



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«МИРЭА – Российский технологический университет»  
**РТУ МИРЭА**

---

**Институт информационных технологий  
(ИТ)  
Кафедра инструментального и прикладного программного обеспечения  
(ИиППО)**

**КУРСОВАЯ РАБОТА**  
по дисциплине: Программное обеспечение локальных сетей  
направления профессиональной подготовки: 09.03.04 «Программная инженерия»

Тема: Анализ сетевого трафика с помощью программы PRTG

Студент: Миронов Алексей Дмитриевич Группа:  
ИКБО-02-19

Работа представлена к защите \_\_\_\_\_ (дата) Миронов /Миронов А.Д./  
(подпись и ф.и.о. студента)

Руководитель: ассистент, Лепёхин Владимир Викторович

Работа допущена к защите \_\_\_\_\_ (дата) \_\_\_\_\_ /Лепёхин В.В./  
(подпись и ф.и.о. рук-ля)

Оценка по итогам защиты:

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_

(подписи, дата, ф.и.о., должность, звание, уч. степень двух преподавателей, принявших  
защиту)

М. РТУ МИРЭА. 2021 г.

## СОДЕРЖАНИЕ

1. Введение.....	3
1.1 Цель.....	3
1.2 Предназначение программы PRTG.....	3
2. Общее описание исследуемого ПО.....	3
3. Описание реализаций на основе исследуемого ПО.....	14
4. Заключение.....	20
5. Список                    использованных                    информационных источников.....	20

## **1. Введение**

В наше время практически все компании используют интернет для различных нужд. Будь то крупные IT корпорации или даже салоны красоты. Часто в компаниях бывает много тысяч сотрудников и тогда количество трафика и его назначение становится трудно отследить. Для этих целей были созданы программы для контроля трафика. Сейчас их довольно много и одно из самых популярных – PRTG.

### **1.1 Цель**

Данная работа проведена с целью изучения работы программы PRTG, а также её особенностей и сфер применения. В данной работе будут разобраны такие вещи как: Интерфейс программы PRTG, различные методы настройки и использования. А также некоторые примеры реального применения данной программы

### **1.2 Предназначение программы PRTG**

Данная программа предназначена для мониторинга , визуализации и контроля использования сети.

## **2. Общее описание исследуемого ПО**

Ключевыми особенностями программы PRTG являются следующие факторы:

### **Производительность**

Большие установки способны довольно значительно нагружать систему мониторинга. В результате проблем с производительностью, вызванных высокими нагрузками, часто появляются искажения в результатах мониторинга. Зачастую это приводит к недовольству пользователей. Повышается риск отказов и сбоев. Программа PRTG может довольно неплохо справляться с высокими нагрузками, и может предлагать оптимальные стратегии для избежания проблем с производительностью.

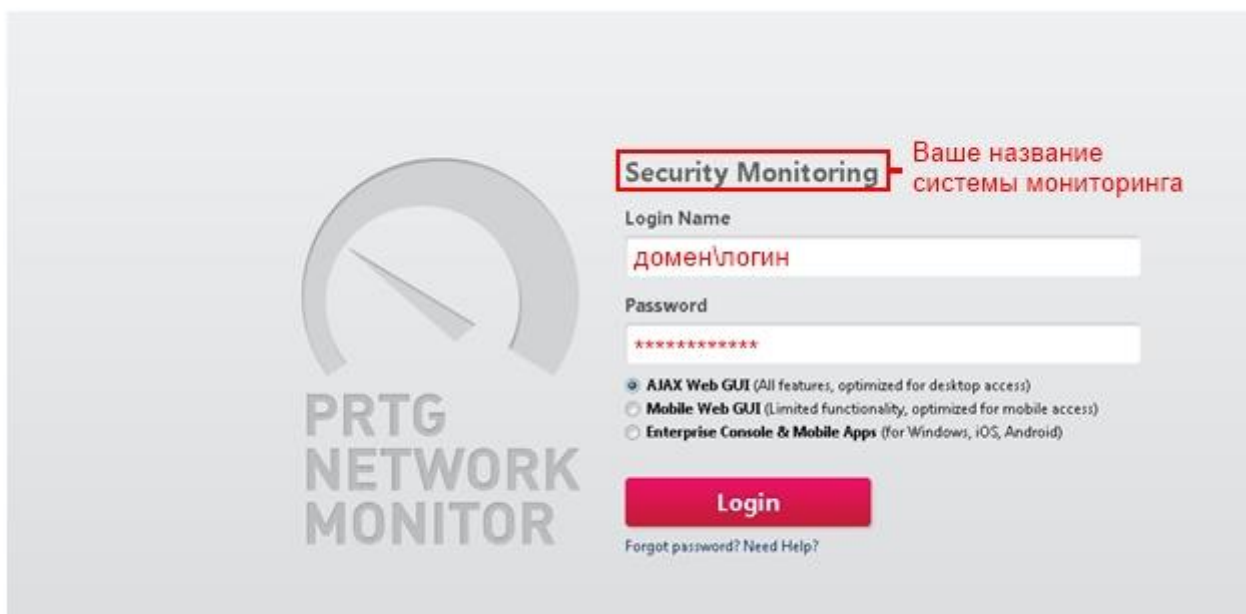
### **Совместимость**

Системы мониторинга могут являться центральными компонентами ИТ-инфраструктуры, поэтому важным фактором является то, что система мониторинга должна быть совместима со сторонними решениями. Программу PRTG можно совместить с устройствами и программами от любых производителей, многофункциональный API дает возможность создавать необходимые решения для мониторинга.

### Распределенные среды

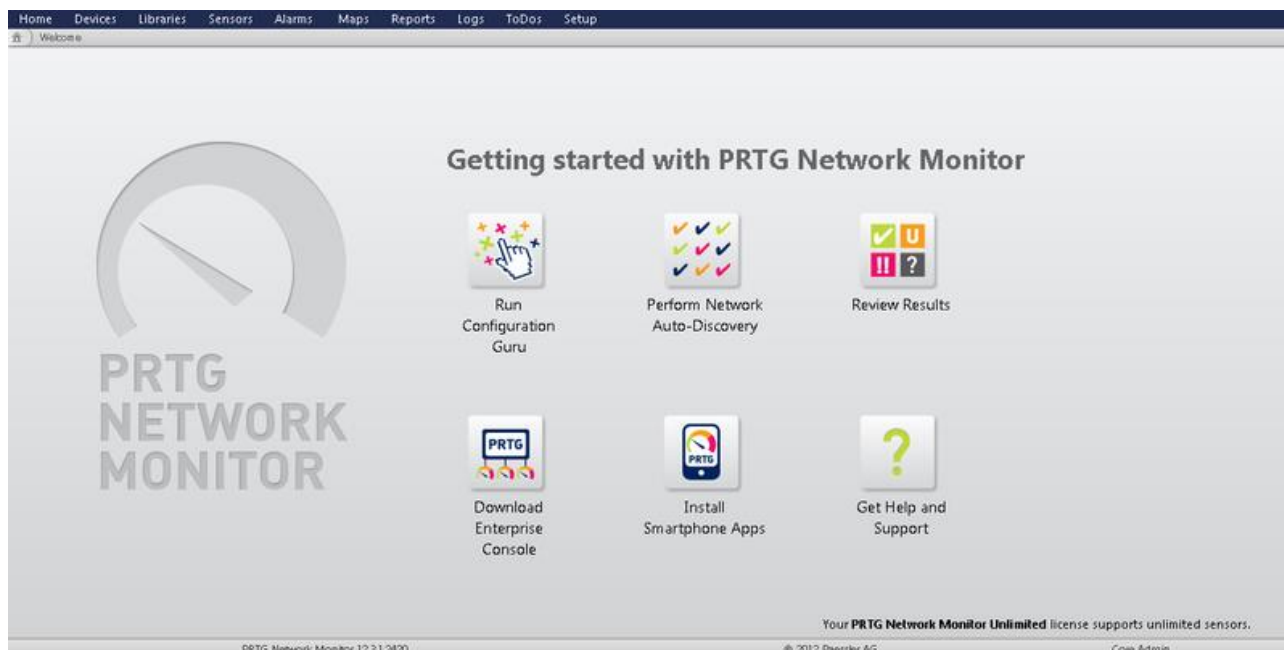
Большая инфраструктура сети может включать в себя несколько локальных сетей. С помощью PRTG можно создать простое решение для управления распределенным мониторингом и поддержкой. Это даёт полный обзор всех сетей инфраструктуры и помогает избежать проблем с распределением зон ответственности между сотрудниками и подразделениями.

Данная программа имеет несколько интерфейсов, среди них Web-интерфейс и desktop.

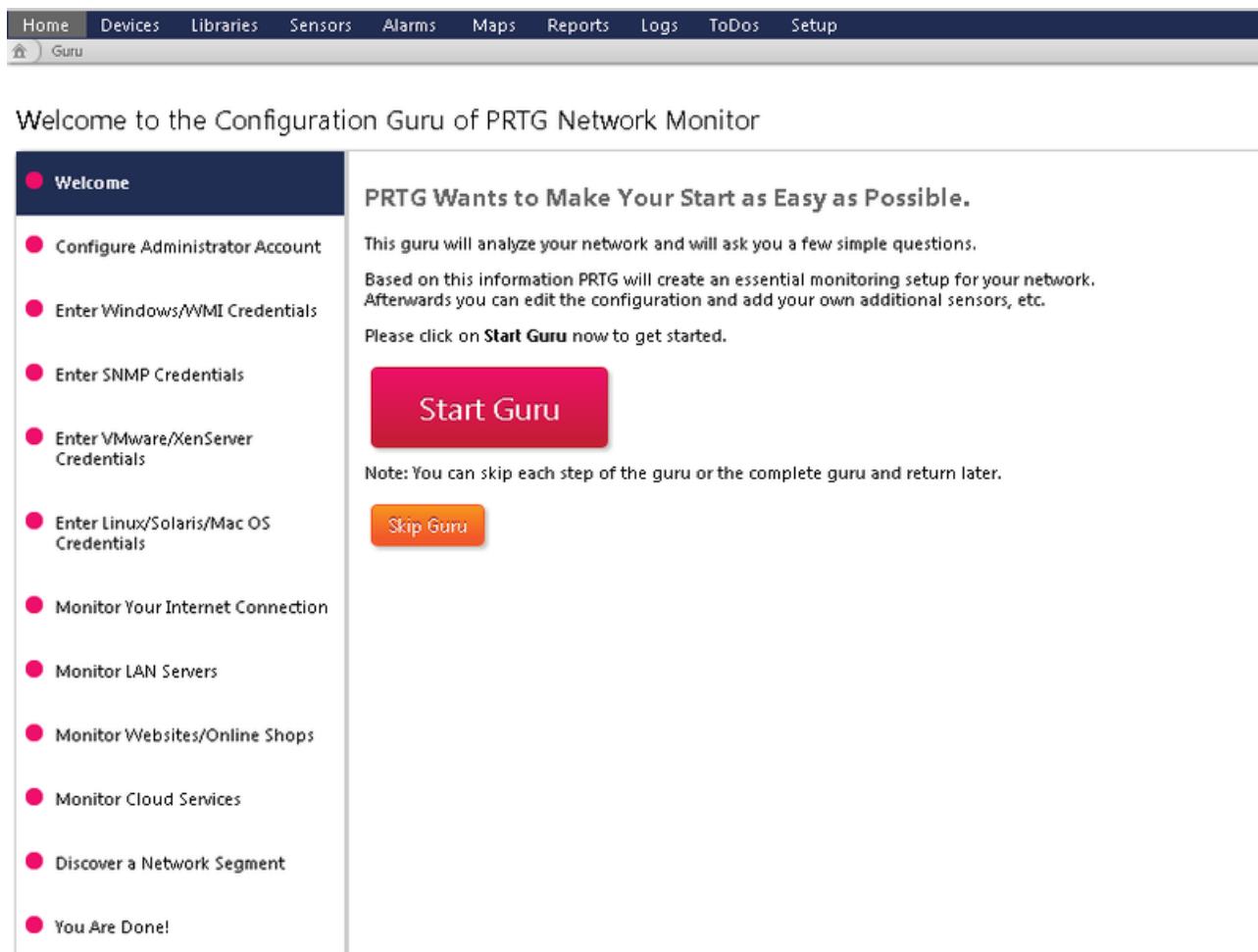


В данном случае показан вход в систему через Web-интерфейс. Его можно использовать как с компьютера так и с мобильного устройства или же с любого другого устройства, поддерживающего Web интерфейсы. Данная система поддерживает доменные учетные записи, однако учетную запись можно создать вручную.

После входа появится экран приветствия:



При первоначальном входе в систему рекомендуется пройти по ссылке **Run Configuration Guru** которая поможет сразу же настроить большинство изначальных конфигураций:



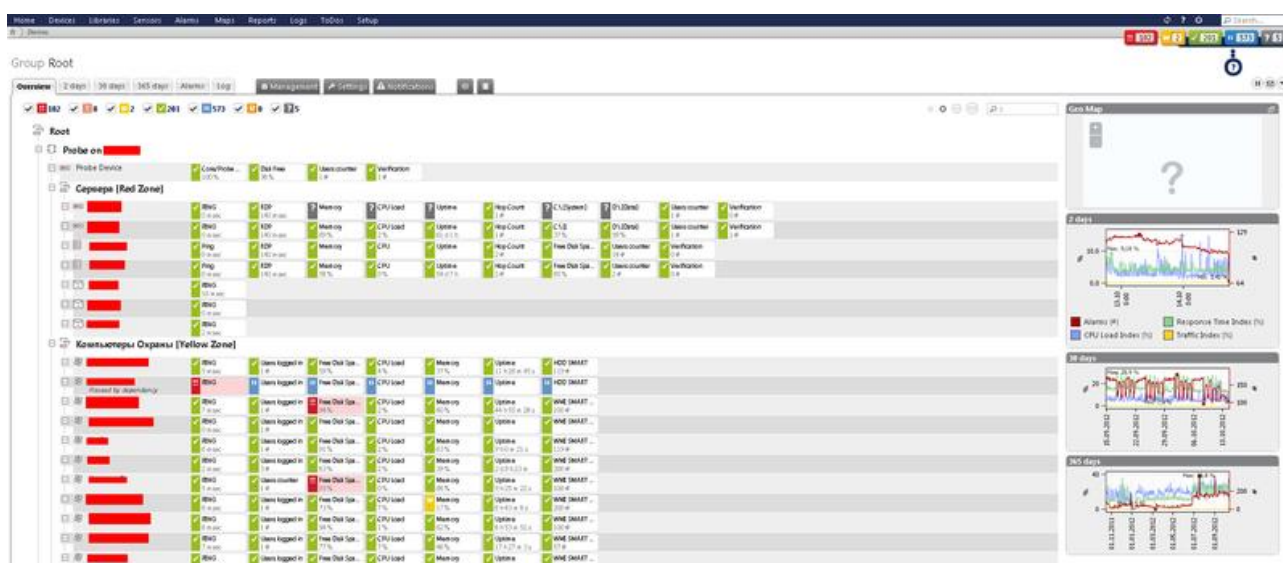
На этой странице можно настроить следующие параметры:

- Логин и пароль корневого аккаунта администратора (core admin)
- Данные для использования с WMI сенсорами (зачастую это учетная запись, которая имеет администраторские полномочия в домене)
- При использовании UNIX или LINUX системы, так же можно прописать данные ваших УЗ.
- Данные для соединения с интернетом (например, в случае, если организация использует прокси-сервер) — доступ к интернету полезен как минимум тем, что с его помощью можно активировать систему без отправки на почту компании раessler кодов, а напрямую, но и конечно же

при хорошей скорости интернета программа может самостоятельно скачивать и устанавливать обновления.

- Поиск персональных компьютеров, серверов и прочего периферийного оборудования в автоматическом режиме (если сеть или сегмент сети небольшой и не будет искаться несколько сотен машин).

После базовой настройки откроется окно, на котором отображаются все ваши устройства и сенсоры:



В этом окне можно увидеть множество цветовых индикаторов, которые означают следующее:

**Красный** — ошибка \ недоступно \ превышение заданного параметра \ недостаток до заданного параметра

**Оранжевый** — нетипичное поведение сенсора (Пример: Пинг в данный момент 200 ms, при среднем пинге на данном устройстве в данное время дня \ недели 110 ms)

**Желтый** — предупреждение (сенсор приближается к критичным границам)

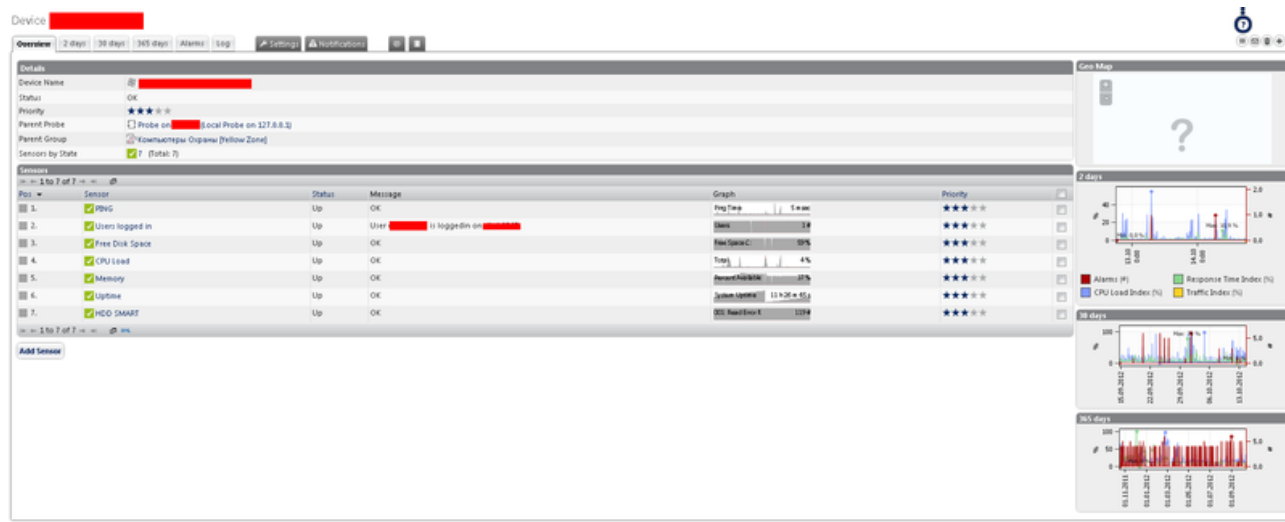
заданного параметра или же стал недоступен в момент прошлой проверки)

**Зеленый** — штатное поведение сенсора

**Синий** — пауза (устанавливается либо вручную, либо автоматически). В паузу сенсор может поставить как администратор, так и сама система по нескольким причинам: главный для устройства сенсор недоступен и все остальные сенсоры устройства установлены в режим паузы; слишком большое количество запросов одновременно — сенсор будет перезапущен после получения данных с других сенсоров.

**Серый** — не получены данные с сенсора (только включили, только закончился режим паузы)

В данном примере рассмотрен один из вариантов решения в помощью PRTG для нового добавленного компьютера:



В этом окне можно увидеть несколько строчек описывающих состояние устройства, которые означают:

**Ping** — стандартный ping до машины. Главный сенсор на устройстве.



**Users logged in** — кто залогинен на данной конкретной машине.

**Free Disk Space** — % свободного места на жестком диске.

**CPU Load** — % загрузки процессора(-ов).

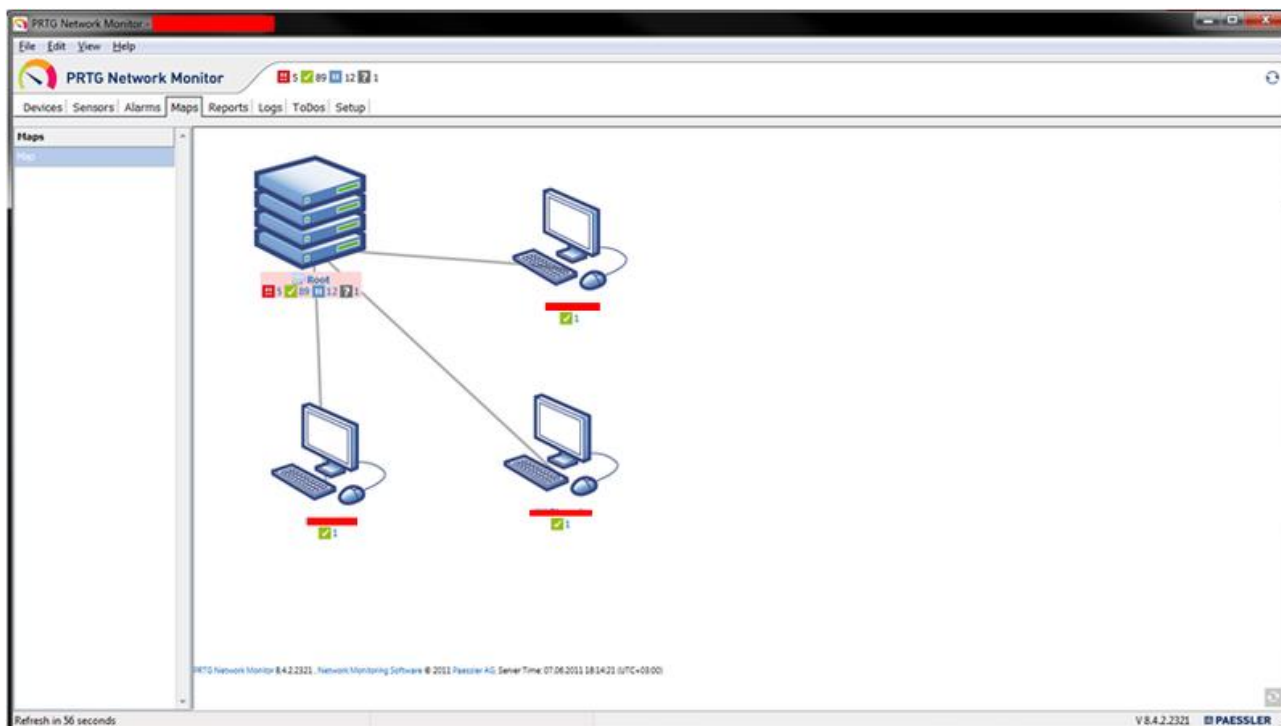
**Memory** — % использования памяти.

**Uptime** — время с момента последней перезагрузки ПК. Установлено ручное предупреждение — свыше 14 дней — оповещать администратора.

**HDD Smart** — проверки нескольких параметров чтения \ записи жесткого диска.

Существует 2 варианта представления устройства в системе:

1. Группировка сенсоров внутри устройств
2. Режим карты — пользователь сам рисует \ моделирует карту расположения своих устройств для более удобного визуального восприятия.



На данный момент в системе доступно множество различных сенсоров  
Сенсоры можно разделить на следующие условные категории:

- Common Sensors
- Bandwidth Monitoring Sensors
- Web Servers (HTTP) Sensors
- SNMP Sensors
- Windows/WMI Sensors
- Linux/Unix/OS X Sensors
- Virtual Servers Sensors
- Mail Servers Sensors
- SQL Database Servers Sensors
- File Servers Sensors
- Various Servers Sensors
- VoIP and QoS Sensors
- Hardware Parameter Sensors
- Custom Sensors

Меню добавления сенсоров (с версии 11 и выше):

Add Sensor to [REDACTED] (Step 1 of 2)

Search directly	Monitor What?	Target System Type?	Technology Used?
<input type="text" value=""/>	<input type="checkbox"/> Availability/Uptime	<input type="checkbox"/> Windows	<input type="checkbox"/> Ping
	<input type="checkbox"/> Bandwidth/Traffic	<input type="checkbox"/> Linux/macOS	<input type="checkbox"/> SNMP
	<input type="checkbox"/> Speed/Performance	<input type="checkbox"/> Virtualization OS	<input type="checkbox"/> WMI
	<input type="checkbox"/> CPU Usage	<input type="checkbox"/> File Server	<input type="checkbox"/> HTTP
	<input type="checkbox"/> Disk Usage	<input type="checkbox"/> Email Server	<input type="checkbox"/> SSH
	<input type="checkbox"/> Memory Usage	<input type="checkbox"/> SQL Server	<input type="checkbox"/> Packet Sniffing
	<input type="checkbox"/> Hardware Parameters		<input type="checkbox"/> NetFlow, sFlow, JFlow
	<input type="checkbox"/> Network Infrastructure		
	<input type="checkbox"/> Custom Sensors		

Matching Sensor Types - Count: 136

Ping	Ping Jitter	Traceroute	Port
Monitors connectivity using Ping	Returns the Statistical Jitter value for Pings to the parent device.	Gets the number of hops to the parent device and alerts if the route has changed.	Monitors a network TCP/IP port

Сенсор можно найти несколькими способами:

1. Выбрать категорию и из нее выбрать нужный сенсор.
2. Найти нужный сенсор в списке снизу
3. Ввести часть названия сенсора и выбрать из предложенных вариантов.

Зачастую в реальных задачах используются далеко не все сенсоры. Всего нескольких десятков сенсоров будет достаточно для полного контроля устройства.

Программа также может формировать отчеты в автоматическом режиме.

Пример ежемесячного регионального отчета:

## Report Uptime Security ping monthly

**Run Now** | **Stored Reports** | **Settings** | **Select Sensors Manually** | **Sensors Selected by Tag**

**Run Report "Uptime Security ping monthly"**

Report for

☐ **Current Period:** This month (01.10.2012 - 31.10.2012)


☐ **Previous Period:** Last month (01.09.2012 - 30.09.2012)

☐ **Select A Period**

☒ **Select Date Range Manually**


Start Date:

07.10.2012



End Date:

14.10.2012



Quick range

**Processing Options**

File Format and Delivery

☒ **View Report as HTML**

☐ **Create and store PDF file** (A ToDo will be sent when done)

☐ **Create PDF file, store it and send by e-mail**

В данном случае отчет установлен в автоматический режим, однако у пользователя есть возможность ручного запуска процесса.

Существует 3 основные опции выпуска отчетов:

1. Просмотр в онлайн режиме html страницу с отчетом.
2. сохранить отчет в виде PDF файла на сервере и уведомить об окончании формирования отчета по почте
3. Отправить сам PDF файл конечному пользователю

На вкладке **Stored Reports** можно увидеть все сохраненные на диске файлы.

При сохранении отчета в PDF, то выглядеть он будет примерно следующим образом:

Uptime Security ping monthly (01.09.2012 0:00:00 - 01.10.2012 0:00:00 24 / 7)



В данном случае использовано графическое представление данных. Если необходимо получить конкретную информацию, то можно формировать отчеты в текстовом виде в разрезе, например 5 минут. Тогда можно получать вместо картинки строки вида:

**01.01.2012 09:00:00 — 01.01.2012 09:05:00 Ping 100% Available**

Большинство отчетов достаточно настроить только 1 раз, протестировать его и больше не возвращаться к нему.

Программа PRTG также обладает функционалом логирования. Логируется абсолютно всё, начиная от поведения сенсоров, заканчивая Формированием отчетности, которая в последующем будет отправлена в смс сообщении или выслана на электронную почту.

Пример лога:

.og

Log Entries					
+ - 1 to 50 +					
Date Time	Parent	Type	Object	Status	Message
14.10.2012 19:34:56		VM Memory	Memory	Up	51 %
14.10.2012 19:31:10		Ping	PING	Up	0 msec
14.10.2012 19:31:09		Ping	PING	Warning	Request timed out (ICMP error # 11010)
14.10.2012 19:29:28		VM Memory	Memory	Warning	11 % (Percent Available Memory) is below the warning limit of 20 %
14.10.2012 19:21:09		Ping	PING	Up	0 msec
14.10.2012 19:21:09		Ping	PING	Warning	OK
14.10.2012 19:15:40		VM Memory	Memory	Warning	2 % (Percent Available Memory) is below the warning limit of 20 %
14.10.2012 19:11:10		Ping	PING	Up	0 msec
14.10.2012 19:11:10		Ping	PING	Warning	OK

Интерфейс логов интуитивно понятен и прост в использовании. Цветовые маркеры сигнализируют о критичности события.

### 3. Описание реализаций на основе исследуемого ПО

Несколько примеров использования PRTG в реальных задачах:

Первый пример – поиск нарушителей.

Нарушителем в данном конкретном случае считается любой пользователь, который не является владельцем конкретного устройства.

Для поиска нарушителя будет использоваться 2 сенсора типа Users logged in. Первый сенсор будет отображать реальную картину — кто в данный момент выполнил вход на машину (и выполнил ли вход вообще), а второй сенсор будет иметь на себе фильтр с usernames разрешенных сотрудников (т.е. эти usernames не будут отражаться).

На второй сенсор устанавливается оповещение — если количество пользователей больше 0, то немедленно оповестить администратора по почте. Username нарушителя отправится в письме вместе с именем и IP адресом машины, куда сотрудник пытался зайти.

Данный способ хорошо себя показывает в случае, если необходимо оперативно проверять тех, кто выполнял вход на устройство.

Второй пример:

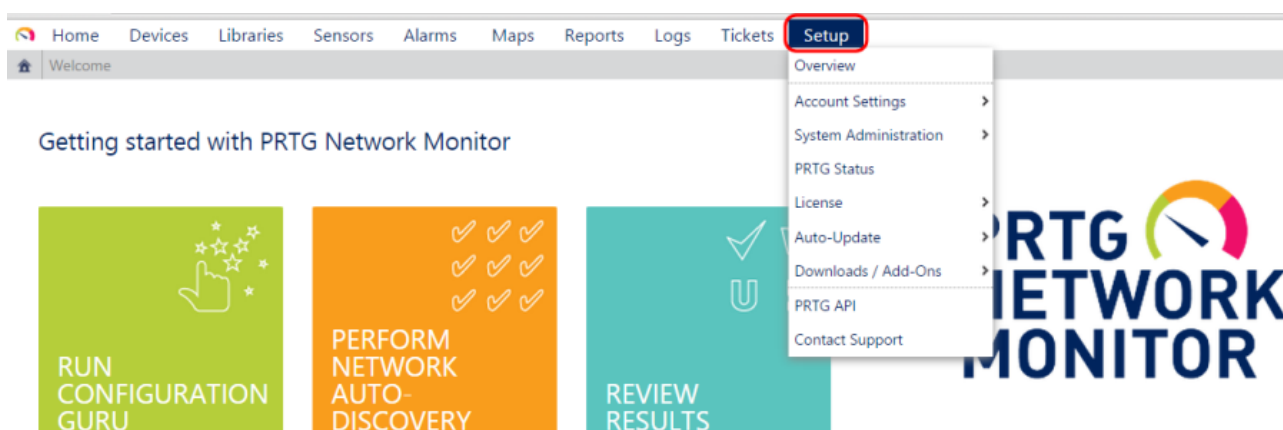
PRTG Network Monitor и NetPing SMS для отправки SMS-уведомлений на основе SNMP TRAP сообщений

Для реализации вышеописанного функционала необходимы:

1. шлюз для отправки и приёма SMS команд NetPing SMS с установленной SIM картой;
2. настроенная система мониторинга PRTG Network Monitor

Мы рассмотрим только 2-й пункт.

Для того, чтобы настроить SMS-уведомление в системе мониторинга PRTG, необходимо перейти по вкладке «Setup» в основные настройки системы:



Переходим во вкладку «Notifications»

## ACCOUNT SETTINGS



### My Account

Please choose this option to edit your personal account settings like email address, password, timezone, etc.



### Notifications

Notifications offer various notification methods through which you are informed in case a sensor trigger is activated.



### Notification Contacts

Manage the contact information that PRTG uses to send you notifications.



### Schedules

Using Schedules you can pause monitoring for groups, servers or sensors (and notifications) based on time and day of week.

Для получения доступа к странице «Notifications» необходимо ввести имя пользователя и пароль администратора системы:

Please Re-Enter Your Credentials

## YOU MUST RE-ENTER YOUR CREDENTIALS TO GAIN ACCESS TO ADMIN PAGES

Login Name

Password

Login

Cancel

После авторизации появится таблица «NOTIFICATIONS», в которую нужно добавить новое уведомление при помощи кнопки «Add new notification»:

## Account Settings



My Account



Notifications



Notification Contacts



Schedules

## NOTIFICATIONS

Show notifications tagged with

1 to 5 of 5

Object	Active/Paused
Email and push notification to admin	Active
Email to all members of group PRTG Users Group	Active
Ticket Notification	Active

1 to 5 of 5



Add new notification

В окне настройки нового уведомления «Add notification» указать название



уведомления в поле «Notification Name» и нажать чек-бокс «SEND SNMP TRAP». В области настройки «SEND SNMP TRAP» требуется заполнить параметры для отправки SNMP trap сообщений на шлюз NetPing SMS.

☐ SEND EMAIL  
☐ SEND PUSH NOTIFICATION<sup>BETA</sup>  
☐ SEND SMS/PAGER MESSAGE  
☐ ADD ENTRY TO EVENT LOG  
☐ SEND SYSLOG MESSAGE  
☒ SEND SNMP TRAP

Host/IP	192.168.8.100
SNMP Port	162
Community String	SWITCH
Specific Trap Code	1
Message ID	0
Message	[Hostname] %device %name %status %down (%message)
Agent IP	

☐ EXECUTE HTTP ACTION  
☐ EXECUTE PROGRAM

**Host/IP** – IP адрес или DNS имя компьютера, на который будут отправляться SNMP trap сообщения;

**SNMP Port** – номер UDP порта для trap сообщений. По умолчанию: 162;

**Community String** – значение Community при доступе к устройству по протоколу SNMP;

**Specific Trap Code** – целое значение, которое поможет идентифицировать trap. По умолчанию: 0;

**Message ID** – идентификатор, который позволяет определить оригинальный trap;

**Message** – информационное сообщение о состоянии датчика или устройства;

**Agent IP** – IP адрес агента. Оставить поле пустым для использования IP адреса собственного PRTG сервера

После того, как все параметры нового уведомления будут заполнены заполнения необходимо сохранить настройки нажатием кнопки «Save».

В результате этих действий новое уведомление появится в таблице «Notification»:

## NOTIFICATIONS

Show notifications tagged with	
1 to 4 of 4	
Object	Active/Paused
Email and push notification to admin	Active
Email to all members of group PRTG Users Group	Active
Notification_SMS_via_SNMP_trap	Active
Ticket Notification	Active
1 to 4 of 4	

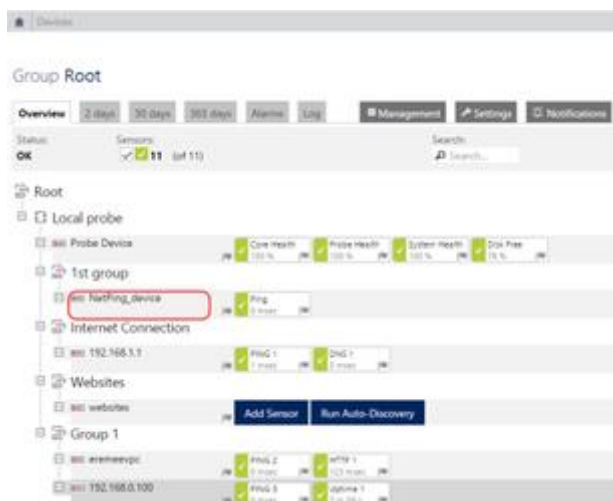
+ Add new notification

Для того, чтобы созданное SMS-уведомление работало, его нужно применить к необходимым сенсорам или устройствам в системе PRTG.

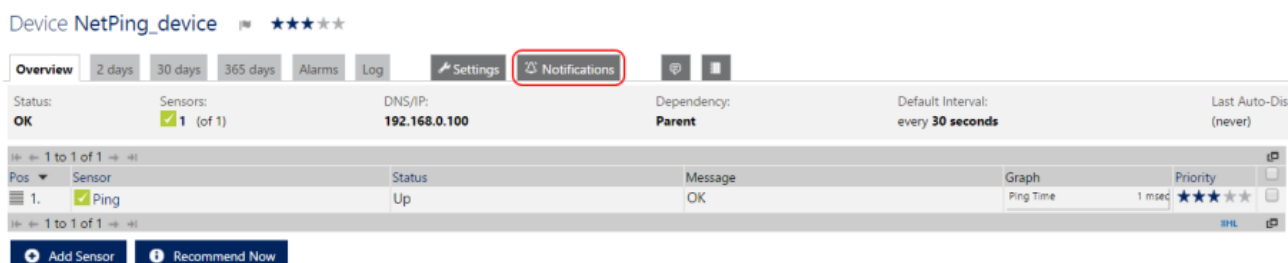
Ниже приведен пример использования SMS-уведомления, которое будет срабатывать при пропадании и появлении устройства в локальной сети. Для этого нужно выбрать необходимое устройство в PRTG, которое проверяется на доступность командой «Ping». Выбор производится на странице «Devices»:



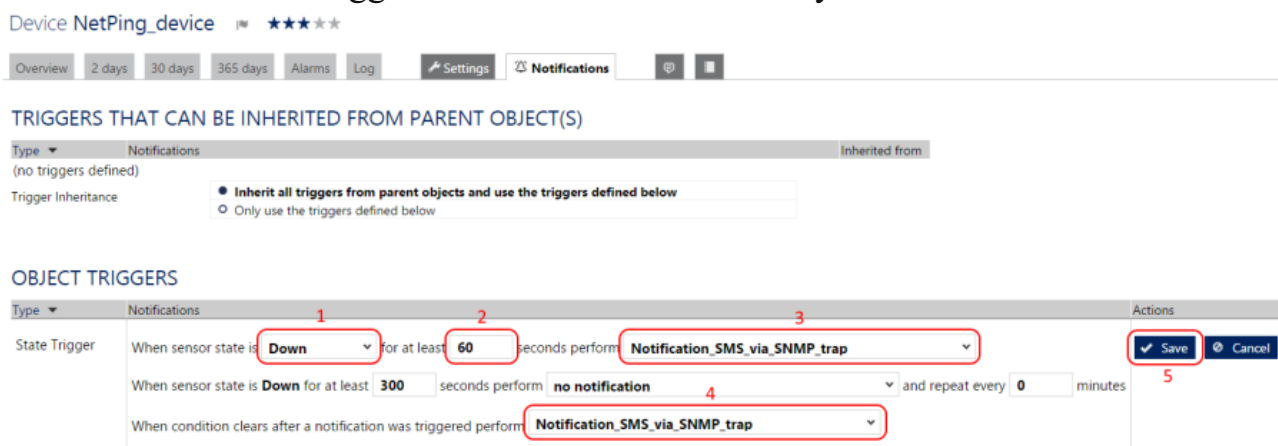
На странице «Devices» из списка устройств, настроенных на мониторинг, для примера выберем устройство «NetPing\_device». Выбор осуществляется нажатием курсора мыши по названию устройства:



Откроется страница «Device NetPing\_device», в которой перечислены все сенсоры данного устройства. Как видно из скриншота ниже устройство «NetPing\_device» настроено только на проверку доступности посредством команды «Ping». Для применения созданного уведомления «Notification\_SMS\_via\_SNMP\_trap» необходимо перейти на вкладку «Notifications»:



На вкладке «Notifications» настраивается реакция на изменение статуса сенсоров выбранного устройства. Для получения SMS-уведомления при изменении состояния сенсора «Ping» необходимо добавить триггер нажатием кнопки «Add State Trigger» и заполнить соответствующие поля:



где:

- 1 – условие при котором будет вызвано уведомление. В этом примере триггер будет активирован, когда сенсор находится в состоянии «Down»;
- 2 – интервал времени, через который сработает триггер. Этот интервал позволяет избежать ложных срабатываний;
- 3 – метод отправки уведомлений при срабатывании триггера;
- 4 – метод отправки уведомлений, когда условие перестает выполняться;
- 5 – сохранение параметров триггера

На этом настройка PRTG окончена.

На этом примере подробно разобрана настройка PRTG для конкретной задачи.

#### **4. Заключение**

В данной курсовой работе был рассмотрен основной функционал программы PRTG и некоторые примеры его применения. Также были разобраны основные режимы работы и интерфейсы этих режимов. Были изучены различные типы сенсоров и способы их применение. Произведено ознакомление с принципом работы программ анализа и контроля трафика различных сетей, способы использования и их предназначение.

#### **Список использованных информационных источников:**

1. Интернет-ресурс [URL]: <https://ru.wikipedia.org/wiki/PRTG> (Дата обращения: 07.05.2021).
2. Интернет-ресурс [URL]: <https://www.ru.paessler.com/prtg> (Дата обращения: 07.05.2021).
3. Интернет-ресурс [URL]: [https://www.paessler.com/manuals/prtg/available\\_sensor\\_types](https://www.paessler.com/manuals/prtg/available_sensor_types) (Дата обращения: 08.05.2021).
4. Интернет-ресурс [URL]: <https://habr.com/ru/post/154747/> (Дата обращения: 09.05.2021).
5. Интернет-ресурс [URL]: <https://networkguru.ru/8-luchshikh-programm-dlia-analiza-setevogo-trafika/> (Дата обращения: 07.05.2021).
6. Интернет-ресурс [URL]: <http://www.netping.ru/Blog/primer-nastrojki-prtg-network-monitor-i-netping-sms-dlya-otpravki-sms-vedomlenij-na-osnove-snmp-trap-soobshhenij/> (Дата обращения: 08.05.2021).