Report Manager 1.6.0

Technical documentation

Katarzyna Wladyszewska, Hadden Sp.J.

Report Manager 1.6.0: Technical documentation

by Katarzyna Wladyszewska

Published April 2010

HADDEN MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MANUAL, INCLUDING, BUT NOT LIMITED TO, THE WARRANTY OF DESIGN, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

List of Tables

Chapter 1. Conventions

The following typographical conventions are used in this manual:

Table 1.1. The typographical conventions used in this manual

Font	What the font represents	Example
Italic	Environment variables.	The name is kept in environmental variable *$DAVIDPRIVDIR*...
Italic	Synopsis options.	[*-l,--log-facility log_facility*]
Bold	Names of programs and products.	**damcsud** is a part of **Operation Manager-a**.
`Computer`	Names of options and menus.	There is `Show tool bar` option in `View` menu.
`Computer`	Names of files and directories.	... reads its configuration file `.damadbudrc`.
`Computer`	Names of windows and dialog fields.	In `A sessions property` window, in `Sticking string` field, you can write...
`Computer`	Names of buttons.	Pressing `Apply` button lets you apply changes.
`Computer Bold`	Math formulas.	**`exp( -x ), when a = 0 1 / pow( a , a ) * pow( x , a ) * exp( -x + a ), when a > 0`**.
`Computer Bold`	Terms used in David system terminology.	**`SNMP Data`** - a kind of data...

`Computer Bold`	Contents of configurations files.	**`action`**
		`{`
		`...`
		`}`

Chapter 2. General information about David system

2.1. General

David systemis a network management system. It is a packet of applications (modules) that allows computer network to be monitored and managed in real-time through the Internet. There is only one condition that managed devices must meet. Each device must provide SNMP (Simple Network Management Protocol) service. SNMP is the most common management protocol in the Internet so that requirement shouldn't be difficult to meet. Here is the list of typical devices that can be monitored:

- IP routers,
- ATM switches,
- manageable ethernet switches,
- UPSes with a SNMP adapter,
- TV-SAT modems that allow IP devices to work in TV cable networks,
- computers.

One of the most important feature of **David system** is its architecture. It's built of high level configureable and independent from one another modules. This principle is the most essential rule of the project. In consequences, in th metter of speaking, the same modules may build different management system. Here are the main features of **David system**:

- general thinking in information flow controlling that come form high level independence of modules of the system,
- high level configureability of the system modules that allows a special configuration of **David system** to reach end-user expectations so close as it's only possible,
- the system scalability, so you can build up the system adding additional modules in very easy way; note that these modules needn't to be part of **David system** at all; adding another monitored devices to the system is a very easy procedure,
- using shell scripts in information processing is opportunity for modeling information and influence on processing it,
- all configuration files of **David system**, files with input/output data and log files are text files,

- using SNMPv1, SNMPv2C and SNMPv3 to communicate with monitored devices.

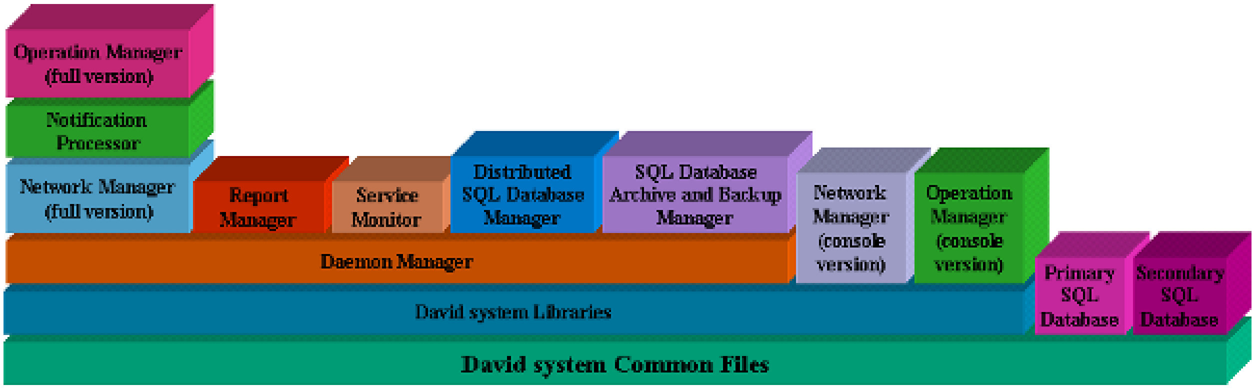
2.2. David system architecture

Table 2.1. David system products

Product	**Description**
David system Common Files	The product, during its installation, prepares the rudimentary directory tree for other products of **David system**. It also contains some essential and common files for all the products. Thus, this is a fundamental product of **David system** required by other its products.
Primary SQL Database	The product installs the primary SQL database of **David system**. Every single installation of **David system** must have only one the primary database.
Secondary SQL Database	The product installs the secondary SQL database of **David system**. Each installation of **David system** may have many secondary databases or none. It allows to distribute the SQL database of **David system** among many servers.
David system Libraries	This product provides libraries of **David system** required by its applications. Many other products of **David system** require that one.
Daemon Manager	It engages in running and terminating daemons of **David system** as well as monitoring of their work.
Network Manager (full version)	The product using SNMP protocol allows to visualise a topology of monitored networks and auto-discover devices in managed networks. The state of monitored devices also is visualized. The product also collects data from monitored devices using SNMP protocol and allows you to manage user accounts.
Network Manager (console version)	The product, through a graphic application, allows to visualize a topology of monitored networks and shows states of monitored resources. It allows you to control daemons monitoring devices as well as that ones gathering data. Currently, most of functions of that application is obtainable through web applications.
Notification Processor	The product chiefly engages in processing SNMP Trap notifications coming from monitored devices to management stations. The received messages can be formatted to the human readable forms, and then recorded as well. The processed notifications can be passed on to future processing.
Operation Manager (full version)	It can run specified actions on the basis of received data. Sophisticated estimation process depends on information coming from other products of **David system** and correlation of that information. It tries to build more intelligent and useful notifications then just simple reactions to incoming

Product	Description
	events. The graphic application displays notifications about received events and allows to play audio files as well as reading messages by an outer speach synthesizer.
Operation Manager (console version)	The product contains a graphic application displaying notifications about events and allowing to play audio files as well as reading messages by an outer speach synthesizer.
Report Manager	The product processes recorded SNMP Trap notifications, entries about pending operations and entries about state changes of monitored devices (ping objects, network interfaces and BGP peers), and generates raports on the basis of them. Raports can be viewed using a Web application.
Service Monitor	The product monitors selected network services on application level. In order to do this it monitors selected TCP ports of specified hosts. It checks both availability of ports and a correct reaction for a few selected network protocols (HTTP, SMTP, FTP). It also can verify correctness of work of selected services by verification of received data. Results of its work can be viewed as reports and graphs made available by a Web application.
SQL Database Archive and Backup Manager	It archives the SQL Database used by **David system** applications.
Distributed SQL Database Manager	It allows to devide the database of **David system** into one primary database and many secondary ones. Such step boosts performance of the system and decreases load of the servers where daemons of **David system** work. The migration takes place during the rutine work of the system. Such division may be altered many times.

Dependences between the **David system** products are shown on the following chart:.


Operation Manager (full version)
Notification Processor
Network Manager (full version)
Report Manager
Service Monitor
Distributed SQL Database Manager
SQL Database Archive and Backup Manager
Network Manager (console version)
Operation Manager (console version)
Daemon Manager
Primary SQL Database
Secondary SQL Database
David system Libraries
David system Common Files

David system functionality can be very large and it depends on particular configuration a lot. The most important features of **David system** are:

- discovering and visualization of monitored networks topology including visualization of states of particular nodes;

- possibility of building control panels to monitored devices (they must support SNMP protocol), regardless of device providers;
- formatting and recording SNMP Traps sent by agents working on monitored devices;
- automatic reaction to specified SNMP Traps received from monitored devices;
- possibility of identification of an operator that has received an alert from the system about a problem;
- collecting data concerning parameters of monitored devices;
- automatic reaction to incorrect values of data that were found during data collecting;
- recording pending cases, processed by the system, which have been created as responses for events detected by the system in a monitored network;
- monitoring selected network services on application level.

Chapter 3. Terminology

3.1. Authorization process made by David system products

The modules of David system which need to do an authorization of message senders (i.e. **damsnmpdaud**, **dnmmsd**, **dgnsd**), use the library, that checks whether an IP address of a sender matches with any record found in the file `.known.host`. The library expects to find the file in a directory pointed by a variable *confdir* in the file `/etc/system-david.conf`.

Records in the file `.known.host` are regular expressions specifying acceptable IP addresses.

3.2. David system terminology used in the documentation

There is an explanation of some terms, that are used in David system and its documentation:

- **`massages (information)`** - data received by interfaces of **Operation Manager**, its data analysers and **Cases Database Unit** of the product.

- **`notifications`** - the term often is used in the products: **Notification Processor**, **Operation Manager** and **Report Manager**; There are mostly data, that a source are SNMP agents working on network monitored devices.

- **`events`** - the term often is used in the products: **Operation Manager** and **Report Manager**; and it describes a being, that a source is SNMP Trap or SNMP Data; an **`event`** is always a part of a **`case`**;

- **`cases`** - the term often is used in the products: **Operation Manager** and **Report Manager**; and it describes a group of events connected one another; one **`event`** at last must be included in a **`case`**;

- **`SNMP Trap`** - a kind of data of **Operation Manager** product, which a source are received responses from SNMP agents; SNMP Traps aren't answers on the requests sent by a management station, but they are sent by agents managing network interfaces and processed by **Notification Processor** product;

- **`SNMP Data`** - a kind of data of **Operation Manager** product, which a source are received responses from SNMP agents on request which a management station sent to them by **Network Manager**.

Chapter 4. Installation

4.1. The main configuration file of David system

The essential configuration file of David system in `/etc/david-system.conf`. It contains entries as pairs: key = value. Basically, except the entry `default_email_recipient`, there is no such need to modify any record in that file. All necessary modifications are made during installation processes of particular David system products. Below, there is a list of all entries along with their descriptions that may occur in this basic configuration file.

- `user` - a name of the user with which rights all daemons of David system works;
- `default_email_recipient` - the default e-mail address where messages from David system applications are sent;
- `bindir` - the directory containing David system applications (default: /usr/bin/david-system);
- `libdir` - the directory containing David system libraries (default: /usr/lib/david-system);
- `incdir` - the directory containing David system headers (default: /usr/include/david);
- `confdir` - the directory containing David system configuration files (default: /etc/david-system);
- `logdir` - the directory containing log files of David system applications (default: /var/log/david-system);
- `sharedir` - the directory containing various files (images, audio files, web files) of David system (default: /usr/share/david-system);
- `docdir` - the directory containing various files (images, audio files, web files) of David system (default: /usr/share/david-system);
- `vardir` - the directory containing archive files of David system SQL database (default: /var/lib/david-system);
- `is_sqldb_installed` - the flag that indicate whether the SQL database of David system has been installed or not.

4.2. Dedicated account for service of David system

There is no needs to run any David system module as superuser (usually an account `root` with UID equals 0). Even if some David system daemon requires root rights when starting, there is always possibility to specify, as one of the daemons starting arguments, a user that rights should be taken.

It is a good idea to add a new user to an operating system, under which control David system will work.

4.3. Directories of David system

This hierarchy depends on a particular configuration of David system. In the default system configuration, David system contains the following directories:

- `/usr/bin/david-system` - binaries and shell scripts;
- `/etc/david-system` - configuration files;
- `/usr/share/doc/david-system` - the documentation;
- `/usr/share/david-system` - graphic and audio files, web portal;
- `/usr/include/david` - David system header files;
- `/usr/lib/david-system` - David system libraries;
- `/var/log/david-system` - log files;
- `/var/lib/david-system` - archive files of the David system SQL database;

4.4. Configuration of syslogd daemon

David system modules use `syslog` subsystem available on UNIX platforms. Default configuration of the system modules causes that log messages are sent with local6 `facility`. It may be changed for every module during its startup. Its recommended to configure `syslogd daemon` to write all messages from David system modules into one place (one or more files with characteristic name i.e.: david.log).

Chapter 5. Report Manager requirements

The following requirements must be met by a management platform on which **Report Manager** will work:

- installed, compatible version of **Daemon Manager**.

Chapter 6. Installation

6.1. Installation from the RPM package

You must be `root` to install the product. The typical installation looks as this one following below:

- Install the product:

```
rpm -i david-xxx-rm-yyy.rpm
```

6.2. Installation from the script

You must be `root` to install the product. The typical installation looks as this one following below:

- Uncompress and unpack the archive:

```
gunzip david-xxx-rm-yyy.i386.tar.gz
tar xf david-xxx-rm-yyy.i386.tar
```

  The operations create david-xxx-rm-yyy.i386 directory in your current directory.

- Change your current directory to david-xxx-rm-yyy.i386:

```
cd david-xxx-rm-yyy.i386
```

- Read LICENSE file from the current directory and CONTINUE THE INSTALLATION, ONLY WHEN YOU ACCEPT ALL CONDITIONS INCLUDED IN THE LICENSE.

- Run the installation script:

```
./install
```

Chapter 7. General

7.1. Functionality

Report Manager makes possible:

- creating hourly reports on the basis of SNMP Trap notification filters, defined by a user;
- creating hourly reports on the basis of registered case filters, defined by a user;
- creating hourly reports on the basis of monitored item (such as: ping objects, network interfaces and BGP peers) filters, defined by a user;
- visualisation of generated reports as daily, monthly and yearly graphic reports.

7.2. Description

Report Manager processes registered SNMP Trap notifications, entries concerning pending cases and entries concerning changes of states of monitored devices (ping objects, network interfaces and BGP peers), and generates raports on the basis of them.

Raports are generated on the basis of filter defined by a user.

Visualisation of generated reports is made using Web application. It filters raport results and joins small reports into larger ones, covers the same longer periods of time.

7.3. Related articles

Report Manager (dreportd)

Report Manager Configurator

Report Browser

Chapter 8. Report Manager (dreportd)

8.1. General

dreportd is **Report Manager** and it is a part of product **Report Manager**. It is a daemon process which works all the time the system is running and it processes recordered data every hour to generate a report in last hour. The data processing is corresponded with a configuration of the filters defined by a user using Report Manager Configurator.

8.2. Synopsis

dreportd can be run with the following options: [*-P,--pid-file filename*] [*-l,--log-facility log_facility*] [*-L,--log-level log_level*] [*-u,--run-as-user username*] [*--reports-since date*] [*--background*] [*-v,--version*] [*-h,--help*]

8.3. Options

Table 8.1. dreportd options

Option	**Description**
-P,--pid-file filename	Write PID to the specified file.
-l,--log-facility log_facility	Choose log facility: daemon | user | local0 | ... | local7 (default: local6).
-L,--log-level log_level	Choose log level (on stderr and syslog) i.e. messages of selected level and more important levels will be logged: emerg | alert | crit | err | warning | notice | info | debug0 | ... | debug2 (default: notice).
-u,--run-as-user username	Drop root privileges and run server as the specified user.
--reports-since date	Generate reports since specified date if no report has been generated yet (date format: 'yyyy/mm/dd hh').
--background	Go to background after startup.
-v,--version	Display version number on stderr and exit.
-h,--help	Display this help and exit.

8.4. Description

After startup, the program checks if it has outstanding reports to do. If it has them to do, it will successively make them. Otherwise it makes report in a current hour.

Outstanding reports can be made in a few coincidences. The program tries to find the last report which was finished correctly. If the program doesn't find the report in the last hour, it will make reports in successive periods of time beginning from the last report which was finished correctly. If the program finds no reports, it will make report in a current hour. If it is running with --reports-since option which relates to the past, it will make reports from a selected period of time.

If **dreportd** makes all possible outstanding reports, it begins its normal work. It waits for a lapse of full hour (i.e.: 15:00, 18:00 etc.) and makes a report in last, full hour. In first order it generates reports about SNMP Trap entries, and then about entries related to pending cases, and at the end about monitored devices (ping objects, network interfaces, BGP peers).

Report generating is finished a confirmation of the correct report making. Only these reports are treated as correct.

8.4.1. Processing of filters relating to SNMP Trap entries

On the basis of filters defined by a user, SQL statements are built. Then, their result of work is suitable interpreted. Each command is generated using a single filter. In the first order during a statement generating, the entires from `Group by` group of Report Manager Configurator are processed, according to an order of entries which is given in a configuration. Next, the entries from `Custom filters` group are used, and at the end the entries of `Rules` group. The `Field` columns for all three groups include a list of the fields, that characterized entries about SNMP Trap messages.

After building of SQL command, it is executed and each row of its result is interpreted using entries of `Group by` group and `Custom filters` one. At the beginning interpretation is executed with the aid of entries of `Group by` group. Each entry of the group corresponds with a single column of command result, that contents is interpreted according to a specification of `Treat as` and `Show` fields of a given entry.

`Treat as` field can take on the following values: `BGPPEER`, `NETINTERFACE`, `OBJECT`, `PINGOBJECT`. The field also can be empty (`--skip--` option of Report Manager Configurator). The values shows, how the contents of next columns of command result, that create through working of entries from `Group by` group, will be interpreted, and then translated into names of monitored devices (i.e.: names of devices, descriptions of network interfaces, entires of BGP peers).

`Show` field can take on the following values: `Yes`, `No`, `When others failed`, `If success`. The values show, how the contents of next columns of command result, that create through working of entries from `Group by` group, will be interpreted, and if the contents is including to the result of row processing. The values `Yes` and `No` don't need an explanation. The value `If success` means, that it will be taken into consideration, if it isn't empty, while `When others failed` value means, that it will be used, when values for all entries of `Group by` group are empty. The entry is a type of the stand-by entry.

The interpretation of the statement result with the aid of entries from `Custom filters` group is generated through `Filter` and `Result` fields. A suitable column contents of the command result, that was created through working of a given entry from Custom filters group, is parsed according to contents of Filter field and translated into an inscription according to contents of Result field.

8.4.2. Processing of filters concerning entries about pending cases

The processing of filters concerning entries about pending cases is similar to the processing of filters for SNMP Trap entries. One difference is a contents of Field columns for next three groups of each filter. In this case, Field columns include a list of fields concerning entries about pending cases.

8.4.3. Processing of filters concerning entires about monitored objects

The processing of filters concerning entires about monitored objects is made on the basis of filters defined by an administrator. Each filter includes a field describing a kind of the object which it concerns. Using the field, **dreportd** knows, where it will find entries concerning this kind of objects. Each filter can include a list of the allowable device types, which it concerns. By this, useless information is limited, that will be able to create as result of processing of a given filter (currently it concerns only network interfaces). A user can done a specification of the allowable devices in Allowed devices group of Report Manager Configurator.

8.5. Related articles

Report Manager Configurator

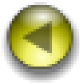
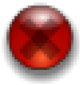
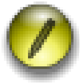
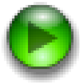
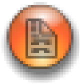
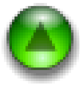
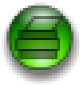
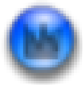
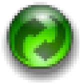
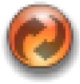
Report Browser

Chapter 9. Buttons the most often used in Web applications

9.1. The buttons meaning

There are the buttons, in the chart below, that occur the most often in Web applications. Their fucnction in particular applications is similar and even identical sometimes. Some of the buttons can have additional functions, that were described during descriptions of the particular applications.

Table 9.1. The buttons the most often used in Web applications

Button	Description
	It allows you to recover to a previous page.
	It deletes an item i.e.: it closes a case, sets an event in a passive state etc.
	It allows you to get to an edition of a given item.
	It confirms an operation and makes it (i.e.: generating of a report using selected criterions).
	It allows you to get to a detailed view.
	It allows you to get to a higher level of item hierarchy.
	It opens a new window with data which are prepared for a printout.
	It allows you to get to a presentation of the graph with data for a given item (Collection Browser).
	It reloads a page view.
	It accepts changed values as current one.

Button	**Description**
📄	It allows you to get to a report for a given item (Node Reporter).
❗	It lets you get to a Trap browser for a given item (Trap Browser).
▼	It lets you get to a report browser (about cases) for a given item (Recorded Operation Browser).
💾	It saves changes, that were done by a user.

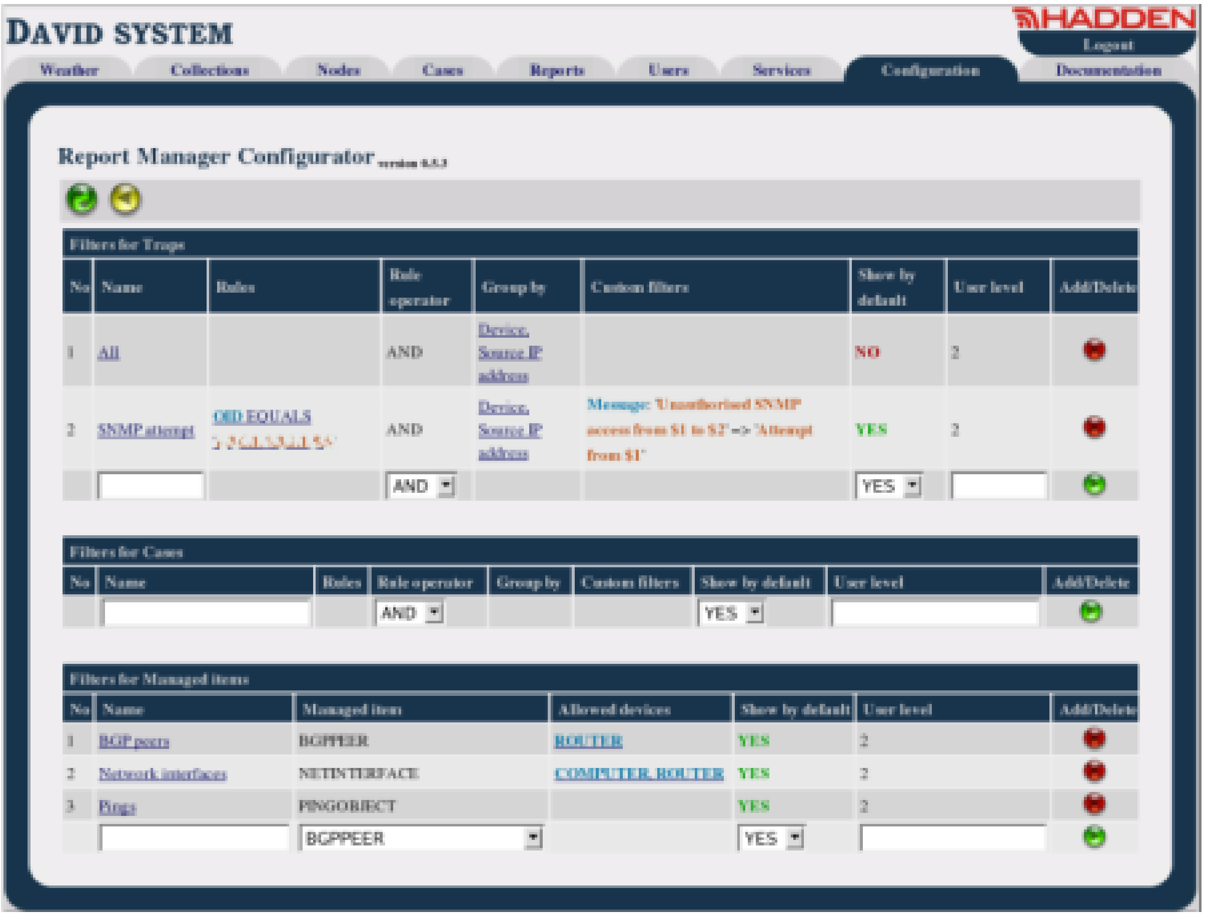
Chapter 10. Report Manager Configurator

10.1. General

Report Manager Configurator is a Web application and it is a part of **Report Manager**. The configurator allows you to control a work of Report Manager (dreportd) through defining filters, that help to generate reports.

10.2. Description

10.2.1. Default view of the application



Report Manager Configurator version [illegible]

Filters for Traps

No	Name	Rules	Rule operator	Group by	Custom filters	Show by default	User level	Add/Delete
1	All		AND	Device, Source IP address		NO	2	
2	SNMP attempt	OID EQUALS '[illegible]'	AND	Device, Source IP address	Message: 'Unauthorized SNMP access from $1 to $2' -> 'Attempt from $1'	YES	2	
			AND			YES		

Filters for Cases

No	Name	Rules	Rule operator	Group by	Custom filters	Show by default	User level	Add/Delete
			AND			YES		

Filters for Managed items

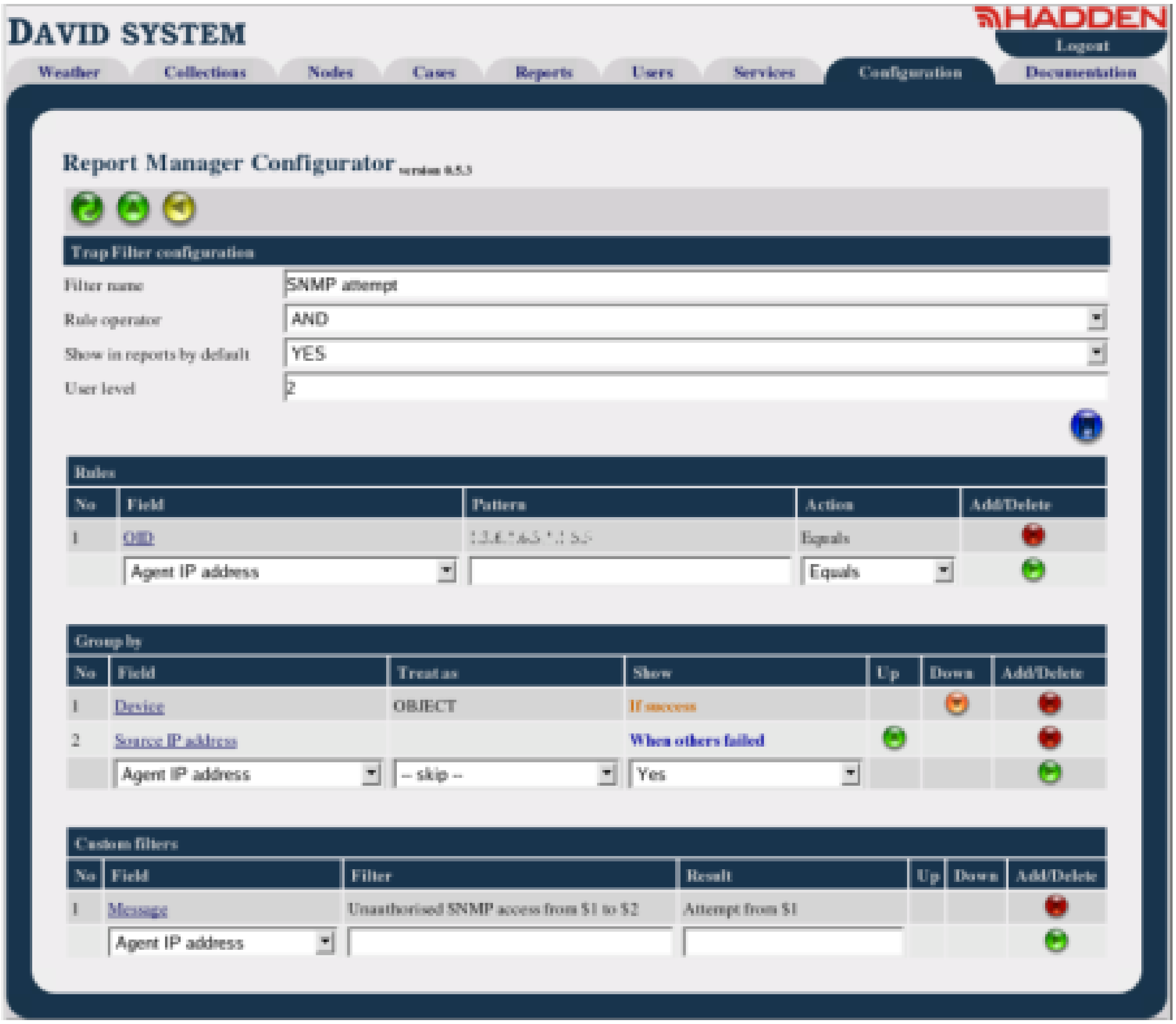
No	Name	Managed item	Allowed devices	Show by default	User level	Add/Delete
1	BGP peers	BGPPEER	ROUTER	YES	2	
2	Network interfaces	NETINTERFACE	COMPUTER, ROUTER	YES	2	
3	Pings	PINGOBJECT		YES	2	
		BGPPEER		YES		

Report Manager Configurator it is one of the applications accesible in `Configuration` tab. A main view of the application presents a list of all defined filters of particular types. Three types of filters are accesible: concerning SNMP Trap data, concerning registered entries about pending cases and concerning entries about monitored objects. A list of each type as its last row includes edit fields, that allow to sepcify its new item and add it to the list. The fields differs in depending on a filter type, that a new item is defined. Meaning of particular columns for different filter types are described in this document, in part about Report Manager.

Three columns described below are common for all types of filters. There are: `Show by default` - shows if working results of filters are default presented through Report Browser, `User level` - a minimum level of a user needed to a filter edition and `Add/Delete` - allows to add and delete an existed filter.

Links in particular columns allow to go to an edition of the selected filter.

10.2.2. Edition of filters dealing with SNMP Trap entries



Report Manager Configurator version 0.5.3

Trap Filter configuration

Filter name	SNMP attempt
Rule operator	AND
Show in reports by default	YES
User level	2

Rules

No	Field	Pattern	Action	Add/Delete
1	OID	[illegible]	Equals	●
	Agent IP address		Equals	●

Group by

No	Field	Treat as	Show	Up	Down	Add/Delete
1	Device	OBJECT	If success		●	●
2	Source IP address		When others failed	●		●
	Agent IP address	-- skip --	Yes			●

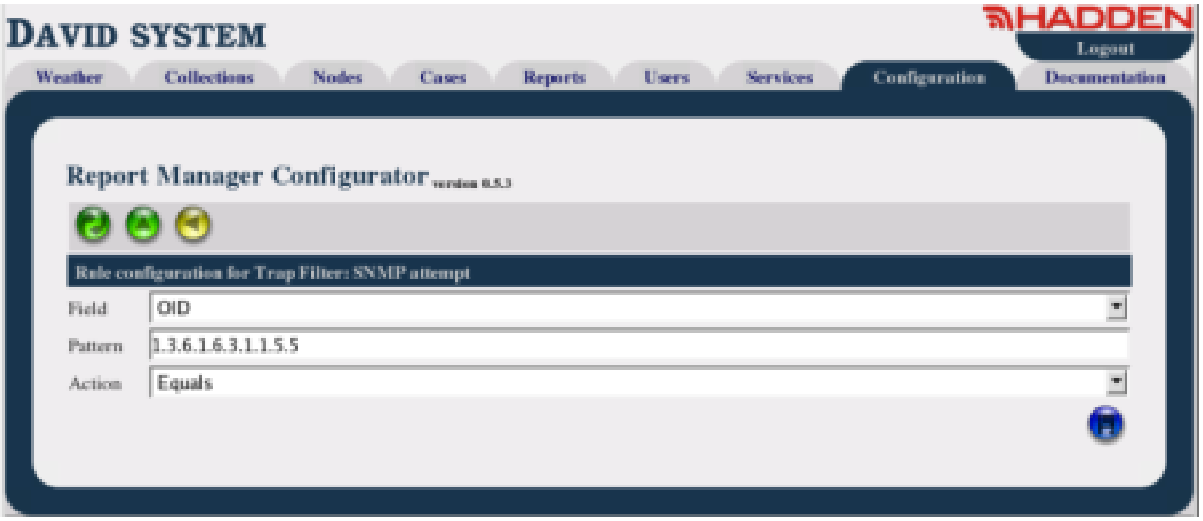
Custom filters

No	Field	Filter	Result	Up	Down	Add/Delete
1	Message	Unauthorised SNMP access from $1 to $2	Attempt from $1			●
	Agent IP address					●

In the top part of the application edition fields are placed, that allow to change a filter name, a type of logical operation (AND or OR) which occurs between entries in `Rules` group, a condition, or wroking results of filter, that are presented by Report Browser, a minimum user level needed to an edition of the filter.

Particular groups of entires defining a given filter include characteristc columns of themselves. Additionally each column includes `Add/Delete` column, that has buttons allowing to add or delete an exited entry. Group by group includes two additional columns Up and Down allowing to move up or down particular entries.

Each group includes fields, in the last row, allowing to add a new entry to the group. Field columns include links allowing to edit particular entries.

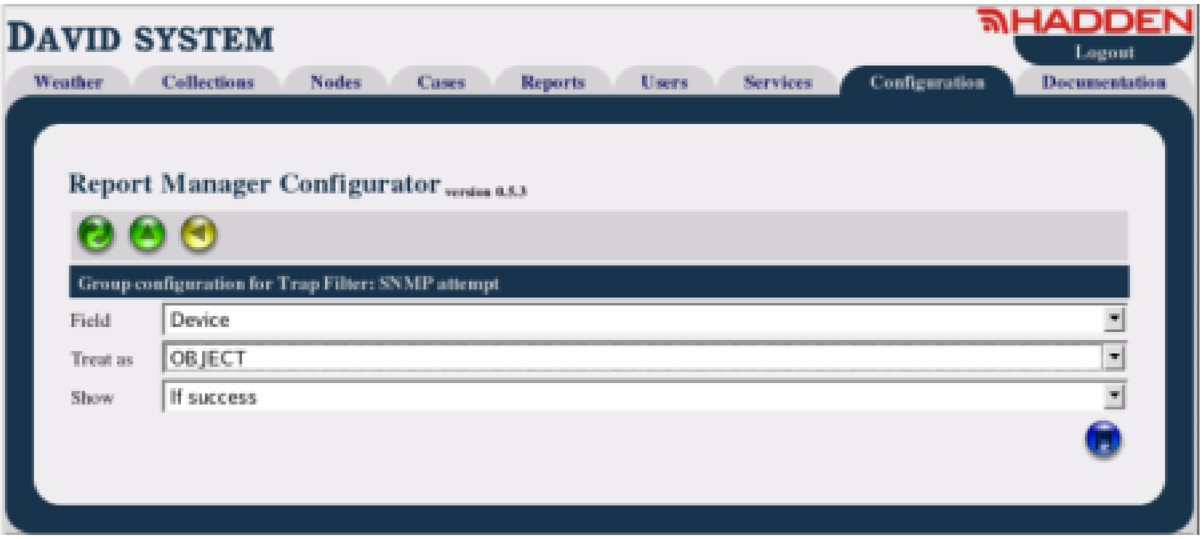


Report Manager Configurator version 0.5.3

Rule configuration for Trap Filter: SNMP attempt

Field: OID
Pattern: 1.3.6.1.6.3.1.1.5.5
Action: Equals

An edition of Rule group consists in a sepecification of the fields: Field, Pattern and Action. Their meaning was described in a part of the document which concerns Report Manager.

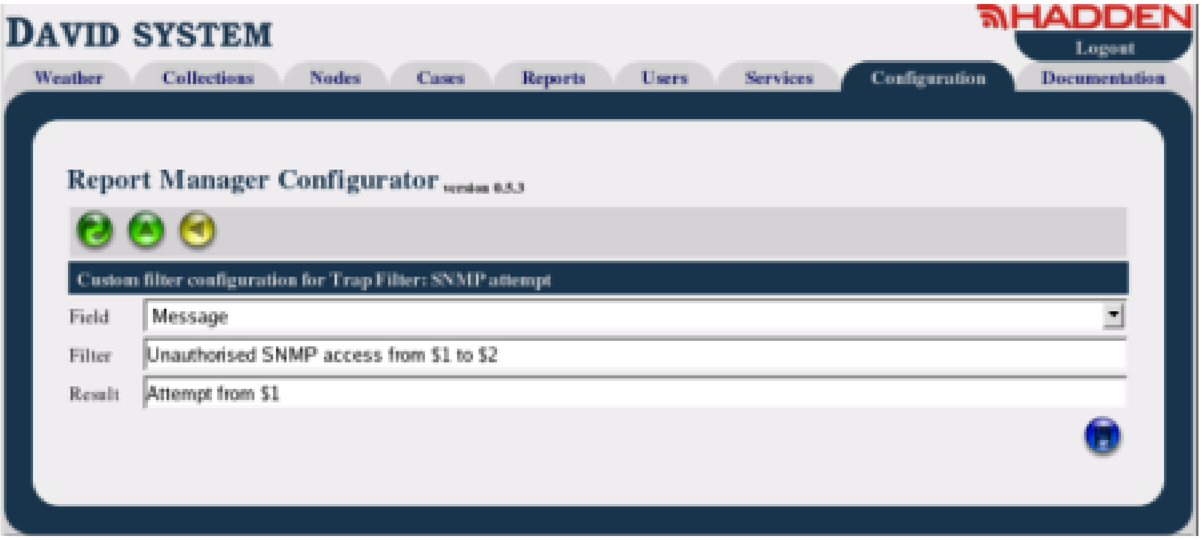


Report Manager Configurator version 0.5.3

Group configuration for Trap Filter: SNMP attempt

Field: Device
Treat as: OBJECT
Show: If success

An edition of Group by group consists in a sepecification of the fields: Field, Treat as and Show. Their meaning was described in a part of the document which concerns Report Manager.



Report Manager Configurator version 0.5.3

Custom filter configuration for Trap Filter: SNMP attempt

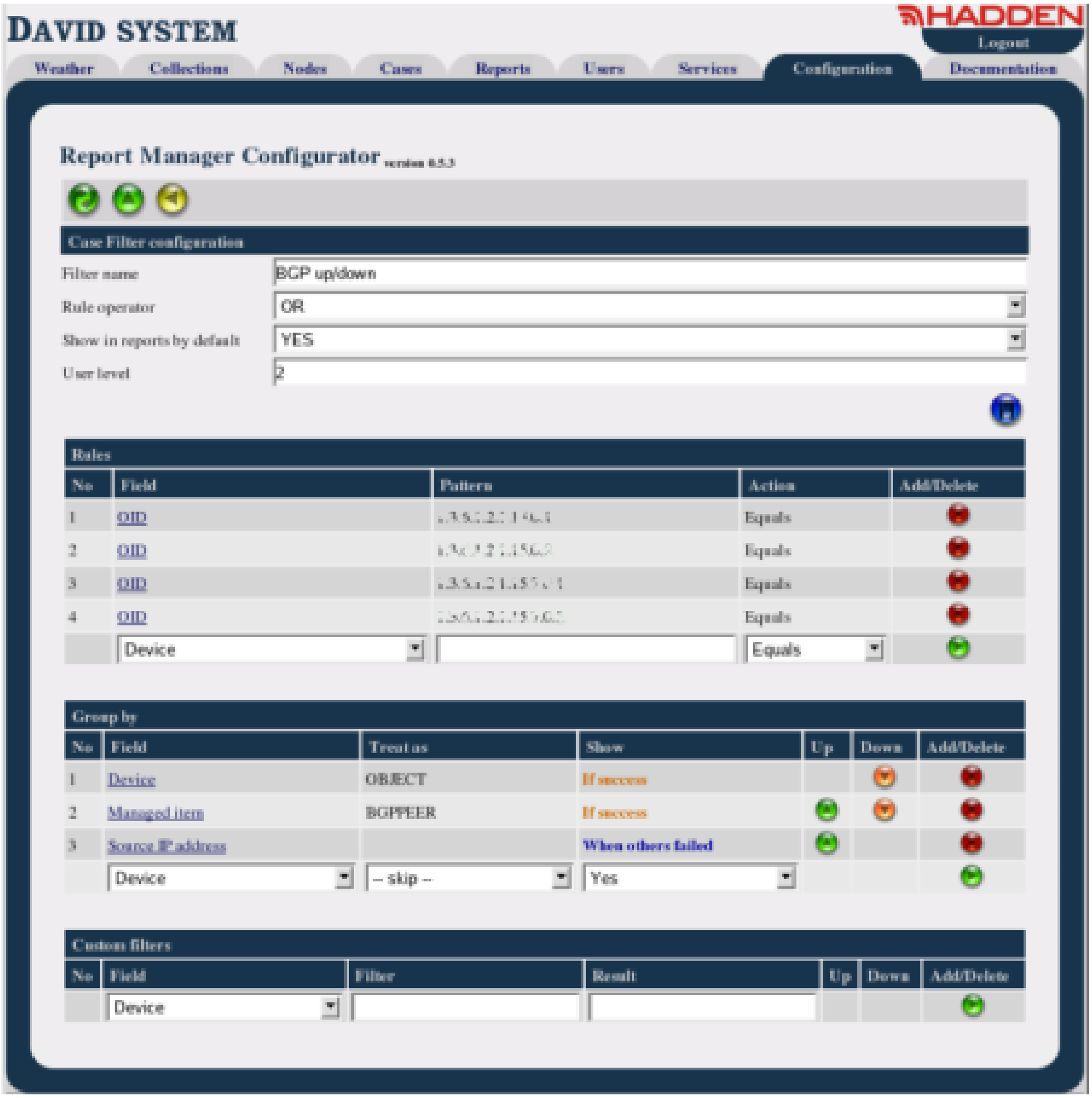
Field: Message

Filter: Unauthorised SNMP access from $1 to $2

Result: Attempt from $1

An edition of `Custom filter` group consists in a sepecification of the fields: `Field`, `Filter` and `Result`. Their meaning was described in a part of the document which concerns Report Manager.

10.2.3. Edition of filters for entries dealing with recordered cases



Report Manager Configurator version 0.5.3

Case Filter configuration

Filter name	BGP up/down
Rule operator	OR
Show in reports by default	YES
User level	2

Rules

No	Field	Pattern	Action	Add/Delete
1	OID	[illegible]	Equals	
2	OID	[illegible]	Equals	
3	OID	[illegible]	Equals	
4	OID	[illegible]	Equals	
	Device		Equals	

Group by

No	Field	Treat as	Show	Up	Down	Add/Delete
1	Device	OBJECT	If success			
2	Managed item	BGPPEER	If success			
3	Source IP address		When others failed			
	Device	-- skip --	Yes			

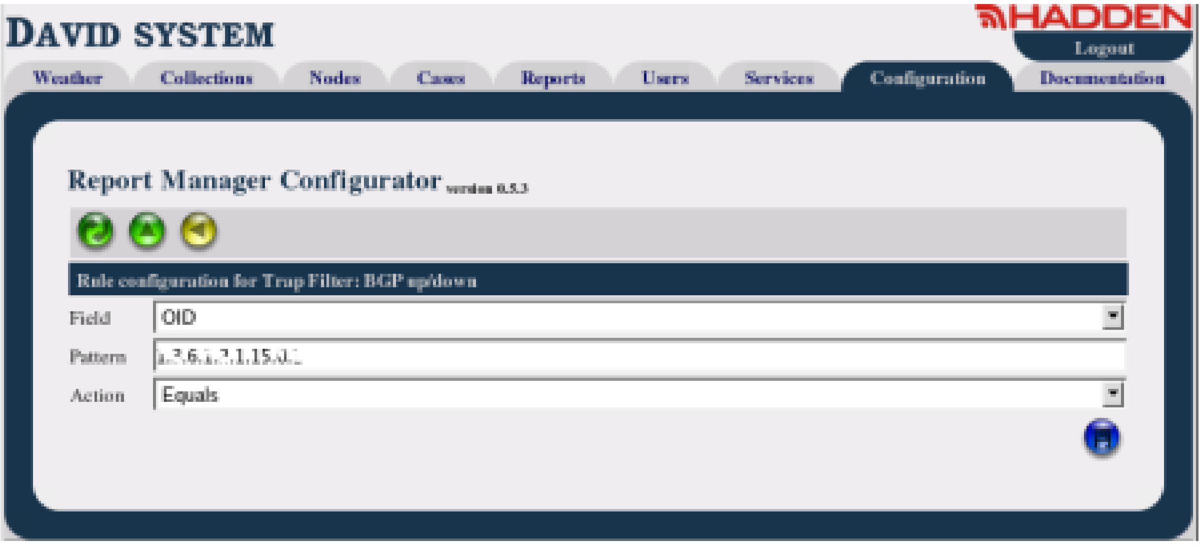
Custom filters

No	Field	Filter	Result	Up	Down	Add/Delete
	Device					

In the top part of the application edition fields are placed, that allow to change a filter name, a type of logical operation (AND or OR) which occurs between entries in `Rules` group, a condition, or wroking results of filter, that are presented by Report Browser, a minimum user level needed to an edition of the filter.

Particular groups of entires defining a given filter include characteristc columns of themselves. Additionally each column includes `Add/Delete` column, that has buttons allowing to add or delete an exited entry. `Group by` group includes two additional columns `Up` and `Down` allowing to move up or down particular entries.

Each group includes fields, in the last row, allowing to add a new entry to the group. `Field` columns include links allowing to edit particular entries.



Report Manager Configurator version 0.5.3

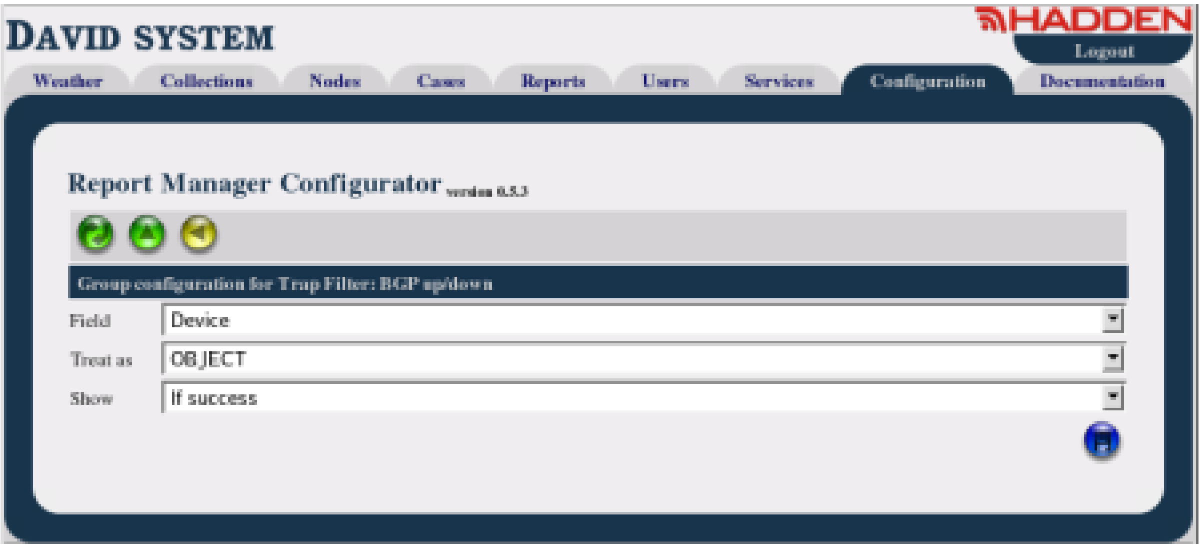
Rule configuration for Trap Filter: BGP up/down

Field: OID

Pattern: 1.3.6.1.2.1.15.0.1

Action: Equals

An edition of `Rule` group consists in a sepecification of the fields: `Field`, `Pattern` and `Action`. Their meaning was described in a part of the document which concerns Report Manager.



Report Manager Configurator version 0.5.3

Group configuration for Trap Filter: BGP up/down

Field: Device

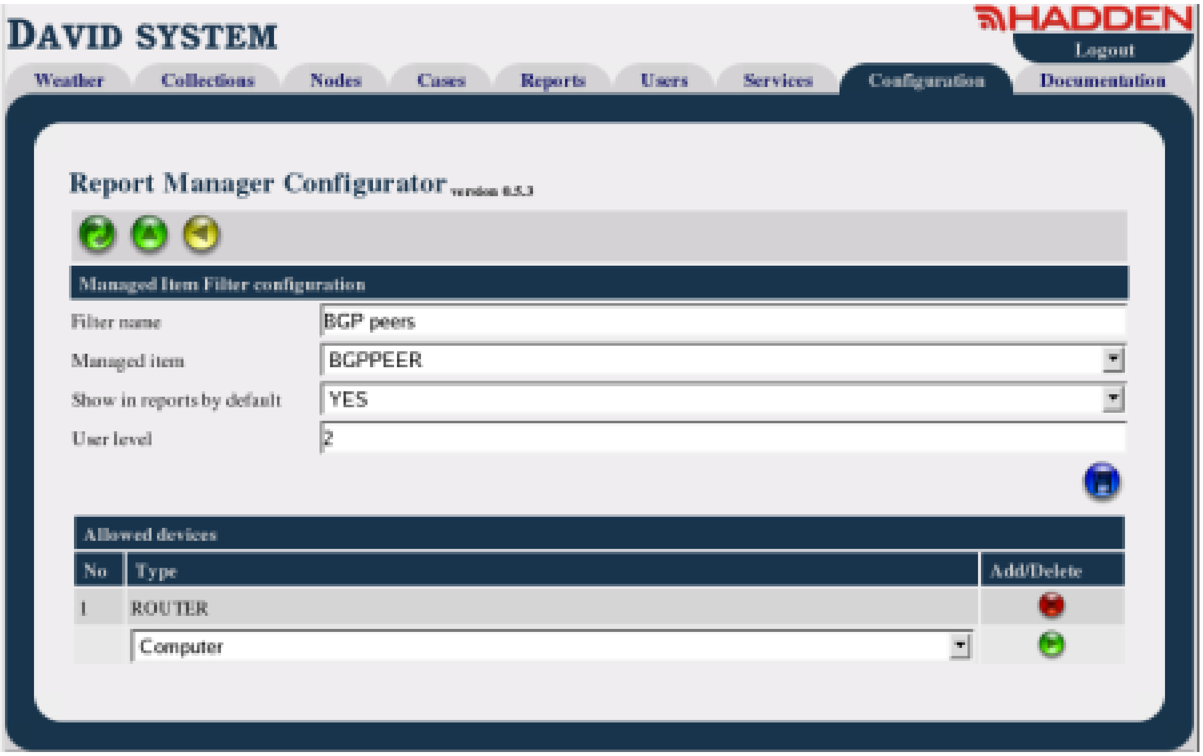
Treat as: OBJECT

Show: If success

An edition of `Group by` group consists in a sepecification of the fields: `Field`, `Treat as` and `Show`. Their meaning was described in a part of the document which concerns Report Manager.

An edition of `Custom filter` group is similar to the edition of the group which concerns SNMP Trap entries. In this way it's seldom used.

10.2.4. Edition of filters concerning entries about monitored objects



Report Manager Configurator version 0.5.3

Managed Item Filter configuration

Filter name	BGP peers
Managed item	BGPPEER
Show in reports by default	YES
User level	2

Allowed devices

No	Type	Add/Delete
1	ROUTER	
	Computer	

In the top part of the application edition fields are placed, that allow to change a filter name, a type of monitored filter which the filter concerns, a condition, or wroking results of filter, that are default presented by Report Browser, a minimum user level needed to an edition of the filter.

A list of device types that is included by working of the filter, is placed in the below part of the application. The column of the list includes buttons allowing to add a new type of a device or delete an existed one. An empty list means, that the filter concerns all types of devices.

10.3. Related articles

Report Manager (dreportd)

Report Browser

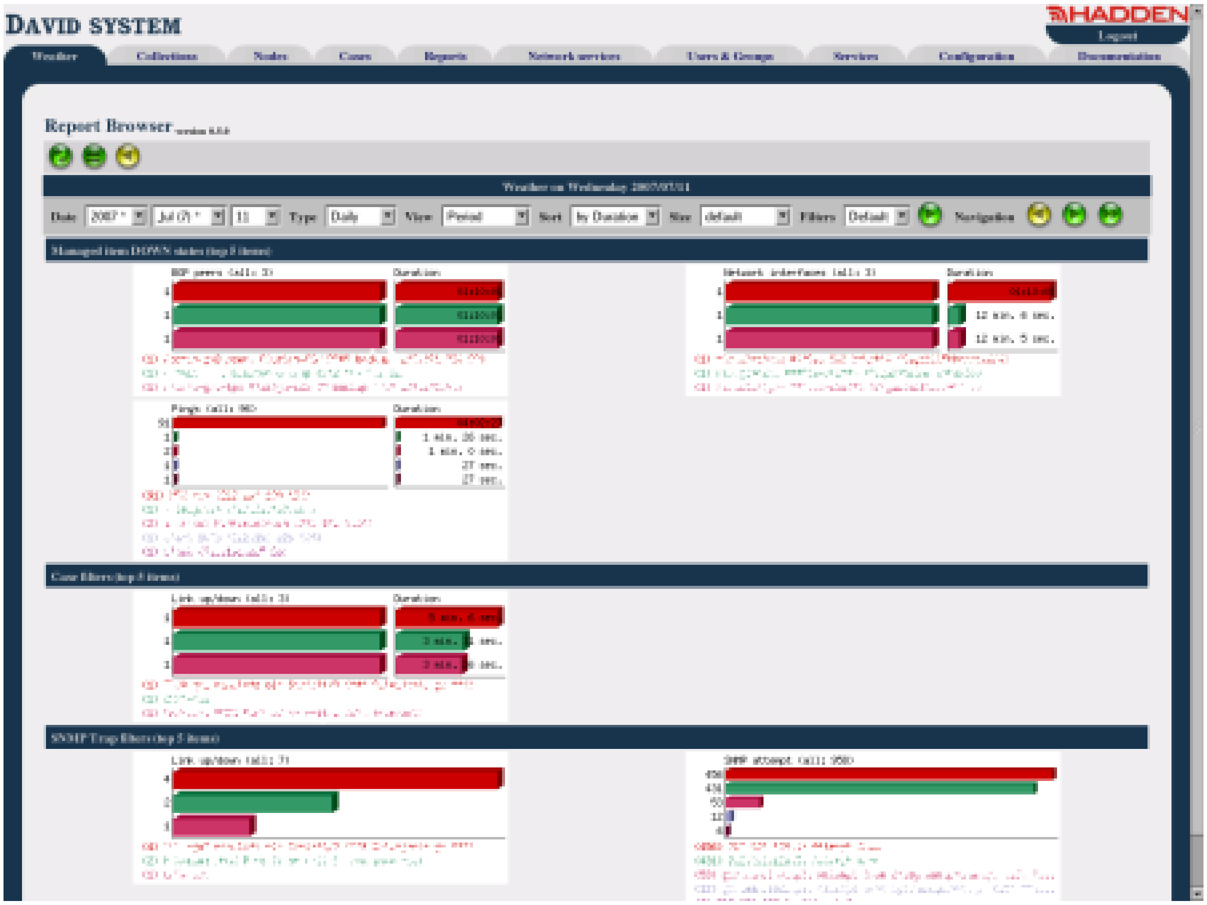
Chapter 11. Report Browser

11.1. General

Report Browser is a Web application and it is a part of **Report Manager** product. It allows you to browse daily, monthly and yearly reports generated by using data, that are a result of Report Manager work.

11.2. Description

11.2.1. Default view of the application



Report Browser is accesible through `Weather` tab. In the top part of the application the toolbar is placed, which is characteristic for all Web application. Below it, there is the toolbar with objects, that define kinds of presented data. Meaning of particular fields presents the chart below:

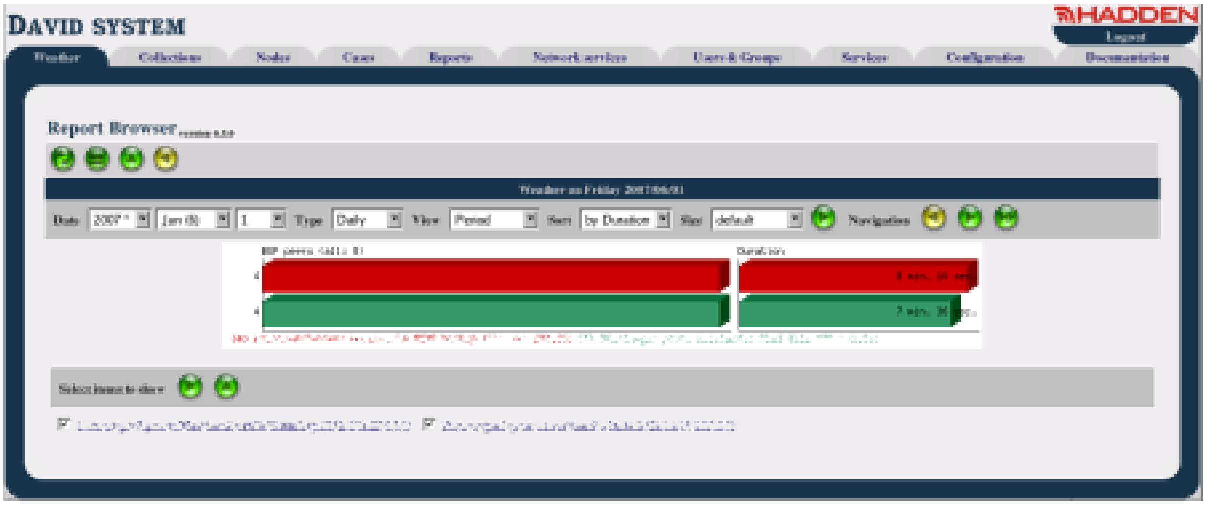
Table 11.1. Report Browser - the toolbar objects

Object	Description
Date	A date, that concerns the report. For a monthly report is no importance a day while for a yearly report is no importance additionally a month.
Type	A report type defining its time range. The following values are possible: daily, monthly and yearly.
View	It means, if a report, sum up a selected period of time, is presenting or a report showing subperiods (i.e.: for daily report subperiods are hours, while for monthly one are days).
Sort	It defines a sort type of results of filter working. A type `by Result` sorts results decreasingly according to a nuber of occurences of particular results. A type `by Duration` sorts results according to duration time of particular entries.
Size	Depending on a context, it sets a width and height of graphs.
Filters	A kind of presented filter results (default filters or all). The field matters in the case of presenting of filter groups, and not in the case of a selected filter.

A report generating according to selected field values is made by pressing the button ▶. At the end of the toolbar navigational buttons are placed, that allow to browse the report results in next periods of time (i.e.: days).

Clicking on a graph bar causes, that you get into the object which it concerns, using **Node Browser**. For results of filters concerning monitored devices, clicking on the bar causes, that you get into the report about a selected object by a selected period of time, using **Node Report Browser**. Clicking out of the graph bar causes, that you get into a working view of a single filter.

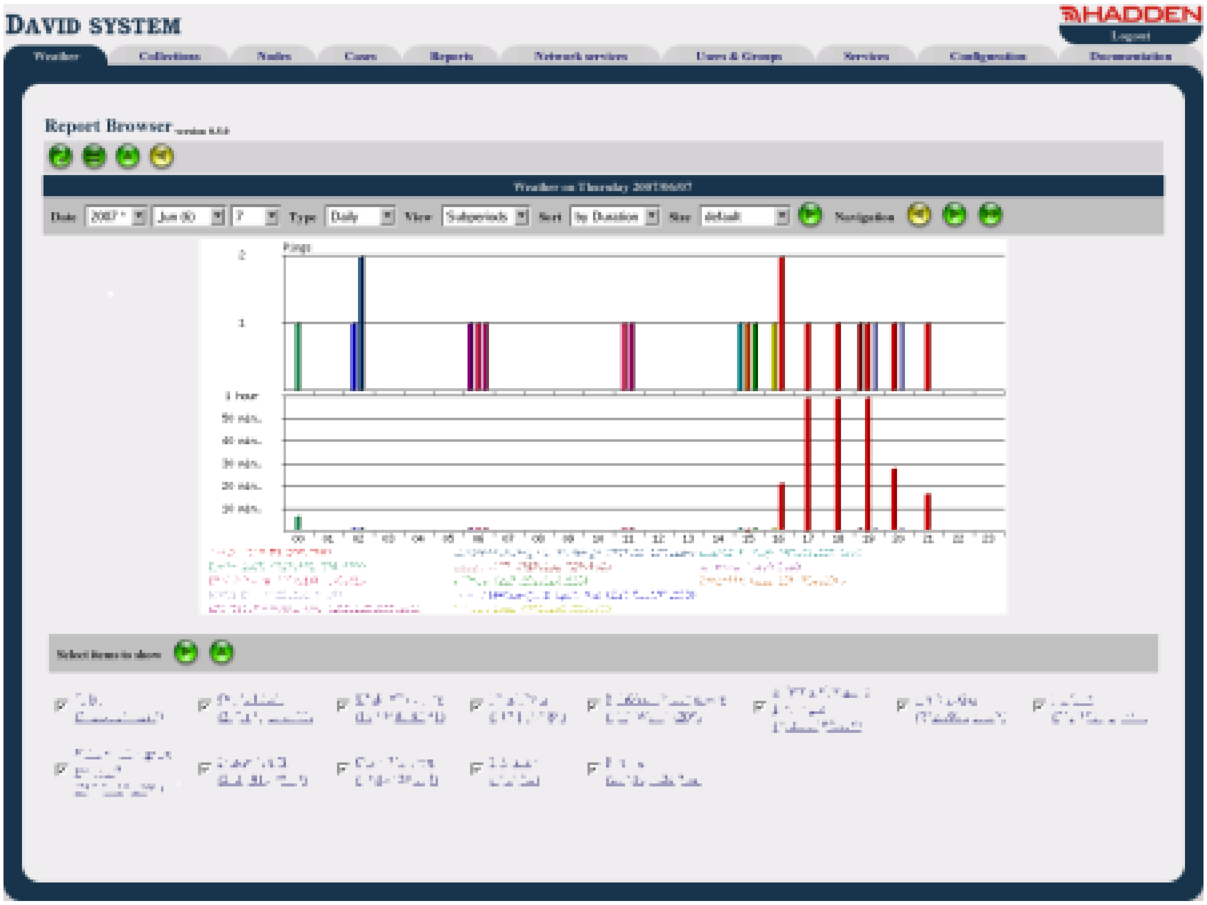
11.2.2. A working view of a single filter



Date: 2007 Jan (6) 1 Type: Daily View: Period Sort: by Duration Size: default

The view shows working results of a single filter and not their groups. The most operations is similar to the view of filters group. There is, below the graph, a list of all generated results for a given filter with selected positions presented on the graph. Thanks this, you can select positions, that you want to place on the graph. The button ▲ restores a selection of default positions.

11.2.3. A working view of a single filter presenting subranges



Weather on Thursday 2007/06/07

Date 2007 Jun (6) 7 Type Daily View Subperiods Sort by Duration Size default Navigation

One difference in comparison with a whole report presenting working results of a single filter is another type of a graph. It shows results devided on subranges of a perid of time.

11.3. Related articles

Report Manager Configurator

Report Manager (dreportd)

Network Manager: Node Browser

Network Manager: Node Report Browser