

Содержание

6 Filtering rules management interface	3
Universal Locking Rules UI	3
Introduction	3
Installation	3
Configuration	3
.env Configuration	3
Key Installation	4
Roles Management	5
Dictionaries Configuration	6
IGW Profiles Management	10
Web Server for Global Lists Configuration	12
Web-server	12
DSCP Rules	13
ASN Filter	14
IP & ASN Excludes	16
IP Excludes	17
ASN Excludes	19
ISP Configuration	21
Creating an ISP Profile	21
Editing ISP Profile	22
Deleting ISP Profile	22
Policing Profile	22
WEB and IP Filter	23
Locking Rules List	23
Creating/Editing Locking Rules	24
Deleting the Locking Rule	25
Domain Check	26
Search the Database (among the blocking rules)	27
Whitelist	27
Whitelist rule list	27
Creating/Editing the white list	28
Deleting a white list rule	29
Whitelist operating mode management	29
Database search (global)	30
Task monitoring	30
Logs	31

6 Filtering rules management interface

Universal Locking Rules UI

Introduction

Universal locking rules (ULR) UI is designed to manage filtering rules on multiple DPIs simultaneously using a graphical interface.

Installation

Equipment or virtual machines with the following characteristics are suitable for the subsystem:

1. CPU 2.5 GHz, 2-4 cores
2. RAM from 8 GB (mainly for sphinx)
3. Hard drive (HDD) 50 GB - 250 GB
4. Cent OS 7+ operating system (we do not recommend to not install minimal, because most of the dependencies will have to be installed manually)
5. Network Card (NIC) from 10 Mbps



We recommend Cent OS 7+ operating system. **Do not not install minimal, because most of the dependencies will have to be installed manually.** If you need to install software on Cent OS 6, make sure that supervisor 3+ is installed. If you do not have the package, please contact technical support.



The locking rules management interface is a special section of [The VAS Experts DPI Graphical User Management Interface ver.2](#). The installation is similar to the script of [The VAS Experts DPI Graphical User Management Interface ver.2](#).

Configuration

.env Configuration

The subnet configuration is handled with .env file.

```
/var/www/html/dpiui2/backend/.env
```

The file contents:

```
#Redirect URL for "White list" service
ULR_WHITE_LIST_REDIRECT_URL=https://google.com

#The period after Ulr tasks data is deleted (days)
ULR_QUEUE_DELETE_TASKS_DAYS_INTERVAL=1

#ASN for IP-exception rules
ULR_IP_EXCLUDE_ASN=64401

#The host for blocked resources list deployment. To connect the blocked
resources server.
ULR_BLACK_LIST_DEPLOY_HOST=<IP address or host of global locks web-server>

#The port for blocked resources list deployment. To connect the blocked
resources server.
ULR_BLACK_LIST_DEPLOY_PORT=22

#Username for blocked resources list deployment. To connect the blocked
resources server.
ULR_BLACK_LIST_DEPLOY_USER=default

#Password for blocked resources list deployment. To connect the blocked
resources server.
ULR_BLACK_LIST_DEPLOY_PASS=

#To use sudo for blocked resources list deployment. (0 - do not use, 1 -
use)
ULR_BLACK_LIST_DEPLOY_SUDO=1

#Black lists saving path.
ULR_BLACK_LIST_DEPLOY_PATH=/var/www/html/blacklists/

#Log Detail Level (0 - info, 1 - debug, 2 - tracing).
ULR_LOAD_LOG_LEVEL=0
```



After changing the .env file, you need to run the command

```
php /var/www/html/dpiui2/backend/artisan queue:restart
```



These settings can be added to the configuration in the Administrator → DPIUI2 Server Configuration section in the The VAS Experts DPI Graphical User Interface ver.2.

Key Installation

To use the Universal Locking Rules UI, you need to activate the ULR-license in DPIUI2 with a command:

```
dpiui2 ulr_lic --make=1
```

Next:

1. Enter license level: standard
2. Enter the license completion date in the Y-m-d format (e.g. 2099-12-31)
3. Enter the license password.

If the data is correct, a success message will be displayed:

```

dpiui2 ulr_lic --make=1
Enter level:
> standard

Enter expire date in Y-m-d format:
> 2099-12-31

Enter password:
>

stdClass Object
(
    [success] => 1
)

```

Roles Management

In the DPIUI2 interface visit the Administrator → Roles section. Create a new role and set read and write permissions in the ulr admin section:

MANAGING USERS AND ROLES / ROLES

+ Roles

Save

Program sections

Code	Section	Best	Desired
administrator_roles	Roles	☐ No	☐ No
administrator_send_error	Send Error	☐ No	☐ No
administrator_dpiu2	Administrator DPIU2	☐ No	☐ No
rescloud	VMs Cloud	☐ No	☐ No
socket	Websocket notifications	☐ No	☐ No
vrt	Universal lock rules	☒ Yes	☒ Yes
vrt_vmb_rules	Universal lock rules / VMs & IP filter	☒ Yes	☒ Yes
vrt_vrtba_rules	Universal lock rules / Virtualbat	☒ Yes	☒ Yes
vrt_policings	Universal lock rules / Applications & policings	☒ Yes	☒ Yes
vrt_an_rules	Universal lock rules / AOA filter	☒ Yes	☒ Yes
vrt_excludes	Universal lock rules / IP & ASN excludes	☒ Yes	☒ Yes
vrt_db_search	Universal lock rules / Database search	☒ Yes	☒ Yes
vrt_tsp_login_profiles	Universal lock rules / TSPs & login profiles	☒ Yes	☒ Yes
vrt_dics	Universal lock rules / Dictionaries	☒ Yes	☒ Yes
vrt_system_state	Universal lock rules / System global state	☒ Yes	☒ Yes
scan	Lawful interception	☐ No	☐ No
scan_connections	Lawful interception / connections	☐ No	☐ No

Next, go to the Administrator→ Users section. Create a new user and set him the role that you created earlier.

Dictionaries Configuration

- Category Dictionary
- Regulators Dictionary



These dictionaries are used for creating/editing locking rules.

Category Dictionary

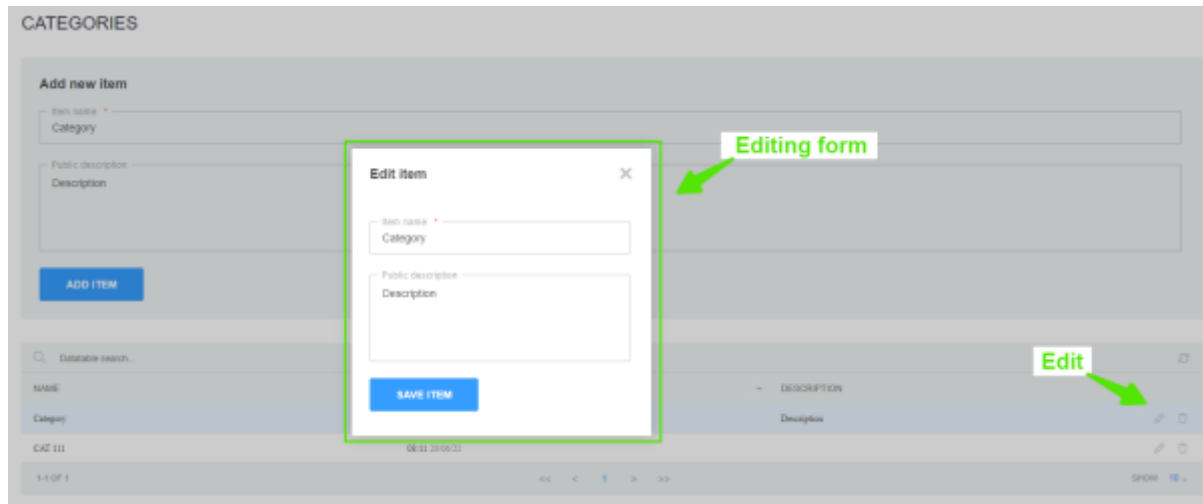
In the Locking Rules management interface go to the Dictionaries → Categories section.

Creating

Fill in the form with category name and description and click the "Add" button.

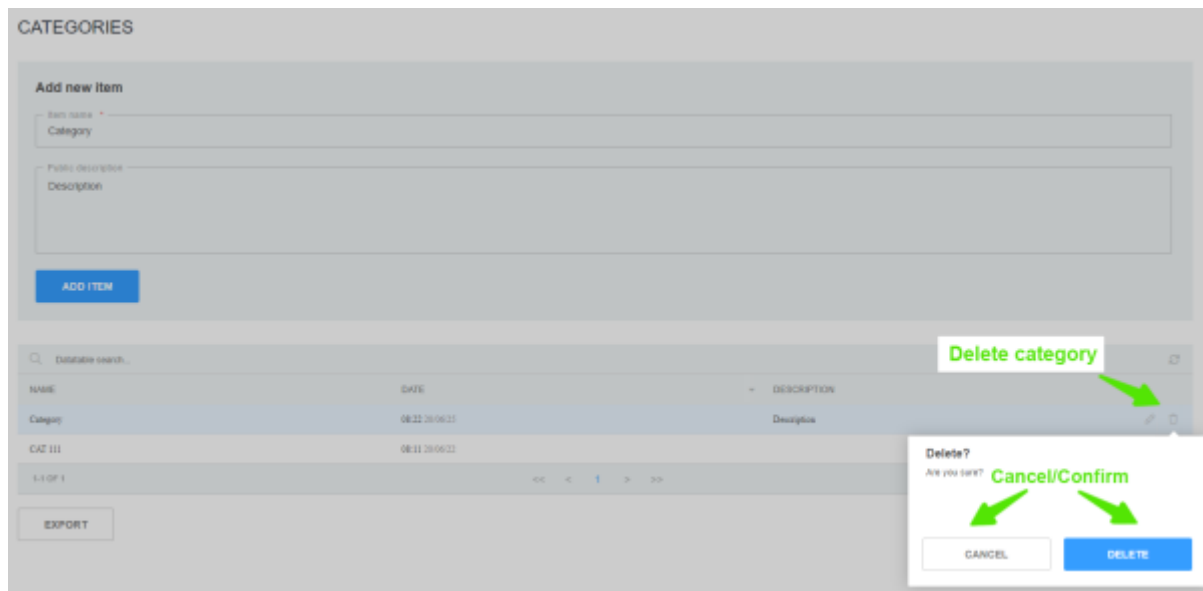
Editing

To edit: click on the category editing button in the categories table. In the form, change the name and/or description of the category, then click the "Save" button.



Deleting

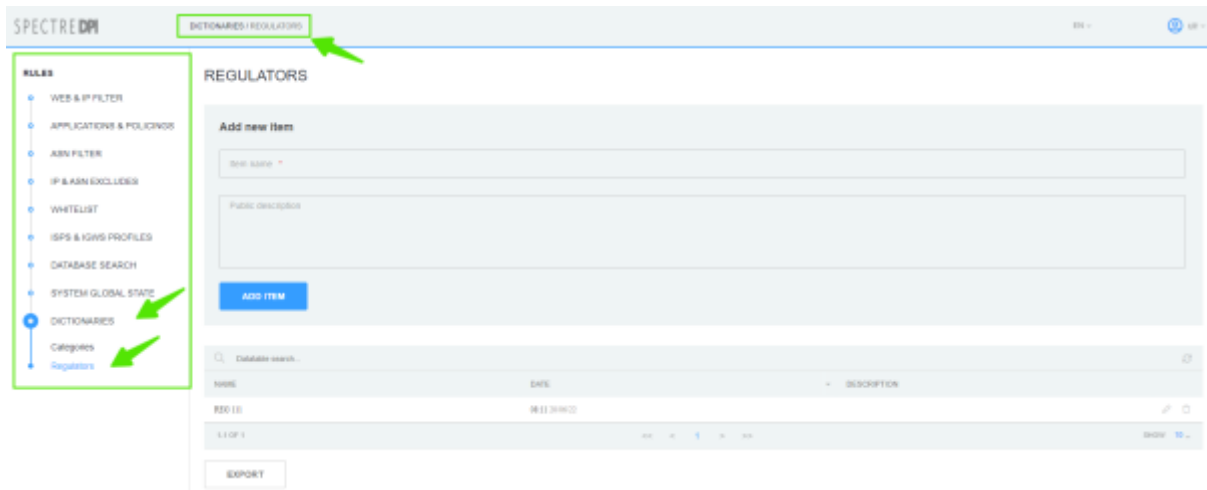
Click on the delete category button in the categories table. In the pop-up window confirm or cancel the action.



Attention: Before deleting a category, make sure there are no rules referring to this category!

Regulators Dictionary

In the Locking Rules management interface go to the Dictionaries → Regulators section.



Creating

Fill in the form with regulator name and description and click the "Add" button.

REGULATORS

Add new item

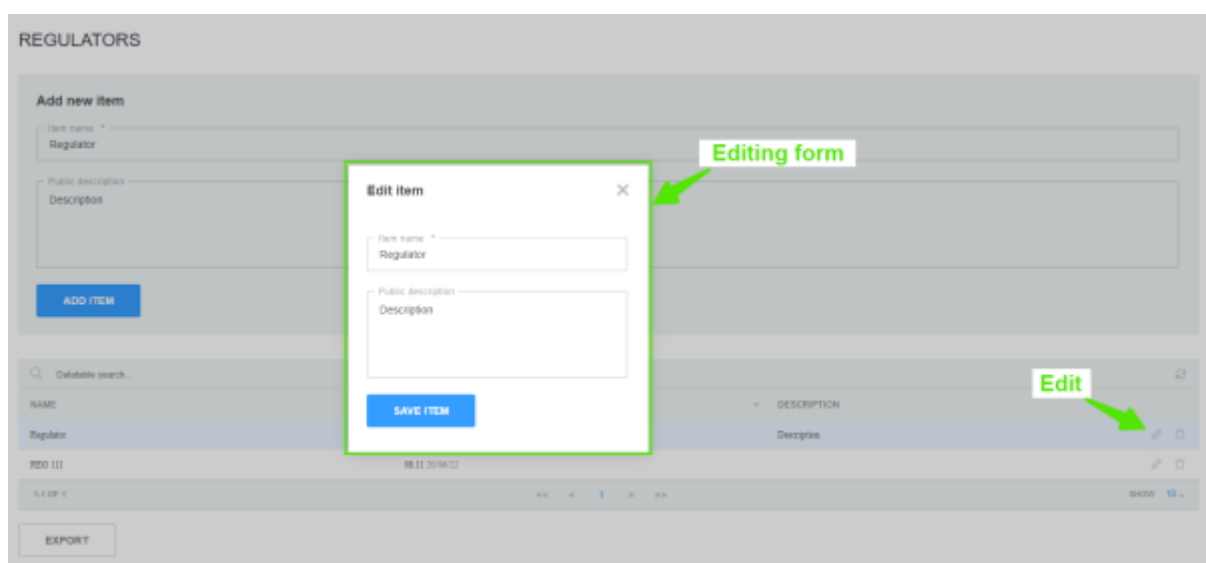
Item name: Regulator

Public description: Description

ADD ITEM

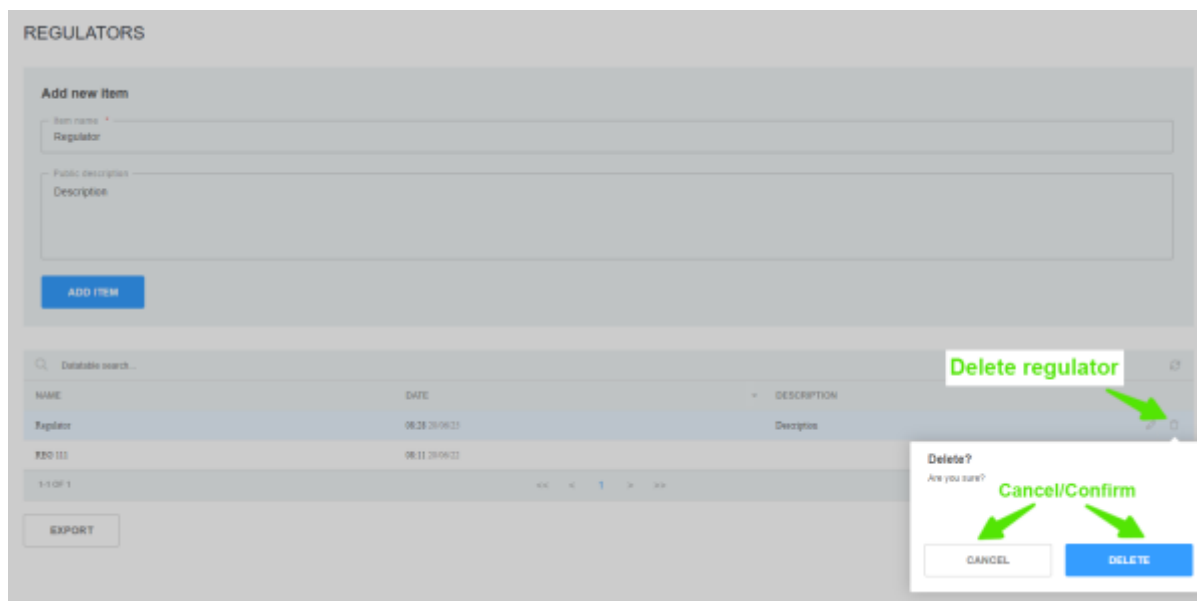
Editing

To edit: click on the regulator editing button in the regulators table. In the form, change the name and/or description of the regulator, then click the "Save" button.



Deleting

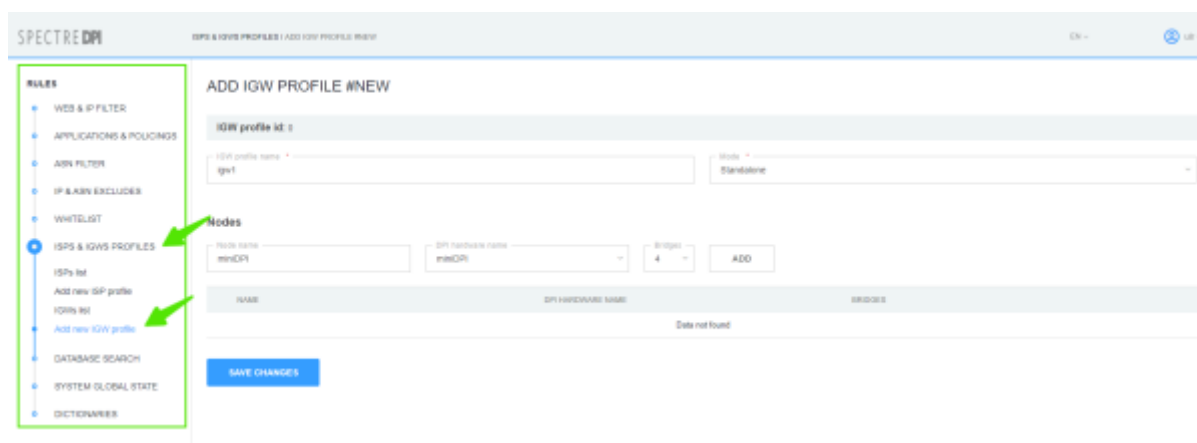
Click on the delete regulator button in the categories table. In the pop-up window confirm or cancel the action.



Attention: Before deleting a regulator, make sure there are no rules referring to this regulator!

IGW Profiles Management

Change to the section "ISPS & IGWS Profiles" → "IGWs List".



Creating

To create new IGW profile change to the section "ISPS & IGWS Profiles"→"Add new IGW profile".

In the form specify:

- Profile name;
- Operation mode (Standalone/Cluster)

- Nodes for the profile (Node name, DPI from the list of available equipment and number of bridges)

ADD IGW PROFILE #NEW

IGW profile id: 1

IGW profile name: Mode:

Nodes

Node name: DPI hardware name: Bridges:

NAME	DPI HARDWARE NAME	BRIDGES
Data not found		

IGW adding form



Before creating IGW profile add FastDPI server in the main section of DPIUI 2 Administrator -> Devices

Editing

In the "ISPS & IGWS Profiles" → "IGWs List" section click the button "Edit profile".

IGWS LIST

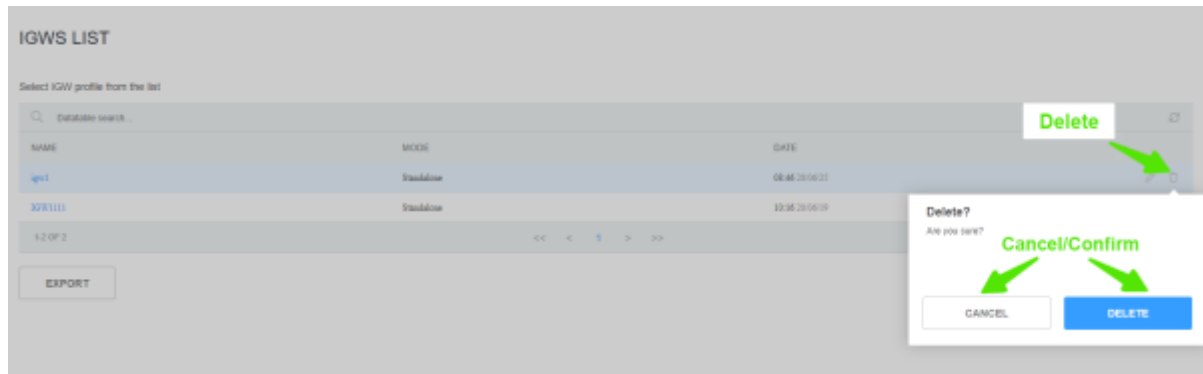
Select IGW profile from the list

Databse search...				REFRESH
NAME	MODE	DATE		
IGW1111	Standalone	10:16 20/05/19	EDIT	DELETE
1-1 OF 1				
EXPORT Edit profile SHOW 10				

The IGW profile creation/editing form will open. Make the changes you need and click "Save Changes".

Deleting

In the "ISPS & IGWS Profiles" → "IGWs List" section click the button "Delete" and confirm/cancel the operation.



Attention: Before deleting a profile, make sure there are no ISP profiles referring to this category!

Web Server for Global Lists Configuration

Web-server

1. Prepare a machine with CentOS7+ installed
2. Create a sudo user without password as described in [Dpiui2: DPI connection details](#) section
3. Run the script:

```
rpm --import http://vasexperts.ru/centos/RPM-GPG-KEY-vasexperts.ru
rpm -Uvh http://vasexperts.ru/centos/6/x86_64/vasexperts-repo-1-0.noarch.rpm
yum install dpiutils -y
yum install httpd -y
yum install unzip -y

mkdir /var/www/html/blacklists
chmod -R 777 /var/www/html/blacklists

echo "
<VirtualHost *:80>
    DocumentRoot \"/var/www/html/blacklists\"

    <proxy *>
        Order deny,allow
        Allow from all
    </proxy>
</VirtualHost>
" > /etc/httpd/conf.d/bl_lists.conf

firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --reload
```

```
systemctl enable httpd.service
systemctl restart httpd.service
```

4. In dpiui2 configuration [specify the web-server access parameters in ULR settings section](#)

5. Specify the path to Custom lock list in the settings of all connected FastDPI servers:

```
# URL dictionary for blocking by HTTP (custom_url_black_list)
custom_url_black_list=http://<IP address of Web-server>/blacklist.dict

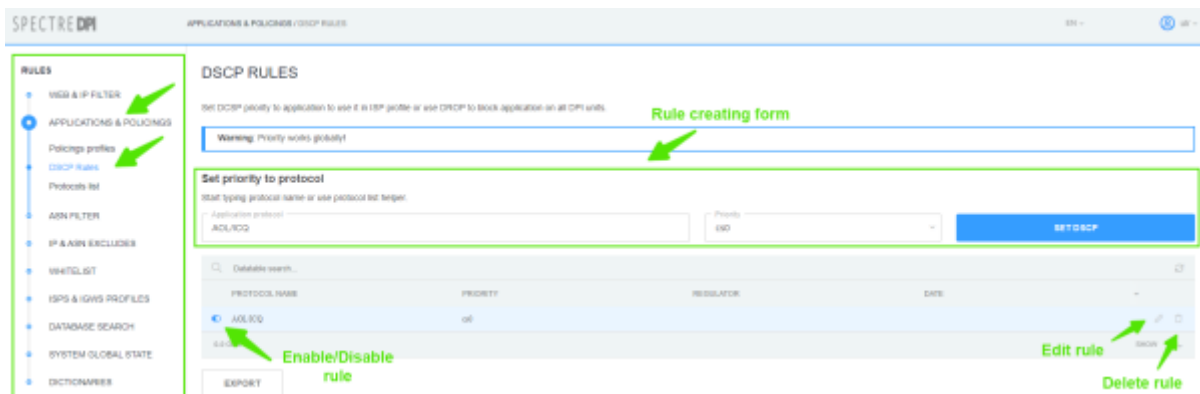
# Names dictionary for blocking HTTPS protocol by certificate
(custom_cname_black_list)
custom_cname_black_list=http://<IP address of Web-server>/blacklistcn.dict

# IP addresses dictionary for blocking HTTPS by IP (custom_ip_black_list)
custom_ip_black_list=http://<IP address of Web-server>/blacklistip.dict

# Host names dictionary for blocking HTTPS by SNI (custom_sni_black_list)
custom_sni_black_list=http://<IP address of Web-server>/blacklistsni.dict
```

DSCP Rules

Change to "Applications and policings" section → "DSCP Rules".



Creating

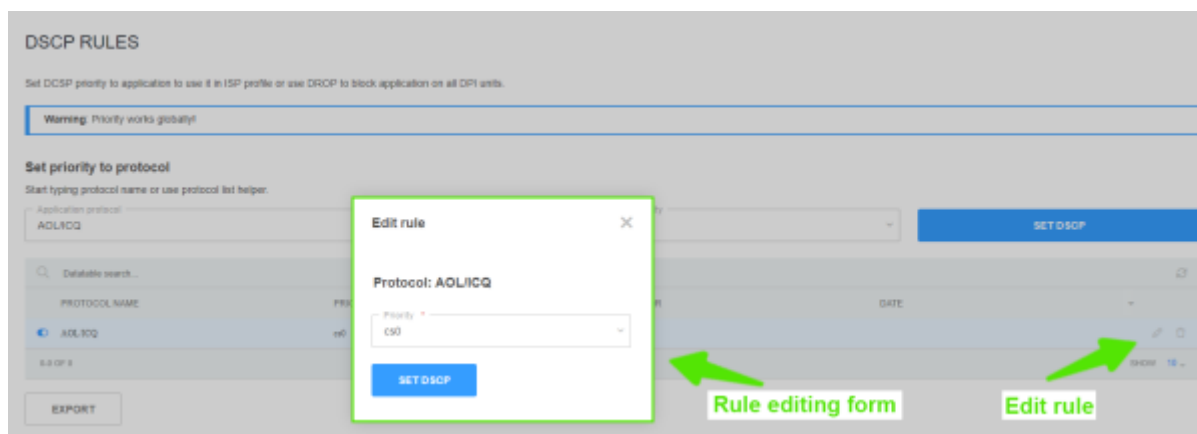
In the form of rule creating:

- Enter the name of application protocol and choose one from the list;
- Choose the priority from the list.

Save the rule by clicking on "Set DSCP" button.

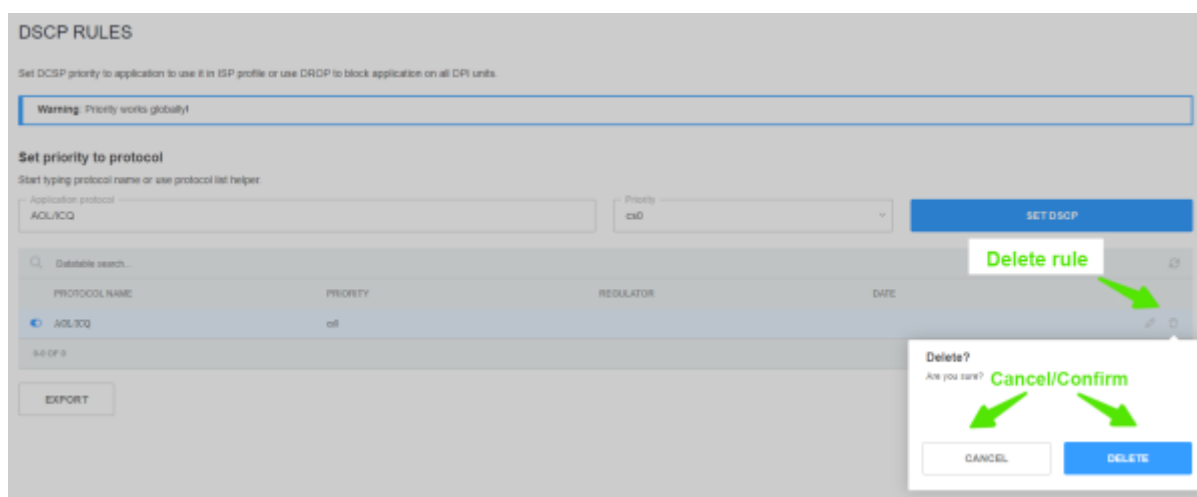
Editing

In the list of DSCP rules click on "Edit rule" button. In the popup editing form set the necessary priority and save changes by clicking on "Set DSCP" button.



Deleting

In the DSCP rules list click the button "Delete rule" and confirm/cancel the operation.



ASN Filter

Change to the "ASN Filter" section.

SPECTRE DPM ADMINISTER DSCP RULES

RULES

- WEB & IP FILTER
- APPLICATIONS & POLICIES
- ASN FILTER**
- IP & ASN EXCLUDES
- WHITELIST
- QoS & QoS PROFILES
- DATABASE SEARCH
- SYSTEM GLOBAL STATE
- DICTIONARIES

DSCP RULES

Set DSCP priority to ASN direction to use it in ISP profile or use DSCP to block ASN traffic on all DPM units

Warning: Priority must be globally!

Rule creating form

Add new rule

AS number: 12345

Priority: 100

Rule name: Rule1

Rule Description: Rule1 Description

SET DSCP

AS NUMBER	RULE NAME	PRIORITY	REGULATIONS	DESCRIPTION	DATE
12345	Rule1	100	up	Rule1 Description	2024-10-26 10:00:00

1 of 1

EXPORT

Edit rule

Delete rule

Enable/Disable rule

Creating

In the form of rule creating:

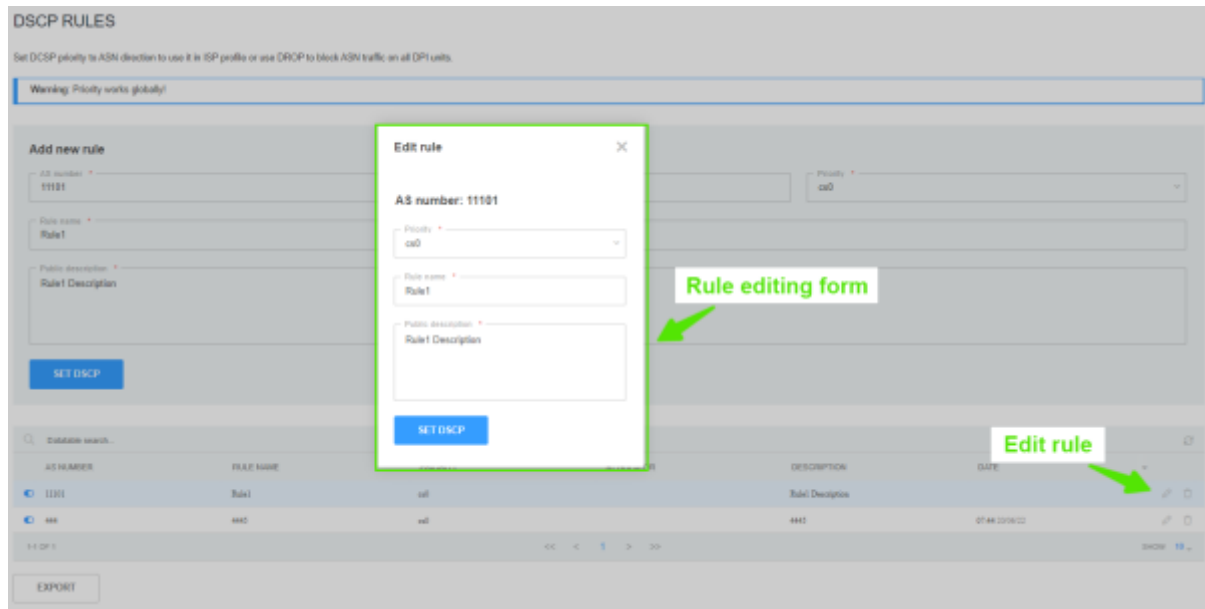
- Specify the number of AS;
- Choose the priority from the list;
- Enter the rule name;
- Enter the rule description.

Save the rule by clicking on "Set DSCP" button.

Editing

In the list of DSCP in ASN direction rules click on the "Edit rule" button. If necessary, in the popup editing form:

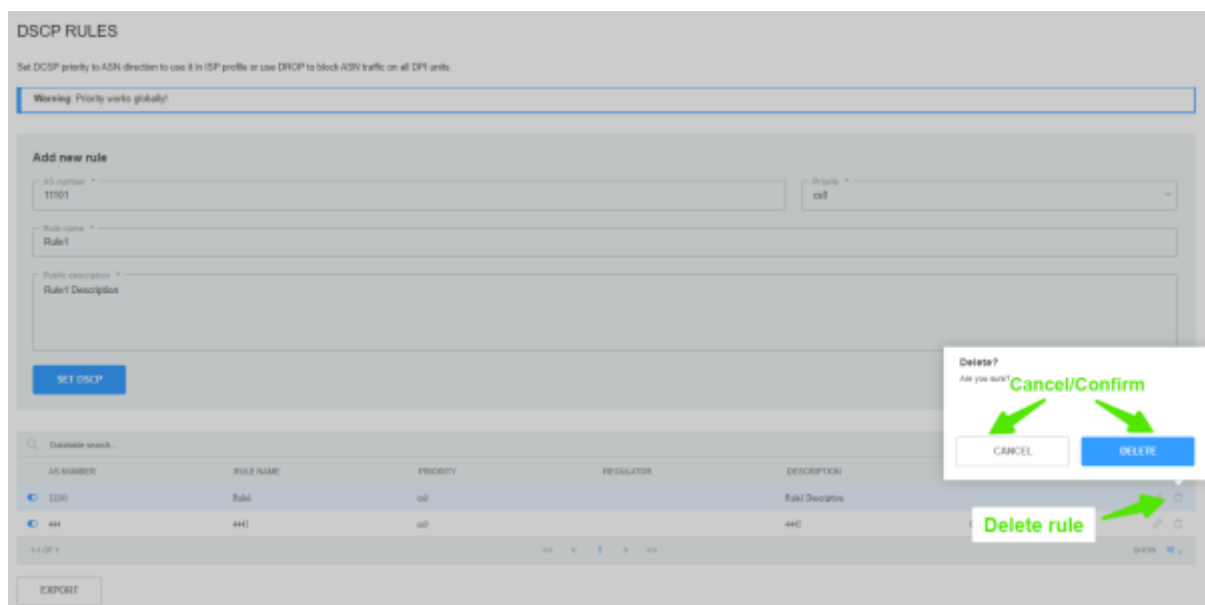
- choose the priority from the list;
- Enter the rule name;
- Enter the rule description.



Save the changes by clicking on "Set DSCP" button.

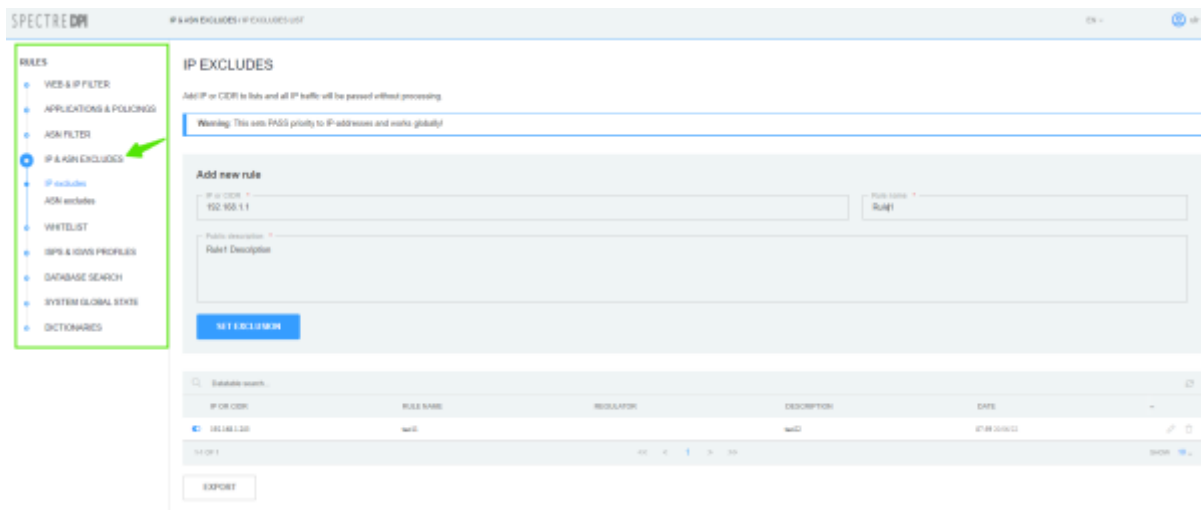
Deleting

In the list of DSCP in ASN direction rules click the button "Delete rule" and confirm/cancel the operation.



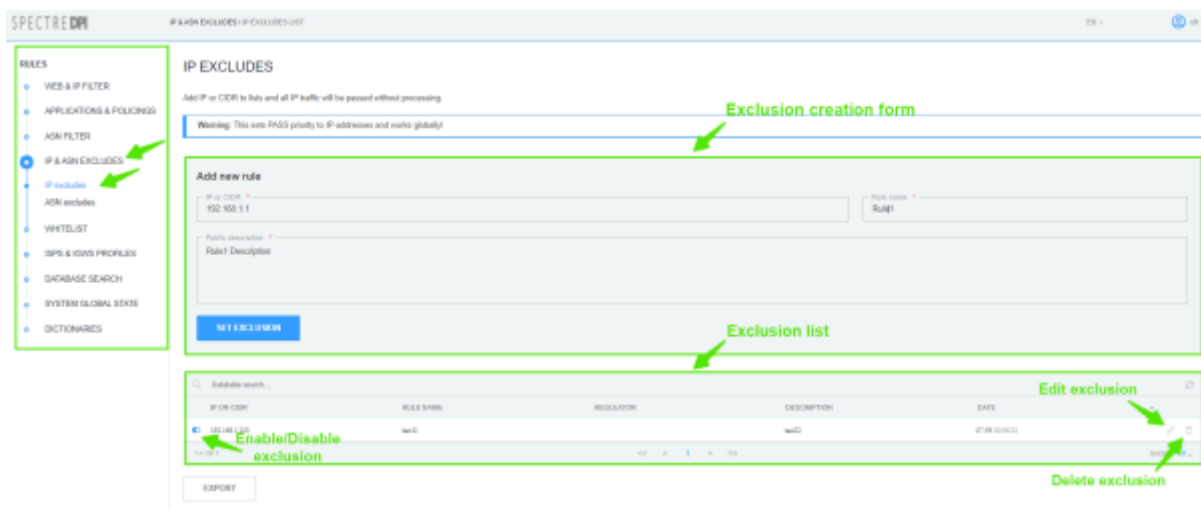
IP & ASN Excludes

Change to the "IP & ASN Excludes" section.



IP Excludes

Change to the "IP & ASN Excludes" section → "IP Excludes".



Creating

In the form of rule creating:

- Specify IP/CIDR;
- Enter the rule name;
- Enter the rule description;

Save the rule by clicking on "Set exclusion" button.

Editing

Click on the button "Edit exclusion". In the form of rule editing you can change:

- name of the rule;
- its description.

Edit rule

IP or CIDR: 192.168.1.203

Rule name * Rule1

Public description * Rule1 Description

SET DSCP

Save the changes by clicking on "Set DSCP" button.

Deleting

In the list of exclusions click the button “Delete exclusion” and confirm/cancel the operation.

IP EXCLUDES

Add IP or CIDR to lists and all IP traffic will be passed without processing.

Warning: This sets PASS priority to IP-addresses and works globally!

Add new rule

IP or CIDR: 192.168.1.1 Rule name: Rule1

Public description: Rule1 Description

SET EXCLUSION

IP OR CIDR	RULE NAME	REGULATOR	DESCRIPTION
192.168.1.1	net1		net2

1 of 1

EXPORT

Delete exclusion

Delete? Are you sure? Cancel/Confirm

CANCEL DELETE

ASN Excludes

Change to the "IP & ASN Excludes" section → "ASN Excludes".

The screenshot shows the SPECTRE DPM interface for IP & ASN Excludes. The left sidebar has a menu with 'IP & ASN EXCLUDES' selected. The main content area is titled 'IP EXCLUDES' and includes a warning message: 'Warning: This sets PASS priority to IP addresses and marks globally!'. Below this is a form to 'Add new rule' with fields for 'IP or CIDR' (containing '192.168.1.1'), 'Rule Name' (containing 'Rule1'), and 'Rule Description'. A 'SET EXCLUSION' button is at the bottom of the form. Below the form is a table with columns: 'IP OR CIDR', 'RULE NAME', 'REGULATION', 'DESCRIPTION', and 'DATE'. The table contains one row with the value '192.168.1.1' in the 'IP OR CIDR' column and 'Rule1' in the 'RULE NAME' column. The 'DATE' column shows '27.08.2022'. There is also an 'EXPORT' button at the bottom.

Creating

In the form of rule creating:

- Specify AS number;
- Enter the rule name;
- Enter the rule description;

Save the changes by clicking on "Set Exclusion" button.

Editing

Click on the button "Edit exclusion". In the form of rule editing you can change:

- name of the rule;
- its description.

Edit rule

AS number: 1234

Rule name *

Rule1

Public description *

Rule1 Description

SET DSCP

Save the changes by clicking on "Set DSCP" button.

Deleting

In the list of exclusions click the button "Delete exclusion" and confirm/cancel the operation.

ASN EXCLUDES

ASN AS numbers to lists and all ASN traffic will be passed without processing

Warning: This sets PASS priority to AS numbers and works globally!

Add new rule

AS number *

Rule name *

Public description *

SET EXCLUSION

Database search...

AS NUMBER	RULE NUMBER	REGULATOR	DESCRIPTION	DATE
1234	name 123451		name 123456	2020-10-06-02

1/1 OF 1

EXPORT

Delete exclusion

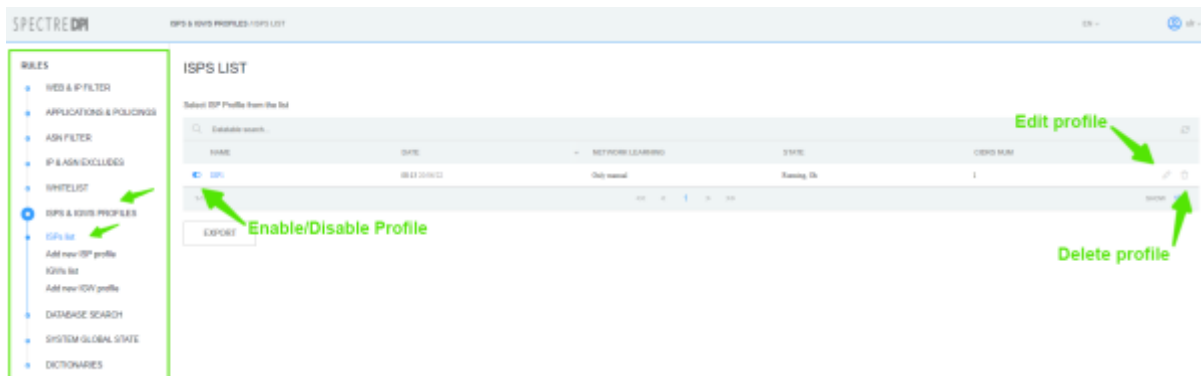
Delete? Are you sure?

Cancel/Confirm

CANCELDELETE

ISP Configuration

Change to the "ISPS & IGWS Profiles" → "ISPs List".

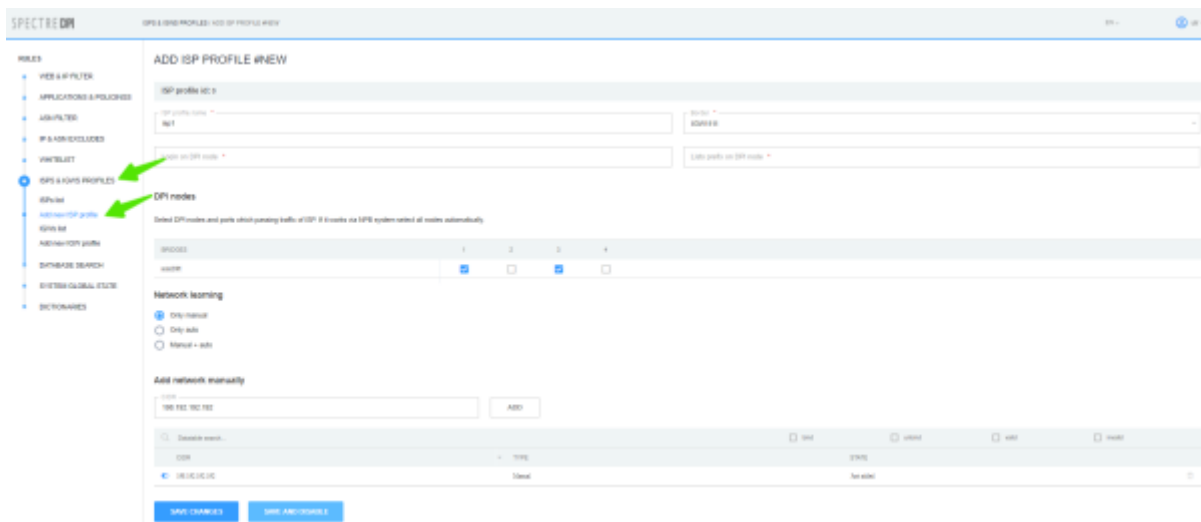


Creating an ISP Profile

To create new IGW profile go to the "ISPS & IGWS Profiles" section → "Add new ISP Profile".

In the form specify:

- Name of ISP profile;
- Choose the border from the list;
- Login to be used on the DPI node;
- Prefix for lists on the DPI node (it will be used as the name of service profile on the node);
- Choose bridges of the border;
- Choose Network training to get the addresses of this profile;
- Specify address/networks of the ISP (if necessary).



Click on the button "Save changes" or "Save and Disable/Enable".



After creation the ISP profile is enabled by default. Only enabled profiles are uploaded to DPI nodes.

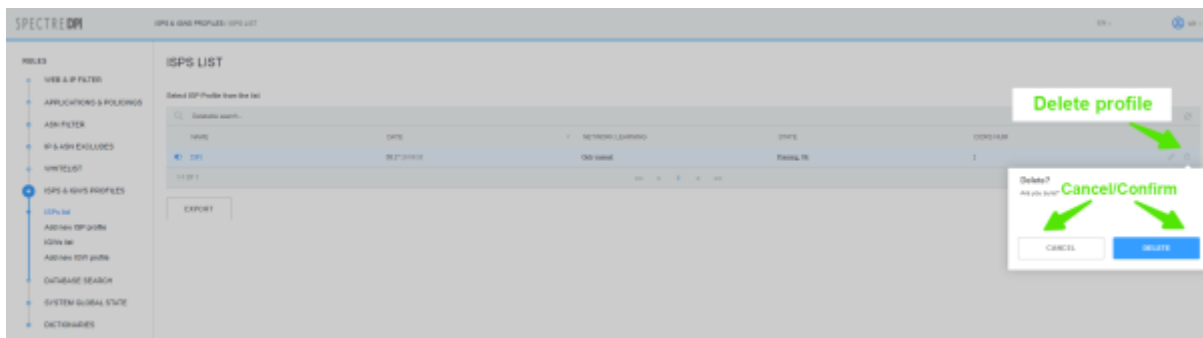
Editing ISP Profile

In the "ISPS & IGWS Profiles" section → "ISPs list" click on the button "Edit Profile".

A modal form for creating/editing ISP profile will pop up; make the changes you need and click on the "Save changes" or "Save and Disable/Enable" button.

Deleting ISP Profile

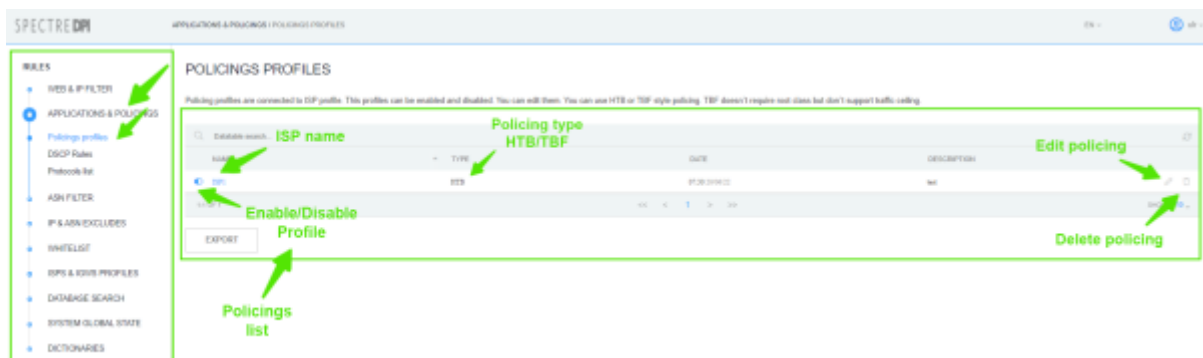
In the "ISPS & IGWS Profiles" section → "ISPs List" click on the "Delete" button and confirm/cancel the action.



Attention: Before deleting the profile, make sure there are no rules referring to this profile!

Policing Profile

Change to the "Applications and Policings" profile → "Policings Profiles".



Editing Policing Profile

Click on the "Edit policing" button.

EDIT APPLICATION POLICING PROFILE #1

Policing profiles are connected to ISP profile. This profiles can be enabled and disabled. You can edit them. You can use HTB or TBF style policing. TBF doesn't require root class but don't support traffic ceiling.

Profile name: ISP1 (Enabled)

ISP profile configuration

Description

test

Policing type: HTB

Inbound profile:

ROOT RATE	110	Unit	Mbps	ROOT CEIL	0	Unit	Bps	☐ Enable
CS0 RATE	0	Unit	Bps	CS0 CEIL	110	Unit	Mbps	☐ Static
CS1 RATE	0	Unit	Bps	CS1 CEIL	110	Unit	Mbps	☐ Static
CS2 RATE	0	Unit	Bps	CS2 CEIL	110	Unit	Mbps	☐ Static
CS3 RATE	0	Unit	Bps	CS3 CEIL	110	Unit	Mbps	☐ Static
CS4 RATE	0	Unit	Bps	CS4 CEIL	110	Unit	Mbps	☐ Static
CS5 RATE	0	Unit	Bps	CS5 CEIL	110	Unit	Mbps	☐ Static

Applications CS0 list

Applications CS1 list

Applications CS2 list

Applications CS3 list

Applications CS4 list

Applications CS5 list

In the popup editing form:

- Enter policing description;
- Choose policing type TBF/HTB (form with class values will look different depending on the type selected)

You can use configuration autocomplete:



- For HTB type: rate=8Bps, ceil=value that was specified in autocomplete form;
- For TBF type: rate=value that was specified in autocomplete form.

To save the changes click on the button "Save profile" or "Save and disable/enable".



Thy policing profile is disabled by default.

Deleting Policing Profile

There are two ways to delete the profile: by clicking "Delete profile" button in the list of policing profiles or the same button on Editing Profile page.

WEB and IP Filter

Linking Rules List

Change to the "WEB and IP Filter" section.

WEB & IP FILTER

Web/IPv4 firewall summary

TYPE	ACTIVE	DISABLED	TOTAL
CD	4	0	4
SD	4	0	4

Last entries in Web/IPv4 register

REGID	DATE	TYPE	RESOURCE NAME	RESOURCE VALIDATED	REGULATOR	REASON
1	11/08/2019 17	SD	malware	*malware	RSG 1	Tam
2	11/08/2019 17	SD	malware	malware	RSG 1	Tam
3	11/08/2019 17	CD	malware	*malware	RSG 1	Tam
4	11/08/2019 17	CD	malware	malware	RSG 1	Tam
5	11/08/2019 17	CD	malware	malware	RSG 1	Tam
6	11/08/2019 17	CD	malware	*malware	RSG 1	Tam
7	11/08/2019 17	SD	malware	*malware	RSG 1	Tam
8	11/08/2019 17	SD	malware	malware	RSG 1	Tam

1/10/19

EXPORT

Edit rule

Creating/Editing Locking Rules

- To create new locking rule for a resource, change to the "WEB and IP Filter" section → "Add new rule";
- To edit an existing rule change to the "WEB and IP Filter" section and click on "Edit rule" button.

In the popup form:

- Choose the regulator;
- Choose the category;
- Enter rule public description;
- Enter rule hidden description;

ADD RULE #NEW

Rule ID: 0

Resource: REG 111

Category: CAT 111

Public description: Public Description

Internal description: Internal Description

This description will be shown if you have public blocked database

This is internal description for you to find this rule to add or change state

Resource

Select type of resource and put the URL, SNI, CN, IP, IP-PORT or CIDR in this field.

Resource: facebook.com

Type: URL

VALIDATE

Validation result: This is SSL/TLS resource. We can block FULL DOMAIN! Next SNI and CN will be added to the list: SNI: facebook.com CN: facebook.com

ADD TO LIST

IMPORT FROM FILE

In the resource validation form, enter the resource and choose its type:

- If it is not necessary to validate the resource, just click on "Add to the list" button;
- Click on the "Check" button. Information about the resource will be displayed. It can be added to the rule locking list. To do this, click the "Add to List" button.

List of resources

TYPE	RESOURCE NAME	RESOURCE VALIDATED	STATUS	Delete resource
☑️ IP	facebook.com	*facebook.com	Valid	🗑️
☑️ IP	facebook.com	facebook.com	Valid	🗑️
☑️ IP	facebook.com	*facebook.com	Valid	🗑️
☑️ IP	facebook.com	facebook.com	Valid	🗑️

CLEAR ALL

☒ **Apply the rule to ISPs from the list**

Select ISP which the rule will be applied

☐ ISP1

SELECT ALL UNSELECT ALL

Actions log

DATE	USER	ACTION	NEW VALUE	OLD VALUE
Data not found				

1/1 OF 1

SHOW

SAVE CHANGES SAVE AND DISABLE

In the subsection for binding rules to ISP profiles:

- If the option "Apply the rule to ISP from the list" is **disabled**, such rule will be global. Resources from this rule will be included in the global lists of blocked resources.
- If the option "Apply the rule to ISP from the list" is **enabled**, such rule will be applied only to those ISP profiles, which are noted in this rule. Resources from this rule will be included in the locking lists for these ISP profiles.

Deleting the Locking Rule

Change to the "WEB and IP Filter" section and click on the "Edit the rule" button.

Select type of resource and put the URL, SNL, CN, IP, IP-PORT or CIDR to this field.

Resource From URL

List of resources

TYPE	RESOURCE NAME	RESOURCE VALIDATED	STATUS	
☑️ IP	facebook.com	facebook.com	Valid	🗑️
☑️ IP	facebook.com	*facebook.com	Valid	🗑️
☑️ IP	facebook.com	facebook.com	Valid	🗑️
☑️ IP	facebook.com	*facebook.com	Valid	🗑️

CLEAR ALL

☒ **Apply the rule to ISPs from the list** The rule will be applied for all ISPs by default.

Actions log

DATE	USER	ACTION	NEW VALUE	OLD VALUE
11.23.2019.01	sb	The rule created		

1/1 OF 1

DELETE rule

SHOW

SAVE CHANGES SAVE AND DISABLE EXPORT RULE

DELETE RULE



Attention: Before deleting a rule, make sure it does not refer to any ISP profile.

Domain Check

Change to the "WEB and IP Filter" section → "Check domain".

The screenshot shows the SPECTRE DPI interface. On the left, a sidebar lists various sections: RULES, APPLICATIONS & POLICIES, ASN FILTER, IP & ASN EXCLUDES, WHITELIST, IPS & IDS PROFILES, DATABASE SEARCH, SYSTEM GLOBAL STATE, and DICTIONARIES. The 'WEB & IP FILTER' section is highlighted with a green box, and arrows point to 'Add new rule' and 'Check domain'. The main area is titled 'CHECK DOMAIN' and contains a form with a 'Resource check' input field and a 'CHECK' button. A green box highlights the input field and button, with an arrow pointing to it labeled 'Domain check form'.

In the "Resource Check" field type in the URL of resource to be checked. Then click on the "Check" button. Information about the specified resource will be displayed below the form:

- SSL/TLS, locking type;
- Certificate information;
- DNS list;
- Recommendations about the values to use to lock this resource.

The screenshot shows the SPECTRE DPI interface with the 'CHECK DOMAIN' results. The 'Resource check' field contains 'Mbc.com' and the 'CHECK' button. Below the form, a green box highlights the 'Certificate info' section, with arrows pointing to it labeled 'Certificate info' and 'SSL/TLS, locking type'.

Certificate general information

Resource name	Mbc.com
IPs	
DNS	www.mbc.com
DNS	api.mbc.com
DNS	www.mbc.com
DNS	www.mbc.com
DNS	www.mbc.com
Total number of IPs	1
SSL	
Signature algorithm	sha256WithRSAEncryption
Key type	RSA
Key size	2048 bits
Serial number	28762228F13A4D47008F74700
Use before	12.06.2020 00:00
Use after	06.06.2020 00:00
Number of uses	2

DNS info			
TYPE	DOMAIN NAME	ADDRESS	TTL
A	Wu.com	10.10.10.10	300
A	Wu.com	10.10.10.10	300
A	Wu.com	10.10.10.10	300
A	Wu.com	10.10.10.10	300
NS	Wu.com	ns1.Wu.com	300
NS	Wu.com	ns2.Wu.com	300
NS	Wu.com	ns3.Wu.com	300
NS	Wu.com	ns4.Wu.com	300
MX	Wu.com	mail.Wu.com	300
MX	Wu.com	mail.Wu.com	300

DNS recursion: No

Result information	
To block this resource only with certificate use	
URI	Wu.com
URI	*Wu.com
URI	Wu.com
URI	*Wu.com

Download file to report to rule

DOWNLOAD FILE 1

DNS list

Recommendations
for resource locking

Search the Database (among the blocking rules)

Change to the "WEB and IP Filter" section → "Search Database".

In the "IP, CIDR, Domain, Notes" field enter the value in accordance with the prompts at the top of the page. Then choose type of search: Full Text, By Resources or By Description. Click on "Search" button.

As a result, all blocking rules that match the selected search parameters will be displayed.

SPECTRE DPI						
Фильтр WEB и IP (поиск по базе)						
ПОИСК ПО БАЗЕ						
Поиск по базе данных Web / IP						
Используйте "*" до и после поискового слова для поиска по шаблону. Используйте "*" до и после для поиска определенной фразы. Больше помощи						
IP: 10.10.10.10, Домен: facebook.com						
Полный текст						
Поиск						
Результаты поиска для 'facebook.com'						
ID	DATA	TYPE	RESOURCE	PROTECTED RESOURCE	ACTION	
1	11.01.2019.02	IP	facebook.com	*facebook.com	Block	
		IP	facebook.com	facebook.com	Block	
		CS	facebook.com	*facebook.com	Block	
		CS	facebook.com	facebook.com	Block	

1 of 4

ЭКСПОРТ

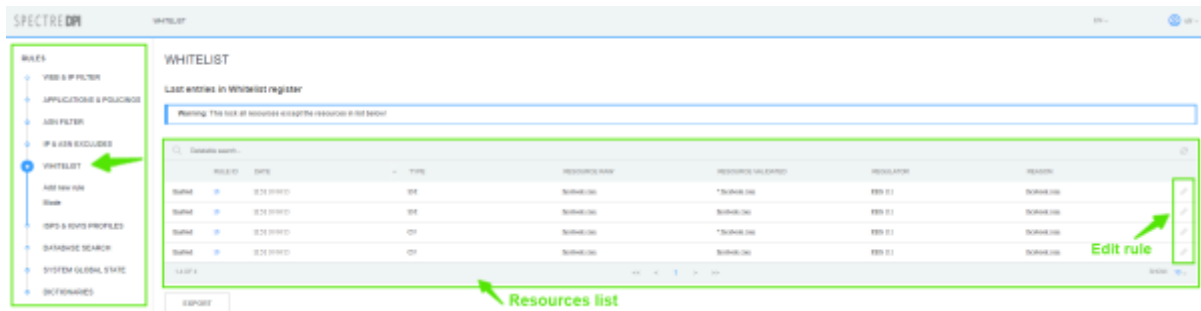
Форма для поиска
правил

Результаты
поиска

Whitelist

Whitelist rule list

Change to the "Whitelist" section.

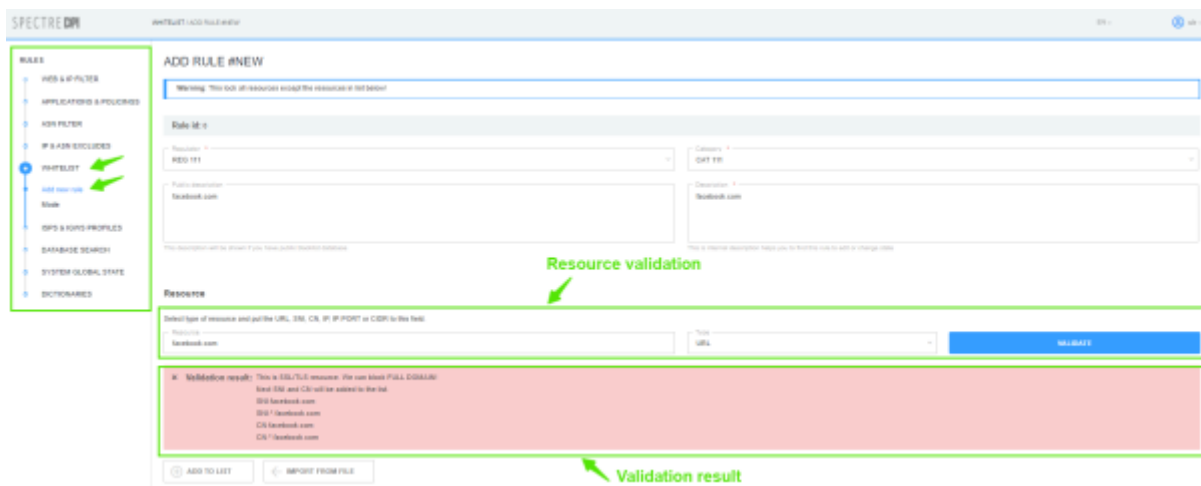


Creating/Editing the white list

- To create a new white list rule change to the "Whitelist" section → "Add new rule";
- To edit an existing rule change to the "White list" section and click on the "Edit rule" button.

In the popup form:

- Choose the regulator;
- Choose the category;
- Enter rule public description;
- Enter rule hidden description;



In the resource validation form, enter the resource and choose its type:

- If it is not necessary to validate the resource, just click on "Add to the list" button;
- Click on the "Check" button. Information about the resource will be displayed. It can be added to the rule locking list. To do this, click the "Add to List" button.

List of resources

TYPE	RESOURCE NAME	RESOURCE VALIDATED	STATUS
❏ D2	Scitank.com	*Scitank.com	1000
❏ D1	Scitank.com	Scitank.com	1000
❏ D2	Scitank.com	*Scitank.com	1000
❏ D1	Scitank.com	Scitank.com	1000

CLEAR ALL

☒ Apply the rule to ISPs from the list

Select ISP which the rule will be applied

☒ ISP1

SELECT ALL UNSELECT ALL

Actions log

DATE	USER	ACTION	NEW VALUE	OLD VALUE
12.12.2019 12	id	The rule created		

1-1 OF 1

SAVE CHANGES SAVE AND DISABLE EXPORT RULE DELETE RULE

Resources list

Applying the rule to ISP profile

In the subsection for binding rules to ISP profiles:

- If the option “Apply the rule to ISP from the list” is **disabled**, such rule will be global. Resources from this rule will be included in the global lists of blocked resources.
- If the option “Apply the rule to ISP from the list” is **enabled**, such rule will be applied only to those ISP profiles, which are noted in this rule. Resources from this rule will be included in the locking lists for these ISP profiles.

Deleting a white list rule

Change to the “Whitelist” section and click on the “Edit the rule” button.

Resource

Define type of resource and put the URL, DNS, CIDR, IP, PORT or CIDR to this field

Resource Type

ADD TO LIST IMPORT FROM FILE

List of resources

TYPE	RESOURCE NAME	RESOURCE VALIDATED	STATUS
❏ D1	Scitank.com	Scitank.com	1000
❏ D2	Scitank.com	*Scitank.com	1000
❏ D1	Scitank.com	Scitank.com	1000
❏ D2	Scitank.com	*Scitank.com	1000

CLEAR ALL

☒ Apply the rule to ISPs from the list This rule will be applied for all ISPs by default

Actions log

DATE	USER	ACTION	NEW VALUE	OLD VALUE
12.12.2019 12	id	The rule created		

1-1 OF 1

SAVE CHANGES SAVE AND DISABLE EXPORT RULE DELETE RULE

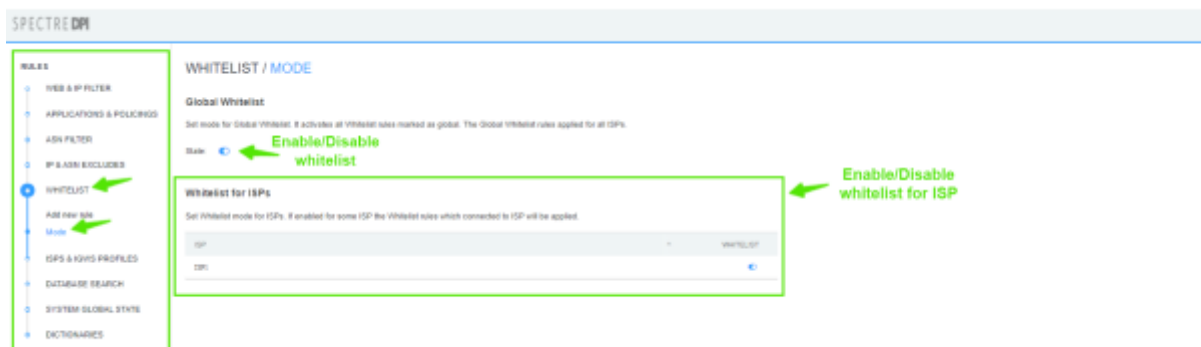
Delete rule



Attention: Before deleting a rule, make sure it does not refer to any ISP profile.

Whitelist operating mode management

Change to the “Whitelist” section → "Mode".



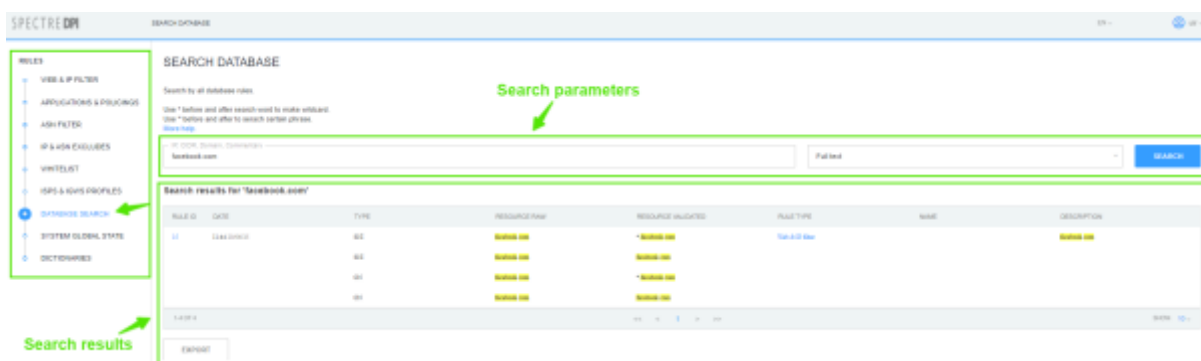
- With the global whitelist mode enabled, the whitelist service is applied to all ISP profiles and resource lists are formed only from global whitelist rules;
- When the whitelist mode is enabled for a separate ISP profile, the service is applied only to ISP which has it enabled. The lists are formed only from white list rules which refer to this ISP profile;
- If both mode are enabled, global and separate ISP rules lists are concatenated. For other ISPs, the whitelist service is used with only the global whitelist rules.

Database search (global)

Change to the "Database search" section.

In the "IP, CIDR, Domain, Comment" field enter the value in accordance with the prompts at the top of the page, choose search type: Full Text, By Resources or By Description. Click on "Search" button.

As a result, all blocking rules (with type specified) that match the selected search parameters will be displayed.



Task monitoring

Change to the "State of the system" section.

SYSTEM GLOBAL STATE TASKS LIST

TASKS LIST

Export tasks list

ID	TYPE	ACTION	STATUS	STATUS DESCRIPTION	DATE
01	Gen	CreateOutfile	Success		10.11.2019 10:00
011	Gen	CreateOutfile	Success		10.11.2019 10:00
012	Gen	CreateOutfile	Success		10.11.2019 10:00
013	Gen	CreateOutfile	Success		10.11.2019 10:00
014	Gen	CreateOutfile	Success		10.11.2019 10:00
015	Gen	CreateOutfile	Success		10.11.2019 10:00
016	Gen	CreateOutfile	Success		10.11.2019 10:00
017	Gen	CreateOutfile	Success		10.11.2019 10:00
018	Gen	CreateOutfile	Success		10.11.2019 10:00
019	Gen	CreateOutfile	Success		10.11.2019 10:00
020	Gen	CreateOutfile	Success		10.11.2019 10:00
021	Gen	CreateOutfile	Success		10.11.2019 10:00
022	Gen	CreateOutfile	Success		10.11.2019 10:00
023	Gen	CreateOutfile	Success		10.11.2019 10:00
024	Gen	CreateOutfile	Success		10.11.2019 10:00
025	Gen	CreateOutfile	Success		10.11.2019 10:00
026	Gen	CreateOutfile	Success		10.11.2019 10:00
027	Gen	CreateOutfile	Success		10.11.2019 10:00
028	Gen	CreateOutfile	Success		10.11.2019 10:00
029	Gen	CreateOutfile	Success		10.11.2019 10:00
030	Gen	CreateOutfile	Success		10.11.2019 10:00
031	Gen	CreateOutfile	Success		10.11.2019 10:00
032	Gen	CreateOutfile	Success		10.11.2019 10:00
033	Gen	CreateOutfile	Success		10.11.2019 10:00
034	Gen	CreateOutfile	Success		10.11.2019 10:00
035	Gen	CreateOutfile	Success		10.11.2019 10:00
036	Gen	CreateOutfile	Success		10.11.2019 10:00
037	Gen	CreateOutfile	Success		10.11.2019 10:00
038	Gen	CreateOutfile	Success		10.11.2019 10:00
039	Gen	CreateOutfile	Success		10.11.2019 10:00
040	Gen	CreateOutfile	Success		10.11.2019 10:00
041	Gen	CreateOutfile	Success		10.11.2019 10:00
042	Gen	CreateOutfile	Success		10.11.2019 10:00
043	Gen	CreateOutfile	Success		10.11.2019 10:00
044	Gen	CreateOutfile	Success		10.11.2019 10:00
045	Gen	CreateOutfile	Success		10.11.2019 10:00
046	Gen	CreateOutfile	Success		10.11.2019 10:00
047	Gen	CreateOutfile	Success		10.11.2019 10:00
048	Gen	CreateOutfile	Success		10.11.2019 10:00
049	Gen	CreateOutfile	Success		10.11.2019 10:00
050	Gen	CreateOutfile	Success		10.11.2019 10:00
051	Gen	CreateOutfile	Success		10.11.2019 10:00
052	Gen	CreateOutfile	Success		10.11.2019 10:00
053	Gen	CreateOutfile	Success		10.11.2019 10:00
054	Gen	CreateOutfile	Success		10.11.2019 10:00
055	Gen	CreateOutfile	Success		10.11.2019 10:00
056	Gen	CreateOutfile	Success		10.11.2019 10:00
057	Gen	CreateOutfile	Success		10.11.2019 10:00
058	Gen	CreateOutfile	Success		10.11.2019 10:00
059	Gen	CreateOutfile	Success		10.11.2019 10:00
060	Gen	CreateOutfile	Success		10.11.2019 10:00
061	Gen	CreateOutfile	Success		10.11.2019 10:00
062	Gen	CreateOutfile	Success		10.11.2019 10:00
063	Gen	CreateOutfile	Success		10.11.2019 10:00
064	Gen	CreateOutfile	Success		10.11.2019 10:00
065	Gen	CreateOutfile	Success		10.11.2019 10:00
066	Gen	CreateOutfile	Success		10.11.2019 10:00
067	Gen	CreateOutfile	Success		10.11.2019 10:00
068	Gen	CreateOutfile	Success		10.11.2019 10:00
069	Gen	CreateOutfile	Success		10.11.2019 10:00
070	Gen	CreateOutfile	Success		10.11.2019 10:00
071	Gen	CreateOutfile	Success		10.11.2019 10:00
072	Gen	CreateOutfile	Success		10.11.2019 10:00
073	Gen	CreateOutfile	Success		10.11.2019 10:00
074	Gen	CreateOutfile	Success		10.11.2019 10:00
075	Gen	CreateOutfile	Success		10.11.2019 10:00
076	Gen	CreateOutfile	Success		10.11.2019 10:00
077	Gen	CreateOutfile	Success		10.11.2019 10:00
078	Gen	CreateOutfile	Success		10.11.2019 10:00
079	Gen	CreateOutfile	Success		10.11.2019 10:00
080	Gen	CreateOutfile	Success		10.11.2019 10:00
081	Gen	CreateOutfile	Success		10.11.2019 10:00
082	Gen	CreateOutfile	Success		10.11.2019 10:00
083	Gen	CreateOutfile	Success		10.11.2019 10:00
084	Gen	CreateOutfile	Success		10.11.2019 10:00
085	Gen	CreateOutfile	Success		10.11.2019 10:00
086	Gen	CreateOutfile	Success		10.11.2019 10:00
087	Gen	CreateOutfile	Success		10.11.2019 10:00
088	Gen	CreateOutfile	Success		10.11.2019 10:00
089	Gen	CreateOutfile	Success		10.11.2019 10:00
090	Gen	CreateOutfile	Success		10.11.2019 10:00
091	Gen	CreateOutfile	Success		10.11.2019 10:00
092	Gen	CreateOutfile	Success		10.11.2019 10:00
093	Gen	CreateOutfile	Success		10.11.2019 10:00
094	Gen	CreateOutfile	Success		10.11.2019 10:00
095	Gen	CreateOutfile	Success		10.11.2019 10:00
096	Gen	CreateOutfile	Success		10.11.2019 10:00
097	Gen	CreateOutfile	Success		10.11.2019 10:00
098	Gen	CreateOutfile	Success		10.11.2019 10:00
099	Gen	CreateOutfile	Success		10.11.2019 10:00
100	Gen	CreateOutfile	Success		10.11.2019 10:00

This section displays the task queue, status and time.

To see the details of the task, click on "Task Details".

Logs

The logs for this section are stored in files:

```
/var/www/html/dpiui2/backend/storage/logs/ulr*.log
```

Log detail level is specified with `ULR_LOAD_LOG_LEVEL` option in the `.env` configuration file.