellow.

Once you have selected the rows, click on the **Filter Selected** option to generate a view of the filtered elements. To delete this filter, click on the **Exclude Selected** button.

You may carry out individual actions on each of the table elements. When you click on one, a submenu with the following options appears:

Filter: adds the filter to include the relevant element in the data displayed.

Exclude: adds the filter to exclude the relevant element from the data displayed.

Total	Selected (2 rows)	Visible Rows	Visible/Total	
23.28 Mbps	35.34 Mbps	6	100.00%	

Filter Selected

Exclude Selected

Sensor	%	bps	packets
tmadrid	71.91%	16.74 Mbps	10.21 Mpkts
test-rbsupport	21.46%	5.0 Mbps	3.39 Mpkts
lbarcelona	3.5%	815.08 Kbps	596.59 Kpkts
router-757/03317	3.04%	707.09 Kbps	510.45 Kpkts

5.3 Views: multiple options to display data

Views offer multiple ways in which to display data associated with network traffic. The options available in the Traffic App are as follows:

- **Tops**: event aggregation based on a unit that shows the most outstanding. Adds the total data from different events and shows it as one.
- **Raw**: displays the raw data of all events (classified by attribute and time period).
- **Compare**: compares time intervals to analyze differences in the state of the network.
- **Unique**: shows the different elements that have interacted with the network based on the attribute.

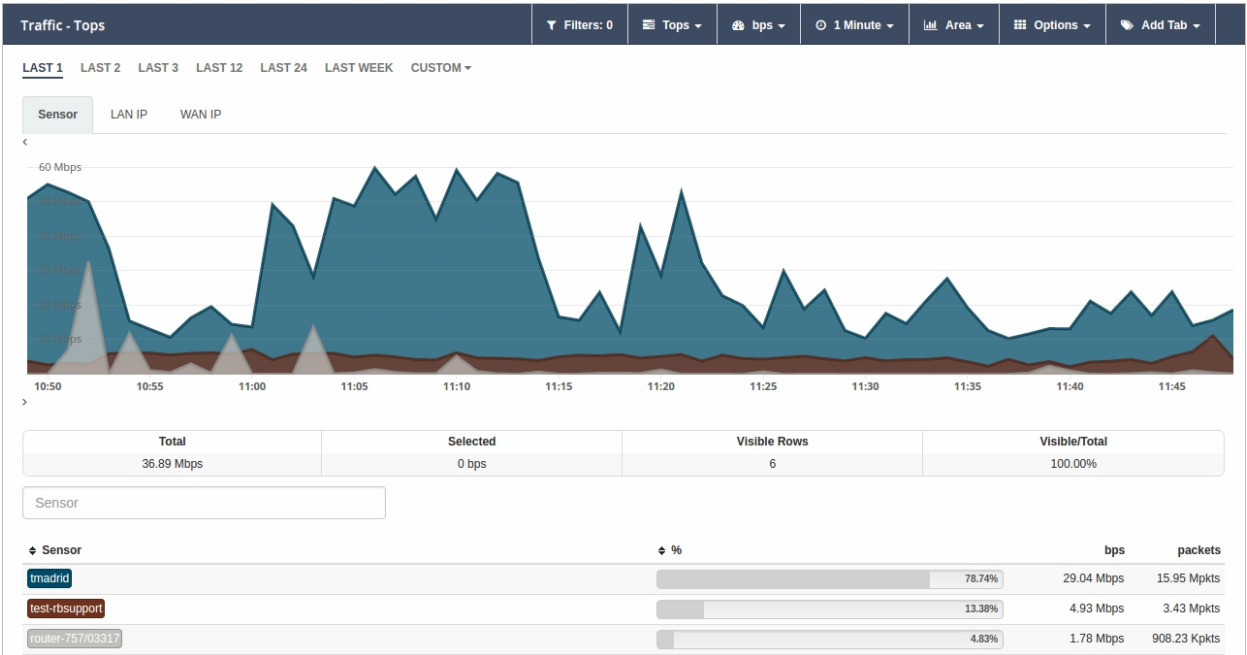
Note

The options displayed under the **Options** tab and the **Add tab/Columns** attributes will vary depending on the type of view chosen.

Don't forget to combine the views with the different types of graph. This provides multiple data analysis options.

5.3.1 Tops

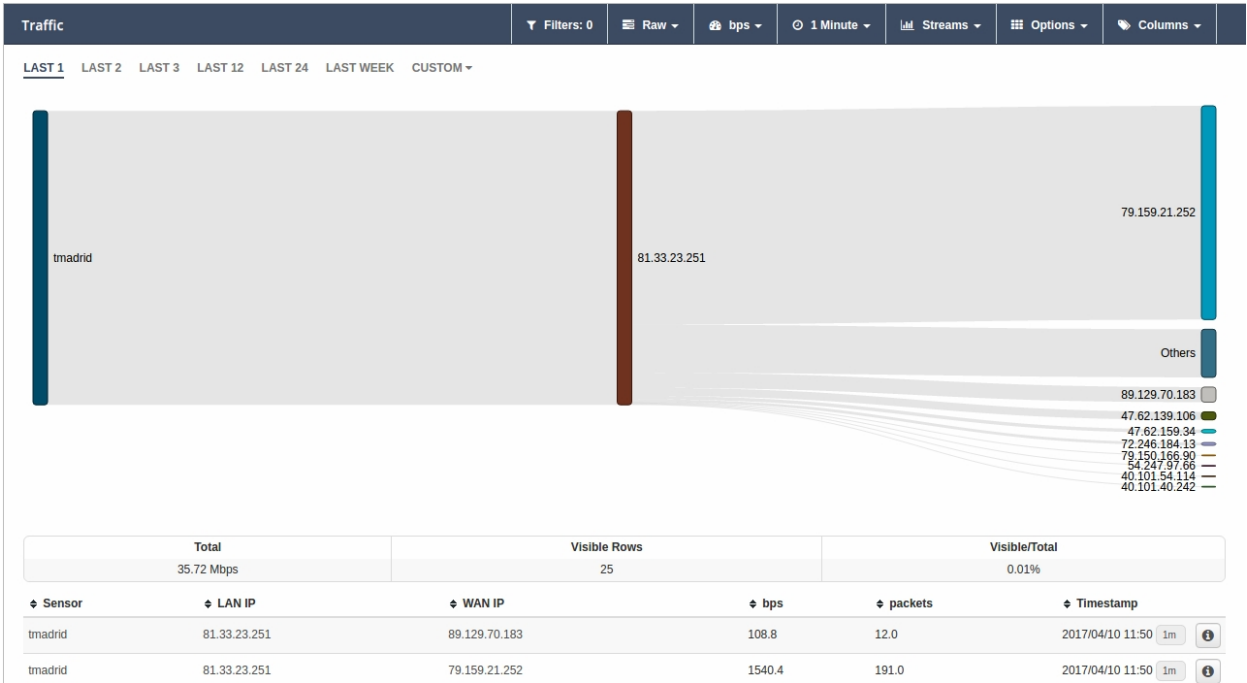
The **Tops** view allows us to see the most significant events per time interval selected. What we see in the graph is the sum of those events shown as one. If we hover the mouse over the graph, we will see a breakdown of the event per day, time, scale or attribute.



5.3.2 Raw

This view displays the raw data of all events. Thus, we will see all events split into time frames.

The data table will show all events in chronological order. If you wish to see more, simply go to the end of the table and previous events will appear.



7.18 Kbps , 1.0 pkts on 2017-04-10 13:25:00 +0200

Application

Application: IANA-L4:53854Engine: IANA-L4Selector: 0

Flow

Direction: downstream

Interface

LAN Interface: localWAN Interface: ppp1

Location

WAN IP AS: TELEFONICA DE ESPANAOrganization: TeldatService Provider: TeldatNamespace: TeldatMarket: Spain

Network


Sensor: tmadridWAN IP Name: 80.24.0.30LAN IP: 96.163.0.0Protocol: 254LAN IP Name: 96.163.0.0TOS: 187WAN IP: 80.24.0.30Sensor Type: netflowv10

Transport

LAN L4 Port: 0WAN L4 Port: 0

UUIDs

Service Provider UUID: 5c662555-8793-4319-8337-9da9cca9213bNamespace UUID: 12f4bb0e-b71e-4a49-9672-b6eefcabab54Market UUID: f9b97291-7544-46ba-a423-09269d9f9e7eOrganization UUID: 196d4442-0f84-46b5-a0ae-116e118e6484

 **Note**

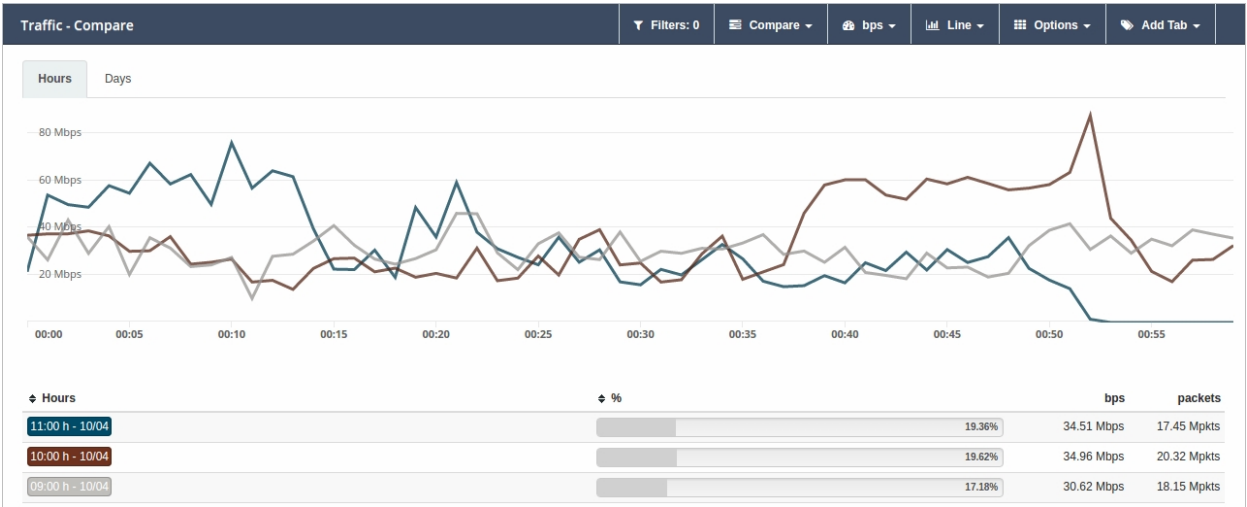
As you can see in the figure, the graph that best illustrates the Raw view is data flow or **Streams**.

In the Raw view, attributes are displayed in columns.

5.3.3 Compare

This view helps compare the hourly, daily, weekly and monthly evolution of events. Thanks to this tool, the user can easily spot the moment where the network was most used based on various parameters (such as the bytes consumed, the packets transferred, or the flows received).

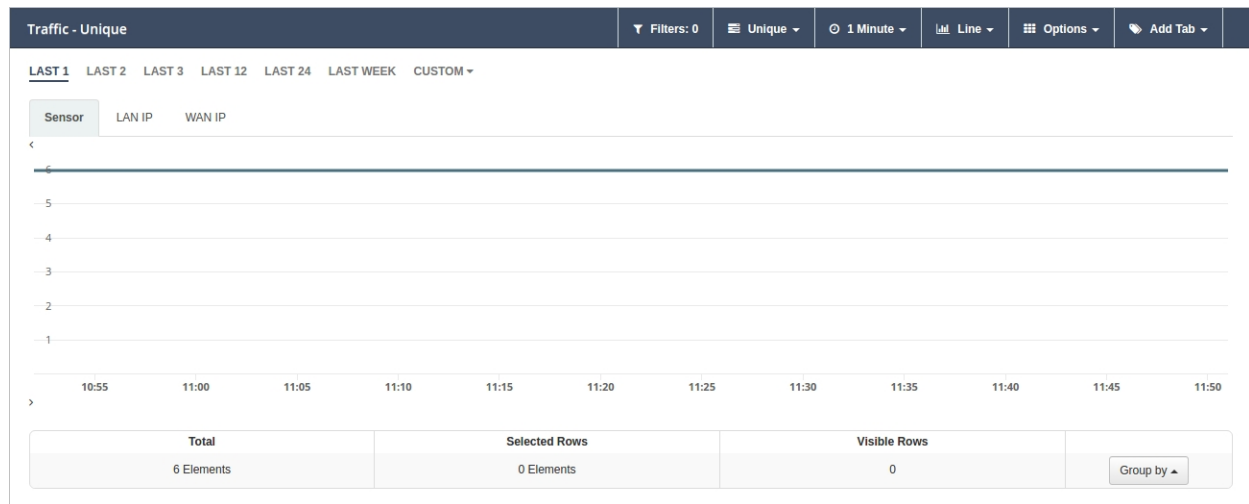
The data table shows the sum of the values for each time interval.



5.3.4 Unique

Through the **Unique** view, the user can gather information on the different elements that have interacted, at least once, with the network over a given period of time.

Selecting the group of attributes to analyze is also possible by clicking on the **Group by** option.



5.4 Types of aggregation

This option allows the user to pick the unit of measure in which he/she wants results to be shown.

These are the different units and metrics you will find in this tab:

- bps
- bytes
- packets
- packets/s
- flows
- flows/s

<input checked="" type="checkbox"/> bps	
<input type="checkbox"/> bytes	
<input checked="" type="checkbox"/> packets	
<input type="checkbox"/> packets/s	
<input type="checkbox"/> flows	
<input type="checkbox"/> flows/s	



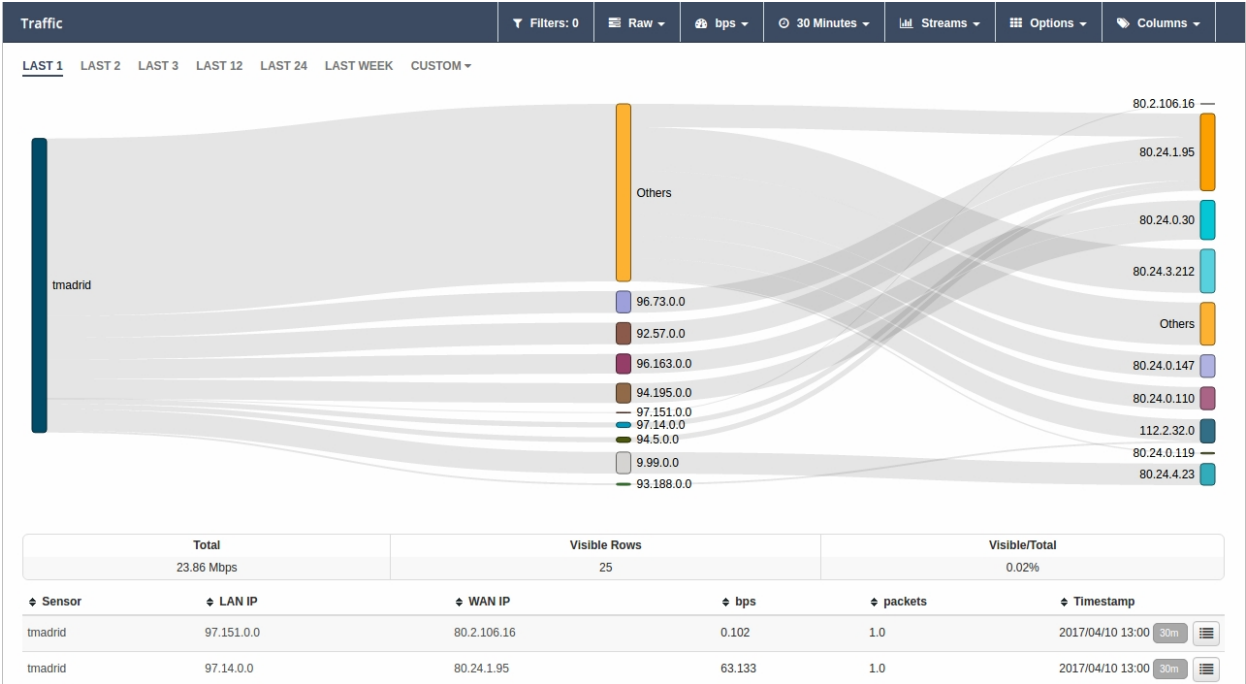
Note

Optimize your metrics by combining different types of aggregation with the granularity options available (level of temporal detail).

5.5 Granularity

The term “granularity” refers to the amount of detail with which we can view events. Granularity options vary depending on the time range displayed (1h., 2h., last week, last month, all, etc.).

- 1 Minute
- 2 Minutes
- 5 Minutes
- 15 Minutes
- 30 Minutes
- all



Note

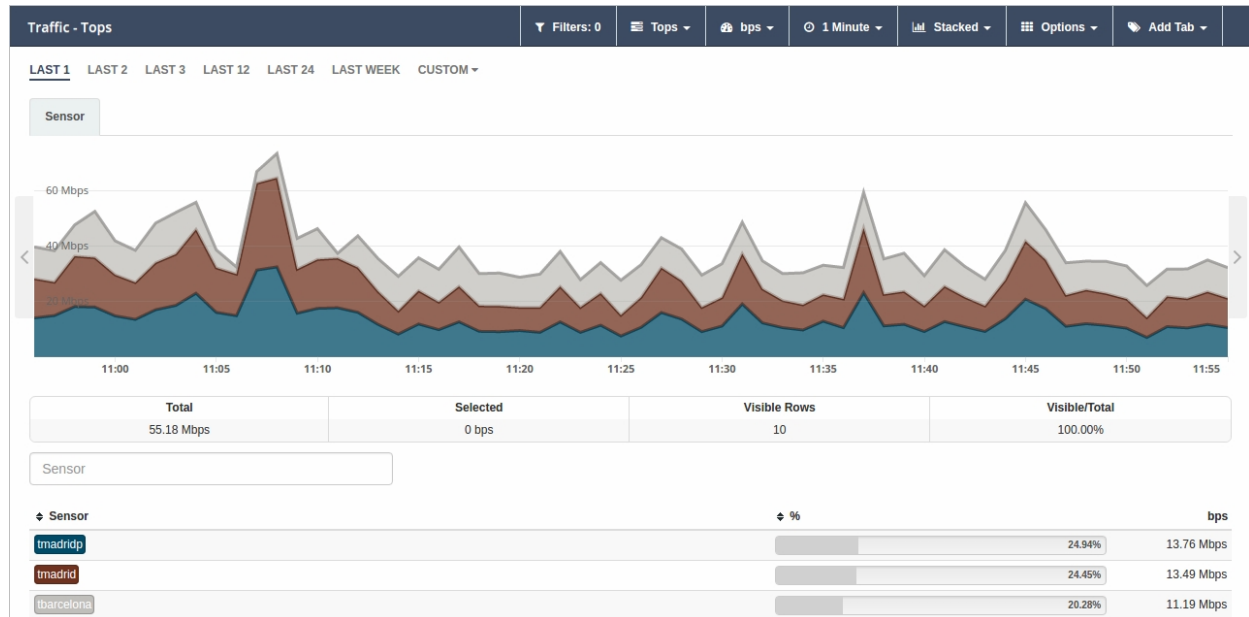
The Raw view is the best choice to analyze data in detail.

5.6 Types of charts

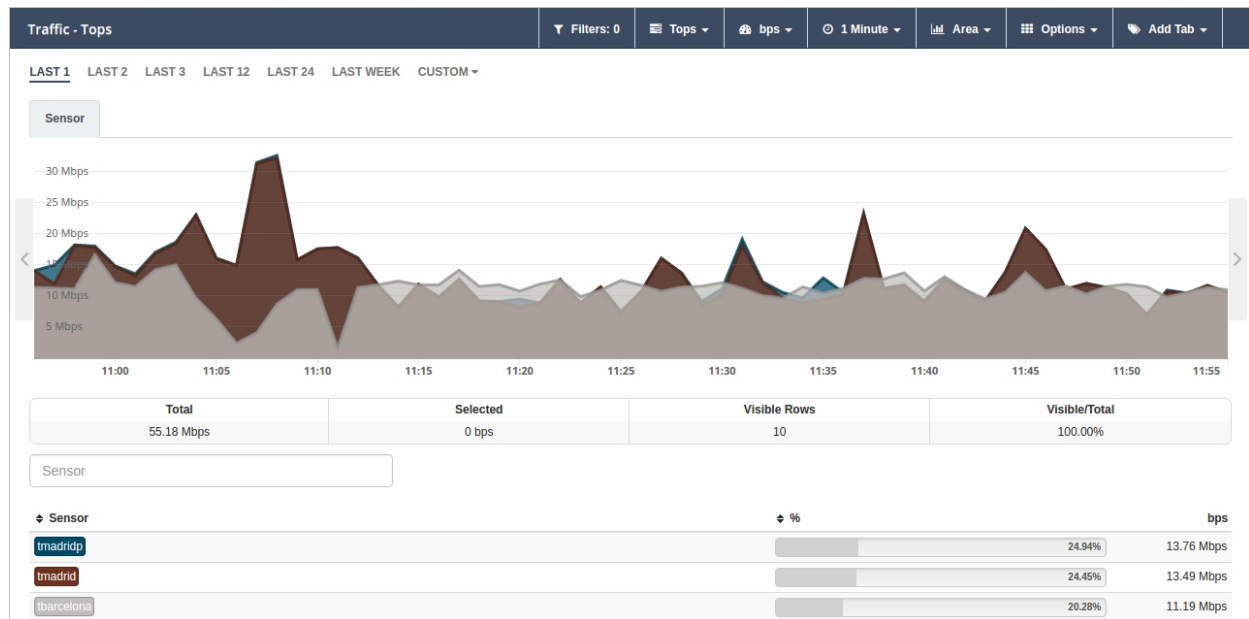
Selecting the type of graph in which you wish to see the collected data is possible. The options available are very similar to the ones shown when creating custom widgets (see the chapter on Dashboards).

The graphs available will vary depending on the view currently selected. All of them will represent the values selected based on time, granularity and aggregation, as well as on the options available per view type. The different graphs available are described below.

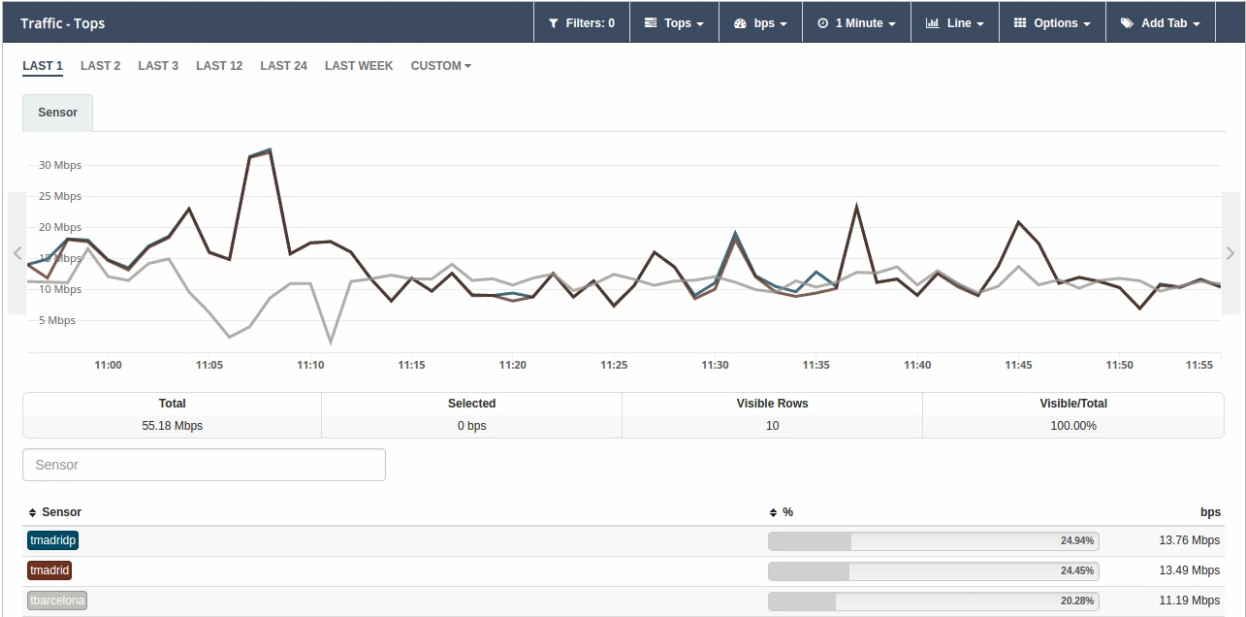
Stacked: set of stacked areas, each one representing the temporal profile of a selected value.



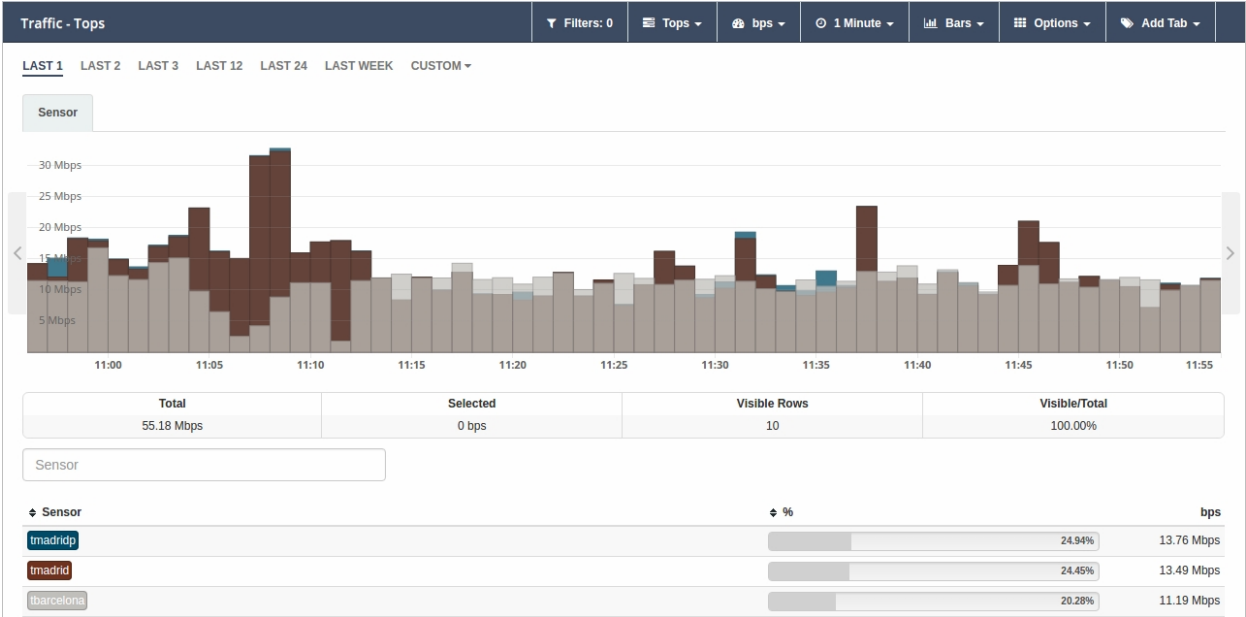
Area: set of overlapping areas, each one representing the temporal profile of a selected value.



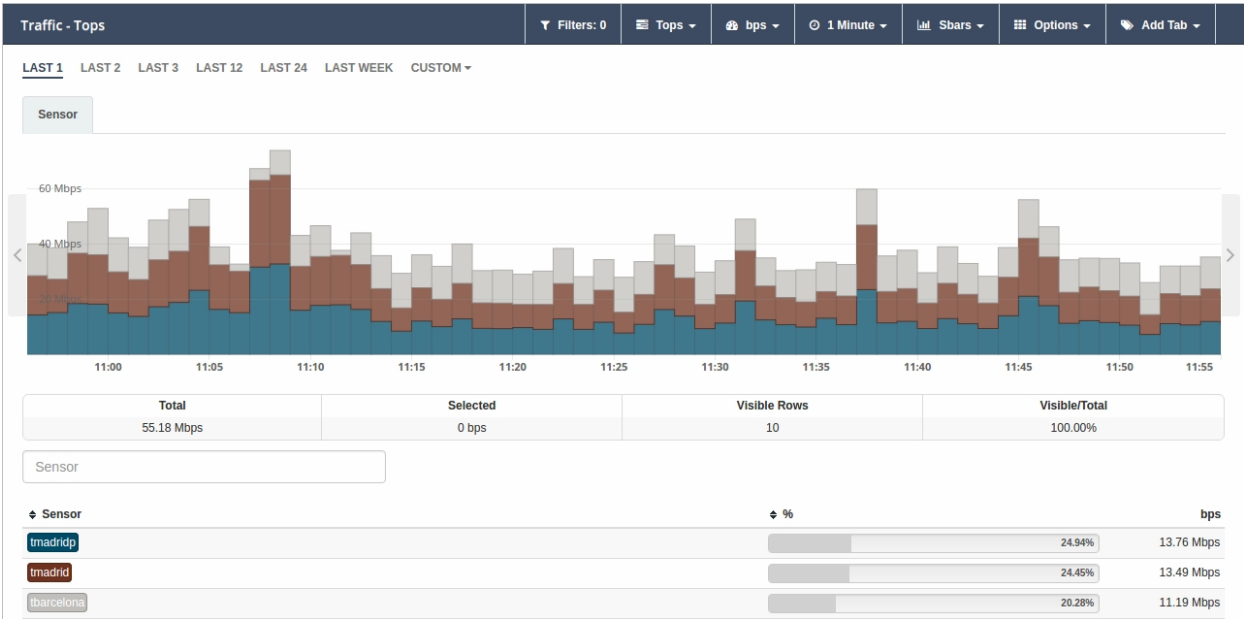
Line: set of overlapping lines, each one representing the temporal profile of a selected value.



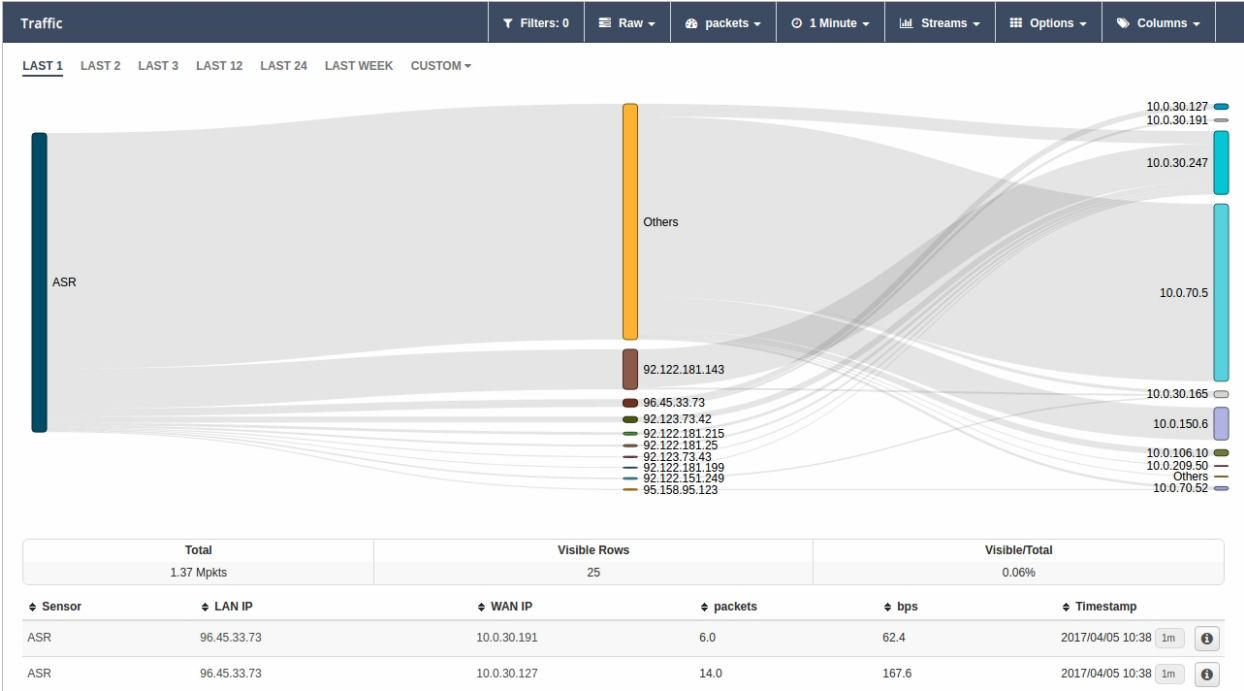
Bars: set of overlapping bars, each color representing the temporal profile of a selected value.



SBars (Stacked Bars): set of stacked bars, each color representing the temporal profile of a selected value.



Streams: set of flows, each representing the relationship between the different attributes. This graph is only available under the Raw view. The image below shows the traffic flows of a sensor between LAN and WAN IPs.



5.7 Options

Each view presents a series of options that allow the user, among other things, to view all traffic, export data to CSV or take the manager to a previous status to analyze past behaviors.

Every option available in this tab is detailed below. The user must bear in mind that the options will vary depending on the view selected.

- **Show Total**: when clicking on this option, a dotted gray line appears in the graph. It represents the sum of all attribute aggregations. When this option is enabled, the list of options will change this element to **Hide Total**. Available in the “Tops” and “Unique” views.
- **Show Total Filtered**: when clicking on this option, a dotted gray line (lighter in color than the one mentioned above) appears in the graph. It represents the sum of the attribute aggregations that appeared when the selected filters where applied. When this option is enabled, the list of options will change this element to **Hide Total Filtered**. Available in the “Tops” view.

- **Export to CSV:** the user obtains a download file in CSV format that includes the data corresponding to the attribute he/she selects (a limit can be set on the number of rows to be included in the file). Available in the “Tops,” “Raw” and “Unique” views.

Export to CSV ✕

Tab

Sensor

Limit

1000

Export Cancel

- **Time machine:** sends the manager to a prior stage. By selecting this option, the user can view the data as if he/she were looking at the information on the day and time indicated. Available in all views.

Time Machine ✕

March 2017

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Time 13:27

Hour

Minute

Go Cancel

- **Save tabs as default:** when enabling this option, the data tabs or columns selected for analysis will show up as default in all new searches. Available in the “Raw,” “Unique” and “Tops” views.
- **Sort Aggregations:** this option allows the user to choose the order in which available aggregations will be displayed. Available in the “Raw,” “Tops” and “Unique” views.

Sort Aggregations ✕

☰ packets

☰ bps

Accept Cancel

- **Sort Columns:** this option allows the user to choose the order in which the available columns will be displayed. Only available in the “Raw” view.

Sort Columns
✕

≡ Sensor

≡ LAN IP

≡ WAN IP

Accept

Cancel

- **Start Reloading:** activates the countdown for data reloading. The user may, at any time, stop this by clicking on **Stop Reloading** (the option that replaces “Start Reloading” once the latter has been enabled). The left end of the bar will show a timer indicating the time a user must wait for reloading. Available in the “Raw” view.

Traffic	↻ 291	▼ Filters: 0	≡ Raw ▼	📦 packets ▼	🕒 1 Minute ▼	📊 Streams ▼	⚙ Options ▼	🗖 Columns ▼
---------	-------	--------------	---------	-------------	--------------	-------------	-------------	-------------

5.8 Attributes: tabs and columns

Attributes help us carry out a customized and comprehensive analysis of every element involved in the network traffic being looked at.

They are organized in **tabs** or **columns**, depending on the type of view selected. The options displayed, except for “Compare”, are common to all views. The “Compare” option only allows data to be compared by weeks or months (not on the basis of attributes).

The attributes a user can use (and the different uses for each), are listed below:

- Application

Application

Engine

HTTP User Agent

Host

Host L2

Referrer

Referrer L2

Selector

Product Type

URL

- Flow

Direction

- Interface

LAN Interface

LAN Description

WAN Interface

WAN Description

- Location

WAN IP Country

WAN IP AS

WAN IP MAP

Service Provider

Namespace

Deployment

Market

Organization

Campus

Building

- Network

Conversation

LAN IP

LAN IP Name

LAN Net Address

WAN IP

WAN IP Name

Protocol

TOS

Sensor Type

Scatterplot

- Transport

LAN L4 Port

WAN L4 Port

TPC flags

- UUID

Service Provider UUID

Namespace UUID

Deployment UUID

Market UUID

Organization UUID

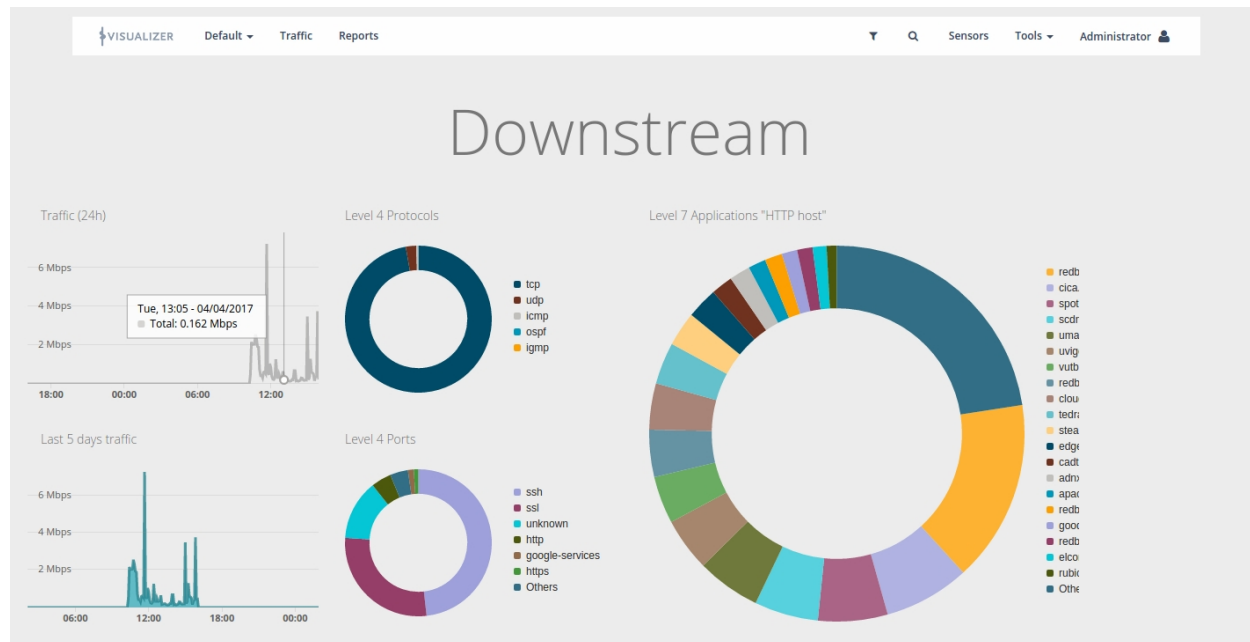
Campus UUID

Building UUID

Chapter 6 Dashboards

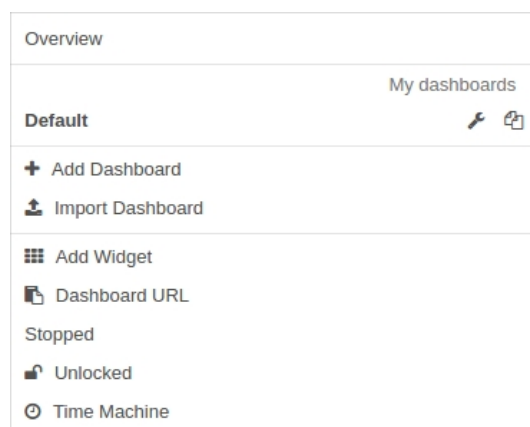
6.1 Dashboard Options

Dashboard is the first option to appear in the menu analysis area. This is the default option on entering the manager web.




The dashboard section displays multiple options:

- List of available dashboards: the first part of the dashboard menu shows the pre-created dashboards available for a user profile. Next to each dashboard, there are two icons:
 - : to view and edit the panel's general configuration.
 - : to clone the selected dashboard.
- Add dashboard/Import dashboard: adds a new personalized dashboard and imports pre-created ones. Any user can export a dashboard to a file and share it with other users (enabling them to import it as required).
- Add widget: adds any widgets you need to customize dashboards.
- Dashboard URL: copies the current dashboard to the system's clipboard.
- Locked/Unlocked: a user can lock/unlock a dashboard he/she is working on so that other users (with permissions) can't edit it.
- Time Machine: allows a user to 'travel in time' and view the results of a specific day and time metric (history).



6.1.1 Editing and cloning available dashboards

Edit a dashboard: General Settings

By clicking on the  icon, a user can always modify the information associated to each available dashboard through the General Settings option.

The following data can be edited in the general dashboard configuration menu:

- **Name.**
- **Set this dashboard as default.**
- **Layout:** visual structure of the widgets and metrics on the dashboard.
- **Description:** describes the content of the dashboard.
- **Background Color.**
- **Dashboard users:** adds and removes users that can view the dashboard and have editing permissions.
- **Dashboard domains:** adds and removes domains included in the dashboard.

The user can also view further available options in the area below the screen:

- **Update dashboard**
- **Cancel**
- **Delete**
- **Convert to report**
- **Export dashboard:** the system creates a zipped file for downloading (mandatory step for a user to import).

Edit dashboard

General Settings

* Name

Default

☐ Set this dashboard as default

Description

Layout

Column-based

Background color

✓

Dashboard users

+ Add

Name	Edit permissions	Remove

Dashboard domains

+ Add

Name	Edit permissions	Remove

Update Dashboard

Cancel

Delete

Convert to report

Export dashboard

- **Clone dashboard:** dashboards can be copied so that other users can import them, etc. Simply assign a name to the copied dashboard.

Clone Default

×

* Name

Clone dashboard

Cancel

6.1.2 Add dashboard

Dashboards provide a visual summary and include the main KPIs needed to analyze a network infrastructure. A user can combine a series of widgets to obtain a simple view of valuable information on the trends, changes and exceptions associated to the traffic generated or passing through his/her network.

Create a new dashboard by selecting the **Add dashboard** option. Next, enter a series of general configuration data and save the changes (**Create dashboard**). Create a blank panel to generate a customized dashboard and then add any widgets.

To edit a dashboard, indicate a series of preferences in the general configuration interface (**General Settings**) as previously described.

The screenshot shows the 'New dashboard' configuration form. It has a dark blue header with the title 'New dashboard'. Below the header is the 'General Settings' section. It contains a text input for '* Name', a checkbox for 'Set this dashboard as default', a dropdown for 'Layout' (currently set to 'Column-based'), a text input for 'Description', and a color palette for 'Background color'. Below this is the 'Dashboard users' section with a table that has columns for 'Name', 'Edit permissions', and 'Remove'. There is an '+ Add' button to the right of the table. Below that is the 'Dashboard domains' section with a similar table and an '+ Add' button. At the bottom of the form are two buttons: 'Create Dashboard' and 'Cancel'.

6.1.3 Import dashboard

Enables the sharing of dashboards with other users and helps provide the manager with information sourced from other compatible applications.



Note

To import a dashboard, the latter must be pre-exported in a zip file and available from the existing files.

Select the file to import and click on **Import dashboard**. The new dashboard will be added to the list of available dashboards.

The screenshot shows the 'Import a dashboard' dialog box. It has a title bar with the text 'Import a dashboard' and a close button (X). Below the title bar is a 'File' section with a 'Choose file' button and a text input field. At the bottom of the dialog are two buttons: 'Import dashboard' and 'Cancel'.

6.1.4 Adding a widget: customizing dashboards

A user can create and add widgets to his/her dashboards to customize the view of data taken from different apps. Preconfigured and 100% customized widgets can be added.

First, select the widget type to add. There are three, depending on what information the user wants to view:

- **Apps**: view data received from different applications.

Traffic

- **State:** view the configuration and state of the network machines and infrastructure.

Infrastructure

- **Format:** configures the content and format of widgets: text, images, URL, etc.

Shapes

Select the widget type

Select the product type:

Traffic

Infrastructure

Shapes

Combination

Cancel

6.1.4.1 Customizing a product widget

Some available widgets can be fully customized. The user can access them and add them to the manager dashboard.



Note

Events received by the Manager are made up of "column: value" pairs. The values in each column are event data.

To customize a widget, first select the data view mode. The user can also select the views to represent their cardinality.

Configuring widgets complying with event views :

- **Bandwidth Line:** predefined widget, which shows bandwidth use in bps. This is displayed as a simple graphic (typical **Traffic** app aspect).
- **Bandwidth:** similar to **Bandwidth line** , but provides more in-depth details (typical Traffic app aspect).
- **Map:** displays global positioning information (typical **Traffic** app aspect).
- **RAW:** displays the raw events (without aggregation).
- **Tops:** aggregates events, complying with an attribute, to show the most important ones. This displays the sum total of the data for different events as a single event.
- **Compare:** time comparative (hours, days, weeks and months) for the most important events.

For instance, this is used to compare traffic time evolution for a specific application.

- **Performance Index:** defines an index, where a user can see the performance of selected events.

Configuring widgets according to cardinality :

- **Single Unique:** use this option to isolate occurrences or events, from a column, for a specified time.
- **Grouped Unique:** use this option to isolate occurrences or events, from a column, for a specified time and grouped according to specified criteria.

6.1.4.2 Customizing a state widget

The user can choose from four types of widgets applicable to the manager configuration options. Use **Infrastructure** to select how you want to view information on the configuration and state of the network infrastructure:

- **Sensor:** Map/Tree.
- **Cluster:** Diagram/Table.
- **Alarm:** insert configuration details in the attached form.
- **Monitor:** Series/Value.

6.1.4.3 Format widgets

The **Shapes** option edits and inserts auxiliary elements in the widgets: such as text, image, widget shape and embed a customized URL.

Integrate these elements into widgets by filling out the form attached to each element, and then apply the changes by clicking on **Create Widget**.

6.1.5 Time machine

Use this option to return the time machine to a previous state (specified by day and time). The user can view the data as if in 'real time'.

'Time travel' offers maximum precision analysis, as the user can select the exact minute he/she wants to consult.

Time Machine

March 2017

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Time

13:27

Hour

Minute

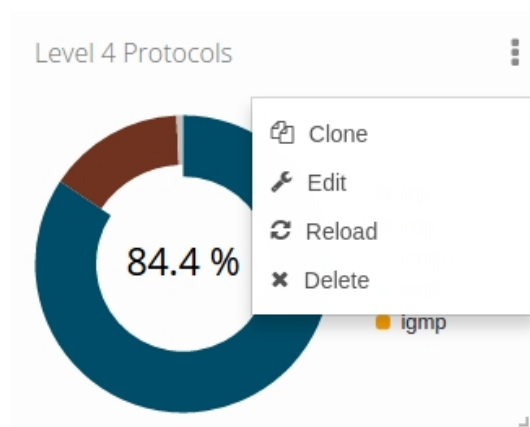
Go

Cancel

6.1.6 Cloning, editing, reloading and deleting widgets from the dashboard

The user can directly access widgets from the dashboard. The pull-down menu (on the upper right-hand corner) provides direct access to the following actions:

- **Clone**: duplicates and directly inserts the widget onto the selected dashboard.
- **Edit**: accesses the widget's general configuration to modify fields.
- **Reload**: updates data.
- **Delete**.



**Note**

If you select **Delete**, the system automatically asks for confirmation. Should you accidentally delete a widget, return to **Add widget** and reinsert it or copy one with similar characteristics and edit it.

Chapter 7 Updating a cluster

This chapter describes the procedure to update a redborder cluster of Manager servers.

This may differ, depending on whether the redborder cluster has access to Internet or not.

7.1 Updating from a remote repository

With Internet access, a redborder ISO isn't required to update a cluster. Simply execute `rb_cluster_update.sh` (script) in the manager node

```
# rb_cluster_update.sh
```

First, select the packages you wish to update. You have two choices: system or redborder packages (the latter requires redborder updating). Here, we've selected redborder packets (option 2).

```
#####
# redBorder cluster ready to be updated
#####
Which packages would you like to update:
  1.- system packages
  2.- redBorder packages
  3.- both
  4.- nothing
Choose an option: 2
```

Next, indicate whether you want to update from a local or remote repository (the latter requires an Internet connection).

Here, we have decided to update from a remote repository and selected option 1.

```
Available repositories:
  1.- remote (repo: http://repo.redborder.com/bintec elmeg GmbH)
  2.- local
Choose an option: 1
```

After checking the current system version, the next step asks which version you want to update. Here, select your version from those available in the remote repository.

```
Detecting available redBorder versions: [ OK ]
  1.- 3.1.79-5
Choose a valid version: 1
```

A script then appears, showing the order the cluster nodes will be updated in.

```
INFO: The following nodes will be updated in the following order:
  * node1
  * node2
  * node3
Are you sure you want to continue? (y/N) y
```

At this point, the procedure to update a cluster begins.

7.2 Updating from ISO (offline mode)

A redborder ISO is needed to update a cluster without Internet access. The master cluster node is updated (in the local repository) from the ISO. The master can be subsequently used for the rest of the nodes in the cluster.

First, execute the **`rb_cluster_update.sh`** script.

Once executed, a wizard opens to guide you through the updating process.

Next, select the packets to update. You can opt for system or redborder packages (the latter will need to be

updated). Here, we've selected redborder packages (option 2).

```
#####
#  redBorder cluster ready to be updated
#####
Which packages would you like to update:
  1.- system packages
  2.- redBorder packages
  3.- both
  4.- nothing
Choose an option: 2
```

Next, indicate the repository you want to update: local or remote (the latter requires an Internet connection).

In this example, we're going to update the system from a local repository and select option 2.

```
Available repositories:
  1.- remote (repo: http://repo.redborder.com/bintec elmeg GmbH)>
  2.- local
Choose an option: 2
```

The program then asks if you want to update the local repository from a redborder ISO. You can include a new redborder version in the local repository where it can be used by all cluster nodes.

```
Would you like to update local repo from a new ISO file? (y/N) y
Set redBorder ISO path: /tmp/redBorder-3.1.79-5-x86_64-6.5-enterprise.iso
Mounting ISO and copying files in local repo
```

After checking the current system version, the next step asks which version you want to update. Select from those available in the local repository.

```
Detecting available redBorder versions:          [ OK ]
  1.- 3.1.79-5
Choose a valid version: 1
```

Once you've selected the version, the program indicates the cluster nodes to update. You are asked to confirm prior to starting the procedure.

```
INFO: The following nodes will be updated in the following order:
  * node1
  * node2
  * node3
Are you sure you want to continue? (y/N) y
```

Once confirmed, the process of cluster updating begins.

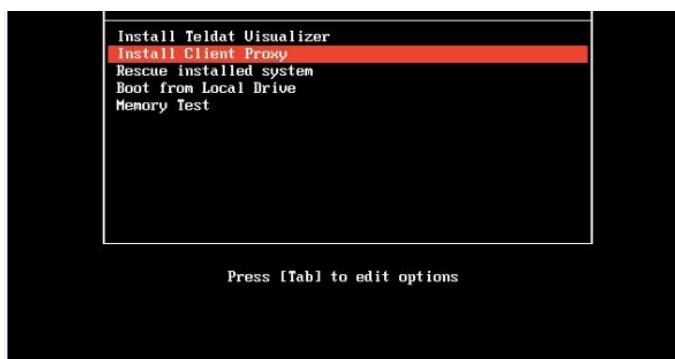
Chapter 8 Client Proxy

8.1 Introduction

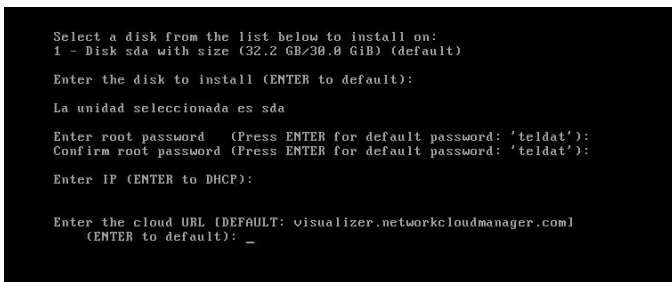
The client proxy is a special type of sensor. More than a sensor, it's really a system that goes beyond simply indicating where a cluster is installed and where sensors can be directly associated. This is useful as it can be installed and associated to sensors on networks and installations when sensors cannot directly access the managers' cluster (or the cloud service) due to security policies.

8.2 Installation

This is installed in a similar way to the manager. Use the same ISO image and select "Install Client Proxy" from the installation menu (after booting the ISO).

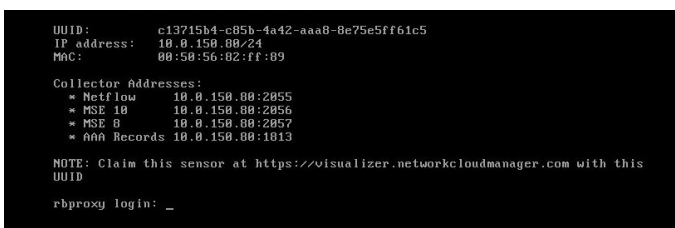


A list of questions then appears, with default answers (similar to the manager installation process). The only difference is that, here, you are asked for the cluster URL to connect to the default cloud URL (visualizer.networkcloudmanager.com).



The installation process will then begin.

Once installed, the system restarts. The following content will then be displayed on the terminal:

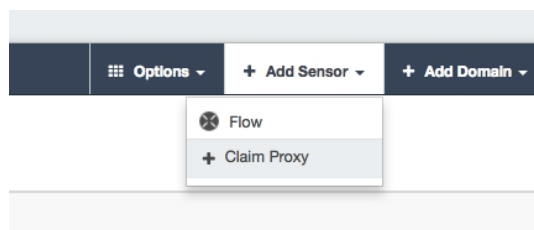


This shows information on the UUID assigned to the client proxy, its IP address, the MAC and information on the cluster services:

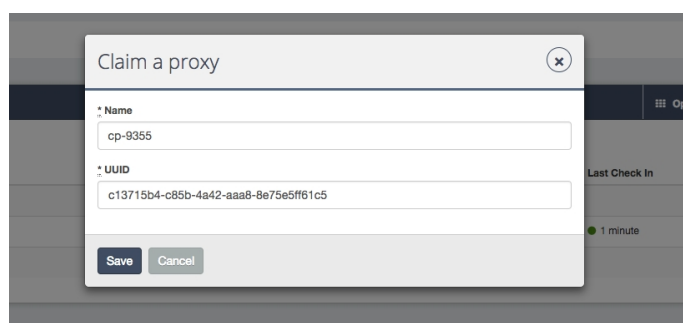
8.3 Register

Once the client proxy is installed, register the device in the cluster (on-premise or cluster in the cloud). The client proxy needs an unrestricted https/443 access to said cluster (on-premise or cloud) to successfully register said device.

The registration process consists in the client proxy identifying as an unclaimed sensor in the cluster. As the client proxy UUID is known a priori (from the installation process), use it to locate the device (list of unclaimed sensors). Access the redborder web and go to Sensors # add sensor # Claim proxy.

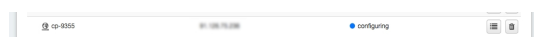


Next, enter a name and the UUID (from the installation).

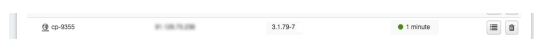


If the client proxy, with said UUID, exists on the list of unclaimed, the system locates it and assigns a namespace (pertaining to the user as simply another sensor).

The configuration displays the process status (see the following figure):



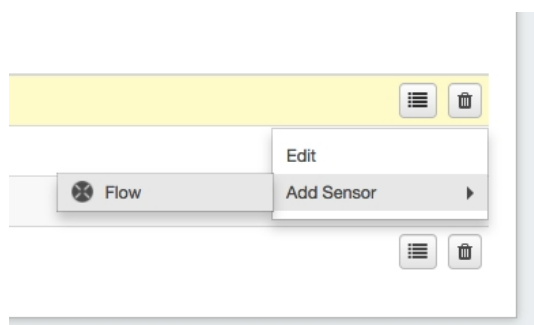
If successful, once the configuration and the registration and reclaim process are complete, the new status will appear:



8.4 Managing the sensors

You can register sensors managed by the client proxy in a similar way to registering a cluster. First, go to sensor information. There is a menu button to the right of the client proxy row. Click on this to open the following options:

- **Edit:** Accesses information on the client proxy.
- **Add Sensor:** Adds sensors to the client proxy.



8.5 Updating

Update the client proxy in the same way as any distribution software package, through a yum repository and execute the following:

```
[root@cp-9355 ~]# yum update redBorder-proxy
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.tedra.es
 * elrepo: mirrors.coreix.net
 * epel: mir01.syntis.net
 * extras: mirror.tedra.es
 * updates: mirror.tedra.es
Setting up Update Process
Resolving Dependencies
--> Running transaction check
---> Package redBorder-proxy.x86_64 0:3.1.79-7 will be updated
---> Package redBorder-proxy.x86_64 0:3.1.79-9 will be an update
--> Finished Dependency Resolution
Dependencies Resolved

=====
Package                        Arch          Version        Repository     Size
=====
Updating:
 redBorder-proxy                x86_64        3.1.79-9       redBorder      220 M
Transaction Summary
=====
Upgrade      1 Package(s)
Total download size: 220 M
Is this ok [y/N]: y
Downloading Packages:
redBorder-proxy-3.1.79-9.x86_64.rpm           | 220 MB    00:21
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
Warning: RPMDB altered outside of yum.
  Updating      : redBorder-proxy-3.1.79-9.x86_64
chef-client already stopped
Stopping nprobe/log (pid: 25408) [ OK ]
Waiting for nprobe to stop completely (pid: 25407)[ OK ]
Stopping rb-sociald (pid: 26242) [ OK ]
Stopping rb-sociald/log (pid: 26240) [ OK ]
Waiting for rb-sociald to stop completely (pid: 26239)[ OK ]
Stopping n2klocd (pid: 25542) [ OK ]
Stopping n2klocd/log (pid: 25541) [ OK ]
Waiting for n2klocd to stop completely (pid: 25540)[ OK ]
Stopping freeradius (pid: 25898) [ OK ]
Stopping freeradius/log (pid: 25897) [ OK ]
Waiting for freeradius to stop completely (pid: 25896)[ OK ]
Stopping nmspd (pid: 26031) [ OK ]
Stopping nmspd/log (pid: 26029) [ OK ]
Waiting for nmspd to stop completely (pid: 26028)[ OK ]
```

```

Stopping rb-snmp (pid: 26383) [ OK ]
Stopping rb-snmp/log (pid: 26382) [ OK ]
Waiting for rb-snmp to stop completely (pid: 26381)[ OK ]
Stopping rb-monitor (pid: 25675) [ OK ]
Stopping rb-monitor/log (pid: 25674) [ OK ]
Waiting for rb-monitor to stop completely (pid: 25673)[ OK ]
Stopping k2http (pid: 26850) [ OK ]
Stopping k2http/log (pid: 26847) [ OK ]
Waiting for k2http to stop completely (pid: 26846)[ OK ]
Stopping rb-apspoller (pid: 26639) [ OK ]
Stopping rb-apspoller/log (pid: 26637) [ OK ]
Waiting for rb-apspoller to stop completely (pid: 26636)[ OK ]
Stopping kafka (pid: 22672) [ OK ]
Stopping kafka/log (pid: 22671) [ OK ]
Waiting for kafka to stop completely (pid: 22670)[ OK ]
Stopping zookeeper (pid: 22514) [ OK ]
Stopping zookeeper/log (pid: 22512) [ OK ]
Waiting for zookeeper to stop completely (pid: 22511)[ OK ]
rb-register already stopped
Iniciando snmpd:
Iniciando ntpd:
    - installing ruby version manager (RVM) ... done
Starting zookeeper (pid 1809) 3s; log: (pid 1806) 3s[ OK ]
Starting kafka (pid 1922) 3s; log: (pid 1919) 3s[ OK ]
Starting k2http (pid 2274) 3s; log: (pid 2273) 3s[ OK ]
Starting nprobe (pid 2364) 3s; log: (pid 2361) 3s[ OK ]
Starting rb-sociald (pid 2452) 3s; log: (pid 2449) 3s[ OK ]
Starting rb-snmp (pid 2548) 3s; log: (pid 2545) 3s[ OK ]
Starting nmospd (pid 2654) 3s; log: (pid 2651) 3s[ OK ]
Starting n2klocd (pid 2818) 3s; log: (pid 2816) 3s[ OK ]
Starting freeradius (pid 2905) 3s; log: (pid 2903) 3s[ OK ]
Starting rb-monitor (pid 2991) 3s; log: (pid 2988) 3s[ OK ]
Starting rb-apspoller (pid 3175) 3s; log: (pid 3172) 3s[ OK ]
Starting chef-client (pid 3343) 3s; log: (pid 3342) 3s[ OK ]
Cleanup      : redBorder-proxy-3.1.79-7.x86_64                2/2
Verifying    : redBorder-proxy-3.1.79-9.x86_64                1/2
Verifying    : redBorder-proxy-3.1.79-7.x86_64                2/2
Updated:
redBorder-proxy.x86_64 0:3.1.79-9
Complete!

```



Note

This may take several minutes.

Once complete, the client proxy will be updated (in the repository) with the latest version available.