AutoMonX
The Monitoring Automation Company

AutoMonX Smart Notifications

Deployment guide

Web : https://www.automonx.com
Email : support@automonx.com

Date	Change	Author
06.12.2020	Initial Release	AutoMonX
10.02.2021	SmartNotif Reporter detailed install, Telegram updated	AutoMonX
03.09.2021	New CLI options, Sending messages in an offline / air-gapped environment	AutoMonX
24.04.2022	Syslog notifications	AutoMonX
01.05.2022	Custom SNMP Trap Port	AutoMonX
21.01.2023	New services, Air-gaped (offline) mode, Integration with InfluxDB, Installer, Configuration Wizard	AutoMonX
06.02.2023	Removal of Confidential Information (IP\Hostnames) from sent data.	AutoMonX
23.07.2023	Sending Datadog Events	AutoMonX
26.11.2023	Added Alert Title and Site to Datadog Events	AutoMonX
25.12.2023	Added NNMi incidents sending to Datadog	AutoMonX
24.08.2024	DataDog documentation	AutoMonX

Web : https://www.automonx.com
Email : support@automonx.com

AutoMonX
The Monitoring Automation Company

Contents

Web : https://www.automonx.com
Email : support@automonx.com

AutoMonX
The Monitoring Automation Company

1 Purpose

The purpose of this document is to provide a detailed explanation of the AutoMonX Smart Notifications (SmartNotif) engine and its integration options.

2 Important terms

Monitoring error	Monitoring errors are issues that don't necessary indicate an issue with a device or its components. Monitoring errors occur when the sensor can't poll a monitoring value from a device. Such errors do not mean that there is an issue with the devices' performance or functionality. Because monitoring errors do not indicate an issue with the device's health, they are re-routed to the MonitorOps rather than to the Network/System administrators
System or Network issue	Messages that are related to the health status of devices and their sensors that should be handled by the Network/System administrators (i.e. Device down, Threshold is too High etc)
MonitorOps	The personnel in charge of maintaining PRTG. In small organizations it can be the same person as System/Network administrator

3 AutoMonX Smart Notifications Overview

AutoMonX has developed Smart Notifications, a notification engine with smart filtering mechanism that is tightly integrated with tools such as PRTG and InfluxDB. The smart filtering mechanism provides reliable and focused monitoring notifications to the Network and Systems administrators by re-routing and filtering-out unnecessary notifications. The AutoMonX Smart Notifications also provides additional custom notification channels to 3rd party monitoring systems and dashboards as well as other notifications targets not available natively in PRTG and InfluxDB. The following notification channels are supported:

- **SMTP** - Simple emails (without graphs or links)
- Rich Notification emails with full PRTG functionality (after the smart filtering)
- **SNMP Traps** with custom rich variables and properties for Northbound integration to Enterprise Network monitoring systems
- **Telegram** application notifications
- **Syslog** Notifications
- **DataDog** – sending events to DataDog platform

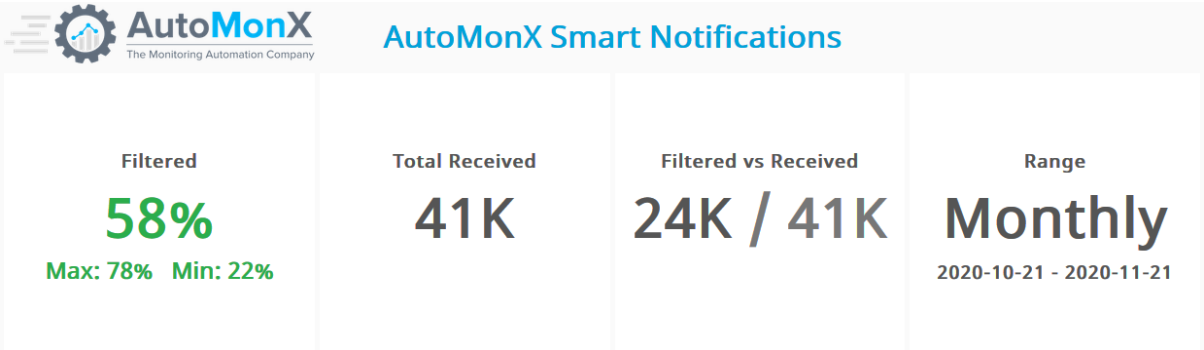
- **Custom exe**: Any additional external executables are supported

4 How Does It Work?

4.1 General

AutoMonX Smart Notifications is a software that replaces the native notification delivery channels of PRTG and InfluxDB. It is configured as an HTTP push notification in the PRTG Notifications Templates or the InfluxDB notifications.

Thanks to its smart filtering algorithm, Smart Notifications differentiates between monitoring errors to actual system or network issues and routes these issues to the relevant administrator (MonitorOps or Network/Systems Admin).



4.2 Compelling Reasons to Use Smart Notifications

Simplify PRTG alerts configuration: Smart Notifications allows to considerably simplify the configuration of notifications and primarily use Down notifications on the global PRTG level vs creating multiple settings in various locations of the PRTG device tree.

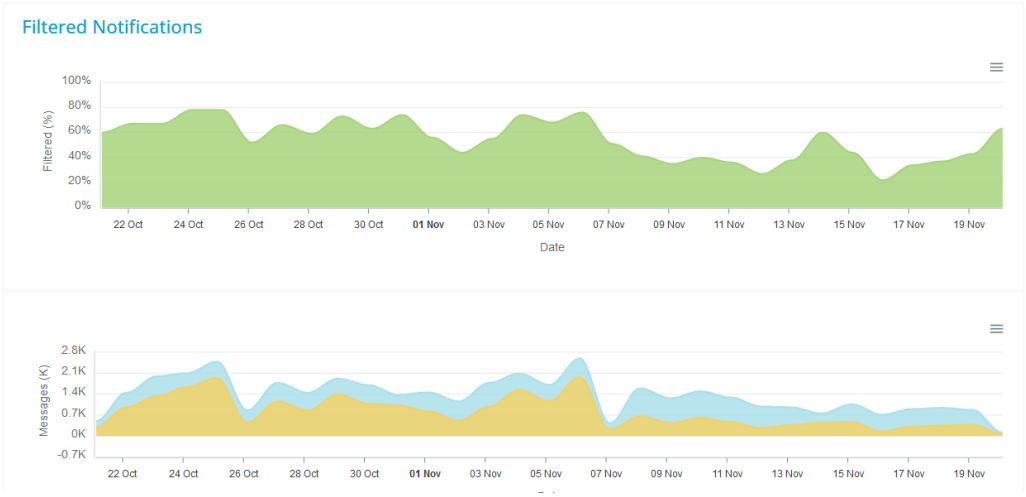
Extending InfluxDB notifications: Introduce many new notification options with seamless integration.

Reduce Noise: Smart Notifications reduces the monitoring notifications noise as it can be configured to route monitoring errors to PRTG administrators while only the relevant network and systems issues are routed to the right Network or Systems administrators. Notifications can be routed via email, SNMP traps, external programs or Telegram.

Correlation: Built-in correlation abilities allow to further reduce the noise during severe network outages and let Network and System teams to focus on real problems

Visibility: Smart Notifications is coupled with Smart Notifications Reporter that allows PRTG administrators to get insights on the flow of notifications, their top destinations and top devices that initiated the notifications.

Security: The off-line mode allows PRTG administrators securely deliver notifications from an air-gaped network to an open network without direct communications (based on secure file transfer / diode) while automatically removing or replacing sensitive information such as IP address and hostnames.



Notification trends can be analyzed in PRTG as Smart Notifications feeds back its statistics to a custom PRTG Sensor:

Web : https://www.automonx.com
Email : support@automonx.com

5 Getting Started with Smart Notifications

5.1 Supported Software versions

Smart Notifications has been tested to support the following software:

Software Type	Versions	Comments
Windows OS	2012R2, 2016, 2019	Standard and Enterprise editions
Virtual Infrastructure	VMWare Cloud or on-prem Azure VM	
PRTG Core and Probe deployments	19.x, 20.x,21.x,22.x	All On-Prem PRTG license types supported
PRTG Cloud	Supported	Requires allowing access from the PRTG Hosted solution to the Smart Notifications server
InfluxDB on-prem or Cloud	v8.x and higher	Requires allowing access from InfluxDB to the Smart Notifications server

5.2 Port requirements

The AutoMonX Smart Notifications requires the following ports to be open for it to function correctly. Please make sure that the local firewall / anti-virus and the external firewalls are configured correctly to allow the sensor pack to function correctly.

Port / URL	Purpose	Direction
SMTP (TCP 25) – Outbound	Sending Email alerts	From PRTG Core to the SMTP server (i.e. Exchange)
https://api.telegram.org Outbound (TCP 443)	Connect to Telegram API	From PRTG Core to Telegram API
SNMP (UDP 162) Outbound	For sending SNMP traps	From PRTG Core to the Northbound IP address of the Enterprise Network Manager

SYSLOG (UDP 514) Outbound	For Sending Syslog Messages	From the PRTG Core server to the destination Syslog Server
Smart Notifications Listener (UDP 8091) - Inbound	Receiving HTTP post notifications from PRTG	From PRTG Core Server to Smart Notifications Server

5.3 Anti-Virus requirements

Smart Notifications initiates many processes during its normal execution. Configure your anti-virus and/or anti-malware software to exclude the Directory where you plan to install Smart Notifications from on-access scanning. This would greatly improve the general performance of AutoMonX Smart Notifications.

5.4 Downloading Smart Notifications

Obtain the installer file by downloading it from the AutoMonX web site at http://www.automonx.com/downloads

Download the NetSNMP binaries from https://sourceforge.net/projects/net-snmp/files/net-snmp%20binaries/ These are required only for SNMP Traps support.

5.5 Requesting a License for Smart Notifications

The initial license file used by Smart Notifications, part of the downloaded zip file, is empty and functions as a place holder. You must activate the sensor by obtaining a license.

To successfully activate the AutoMonX Smart Notifications, you must contact AutoMonX Ltd either by filling the license request form at http://www.automonx.com/smartnotif

Or by sending an email to sales@automonx.com and provide the following information:

- Your first and last name
- Your contact details (corporate email, phone)
- Your business addresses
- The hostname of the machine where you plan to deploy
- The IP address of the machine where you plan to deploy

Important: The hostname is case sensitive. Please use the LicDetailsLocator.exe utility to obtain the hostname and IP address

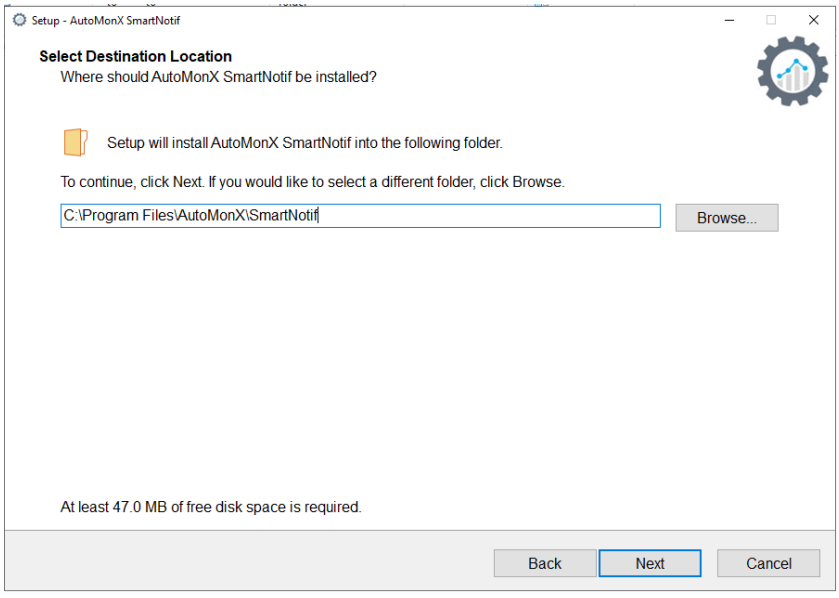
AutoMonX would provide you with a fully functional software evaluation license valid for 30 days. After the end of the evaluation period, you would be required to purchase a perpetual license.

5.6 Activating the Smart Notifications License

You activate Smart Notifications by editing the AutoMonXSmartNotifLicense.dat file via Notepad, pasting the license string you have received via email and saving the file.

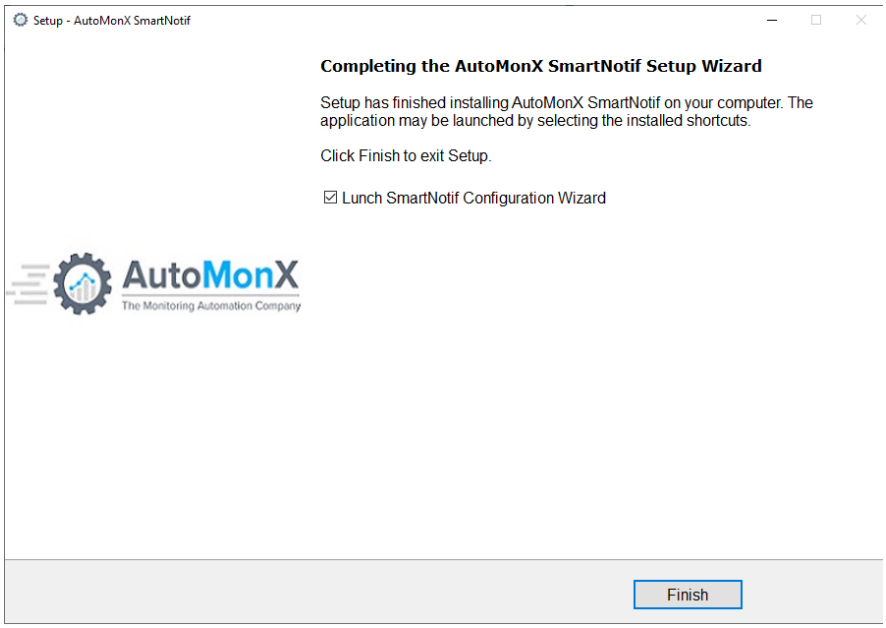
5.7 Installing Smart Notifications

Launch the Smart Notifications Installer as Administrator and you will be greeted with a Welcome screen, Click "Next". On the next page you would need to choose where to install Smart Notifications to, please choose the Install Directory for the Smart Notifications Application and click "Next".
Note that the default install location is: "C:\Program Files\AutoMonX\SmartNotif"



On The following page click on "Install" and the Application would install.

On the last screen of the Installer click on "Finish" and the Configuration Wizard would be launched automatically



Note: You may untick the option to "Lunch Smart Notifications Configuration Wizard" and do so later, however keep in mind that running the Configuration Wizard is mandatory for Smart Notifications to function.

The location of the Configuration Wizard is:

<SmartNotifRootDir>\Backend\ AutoMonX_Configuration_Wizard.exe

Where SmartNotifRootDir is the Install Directory you have chosen during the installation.

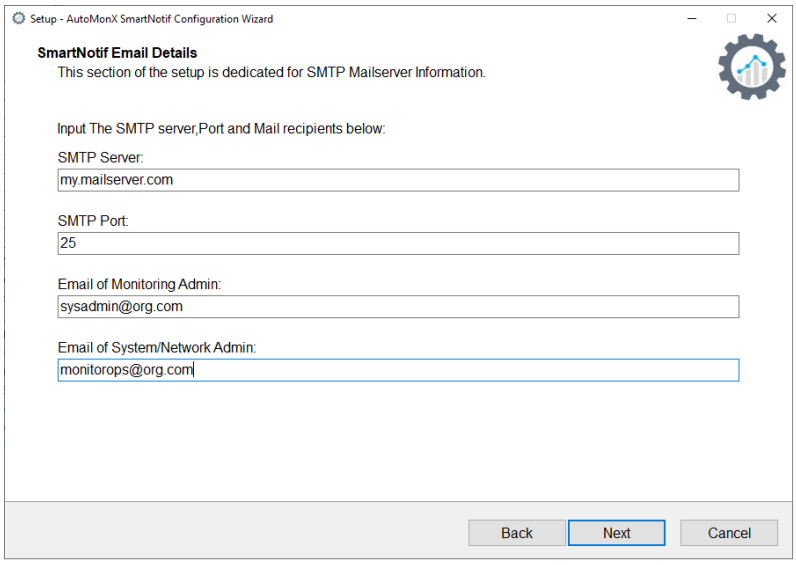
5.8 The Smart Notifications Configuration Wizard

After completing the installation, a Configuration Wizard would be automatically launched. Click Next in the welcome screen.

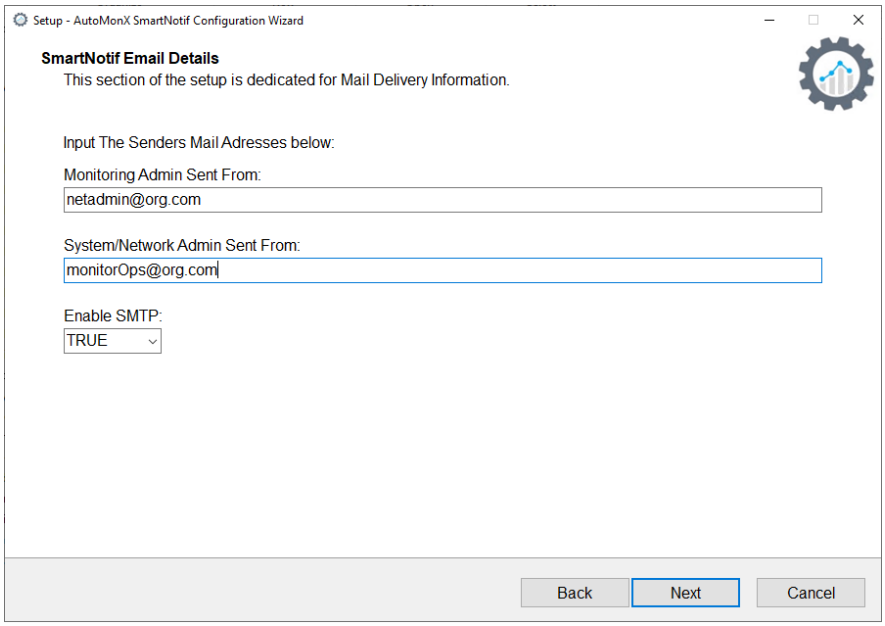
Important: You must configure at least one delivery method (SMTP, Syslog or SNMP) for the Smart Notifications to function

The next two screens allow you to configure the SMTP Settings:

- Under "SMTP Server" type you're SMTP Server (For Example my.mailserver.com)
- Under "SMTP Port" type you're SMTP Port (For Example 25)
- Under "Email of Monitoring Admin" provide the email recipient for System administrators (for example sysadmin@org.com)
- Under "Email of Monitoring\Network Admin" provide the email recipient for MonitorOps (monitoring errors) to be sent (for example monitorops@org.com)
- Click Next



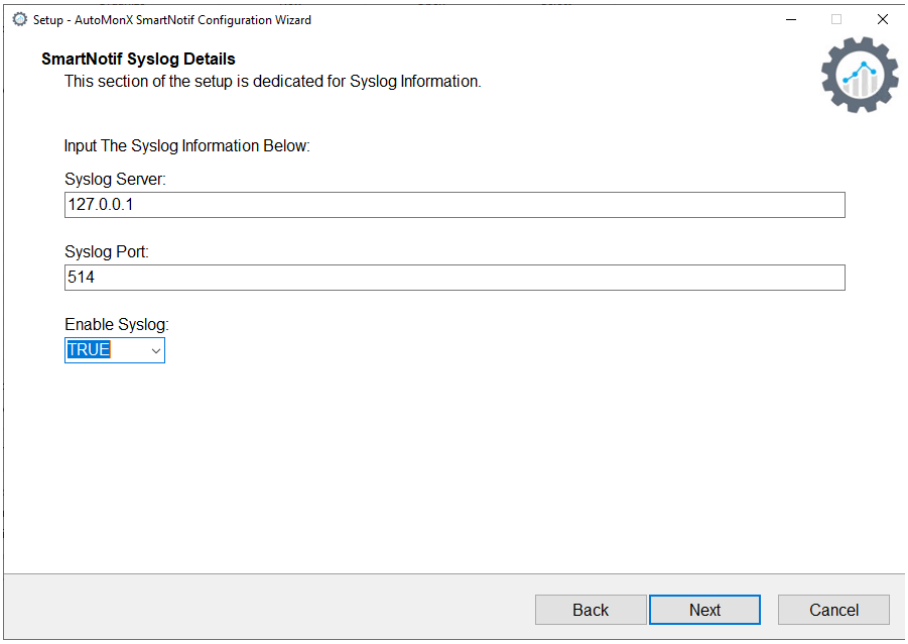
- Under " Monitoring Admin Sent From" type the from email for Network/System issues (for example netadmin@org.com)
- Under "System/Network Admin Sent From" type the from email for MonitorOps issues (for example monitorOps@org.com)
- On the Enable SMTP Drop Down Menu choose True or False for Enabling or Disabling SMTP functionality for Smart Notifications.



On the next screen you would need to configure Syslog Settings:

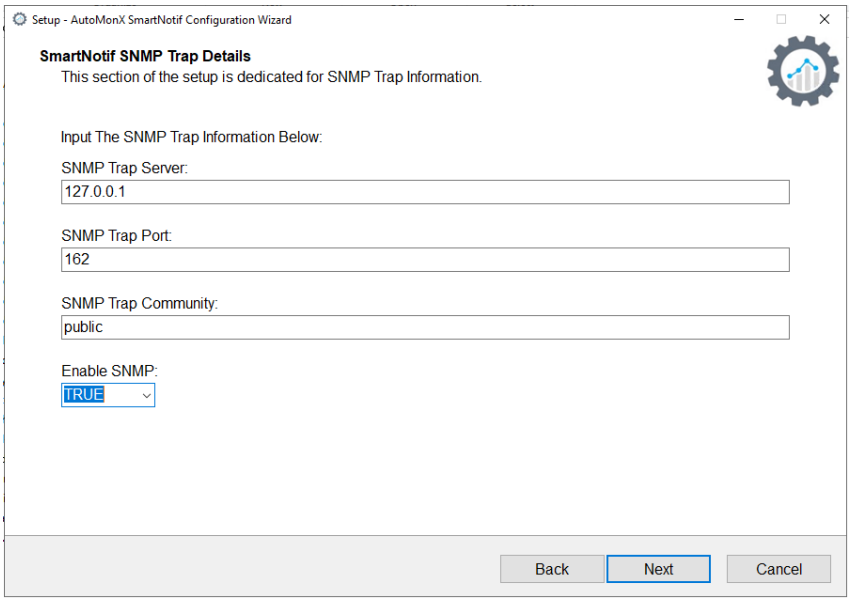
- Under Syslog Server type the IP Address of the Syslog Server (For Example 127.0.0.1)

- Under Syslog Port type the UDP Port of the Syslog server (For Example Port 514)
- On the Enable Syslog Drop Down Menu choose True or False for Enabling or Disabling Syslog functionality for Smart Notifications.



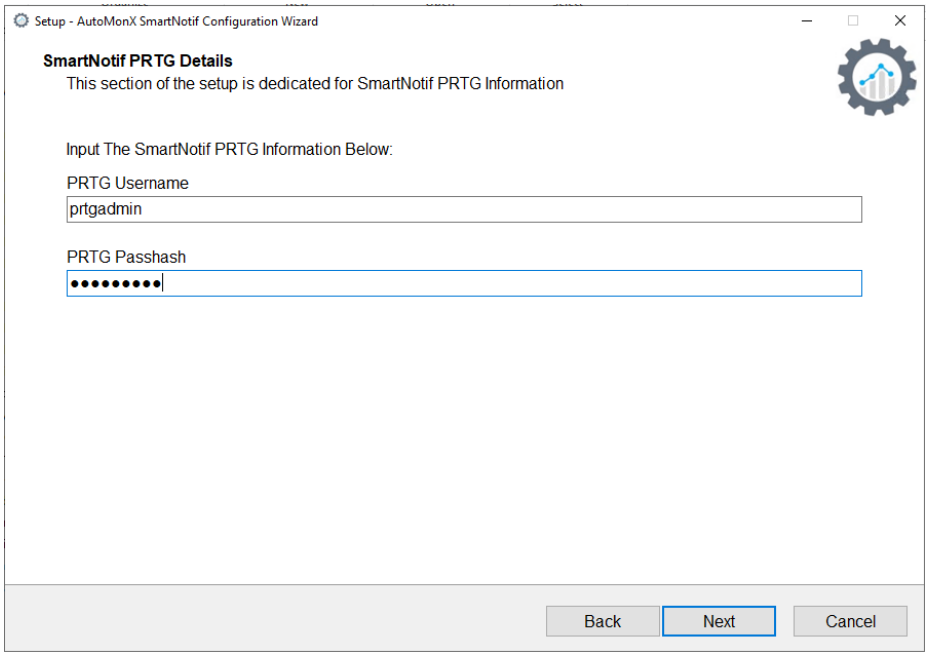
On the following screen you would need to configure SNMP Settings:

- Under SNMP Server type the IP Address of the NMS System SNMP Trap listener (For Example 127.0.0.1)
- Under SNMP Port type the Port of the SNMP server (For Example Port 162)
- On the Enable SNMP Drop Down Menu choose True or False for Enabling or Disabling the SNMP Traps functionality of Smart Notifications.

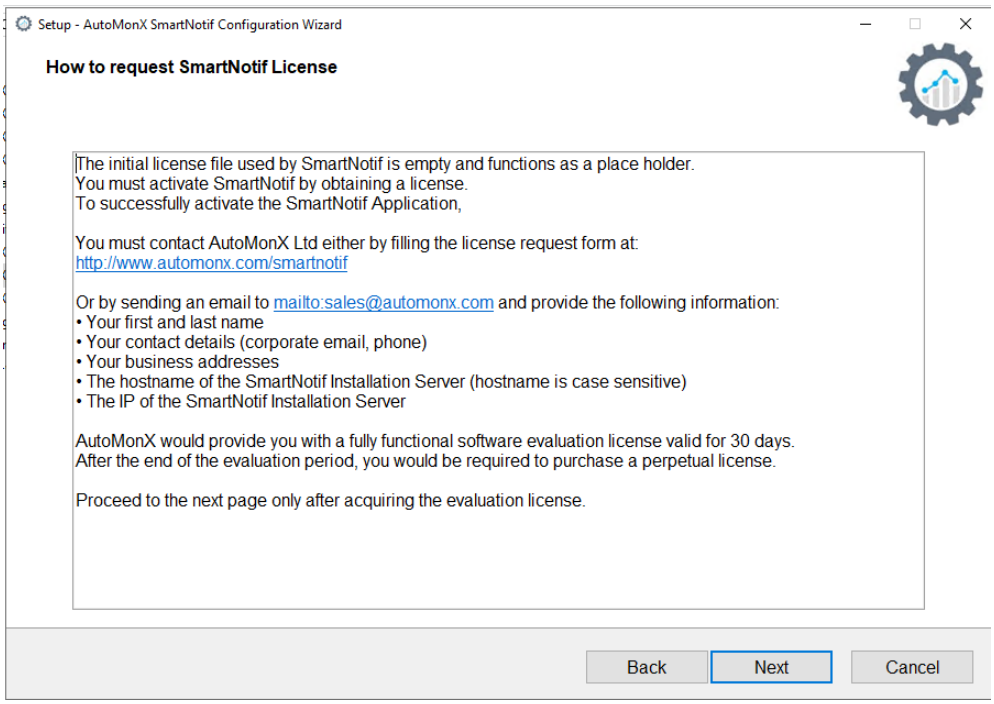


On the next screen you would need to configure PRTG Settings:

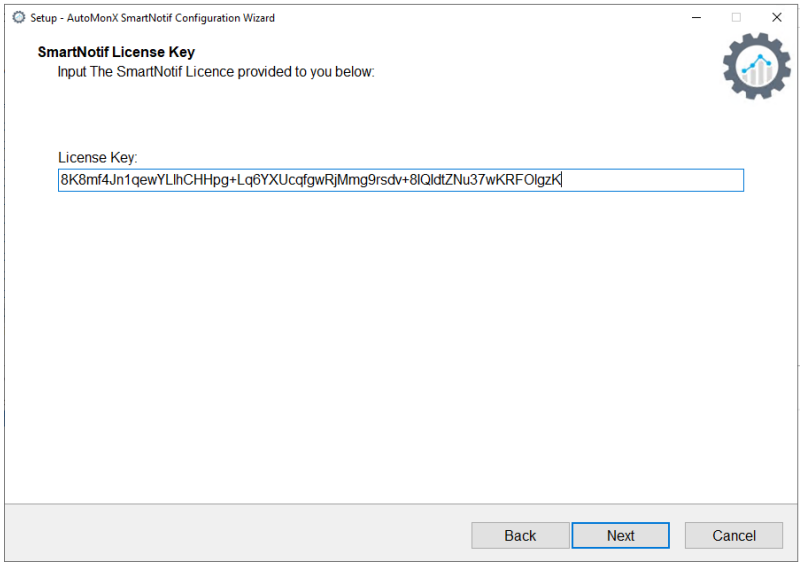
- Under PRTG Username type the preferred PRTG User (for example prtgadmin)
- Under PRTG Passhash type the PRTG User Passhash



Read through the evaluation license request procedure and request the license accordingly.

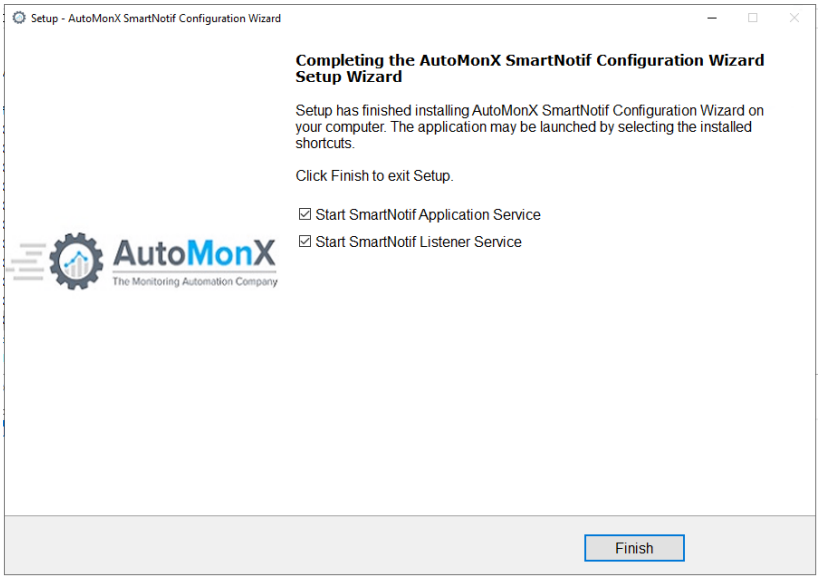


After you have obtained the License Key, click "Next" and paste the key in the "License Key" text box as seen in the picture B:



- Click on "Next" and then on "Install".
- The Wizards' last screen has the Smart Notifications Services marked to start automatically, therefore the Smart Notifications application would start to function right after you would click the Finish button.

- SmartNotif Application – Starts the Smart Notifications Application which processes and sends notifications
- SmartNotif Listener – Starts an HTTP Webserver at Port 8091 (default)

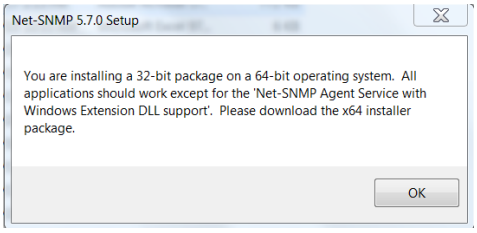


Now the AutoMonX Smart Notifications is configured and ready to use

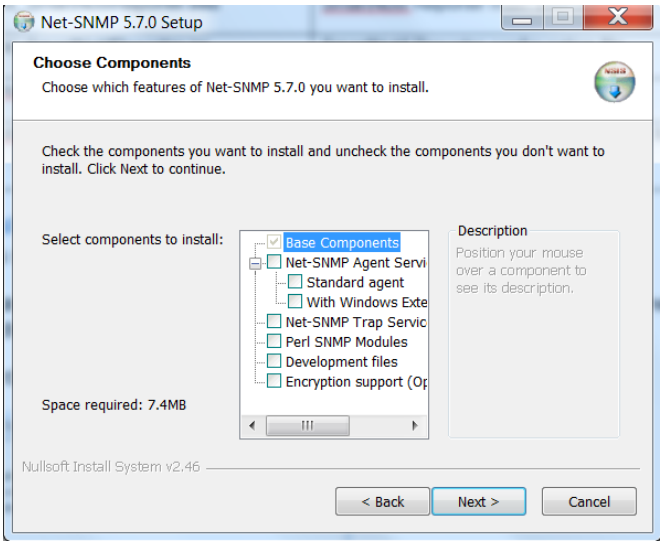
5.9 Installing Net-SNMP

Skip this section if you don't plan to use the SNMP Traps functionality.

1. Run as administrator the installer of Net-SNMP (a file typically named like net-snmp-5.7.0-1.x86.exe).
2. Disregard the popup about Windows 32bit version incompatibility



3. Choose to install only the base components of Net-SNMP



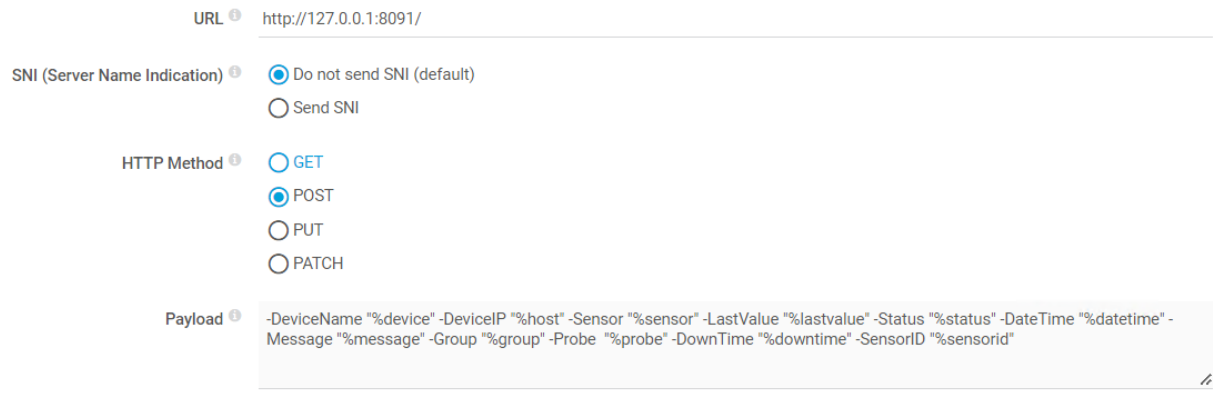
5.10 Configuring PRTG to Send Notifications via Smart Notifications

After installing Smart Notifications, you need to define in PRTG a "Notification Template" which sends all notifications to the SmartNotif Listener Service, this is done the following way:

With an administrative user in PRTG do the following:

1. Go into "Setup" on the top gray bar in PRTG.
2. Go to "Notification Templates" under "Account Settings".
3. Locate the white plus icon on the left side of the screen and click on "Add Notification Template".
4. Scroll down and click "Execute HTTP Action".
5. Under "URL" type " http://127.0.0.1:8091/"
6. Under "HTTP Method" type choose "POST" option
7. Inside the Payload Text Box paste the following:
   -DeviceName "%device" -DeviceIP "%host" -Sensor "%sensor" -LastValue "%lastvalue" -Status "%status" -DateTime "%datetime" -Message "%message" -Group "%group" -Probe "%probe" -DownTime "%downtime" -SensorID "%sensorid"

Below is an example of the PRTG notification configuration:

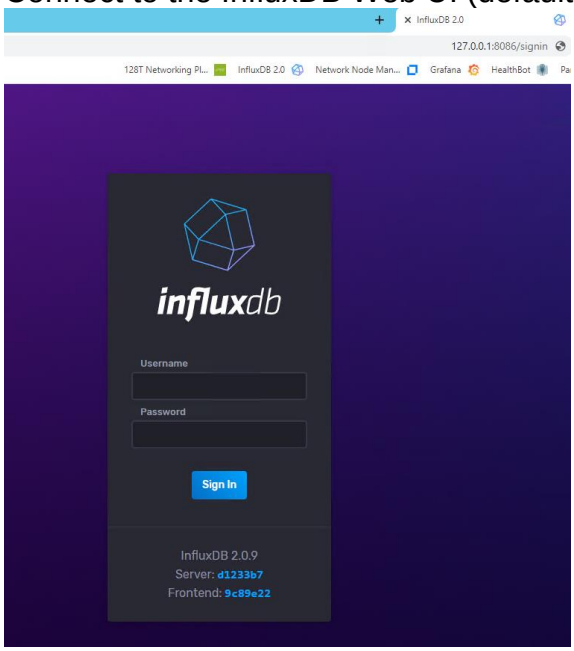


5.11 Configuring InfluxDB to Send Notifications via Smart Notifications

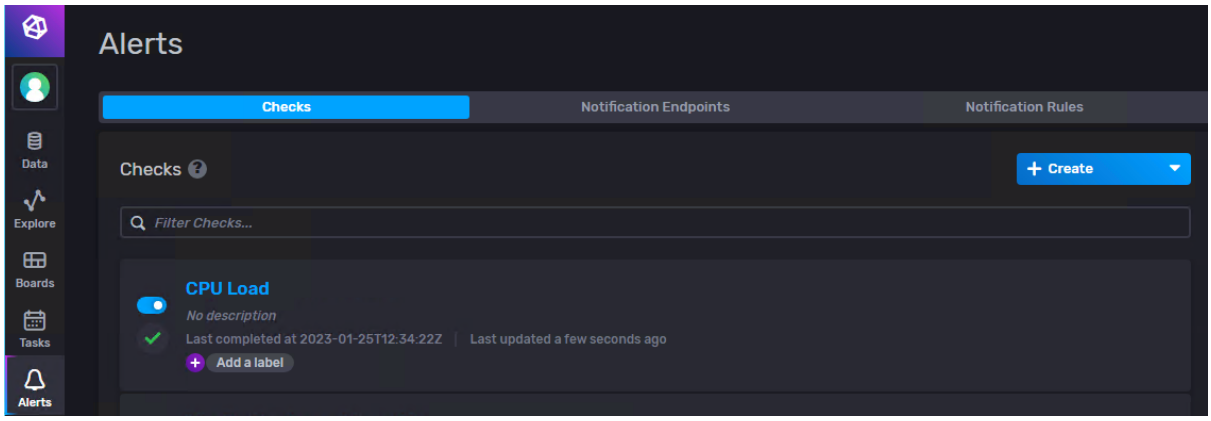
In order to send notifications from InfluxDB via Smart Notifications you need to define the following settings in the InfluxDB Alerts Configuration. For a more detailed explanation on how to configure notifications, please refer to the official documentation of InfluxDB

- Create a Check
- Define a Notification Endpoint
- Create a Notification Rule

Connect to the InfluxDB Web UI (default port 8086)

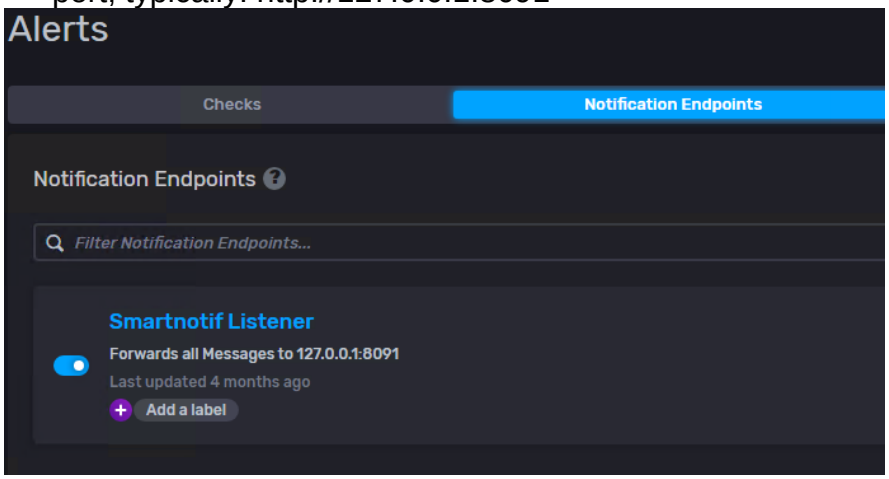


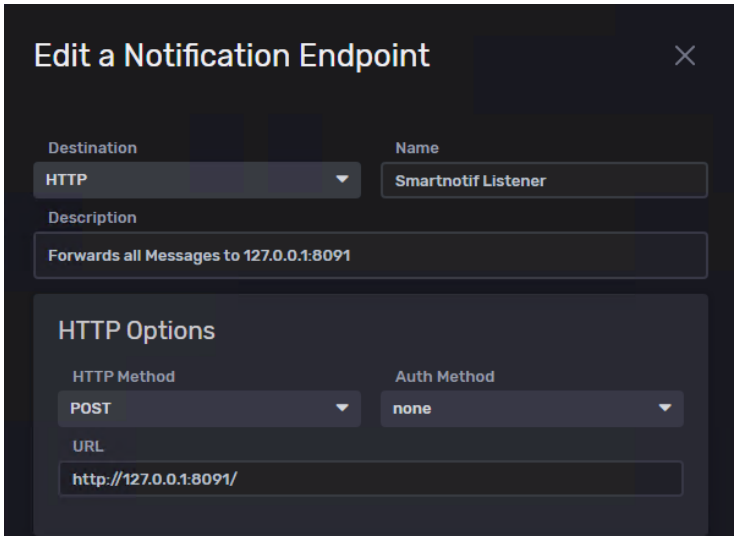
Create a new Check



Create a new Notification Endpoint:

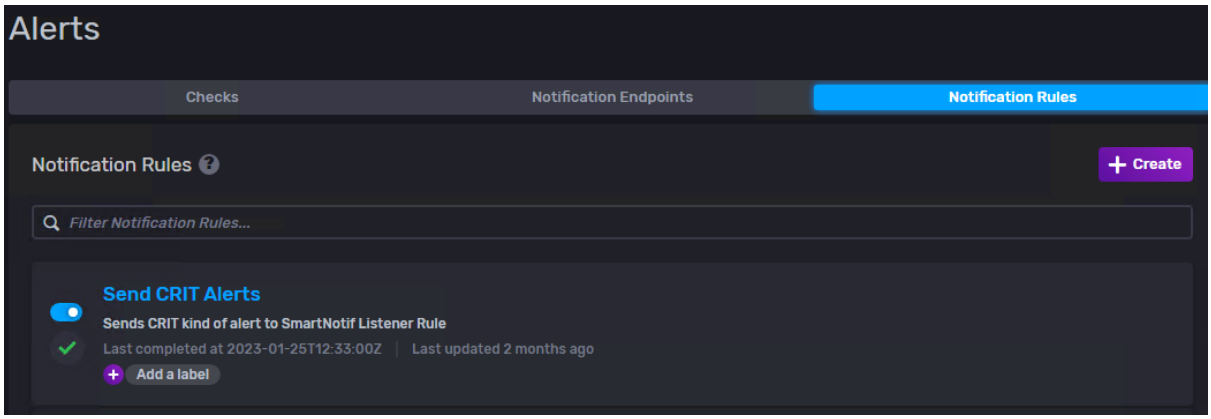
1. Use an HTTP POST to URL where the Smart Notifications is installed and its port, typically: http://127.0.0.1:8091





Web : https://www.automonx.com
Email : support@automonx.com

Create a Notification Rule

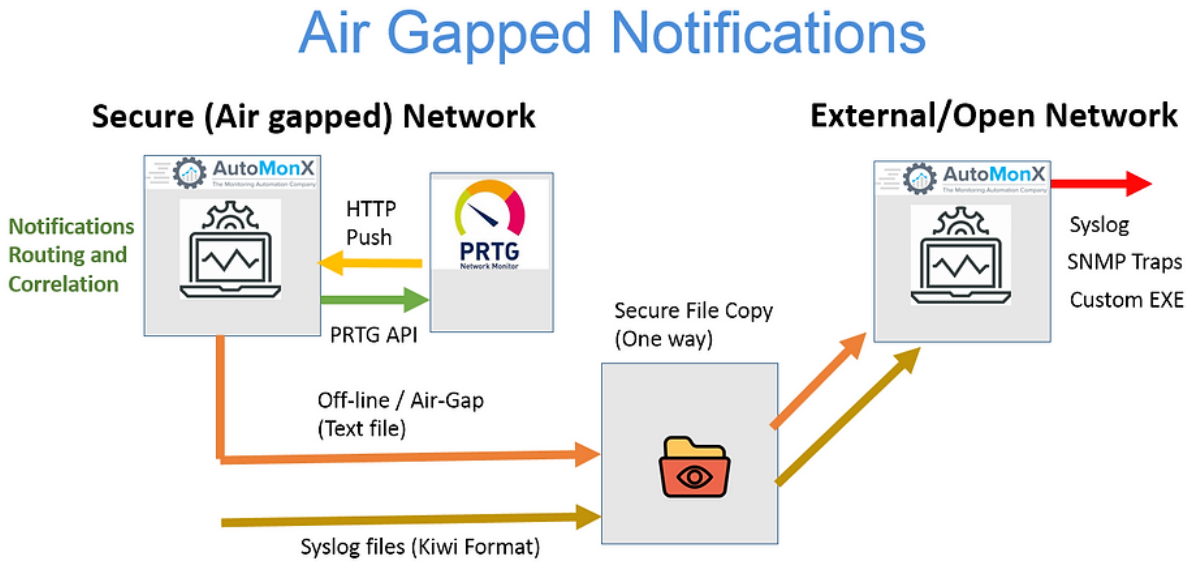


Web : https://www.automonx.com
Email : support@automonx.com

5.12 Sending Notifications from Air-Gaped networks

When you are in charge of managing highly secure networks, such as OT devices networks, financial or government IT assets, you still need ways to monitor them and also notify if availability or performance issues occur. It is also highly important to know if a security incident is happening in such networks.

These highly secure networks are disconnected from the Internet and from any other open network. In many cases these networks are built as"air gaped". It means that there is no physical or wireless network connection from the highly secure network to any other network and vice versa.



Our Smart Notifications solution, originally built for filtering, correlating and sending only relevant notifications in many ways (such as Email, Syslog, SNMP traps etc) can be also used to send notifications over Air-Gaped networks.

Due to the demand of our customers, we have developed an **offline mode** that collects notifications as text files on the air-gaped network side and capable of "replaying" those alerts when these files are copied to an open/less secure network side and send them to multiple different destinations such as SOC management tools (Splunk, Elastic, ArcSight) and/or central monitoring solutions thus reducing the need to deploy stand-alone monitoring and security solutions inside the air gaped networks.

Smart Notifications is a software-based solution, much more cost effective and flexible in
terms of deployment. You would need a secure file copying solution between the air-gaped and the open network. Smart Notifications is neutral in terms of which tool is in use as
long as the notification files are copied to a shared folder from where it can read it. For example, tools like Claroty Platform, Waterfall and many others can be used in conjunction with Smart Notifications.

Offline file sending flow:

1. PRTG\InfluxDB Alerts or any HTTP POST Message capable service sends HTTP POST Message to the host.
2. AutoMonX SmartNotif Listener picks up the message.
3. AutoMonX SmartNotif Listener parses the message.
4. Then the message is written to \SmartNotif\Backend\Logs\ HTTPPayloadData_[datestamp] where [datestamp] is in the form of DDMMYYYY.
5. AutoMonX Smart Notifications Application picks up the HTTPPayloadData and sends all the alerts data line by line to the desired protocols and destinations, with monitoring of the last sent line inside \SmartNotif\Backend\metadata.dat (do not edit this file).

Keeping the information secure - Sanitation of Data

Before notifications are stored in an offline file, there is an optional sanitation of sensitive data. Smart Notifications can automatically remove anything that looks like an IP
address and automatically replace any text string to some other text of your choice. Below is a snippet of the Smart Notifications configuration file where all IP addresses are
removed from the text, and any of the words "OT", "firewall", "topsecret" or "scada" are automatically replaced by the word "internal".

```
SECRET_INFO_REPLACE=TRUE
SECRET_INFO_PATTERNS=OT,firewall,topsecret,scada
SECRET_INFO_REPLACE_STRING=internal
SECRET_INFO_REMOVE_IP=TRUE
```

5.13 Smart Notifications Files

During the installation process, all the required files are copied to their correct locations. Below is an explanation regarding the various files and their usage.

The default installation path is: C:\Program Files\AutoMonX\SmartNotif\

Backend folder

Filename	Purpose
Automonx_SmartNotif.exe	Smart Notifications main executable
AutoMonX_SmartNotif.ini	Smart Notifications configuration file
LicDetailsLocator.exe	License details locator utility
AutoMonXSmartNotifLicense.dat	Smart Notifications license file
AutoMonX_ReqFetch.dll libcrypto-1_1-x64.dll libssl-1_1-x64.dll zlib1.dll	Smart Notifications sensor DLL files
Logs Directory	Smart Notifications Logs folder
Log_Archive Directory	Contains Archived Logs That Smart Notifications Sent
AutoMonX_Configuration_Wizard.exe	Smart Notifications Configuration Wizard
AutoMonX_SmartNotif_Application.exe	Smart Notifications Application Service Executable
AutoMonX_SmartNotif_Listener.exe	Smart Notifications Listener Service Executable
iniEditor.exe	Edits the SmartNotif INI Configuration file (Used in Configuration Wizard)
metadata.dat	Contains last read line of a given log, do not modify this file.
AutoMonX_outage.csv	**Optional**: A file that controls the outage mechanism settings. Use this file to specify the schedules in which notifications will not be sent for specific devices
AutoMonX_corr_errors_snmp_data.dat	Saves data of error messages related to SNMP monitoring errors. Used to filter and correlate such messages to reduce message storms

AutoMonX_corr_errors_wmi_data.dat	Saves data of error messages related to WMI monitoring errors. Used to filter and correlate such messages to reduce message storms
AutoMonX_ExpiredNotif.dat	This file is used to inform the Smart Notifications program when was the last time a license expired notification was sent
AutoMonX_SmartNotif_correlation.dat	Used to store error messages sent by Smart Notifications to facilitate the internal cleanup process

Backend\Logs

Filename	Purpose
AutoMonX_SmartNotif.log	General Application log
AutoMonX_SmartNotifErrors.log	Error Log
HTTPinflux.txt	This log contains Alerts sent by InfluxDB
HTTPPayloadData.txt	This log contains Alerts sent by PRTG
kiwilog.log	This log contains Alerts sent by Kiwi Log Server by Solarwinds

Smart Notifications Reporter Files – PRTG Integration

<Drive>:\Program Files (x86)\PRTG Network Monitor\CustomSensors\EXEXML\AutoMonX\SmartNotifReporter

Filename	Purpose
Automonx_SmartNotifReporter.exe	Smart Notifications Reporter main executable
Automonx_SmartNotifReporter.ini	Smart Notifications Reporter configuration file
Report.tmpl	Smart Notifications Reporter HTML Template
SmartNotifUI_Template	SmartNotif Reporter Template files (css, fonts, images and js files)

5.14 Smart Notifications Windows Services

The Smart Notifications Application consists of two Windows services:

5.15 *AutoMonX Smart Notif Listener Service*

This service is responsible for receiving notifications from InfluxDB or PRTG using the following flow:

- Listening to incoming notifications sent from PRTG or InfluxDB via the HTTP protocol via TCP port 8091.
- When a message is received via HTTP, the message is being processed and written to the appropriate log files:
  - SmartNotif\Backend\Logs\HTTPPayloadData.txt for PRTG.
  - SmartNotif\Backend\Logs\HTTPInflux.txt for InfluxDB.

  Each message is stamped with a local machine timestamp and the appropriate parsed message.

  The operational log of the AutoMonX SmartNotif Listener is available at: SmartNotif\Backend\Logs\ListenerService.log

5.16 AutoMonX SmartNotif Application Service

This service is responsible for sending the notifications that the Listener service has processed via the configured protocols and recipients. AutoMonX SmartNotif Application Service launches the AutoMonX_SmartNotif.exe process and ensures that the application works as intended.

Logging of the AutoMonX SmartNotif Application Operation is available at: SmartNotif\Backend\Logs\ ApplicationService.log

6 Smart Notifications Configuration

6.1 Manual Configuration of Smart Notifications

The AutoMonX Smart Notification requires certain information that must be configured in AutoMonX_SmartNotif.ini file to properly function. It is strongly suggested to use the Configuration Wizard to configure Smart Notifications.

6.2 Minimal Configuration - Email

These are the minimal settings you need to modify for Smart Notifications to function:

Variable Name	Default Value	Description
SMTP_SERVER	**exchangeserver1**	The mail server name or IP used for all SMTP communications
NET_ADMIN_MSGS_MAIL_TO	**sysgroup@domain.co**	Provides the email recipient list for System or Network administrators (Network/System issues).
NET_ADMIN_MSGS_MAIL_FROM	**prtgerrors@mydomain.co**	Configures the From email for Network/System issues (Network/System issues) emails.
Optional – for routing monitoring errors messages to MonitorOps		
MONITOR_OPS_MSGS_MAIL_TO	**MonOps@domain.com**	Provides the email recipient list for MonitorOps (monitoring errors) to be sent.
MONITOR_OPS_MSGS_MAIL_FROM	**prtgerrors@domain.co**	Configures the From email for MonitorOps (monitoring errors) emails. Can be the same value as **NET_ADMIN_MSGS_MAIL_FROM**

6.3 Configuring Smart Notifications Reporter

The AutoMonX Smart Notifications Reporter requires certain information that must be configured in AutoMonX_SmartNotifReporter.ini file to properly function. The default settings should be enough, unless you have modified the name and the location of the Smart Notifications messages log file

Variable Name	Default Value	Description

LOG_PATH	C:\Program Files (x86)\PRTG Network Monitor\Notifications\EXE\	The location of the SmartNotif log file
LOG_NAME	AutoMonX_SmartNotif.log	The name of the Smart Notifications Log file.

6.4 Smart Notifications Configuration - Telegram

These are the minimal settings you need to modify for Smart Notifications to route messages via Telegram.

1. Generate Telegram Token and Group IDs as explained in Appendix A
2. Modify the SmartNotif.INI for Telegram communications
3. Change the notification template settings in PRTG with the Telegram routing options and specify the Group ID(s) for sending messages

Variable	Required Value	Comment
TELEGRAM_NOTIF_ENABLED	**FALSE**	Enable Telegram functionality by setting this variable to TRUE
TELEGRAM_NOTIF_MAX_MSG_LENGTH	**180**	Specifies the maximum size of the message that would be sent through Telegram.
TELEGRAM_TOKEN_ID	**Empty**	Specifies the token ID to for connecting to Telegram.

6.5 Smart Notifications – Routing notifications via Telegram

You must add one of the following options to the Notifications template parameters setting in PRTG for routing messages via Telegram. Both options can be used together or separately. See section 7 for instructions.

- telegram_recip	Sends the Network/System issues using Telegram to system / network administrator. Use a semicolon to specify multiple Group IDs
-telegram_nms_recip	Sends the monitoring errors using Telegram to MonitorOps. Use a semicolon to specify multiple Group IDs

For example, when AutoMonX_SmartNotif.exe is configured with the following Telegram routing options:

- telegram_recip 11345

-telegram_nms_recip 244423

This setting will route the notifications via Telegram as follows:

- For Network/System issues messages to Telegram group ID: 11345
- For MonitoringOps messages, to Telegram group ID: 244423

6.6 Minimal Configuration – SNMP Traps

These are the minimal settings you need to modify for Smart Notifications to send SNMP Traps. You need to make sure that the following variables are set correctly for the SNMP Traps functionality to function:

1. Enable sending of SNMP Traps (SNMP_ENABLED=TRUE)
2. Install Net-SNMP as explained in Installing Net-SNMP and specify its path in SNMP_TRAP_PATH
3. Specify the SNMP Traps destination IP Address (SNMP_TRAPS_SERVER)

Variable Name	Default Value	Description
SNMP_TRAPS_SERVER	127.0.0.1	Destination of the SNMP traps of Network/System issues.
SNMP_TRAP_PATH	Empty	The path to the location of the Net-SNMP snmptrap.exe command. Typically, it would look like c:\snmp\bin\snmptrap.exe
SNMP_ENABLED	TRUE	Activates SNMP traps. Any value other than TRUE deactivates this functionality.
Optional		
SNMP_COMMUNITY	Public	The SNMP community that would be used to send SNMP traps.
SNMP_SEND_MONITOR_OPS_NOTIF	FALSE	Activates sending MonitorOps messages as SNMP traps. Once activated, all message types (Network/System issues and Monitor errors) will be sent as SNMP traps.

6.7 Minimal Configuration – Syslog Messages

These are the minimal settings you need to configure for Smart Notifications to send Syslog messages. You need to make sure that the following variables are set correctly for the Syslog messages functionality to function properly:

Variable Name	Default Value	Description
SYSLOG_ENABLED	TRUE	Any value other than TRUE (case sensitive) would result in Syslog Messages being disabled.
SYSLOG_HOST	Empty	The Server that would receive the Syslog Messages. **Make sure** to use an IP address as the SYSLOG_HOST and not the DNS Name.

6.8 Configuring the Smart Notifications Windows Services

- The AutoMonX SmartNotif Application service does not require any configuration, it just needs to run since the service purpose is to execute the"AutoMonX_SmartNotif.exe" file. All configurations of "AutoMonX_SmartNotif.exe" are configurable via the INI File as explained in this section.
- The AutoMonX SmartNotif Listener has a configurable listener Port, the default port is 8091 and it configurable via the \SmartNotif\Backend\AutoMonX_SmartNotif.ini in the field " LISTENER_PORT", Note that the protocol would always be TCP.

7 Smart Notifications - DataDog Integration

Smart Notifications allows you to send events from various monitoring platforms such as PRTG to DataDog.

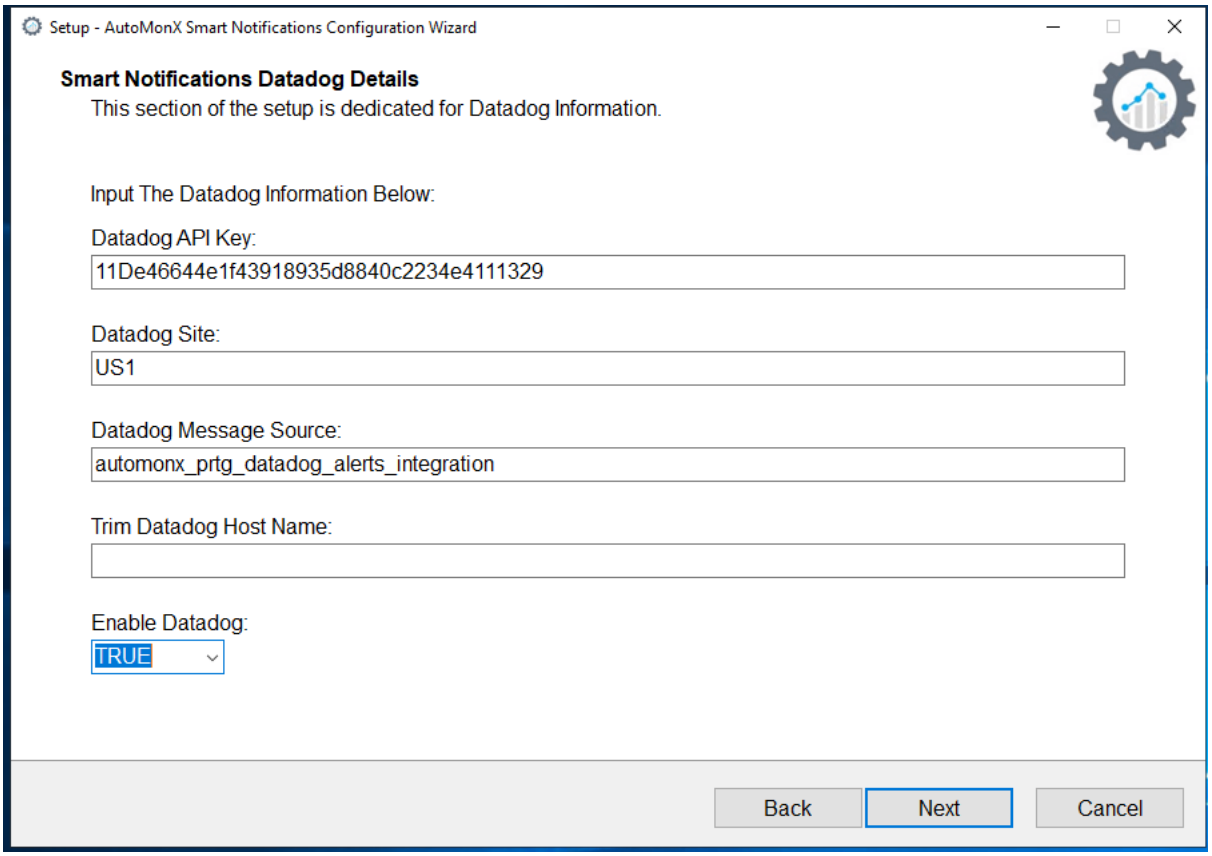
7.1 Configuring the connection to DataDog

You must obtain the details of your DataDog tenant to make sure the connection to DataDog is successful.

- Use your browser to connect to your DataDog tenant
- Find out your DataDog Site Location: https://docs.datadoghq.com/getting_started/site/
- Browse to the API keys section: https://app.<your datadog URL>/organization-settings/api-keys.
  Generate a new API Key and copy it for the next step

Run the Smart Notifications Configuration Wizard as administrator to enable sending of events to DataDog platform, and make sure that the following fields are defined correctly. It is located under the following path:

{drive}:\Program Files\SmartNotif\Backend\AutoMonX_SmartNotif_Configuration_Wizard.exe



Below is the description of each field as appears in the SmartNotif.ini file:

Variable Name	Default Value	Description
DATADOG_ENABLED	FALSE	Any value other than TRUE (case sensitive) would result in Datadog Events sending being disabled.
DATADOG_SITE	EU	This is the site of the of your Datadog Instance. If blank the default is EU. Check your site location at: https://docs.datadoghq.com/getting_started/site/
DATADOG_API_KEY	Empty	You would need to provide the Datadog API Key of your instance.
DATADOG_MESSAGE_SOURCE	PRTG	This field is the source of the Datadog Event. Customize this field to change the event source.
TRIM_HOST_NAME	Empty	This field is able to trim the Device Name constants. For Example if: TRIM_HOST_NAME = my.company.com Then these servers: server1.my.company.com server2.my.company.com Would appear on Datadog events like that: server1 server2

After these sections are correctly set, Smart Notifications would be able to send the logs as DataDog Events.

7.2 Configuring the Integration of PRTG alerts into DataDog

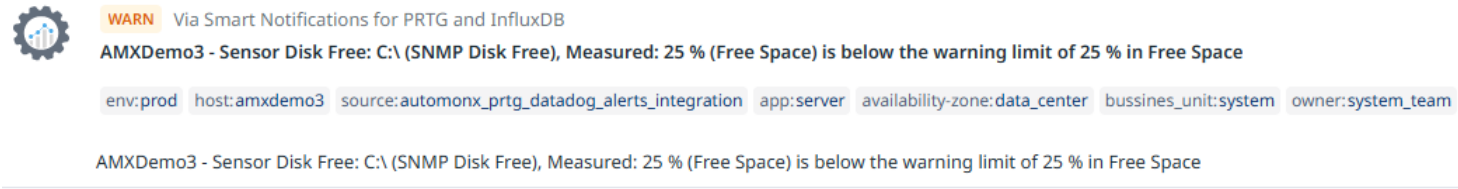
With Smart Notifications you can send PRTG alerts to DataDog and enrich them with multiple tags. To send events with multiple tags you would need to do the following:

1. Configure PRTG Notification Template that sends the tag identifier:
   a. At the top of the page go to Setup.
   b. Click on Add Notification Template.
   c. Scroll down to Execute HTTP Action option and make sure that it is enabled.
   d. Fill in the URL where Smart Notifications installation is.
   e. Set HTTP Method to POST
   f. Paste the following payload:
   -DeviceName "%device" -DeviceIP "%host" -Sensor "%sensor" -LastValue "%lastvalue" -Status "%status" -DateTime "%datetime" -Message "%message" -Group "%group" -Probe "%probe" -DownTime "%downtime" -SensorID "%sensorid" **-DatadogCustomTagFile exampleTag**
   g. Where **exampleTag** is the tag that you wish to see in the Datadog events that are being sent from this specific notification template:

   h. Write down the tag name you gave to this notification template (In the example we used " **exampleTag** ") as you would use it in the next step.

2. Navigate to {Smart Notifications_InstallPath}\SmartNotif\Backend\Tags folder.
3. Create a file in the following naming convention:
   datadog_{TagName}.ini
   For Example using the "**exampleTag**" from previous step:
   datadog_**exampleTag**.ini
4. Open the created file from the previous step, and write the tags in the following format:
   TagName1:TagValue1,TagName2:TagValue2, TagName3:TagValue3
   For example:
   DevieGroup:QA,DataCenter:CentralDC,Environment:Production

5. Save the file after applying all tags.
6. Repeat Steps 2 to 5 for each tagged Notification Template.
7. This is how a PRTG Alarm would like in DataDog:



8 Smart Notifications NNMi Integration into DataDog

Smart Notifications now allows you to send events From NNMi incidents.csv log to DataDog. To enable sending of events from NNMi incidents.csv log to DataDog platform, make sure that the following INI field are defined correctly.

Variable Name	Default Value	Description
NNMi_ENABLED	FALSE	Any value other than TRUE (case sensitive) would disable sending events from NNMi.
NNMi_LOG	Empty	Provide the full location of the NNMi incidents.csv log, for example: C:\path\to\nnmi\logs\incident.csv

After these sections are correctly set, Smart Notifications would be able to send the logs as DataDog Events.

8.1 Configuring NNMi Whitelist

To not be flooded by incidents we have implemented a whitelist that let's you control what events you would see in Datadog from the NNMi log, to modify the Whitelist do the following:

1. Open the NNMi_include_msgs.csv file in:
   {SmartNotifications_InstallPath}\SmartNotif\Backend
   with Excel\ Any text editor you like.
2. Each column represents a "passing criteria" for events to send to Datadog.
   a. SourceNodeName – Filter only by certain SourceNodeName.
   b. Severity– Filter only by certain Severity.
   c. Category– Filter only by certain Category.
   d. Family– Filter only by certain Family.
   e. Origin– Filter only by certain Origin.
   f. Name– Filter only by certain Name.

   Only one filter of each SourceNodeName\ Severity\ Category\ Family\ Origin \ Name is allowed per line, if you want several filters, you could always add another line to the NNMi_include_msgs.csv file.
3. Examples:
   a. To Allow only Critical Severity and SNMP Origin:
      Any,Critical,Any,Any,SNMP,any
   b. To Allow any Major alerts with SNMP Origin where the name contains BGP and UPS:
      andAny,Major,Any,Any,SNMP,UPS
      Any,Major,Any,Any,SNMP,BGP

Note: To allow all metrics from specific field you can type "any" (case-insensitive).

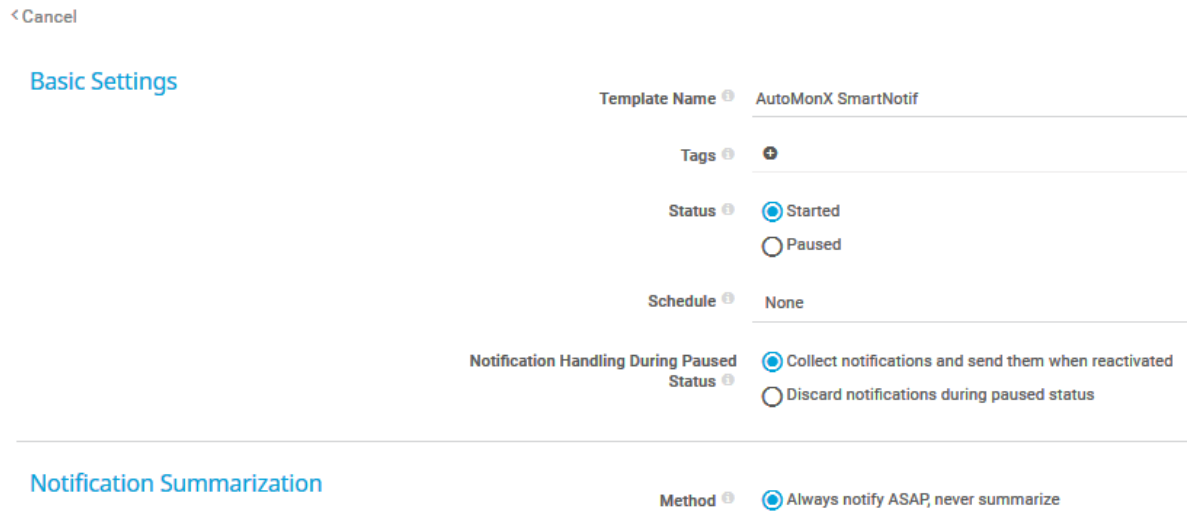
9 Configuring AutoMonX Smart Notifications in PRTG

9.1 Configure Notification Template Parameters

Configure the following options in the Add Notifications menu:

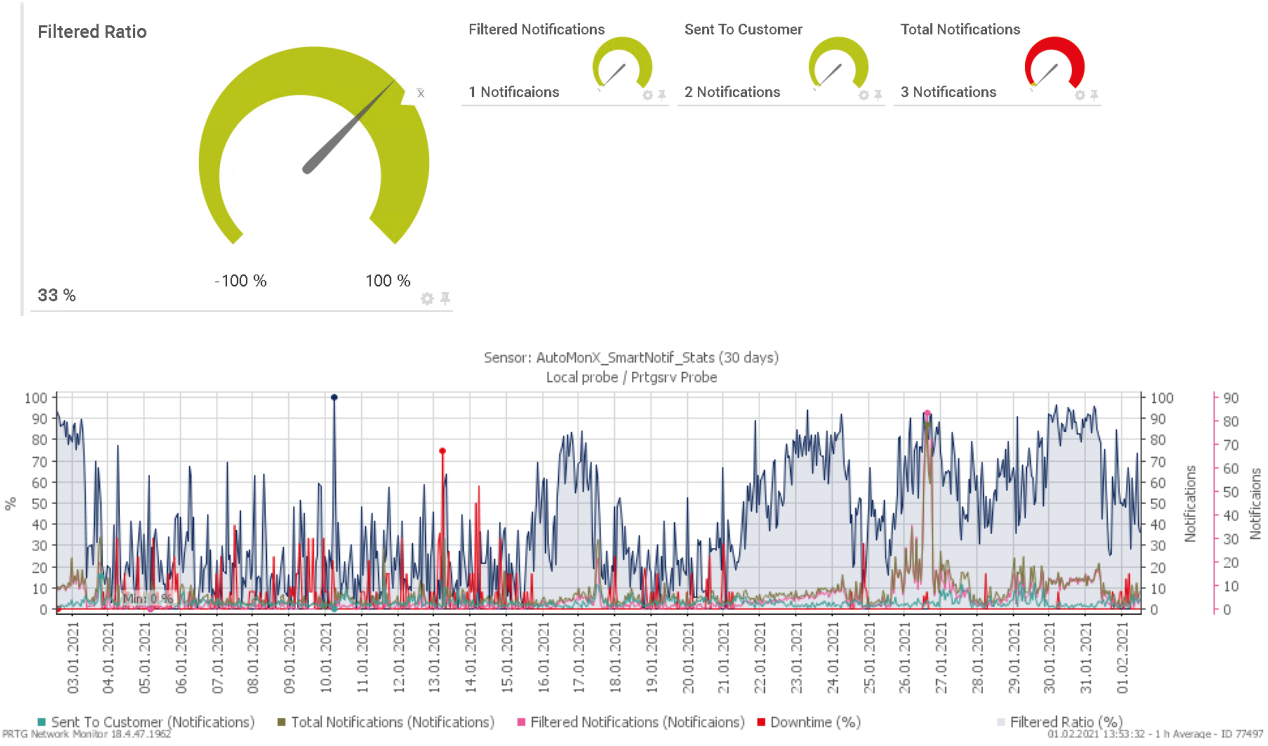
- **Notification Summarization** the **Always notify ASAP**
- Push **Execute Program** to enable state
- Select AutoMonX_SmartNotif.exe
- Add the following line in the Parameters field:
  -DeviceName %device -DeviceIP "%host" -Sensor "%sensor" -LastValue "%lastvalue" -Status "%status" -DateTime "%datetime" -Message "%message" -Group "%group" -Probe "%probe" -DownTime "%downtime" -SensorID %sensorid in the **Parameter** field.

- You can add more optional parameters as specified in the **Program Argument Options** right after the default parameter line.



9.2 Configuring Notifications self-monitoring – Smart Notifications Reporter

The Smart Notifications Reporter provides even greater value to Smart Notifications when configured to provide insights and statistics of the PRTG notifications such as notifications that are sent or notifications that are filtered out by the Smart Notifications algorithm.



You need to configure the Smart Notifications sensor enable monitoring of notification statistics. Assuming that you have deployed the Smart Notifications Reporter as explained in the installation section, do the following:

1. Add a new Custom EXEXML sensor under the Probe device of the PRTG Core server

2. On the "Add Sensor" page, Search for EXE sensor and select "EXE/Script Advanced".

3. Set the name of the sensor to "Smart Notifications Reporter".

4. Select the "AutoMonX_SmartNotIfReporter.cmd" from the drop-down menu.

5. In the "Parameters" field, provide two parameters: -prtg -min 5

a. The first parameter is the sensor mode, it creates a PRTG XML.

Enter -prtg for PRTG mode.

b. The second parameter is the time the sensor will generate notification statistics results on PRTG.

There are 4 options - 5,10,30,60 minutes.

Enter -min and the time.

Examples:

- For generating a PRTG sensor XML that analyze the last 5 minutes of notifications use: -prtg -min 5.

- For generating a PRTG sensor XML that analyze the last 10 minutes of notifications use: -prtg -min 10.

9.3 Configuring Notifications Analysis with Smart Notifications Reporter

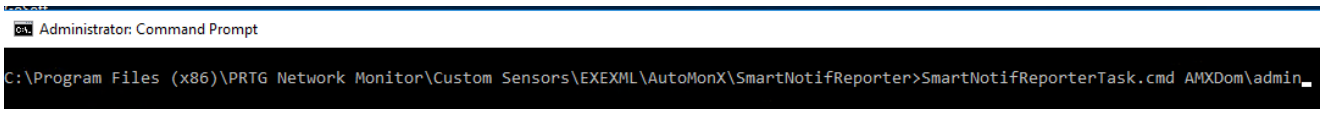
The Smart Notifications Reporter provides a dynamic notifications analysis report based on the actual notifications that are sent by Smart Notifications.
You need to add a Windows task that runs daily the Smart Notifications Reporter to generate the notifications report.

There is a batch file available to add the scheduled task automatically. It is located under the following directory (see section Smart Notifications reporter deployment). It sets the scheduled task to run Smart Notifications Reporter every day at 08:00am.

CustomSensors\EXEXML\AutoMonX\SmartNotifReporter SmartNotifReporter_CreateTask.cmd

In order to run it, open cmd.exe as administrator and run the batch file from the directory it is located:

SmartNotifReporter_CreateTask.cmd <YourDomain>\<username>

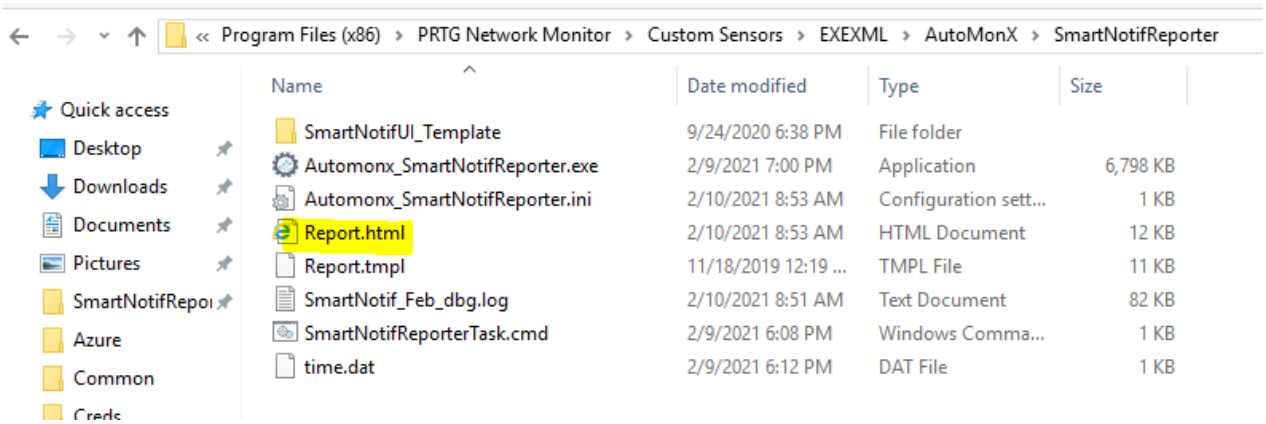


You would be required to provide the password for the user that will be running the scheduled task. If the setting succeeds you will see the following message:

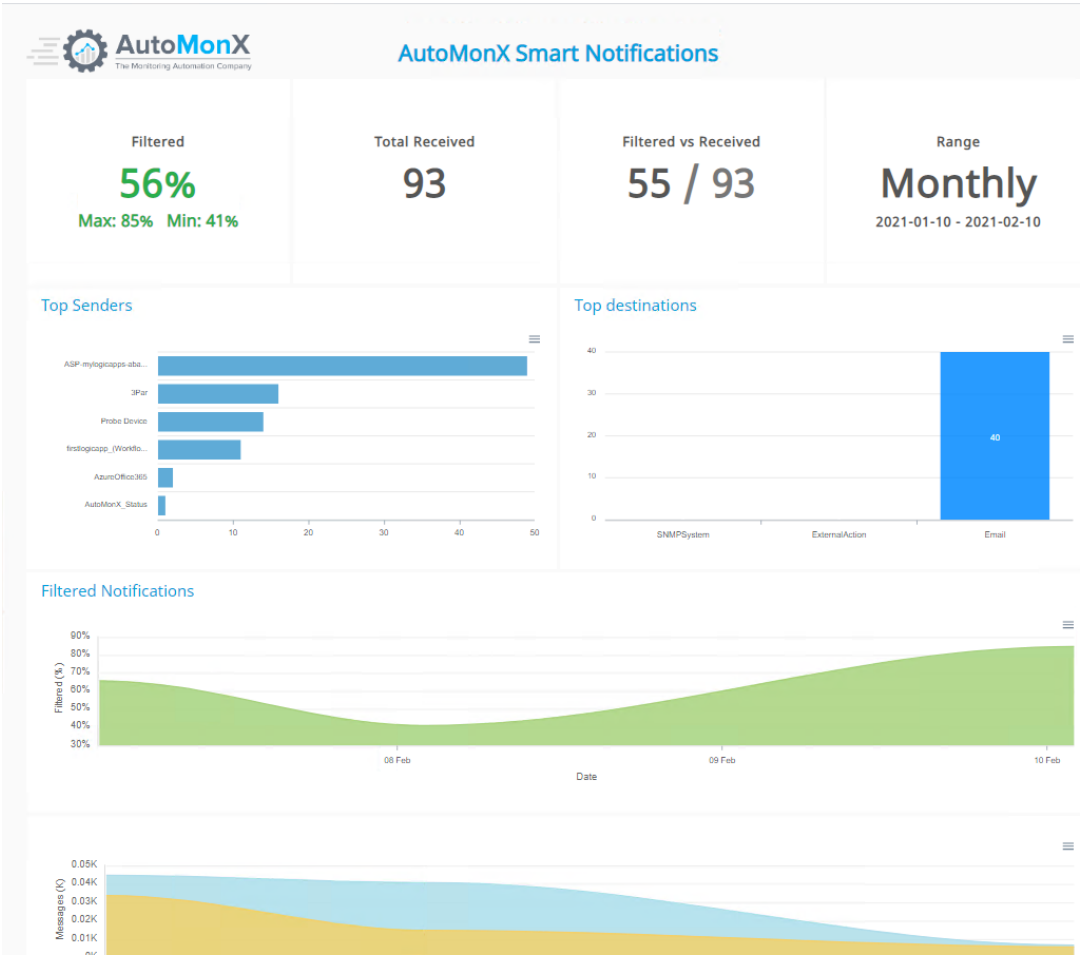
SUCCESS: The scheduled task "AutoMonX\AutoMonX\SmartNotif Reporter" has successfully been created.

9.4 Viewing Smart Notifications Reporter Results

Smart Notifications Reporter generates an HTML file in the same directory as the executable.



Double click on the report and open it with Chrome (for best results) or IE/Edge



10 Customizing Smart Notifications via Advanced Options

The table below details the configuration variables required for Smart Notifications to send notifications using the supported messaging mechanisms

Variable Name	Default Value	Description
SNMP_TRAPS_SERVER	127.0.0.1	Destination of the SNMP traps of Network/System issues.
SNMP_SIGNATURE	AutoMonX _SmartNotif	Custom text used to identify the AutoMonX Smart notifications SNMP Traps for easier parsing of the traps on the NMS side.
SNMP_COMMUNITY	Public	The SNMP community that would be used to send SNMP traps.

SNMP_ENABLED	TRUE	Activates SNMP traps. Any value other than TRUE deactivates this functionality.
SNMP_SPECIFIC_CRITICAL	22	SNMP Specific ID for Network/System issues of critical severity sent via SNMP traps
SNMP_SPECIFIC_NORMAL	21	SNMP Specific ID for Network/System issues of critical severity sent via SNMP traps
SNMP_SPECIFIC_WARNING	25	SNMP Specific ID for Network/System issues of normal severity sent via SNMP traps
SNMP_SEND_ MONITOR_OPS_NOTIF	FALSE	Activates sending MonitorOps messages as SNMP traps. Once activated, all message types (Network/System issues and Monitor errors) will be sent as SNMP traps.
SNMP_MAX_MSG_LENGTH	180	Specifies the message length that would be sent via SNMP traps. Some SNMP trap receivers ignore messages that are too long.
SNMP_TRAP_PATH	Empty	The path to the location of the Net-SNMP snmptrap.exe command. Typically, it would look like c:\snmp\bin\snmptrap.exe
SMTP_SERVER	exchangeserver 1	The mail server name or IP used for all SMTP communications
SMTP_ENABLED	TRUE	Activates SMTP communication. Any value other than TRUE deactivates this functionality
SMTP_SIMPLE_MAIL	FALSE	If set to TRUE Smart Notifications will send simple text notifications without the graphs
MONITOR_OPS_MSGS_MAIL_TO	**MonOps@domain.com**	Provides the email recipient list for MonitorOps (monitoring errors) to be sent. This setting can be overridden by the -prtgadmin option argument, which is also comma separated
MONITOR_OPS_MSGS_MAIL_FROM	**prtgerrors@domain.co**	Configures the From email for MonitorOps (monitoring errors) emails

NET_ADMIN_MSGS_MAIL_TO	**sysgroup@domain.co**	Provides the email recipient list for System or Network administrators (Network/System issues). This setting can be overridden by the -netadmin option argument, which is also comma separated.
NET_ADMIN_MSGS_MAIL_FROM	**prtgerrors@mydomain.co**	Configures the From email for Network/System issues (Network/System issues) emails
SMTP_ADD_CUSTOM_URL	**http://yourcrm.com?=AUTOMONX_HOSTNAME**	Adds a custom URL to the email sent via Smart Notifications for custom integrations with other software such as CRM/HelpDesk. **AUTOMONX_HOSTNAME** is populated automatically with the hostname of the device from PRTG
CONSIDER_NORMAL=TRUE	**TRUE**	Smart Notifications to consider “back to normal” messages. A message with OK severity will be sent out if previously a Network/System issue was sent for the same sensor/channel.
CONSIDER_UNUSUAL	**FALSE**	Smart Notifications to consider Unusual sensor states. (i.e. 1-hour interval average of 6 Mbit/s (Traffic In) is unusually low for this hour of the week). TRUE activates this functionality. Make sure that a notification trigger was configured in PRTG for Unusual states.
CONSIDER_WARNING	**FALSE**	Smart Notifications to consider messages with Warning sensor states. A value of TRUE activates this functionality. Make sure that a notification trigger was configured for Warning states in PRTG.
CONSIDER_PARTIAL	**FALSE**	Tells Smart Notifications to consider messages with Down Partial sensor states. TRUE activates this functionality. Make sure that a notification trigger was configured for Down Partial states in PRTG.

EXTERNAL_NOTIF_COMMAND	**command.exe -p AutoMonX_PARAMETER -msg AutoMonX_MESSAGE**	Tells Smart Notifications which program to execute when an external command is used. The command should be placed in quotation marks. The variables that are available for this command are: **AutoMonX_MESSAGE – This will be replaced with the value of the original message from PRTG.** **AutoMonX_PARAMETER – This will be replaced with the value in -ext_recip or -ext_nms_recip options.**
EXTERNAL_NOTIF_COMMAND_ENABLED	**FALSE**	Tells Smart Notifications to activate external executable notification. Any value other than TRUE deactivates it.
LOG_MESSAGES	**TRUE**	Tells Smart Notifications to write all messages to a text log file called AutoMonX_SmartNotif.log. By default, it is set to TRUE so that Smart Notifications Reporter would be able to analyze the messages flow
SMART_NOTIF_LOG_DIR	**BIN_DIR**	Tells Smart Notifications where to store the messages log file. The default variable BIN_DIR points to the location of the Smart Notifications exe.
TELEGRAM_NOTIF_ENABLED	**FALSE**	Tells Smart Notifications to enable sending messages through Telegram
TELEGRAM_NOTIF_MAX_MSG_LENGTH	**180**	Specifies the maximum size of the message that would be sent through Telegram.
TELEGRAM_TOKEN_ID	**Empty**	Specifies the token ID to for connecting to Telegram.
CLEANUP_ENABLED	**FALSE**	Indicates the operation of the cleanup process. The cleanup process goes through all the down sensors that Smart Notifications has captured and checks their status in PRTG. If the sensor is not Down state, then Smart Notifications sends an UP (OK) message. The cleanup process activity is logged in a cleanup log.

NOTIF_SEND_ON_ACK	**FALSE**	If set to True, Smart Notifications will send a message with Normal severity during the cleanup process for Acknowledged messages. Requires the CLEANUP_ENABLED setting to set TRUE.
PRTG_USER_NAME **PRTG_USER_PASSHASH** **PRTG_SERVER** **PRTG_PORT** **HTTPS_CONNECTION**		The cleanup process requires to connect to the PRTG API. The PRTG connection requires a user with API access with read permissions
LIC_EXPIRE_NOTIF	**MAIL;SNMP;TELEGRAM**	Channels to send License warnings. By default, if license is about to expire daily notifications will be sent via all the notification routing options

10.1 Smart Notifications – Advanced Correlation

The AutoMonX Smart advanced correlation options allow to even further reduce the potential "noise" of multiple notifications that would be sent out when an unplanned major outage happens.

Variable Name	Default Value	Description
CORRELATION_ENABLED	TRUE	Choose if Correlation needs to be Enabled\Disabled
CORRELATION_PER_DEV_COUNT	5	How many notifications same device can send before correlation suppresses further notifications
CORRELATION_PER_DEV_SEC	300	For how long the correlation should wait before suppression kicks-in
CORRELATION_PER_PROBE_COUNT	30	How many notifications from devices located under same PRTG Probe can be sent before correlation suppresses further notifications

CORRELATION_PER_PROBE_SEC	120	For how long the correlation should wait before suppression kicks-in
CORRELATION_DEV_WMI_SEC	600	
CORRELATION_DEV_SNMP_SEC	600	
SEND_ADMIN_WMI_SNMP_CONN_ERRORS	FALSE	If set to TRUE, enables sending notifications to Netadmin/Sysadmin on SNMP and WMI connectivity issues (one per device)

10.2 Smart Notifications – Email Routing Options

Add the following options to override the values configured in the INI file. This is useful when non-default notification routing is required. Both options can be used together or separately.

Command line option	Description
-emails	Sends the Network/System issues using email to system / network administrator, overrides the INI file setting. Use a semicolon to specify multiple recipients
-emails_nms	Sends the monitoring errors using email to MonitorOps, overrides the INI file setting. Use a semicolon to specify multiple recipients
-smtp	Overrides the SMTP_ENABLED INI setting. Examples: -smtp=TRUE will send emails even if the INI is set to FALSE -smtp=FALSE will not send any emails even if the INI is set to TRUE

For example, when AutoMonX_SmartNotif.exe is configured with the following email routing options:

-**emails_nms** monitorTeam@domain.co;monitorTeamLeader@domain.co and

- **emails** sysadmin@domain.co;sysgroup@domain.co

This setting will override the INI settings and route the notifications as follows:

- For Network/System issue message, to sysadmin@domain.co and sysgroup@domain.co
- For monitoring error message, to monitor@domain.co and monitorTeamLeader@domain.co

10.3 Smart Notifications – Using External Commands to Route notifications

Add the following options to override the values configured in the INI file for non-default routing on notifications based on external commands. This is useful when non-default notification routing is required. Both options can be used together or separately.

-ext_recip	Recipient information of a system / network administrator for external notification command. Use a semicolon to specify multiple recipients.
-ext_nms_recip	Recipient information of a MonitorOps for external notification command. Use a semicolon to specify multiple recipients.
AutoMonX_MESSAGE	This variable will be automatically replaced by the value of the PRTG original error message
AutoMonX_PARAMETER	This variable will be replaced by the value in ext_recip or ext_nms_recip options.

For example, when the INI is configured as follows:

```
EXTERNAL_NOTIF_COMMAND="command.exe -p AutoMonX_PARAMETER -msg
AutoMonX_MESSAGE"
```

In order to provide the required notification routing parameters, add in PRTG the following settings to the notification options:

```
-ext_recip System1;System2   -ext_nms_recip  PRTG_Admin
```

Where System1, System2 and PRTG_Admin represent your custom external notification destination groups or recipients.

This setting will instruct Smart Notifications to execute the following commands:

- **Network/System issue message**:

command.exe -p System1 -msg “CPU Utilization is high 90%”

command.exe -p System2 -msg “CPU Utilization is high 90%”

- **Monitoring error message:**

  command.exe -p PRTG_Admin -msg “SNMP Error 2001”

The following table summarizes the use of -ext_recip and -ext_nms_recip options with the command that is defined in the INI file EXTERNAL_NOTIF_COMMAND setting.

Option arguments used. / **Message Type**	**-ext_nms_recip and -ext_recip are used**	**Only ext_recip is used**	**Only ext_nms_recip is used**	**ext_nms_recip and -ext_recip are not used**
Network/System issue Message	The command will execute for each recipient defined in ext_recip.	The command will execute for each recipient defined in ext_recip.	No command will be executed.	The command will execute with default (INI) values
Monitoring Error Message	The command will execute for each recipient defined in ext_nms_recip.	No command will be executed.	The command will execute for each recipient defined in ext_nms_recip.	No command will be executed.

10.4 Smart Notifications – Using Telegram to Route notifications

Add the following options in PRTG Notification template parameters for routing notifications to Telegram recipients. Both options can be used together or separately.

- telegram_recip	Chat id information of a System/Network administrator for Telegram notification. Use a semicolon to specify multiple recipients.
- telegram_nms_recip	Chat id information of a MonitorOps for Telegram notification. Use a semicolon to specify multiple recipients.

For example, when used with the setting below:

EXTERNAL_NOTIF_COMMAND="command.exe -p AutoMonX_PARAMETER -msg AutoMonX_MESSAGE"

In order to provide the required notification routing parameters, add in PRTG the following settings to the notification options:

-telegram_recip <Group_id_1>;<Group_id_2> and -telegram_nms_recip <Group_id_3>

This setting will instruct Smart Notifications to execute the following commands:

- System/Network Issues: Send the message to Telegram with chat id of 1 and 2
- Monitoring errors: Send the message to Telegram with chat id of 3

The following table summarizes the use of -telegram_recip and -telegram_nms_recip options**:**

Option arguments used. / **Message Type**	**Option -telegram_nms_recip and -telegram_recip are used**	**Only -telegram_recip is used**	**Only telegram_nms_recip is used**	**Option -telegram_nms_recip and -telegram_recip are not used**
Network/System issue Message	The command will execute for each recipient defined in -telegram_recip.	The command will execute for each recipient defined in -telegram_recip.	No command will be executed.	The command will execute once.
Monitoring Error Message	The command will execute for each recipient defined in -telegram_nms_recip.	No command will be executed.	The command will execute for each recipient defined in telegram_nms_recip.	No command will be executed.

Web : https://www.automonx.com
Email : support@automonx.com

10.5 Smart Notifications – Outage Control

Smart Notifications can be configured to avoid sending notifications at certain times and for specific devices. This feature is useful when you plan to maintain one or many devices and wish to avoid notifications.

To control the Outage mechanism, you need to add relevant configuration lines to the AutoMonX_outage.csv file as seen below:

<node_name_as_in_prtg>,<hour-frame1>;<hour-frame2>

For Example:

Router1,1-5;21-24;28/10/2021 18-30/10/2021 07;Every Sunday 03 to 15

10.6 Smart Notifications – Advanced Options

Below are some advanced options to use Smart Notifications

-overrideWarn:

This setting is used for cases where the default setting CONSIDER_WARNING is set to false, but warning message are required to be considered for specific Groups/Devices. Without placing this parameter, Smart Notifications will use the INI file's CONSIDER_WARNING setting to determine if the message is defined as a normal or as a warning message.

-refresh

This option starts the cleanup process and initiates sending of Normal severity messages for any resolved error message. This option is used by setting Smart Notifications to run via a scheduled task.

-offline

When Smart Notifications is configured with this option, it will write the notifications to a file instead of sending them. It is useful for generating a notifications log in a secure environment that doesn't have access to Internet and re-play this log on an external machine that has access to Internet. You need to copy the generated log every few minutes to the non-secure environment for the messages to be sent out.

-send_offline

When Smart Notifications is configured with this option, it will read the notifications from the offline log file and send them. You need to setup Smart Notifications to run as a scheduled task to make sure fresh log entries would be sent out.

-test

This option is used to test Smart Notifications functionality by simulating a test message. Refer to Troubleshooting to see more information.

11 Examples of Smart Notifications Usage Options

This is an example on how to configure Smart Notifications to route notifications as follows:

- Email Monitoring errors to prtgadmin1@dom.co, prtgadmin2@dom.co
- Email Network/System issues to sysadmin1@dom.co and sysadmin2@dom.co
- Route to SMS Network/System issues via an external command

This can be achieved by adding the following options to AutoMonX Smart Notifications in the relevant PRTG notification delivery template:

-prtgadmin prtgadmin1@dom.co;prtgadmin2@dom.co -netadmin sysadmin1@dom.co;sysadmin2@dom.co -ext_recip sysGroup -ext_nms_recip prtgGroup

Configure SmartNotif.INI parameter EXTERNAL_NOTIF_COMMAND with the relevant external command (this is just an example of a fictitious external command)

“sms.exe -message AutoMonX_MESSAGE -resp AutoMonX_PARAMETER”

Note: to configure the program to execute a command for a few parameters, separate each parameter with a semicolon. For example, replace -ext_recip sysGroup with -ext_recip sysGroup;sysTeamLdr

The program will execute the following command when a Network/System issue occurs:

“sms.exe -message AutoMonX_MESSAGE -resp sysGroup” and

“sms.exe -message AutoMonX_MESSAGE -resp sysTeamLdr”

12 Advanced Features of Syslog Messages Delivery

The following settings in the configuration file are optional to configure:

SYSLOG_PORT	514	This setting would change the port Syslog Protocol communicates over. **Important** Please set custom port above port 1000 as ports below 1000 often used for Core OS functionality and may disrupt normal flow of operation.
SYSLOG_TITLE	Empty	This setting sets a custom string as the Title of the syslog message.

13 Advanced Features of SNMP Trap Delivery

The following settings in the configuration file are optional to configure:

SNMP_PORT	162	This setting would change the port SNMP Trap Protocol communicates over. **Important** Please set the custom port above port 1000 as ports below 1000 often used for core OS functionality and may disrupt normal flow of operation.

14 SNMP Trap Specific OIDs Mappings

The tables below map the specific OIDs that Smart Notifications sends as SNMP traps to a Northbound NMS platform. It is useful for easier parsing of the PRTG messages. All the variables are of type Octet String.

Enterprise ID: 1.3.6.1.4.1.7087.1, Generic ID: 6 (SNMP v1)

Trap Types (IDs can be modified via the INI file**)**

SNMP Specific OID	Trap Name	Description
22	Down Message	**Error messages**
21	Normal Message	**OK / Clear messages**
25	Warning Message	**Warning messages**

SNMP Variables

SNMP OID	Variable name	Description
.1.3.6.1.4.1.7087.1.1.0	**Device Name**	This device name in the PRTG that sent the message.
.1.3.6.1.4.1.7087.1.2.0	**Sensor Last Value**	The Sensor Last Value reported from PRTG.
.1.3.6.1.4.1.7087.1.3.0	**Threshold**	This is the sensor limit that was triggered
.1.3.6.1.4.1.7087.1.4.0	**Sensor Name**	The Sensor name the sent the message
.1.3.6.1.4.1.7087.1.5.0	**Device Group**	The Group the device is in the PRTG
.1.3.6.1.4.1.7087.1.6.0	**Sensor Id**	The Id of the sensor that sent the message.
.1.3.6.1.4.1.7087.1.7.0	**SNMP Signature**	A Key that is defined in the **SNMP_SIGNATURE** setting in the INI file.
.1.3.6.1.4.1.7087.1.8.0	**Message**	A modified message that was sent from the PRTG. This message is

		more informative than the original message
.1.3.6.1.4.1.7087.1.9.0	**Original Message**	The original message that was sent from the PRTG
.1.3.6.1.4.1.7087.1.10.0	**Down Time**	The sensor down time as reported by PRTG
.1.3.6.1.4.1.7087.1.11.0	**Device IP**	This device IP in the PRTG that sent the message.

Example of a decoded SNMP Trap sent by Smart Notifications:

[1] 1.3.6.1.4.1.7087.1.1.0 (OctetString): linuxsrv.automonx.com
[2] .1.3.6.1.4.1.7087.1.2.0 (OctetString): 95 % (Total)
[3] .1.3.6.1.4.1.7087.1.3.0 (OctetString): 90 %
[4] .1.3.6.1.4.1.7087.1.4.0 (OctetString): Pagefile Usage
[5] .1.3.6.1.4.1.7087.1.5.0 (OctetString): Application Servers
[6] .1.3.6.1.4.1.7087.1.6.0 (OctetString): 77239
[7] .1.3.6.1.4.1.7087.1.7.0 (OctetString): AutoMonX_SmartNotif
[8] .1.3.6.1.4.1.7087.1.8.0 (OctetString): Critical - linuxsrv.automonx.com: Threshold violated for Pagefile Usage. Measured: 95 % (Total), threshold: 90 %
[9] .1.3.6.1.4.1.7087.1.9.0 (OctetString): 95 % (Total) is above the error limit of 90 % in Total

15 Troubleshooting

The AutoMonX Smart Notifications has a diagnostic mode that can help you identify technical issues you may encounter during its usage. The diagnostic mode generates a test message and then displays a detailed debug of the Smart Notifications execution. The debug output will present you with messages that will help you understand the flow of Smart Notifications.

To test Smart Notifications with diagnostic mode, please run the AutoMonX Smart Notification program with the following arguments in cmd.exe:

AutoMonX_SmartNotif.exe -test -debug

Now check the debug log file to view the most recent message and where it was sent.

Below is a table with explanations to help you understand the program's workflow and solve errors.

Appears in debug output / **Issue encountered**	Can't open file	Error message while executing <SNMP/Email/EXE> phase	No error messages during the execution phase
SNMP messages are not received	Make sure that Smart Notifications has read/write permissions on the Notification\EXE folder	The program can't execute the phase using the supplied configuration defined in the INI file and/or argument options	Check if the destination is configured to receive SNMP traps
Email messages are not received	Make sure that Smart Notifications has read/write permissions on the Notification\EXE folder	The program can't execute the phase using the supplied configuration defined in the INI file and/or argument options	Check if the server and the user are configured correctly to receive mail
External program is not executed	Make sure that Smart Notifications has read/write permissions on the	The program can't execute the phase using the supplied configuration defined in the INI file and/or argument options	The AutoMonX Smart Notification will show the output of the external command.

	Notification\EXE folder		

16 Appendix A – Telegram Group Creation and Configuration

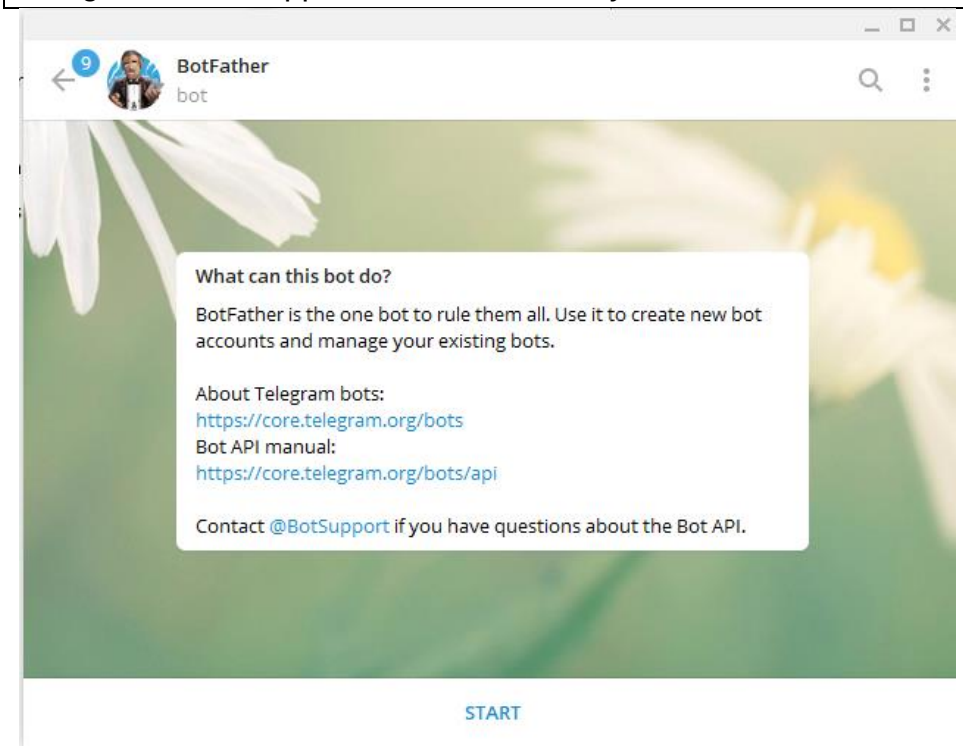
Smart Notifications is capable of routing notifications via the Telegram social network (similar to Whatsapp). In order to enable the routing of PRTG notifications via Telegram you must configure the connection to Telegram and obtain the Telegram Token and Telegram group ID(s).

Telegram Token is used to connect to a Telegram BOT that's assigned to a Telegram message group. The Telegram Group ID is used to indicate the alert group destination. Members of this group will get the notifications that Smart Notifications would send to their Telegram Application.

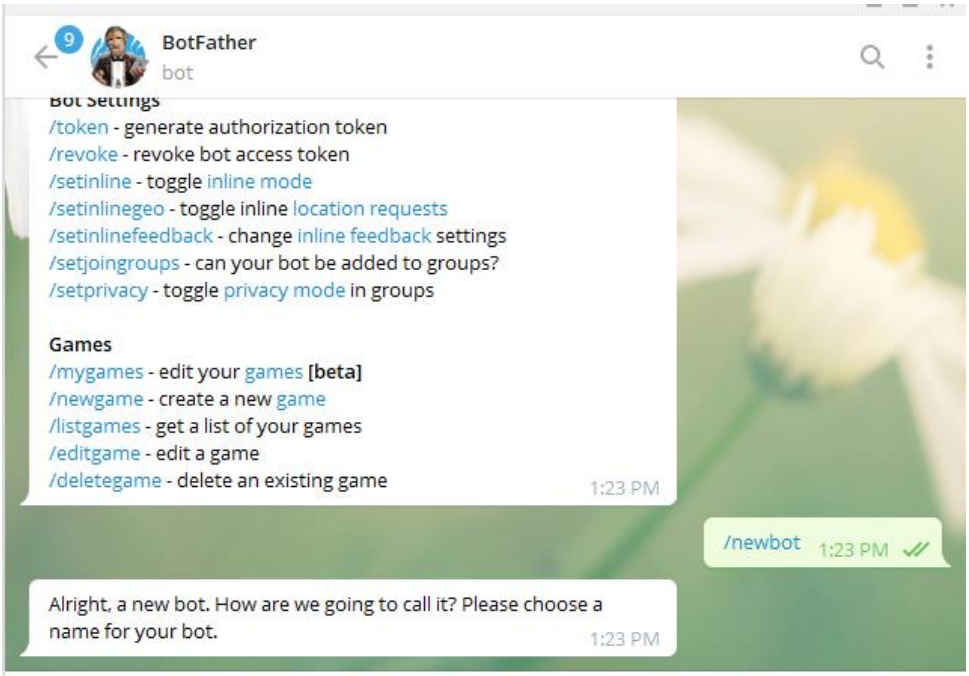
16.1 Getting the Token ID of the BOT:

1. Connect to BotFather to create a bot by pointing your web browser to the following URL: https://telegram.me/BotFather

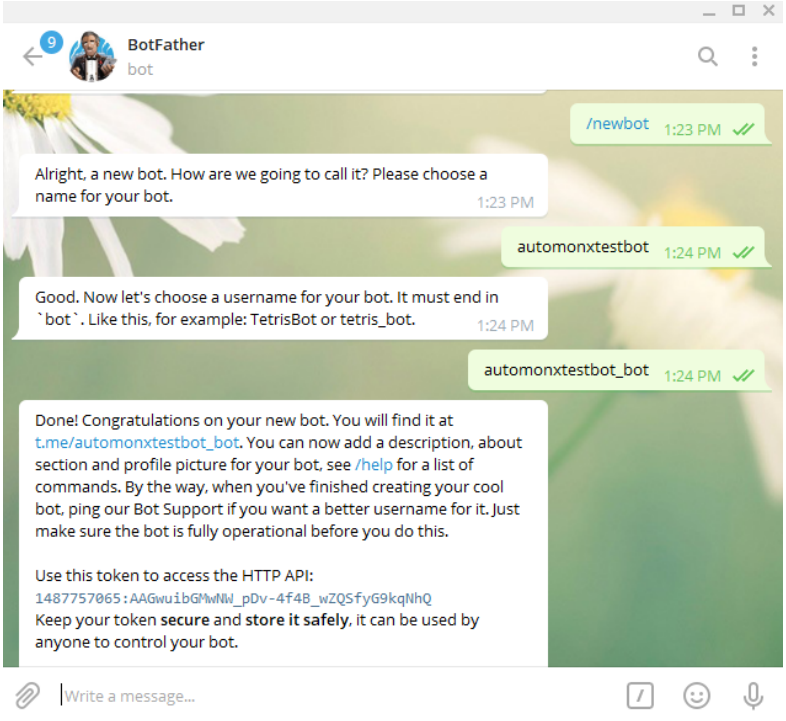
Important: You need to be logged into your Telegram account via the Telegram mobile app or via a browser on your PC



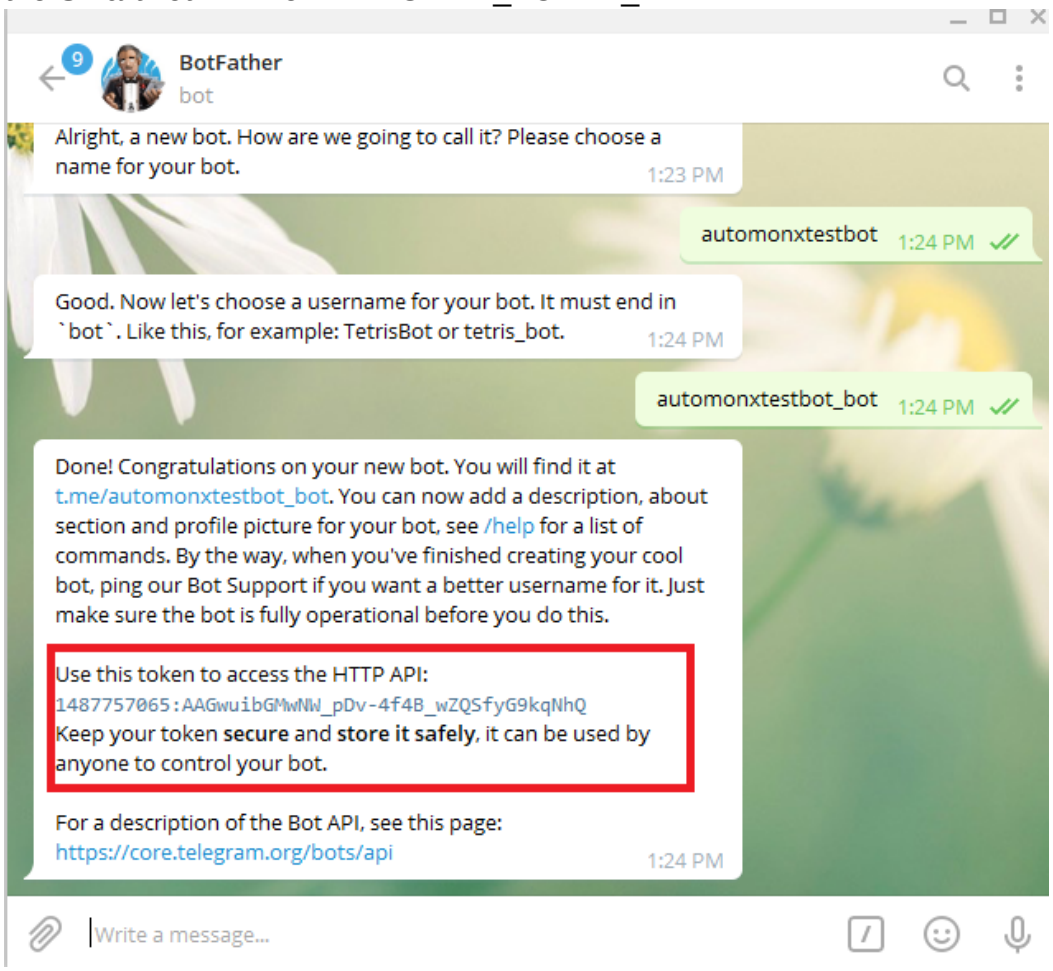
2. Click Start and send the command **/newbot**



3. Create a username and a display name for the Bot. A token will be shown:



4. Copy the Token of the newly created Bot and configure the variable below in the SmartNotif.ini file: TELEGRAM_TOKEN_ID=

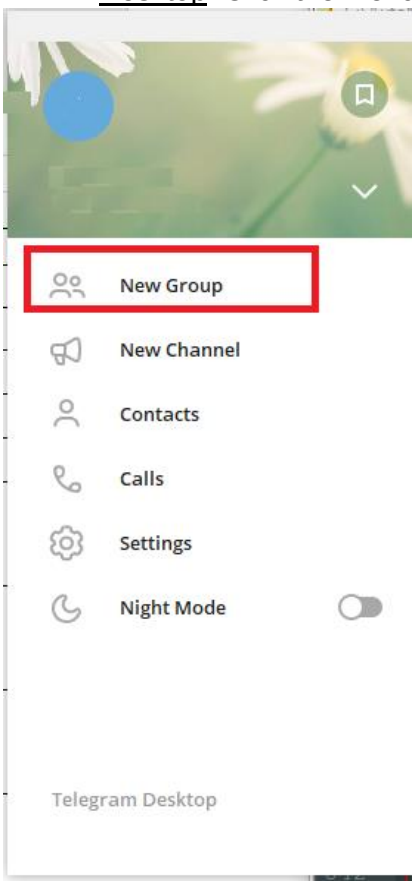


16.2 Create a Telegram Group for Smart Notifications notifications

You need to create a group in Telegram for each type of Notification (i.e. group for System/Network Admins and group for MonitorOps). The same Bot can be a member of both groups. Multiple Bots are not supported at this time.

The members of these groups would receive notifications from Smart Notifications. This newly created group(s) must include the BOT we created earlier as a member with admin permissions and at least one additional Telegram user (except yourself).

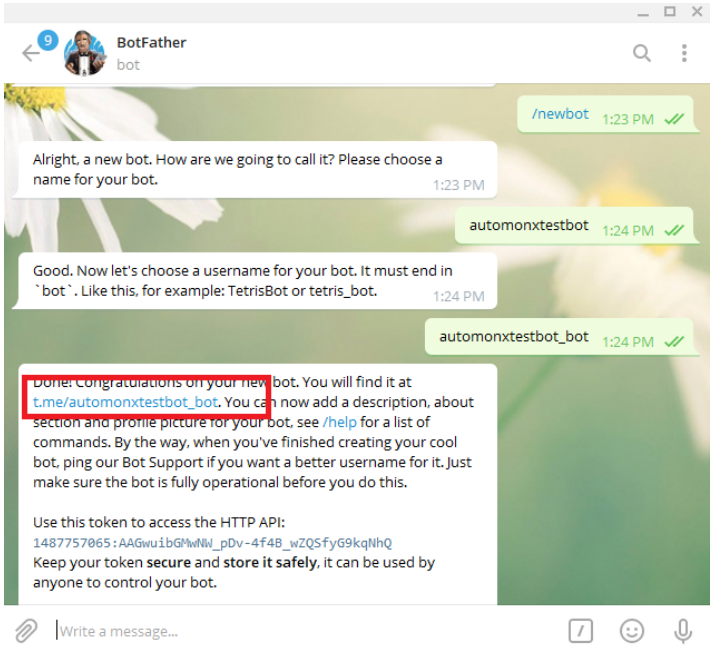
1. Create a new group and assign it a name by one of the options below:
   - iOS: Start a new message (tap the icon in the top right corner in Chats) > '**New Group**'.
   - Android: Tap the circular pencil icon in the chat list > 'New **Group**'. **Telegram**
   - Desktop: Click the menu button in the top left corner > 'New **Group**'.



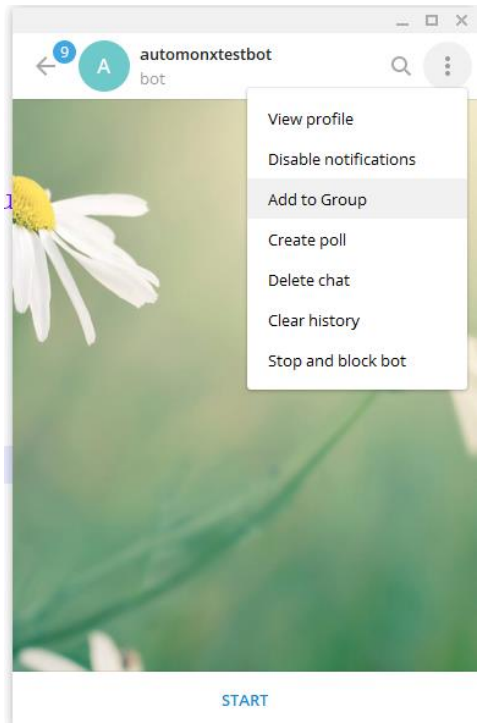
2. **Important**: You must assign another Telegram member (another Telegram user account which is not yours) to the group. At the end of the Group creation process, it will contain 3 members: Your Account, the Bot account and another user account

16.3 Add the Bot to a Telegram Group

Access the Bot page from the BotFather chat via https://telegram.me/BotFather and Click on the Bot name you have previously created



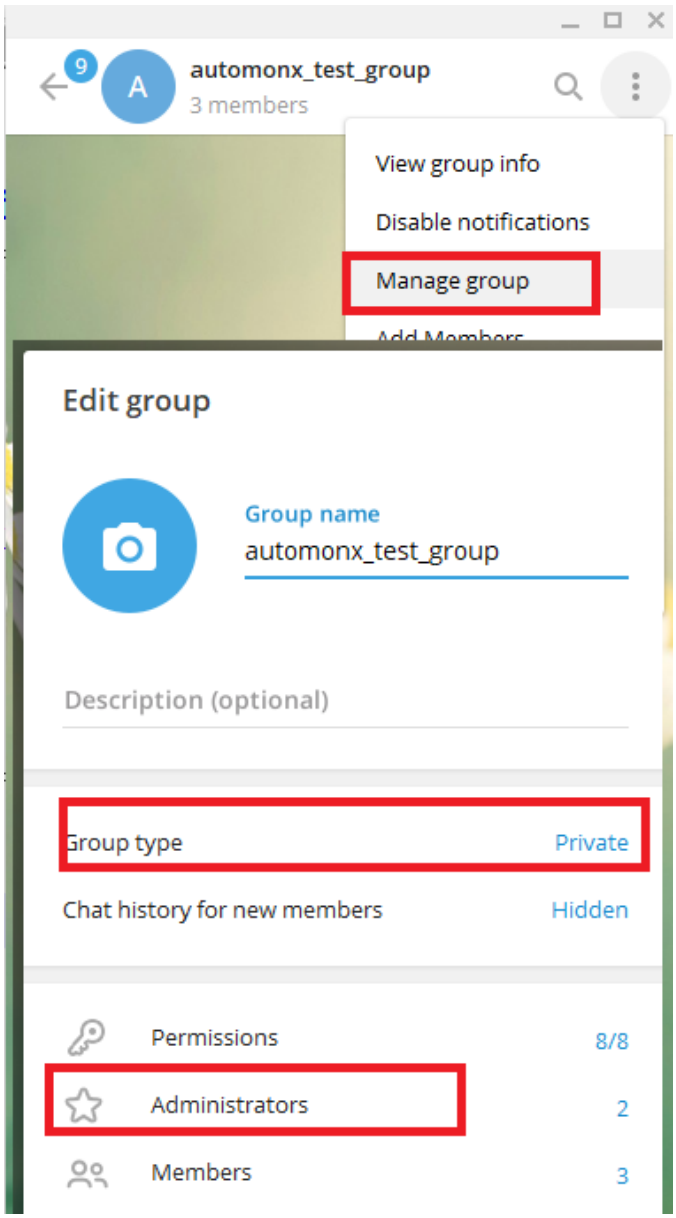
Click Start and Add the Bot to the group(s) you have created



Go Back to the group settings and assign the Bot to become and Admin of the group.

Important: Make sure that the BOT is the group Admin and that the group type stays **private** and click Save.

Web : https://www.automonx.com
Email : support@automonx.com

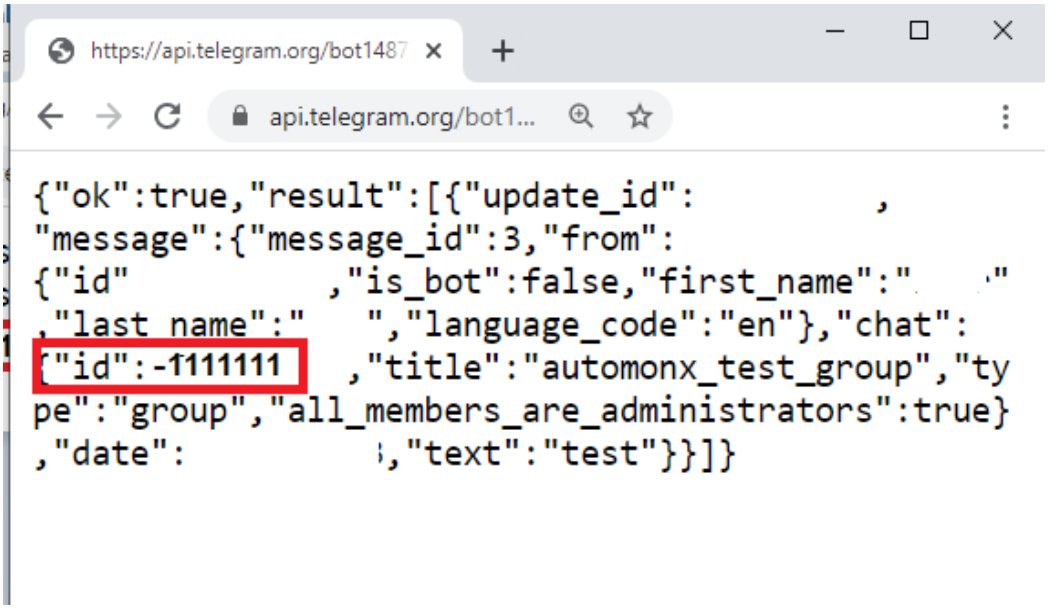


- **Send a test message in the group.**
- Assign additional members to the Group if needed

16.4 Obtaining the Group ID for Smart Notifications to use

Navigate to the following address using a browser:

https://api.telegram.org/bot<telegram_token>/getUpdates



The group ID is the number that starts with the minus symbol is the group ID (without the symbol).