MG-SOFT Corporation

Net Inspector 2017

Version 11

INSTALLATION AND CONFIGURATION GUIDE

(Document Version: 11.2)

Document published on June 27, 2017

In order to improve the design or performance characteristics, MG-SOFT reserves the right to make changes in this document or in the software without notice.

Depending on your license, certain functions described in this document may not be available in the version of the software that you are currently using.

Screenshots used in this document may slightly differ from those on your display.

TABLE OF CONTENTS

1 INTRODUCTION

This guide provides instructions for installing and configuring Net Inspector version 11 for Windows and Linux operating systems.

All command line commands, filenames, paths and examples in this guide are formatted with a fixed width font, e.g., `port = 5223`.

The path to Net Inspector **v11.x** installation directory in this guide is specified as **`//Engine`**. By default, this is equivalent to:

`C:\Program Files\MG-SOFT\Net Inspector 11` on Windows, and

`/usr/local/mg-soft/mgnetinspector` on Linux operating systems.

This guide also references the Net Inspector **`workspace`** directory, where the majority of files containing the program settings and initialization parameters are located. The path to the `workspace` directory is different in Windows and Linux operating systems, as follows:

In Linux, the `workspace` directory full path is:

`/var/mg-soft/mgnetinspector/workspace/`

In Windows, the `workspace` directory full path is:

`C:\ProgramData\MG-SOFT\Net Inspector\Workspace`

The content of this guide is listed in the Table of Contents.

2 ABOUT NET INSPECTOR

MG-SOFT Net Inspector 2017 (version 11) is a powerful fault and performance network management application designed for monitoring the status and performance of managed devices and managing alarms associated with devices in the supervised IPv4 and IPv6 networks.

Net Inspector server automatically discovers and graphically depicts your network by means of icons representing devices and lines representing connections between devices. Then, the server, which runs as a service/daemon application, continually monitors network devices using ICMP, SNMP, WMI and VMware web services and triggers alarms when there is a problem, e.g., if a device or a service (e.g., HTTP, FTP, DNS, SSH, etc.) stops responding, if a monitored metric crosses the user-defined threshold value (CPU load, memory usage, bandwidth usage, etc.), if a monitored process stops running etc. Besides, the software receives event reports (SNMP Trap or Inform), which are sent to it by managed devices when important events occur (link is lost, device is rebooted, chassis temperature is high…).

Net Inspector provides a dynamic, completely web-based graphical user interface. It lets you monitor the status and performance of managed devices, as well as view and manage alarms (acknowledge, clear, filter, find, etc.). The status of every managed device is indicated by the color of its icon, while active alarms are chronologically listed in a dedicated frame using different colors to reflect different severity levels of alarms. This principle lets you tell at a glance if all systems are functioning as expected, and in case of problems, quickly concentrate on them by viewing alarm messages that contain detailed description of the problem.

In addition to fault management, Net Inspector incorporates also full-featured performance management functionalities, effectively covering both crucial network management areas. The advantage of integrated fault and performance management is that the full history of alarms and performance data is available, which allows you to see a more realistic picture of the health of the network and let you bring educated decisions, based on trend reports, regarding its maintenance. Further advantage is that the integrated system enables you to monitor virtually any parameter available through SNMP (vendor-specific metrics), and let you deploy distributed polling engines that enable load balancing and better performance of the management system. Distributed management also makes the system easily scalable without seriously degrading its performance, so the management system's capacity can seamlessly grow with your network.

Net Inspector now supports discovering and monitoring the organization's virtualization infrastructure, i.e., virtualization servers (VMware ESX/ESXi and vCenter and Microsoft Hyper-V) and their virtual machines (VMs). This lets you effectively monitor your virtualization environment's health and resources of virtualization servers and VMs, like the CPU load, memory usage, network utilization and traffic, datastore usage, etc.

Besides, Net Inspector incorporates NetFlow and sFlow monitoring, providing detailed IP traffic statistics, i.e., the applications that generate the most traffic, endpoints (IP addresses) that receive and generate the most traffic, protocols that are used most, etc. This information is obtained by collecting, analyzing and aggregating NetFlow and sFlow packets exported by the network devices. NetFlow/sFlow monitoring effectively complements the standard SNMP monitoring and together they offer a valuable insight

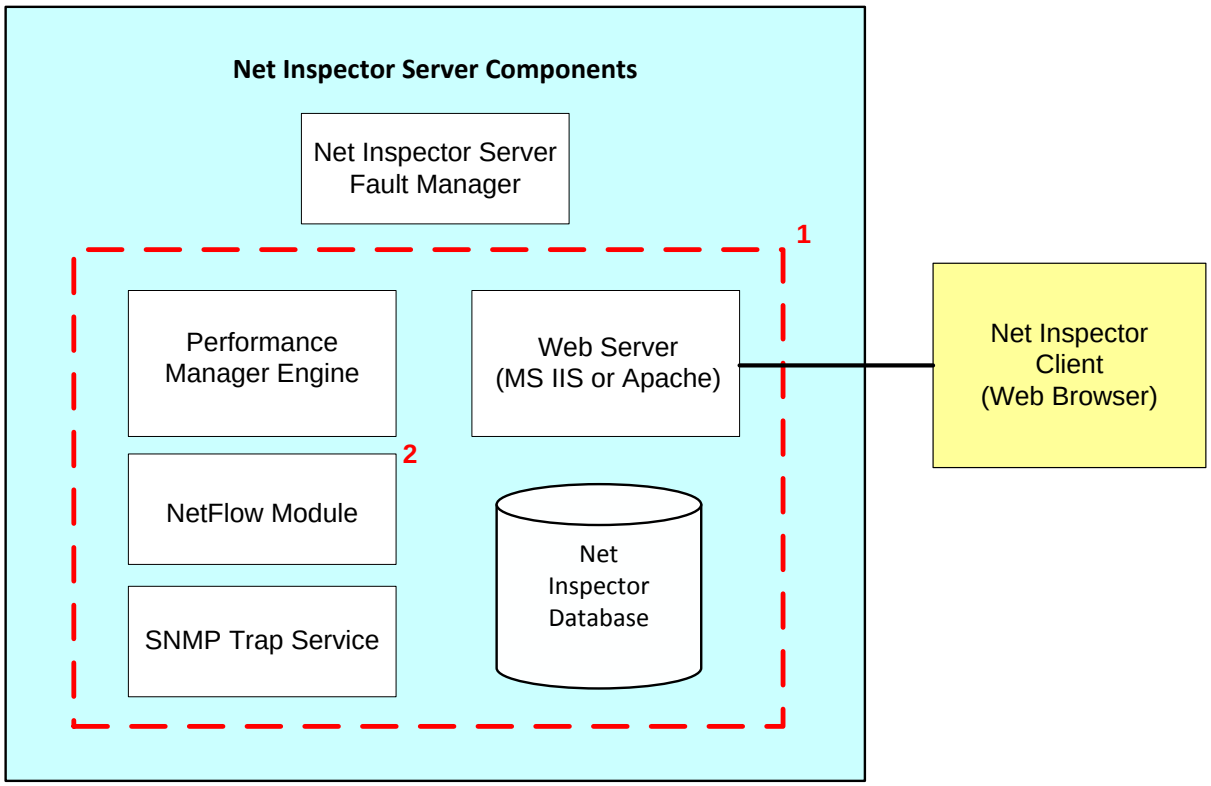
into the network infrastructure and bandwidth utilization and let you easily identify the cause of congestions, etc.

Furthermore, Net Inspector also lets you monitor the IP SLA statistics, including HTTP, FTP, TCP, DNS and VoIP Quality-Of-Service metrics (e.g., MOS, jitter, latency, packet loss, etc.) on devices implementing the IP SLA functionality (e.g., Cisco routers).

Net Inspector Server is available for MS Windows operating systems (Windows Server 2008 R2, Windows 7, Windows Server 2012, Windows 8.x, Windows 10 and Windows Server 2016) and for RHEL/CentOS v7+ and Debian v8+. Net Inspector has a completely web-based user interface that runs in modern web browsers (Chrome, Firefox, Edge, etc.) irrespective of the operating system.

3 NET INSPECTOR ARCHITECTURE

3.1 Main Components of Net Inspector



[1]These modules are also called "distributed modules". In simple configuration, these modules are installed on the same computer as Net Inspector Server (Fault Manager) module. In distributed configuration, these modules are installed also on one or more remote computers.
[2]NetFlow Module is not available in Net Inspector LITE Edition.

Short Description of Net Inspector Components

Net Inspector Server (**Fault Manager**) – Fault Management module that identifies the status of devices and network interfaces, triggers alarms on events reported by polling engine(s) and SNMP Trap service and controls the execution of actions on events (sending e-mails and running commands) through satellite processes (mgmail).

Net Inspector Performance Manager Engine – Performance Management module that is used as polling engine. It runs as a daemon/server application and continually polls devices via ICMP Ping, SNMP, VMware web service API, Microsoft WMI API and monitors the status of 19 well-known network services on managed devices, like

HTTP, SMTP, POP3, IMAP, SSH, FTP, NNTP, … to determine the status (up/down) of managed devices; measure network latency and packet loss and collect device performance parameters (CPU, memory, disk usage), status of processes running on managed computers and network interface statistics. This module supports monitoring the IP SLA metrics on Cisco routers and can also be configured to monitor arbitrary, vendor-specific SNMP parameters. In distributed configurations, this module can also receive SNMP Trap and Inform notification messages and pass them to remote Net Inspector Server. Additionally, this module itself triggers alarms if polled devices stop responding or if monitored parameters cross the threshold values (all alarms are passed further to Net Inspector Server). Performance manager module stores performance related data in the PM database (PostgreSQL).

In Net Inspector Enterprise Edition, more than one performance manager module can be employed to enable distributed network management and load balancing.

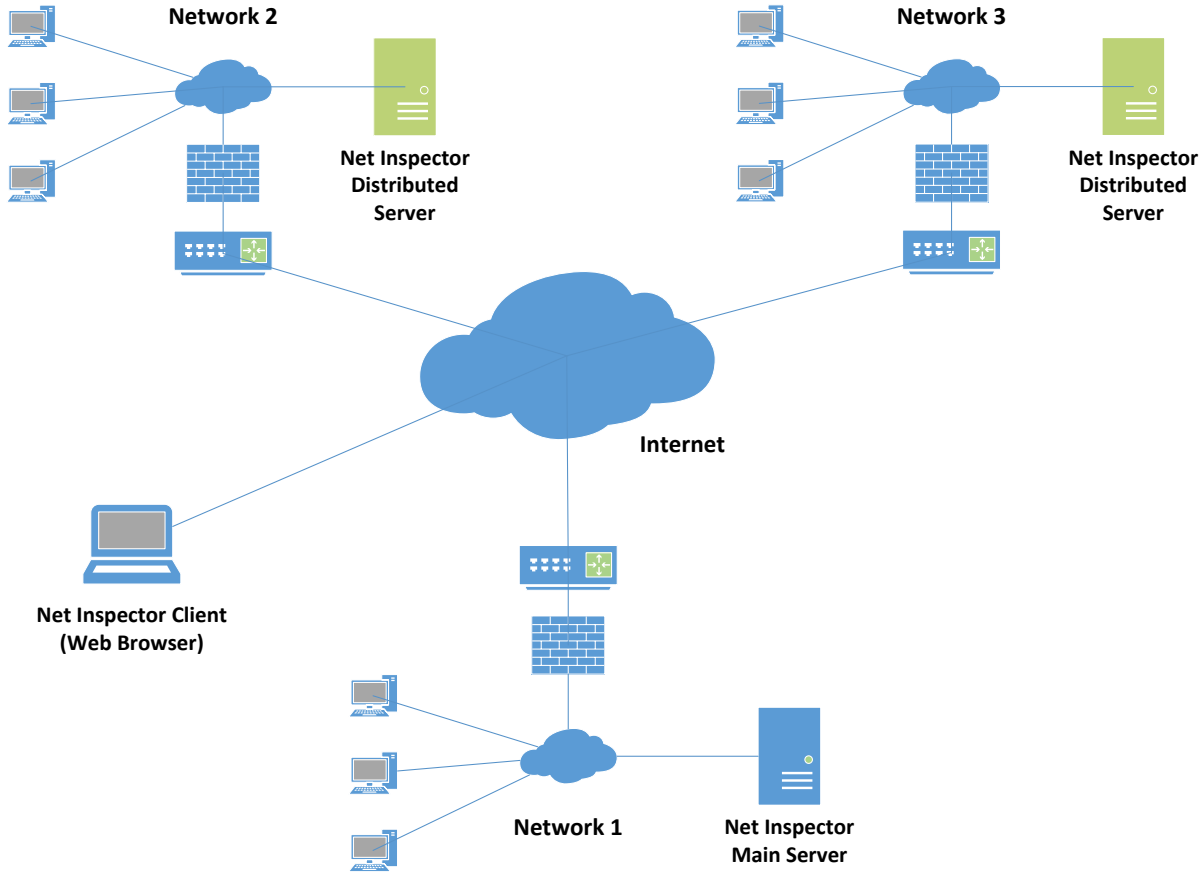
Net Inspector NetFlow Module – NetFlow/sFlow collector and analyzer daemon/service that receives NetFlow and sFlow packets exported from configured NetFlow sources and calculates IP traffic statistics identifying the applications that generate the most traffic (in packets and bytes), endpoints (IP addresses) that receive and send the most data, protocols that are used most, etc.

SNMP Trap Service - MG-SOFT SNMP Trap service that listens on configured ports (default: UDP 162) for incoming SNMP Trap and SNMP Inform notifications messages and passes them to Net Inspector Server (in simple setup) or Net Inspector Performance Manager Engine (in distributed setup), which converts and displays them as alarms.

Net Inspector Database – SQL relational database (PostgreSQL) that stores complete configuration, alarm data history and data collected by the Performance Manager engine and NetFlow module for all managed devices.

Net Inspector Client - Web-based graphical user interface running in a web browser. It lets you connect to the web server (IIS or Apache) on machine where Net Inspector Server is installed in order to view and manage alarms on managed devices, monitor the status and performance of managed devices, as well as configure Net Inspector Server. Recent versions of popular web browsers can be used for this purpose, e.g., Chrome, Firefox, MS IE or Edge, Safari, etc.

Example: Net Inspector Distributed Configuration using 3 Performance Manager Polling Engines (one on the main server, two on remote sites)



3.2 Different Setup Scenarios

3.2.1 Simple Setup – All Components Installed on One Computer

In the simple scenario, all server components are installed and run on the same computer.

For the step-by-step installation procedure that applies to this scenario, please refer to Installing Net Inspector on Windows section or Installing Net Inspector on Linux section, respectively.

3.2.2 Distributed Setup - Some Modules Installed on Remote Computers

MG-SOFT Net Inspector Enterprise Edition supports distributed network management, meaning that distributed modules (Performance Manager, NetFlow module, SNMP Trap service, Web server, database) can be installed and run on remote computers to enable distributed polling, distributed SNMP notification reception and distributed NetFlow and sFlow packet collection. This option also enables load balancing.

The distributed setup scenario involves installing the full Net Inspector package to one computer and Net Inspector distributed modules (additional Performance Manager, NetFlow and SNMP Trap module) to one or more remote computers and connecting those modules to Net Inspector Server, as described in the following sub-section.

Adding Additional Performance Manager Polling Engine and NetFlow Module for Linux to the System

1. Install Net Inspector distributed modules on a remote computer (please note down the computer's IP address). For detailed installation instructions, please refer to the section Installing Net Inspector on Linux section, Option 2: Installing Net Inspector distributed modules.
2. Run the following commands to update the necessary configuration files and connect a distributed Performance Manager polling engine to the main Net Inspector server:

   ```
   cd /usr/local/mg-soft/mgnetinspector/.data/
   ./mg_ni_configure_remote_pm.sh enable_remote IP.IP.IP.IP
   ```

   where `IP.IP.IP.IP` is the IP address of the main Net Inspector server.

3. Net Inspector installation package installs also MG-SOFT NetFlow engine together with Performance Manager and other components of the software. The NetFlow engine is configured to start automatically at system startup and to listen on TCP port 9991 for incoming NetFlow v5 and v9 and sFlow v5 packets.

   If you do not need the NetFlow/sFlow monitoring, you can disable it. To do this, set the NetFlow engine startup mode to off for all runlevels and stop the NetFlow service:

   ```
   chkconfig mgnetflowd off
   /etc/init.d/mgnetflowd stop
   ```

4. Performance Manager polling engine will try to establish a connection with the Net Inspector Server, as configured above.
5. To verify if the new polling engine has been successfully added to the system, use your web browser to login to Net Inspector server and view the new polling engine status in the header section of Net Inspector desktop, as shown the figure below:

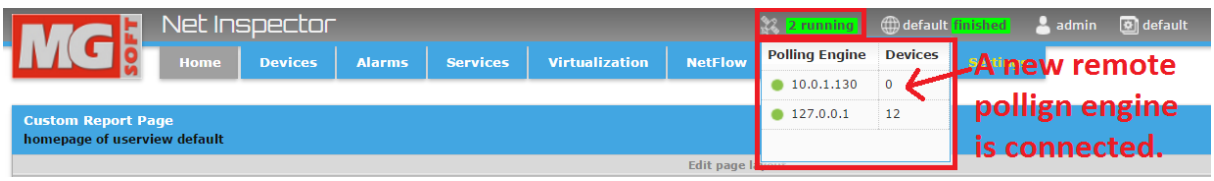


Figure 1: Viewing the status and assigned devices of a newly added polling engine

Assigning Performance Manager Polling Engine to Devices

After adding a new Performance Manager polling engine to the system, one needs to assign it to managed objects in order for the polling engine to start polling those devices and store collected results to the relevant instance of Performance Manager database.

To assign the new poling engine to one or more managed objects:

1. Select the ***Devices tab*** in the Net Inspector header (**1.** in Figure 2) to display the **Devices page** and click the ***Configure*** button (**2.** in Figure 2) in the upper right section of the Devices titlebar to switch into the **Configuration Mode**, as shown below.

Figure 2: Switching to Devices page, Configuration Mode

2. In the Devices page, Configuration Mode, locate the **Device Panel** tab on the right side of the desktop, select the desired devices (**1.**) in it and click the ***Edit Device Properties*** button in the Device Panel toolbar (**2.**), as shown in the figure below.

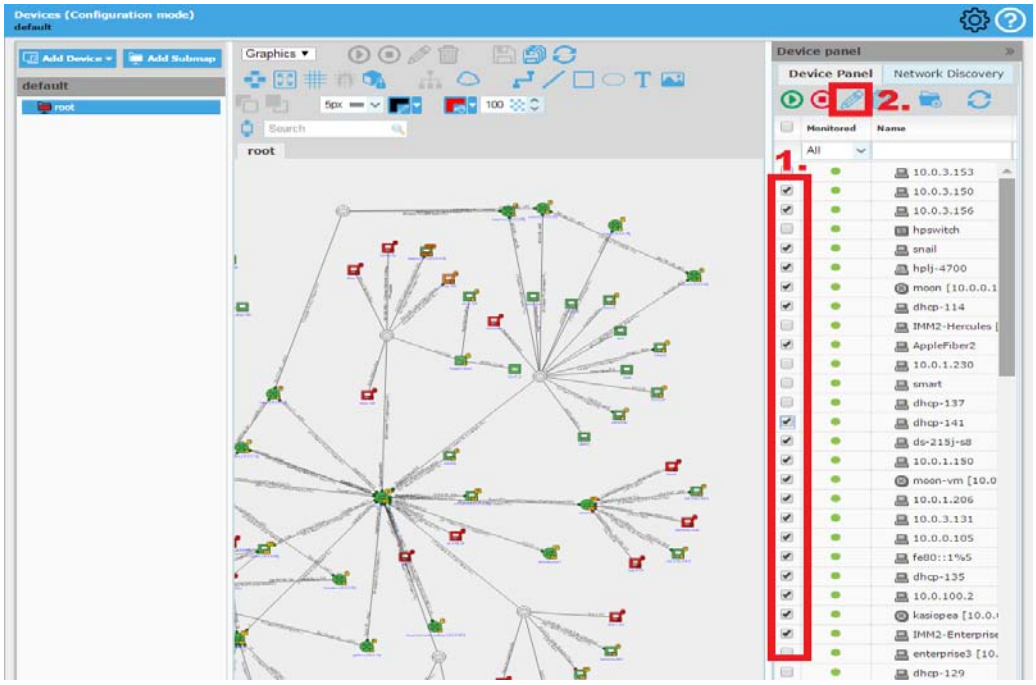


Figure 3: Selecting devices to assign new polling engine to

3. The **Device Monitoring Options** dialog box appears (Figure 4) that lets you set the polling engine for selected devices. Select the IP address of the new polling engine from the ***Polling engine*** drop-down list in the **Device Monitoring Options** dialog box and click the ***Apply*** and ***Close*** buttons.

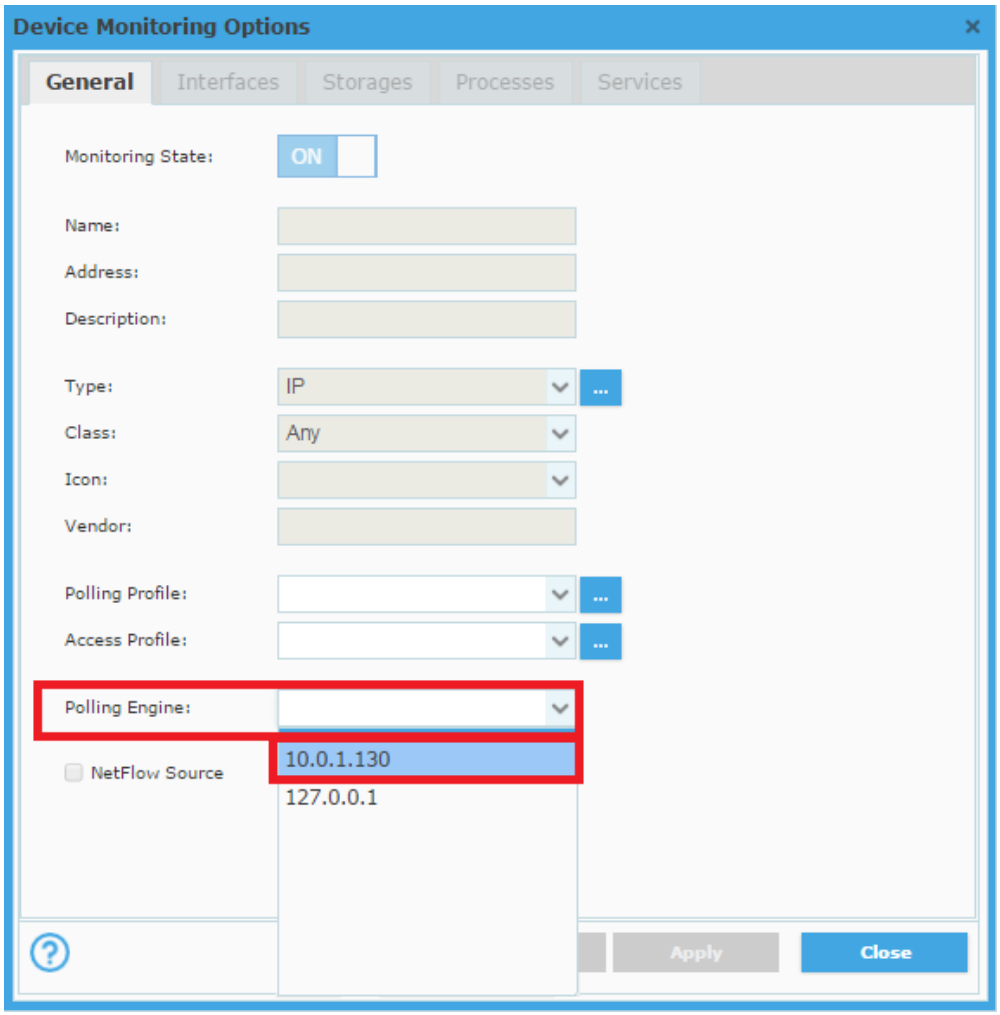


Figure 4: Assigning a new polling engine to multiple devices

4. From this moment on, the selected devices will be polled by the specified polling engine.

3.3 Linux System Integration Files

3.3.1 System (init.d) Startup Files

Service startup files	Description
`/etc/init.d/mgnipgd`	PostgreSQL service for MG-SOFT Net Inspector
`/etc/init.d/mgniengined`	MG-SOFT Net Inspector Server service
`/etc/init.d/mgperfmngd`	MG-SOFT Net Inspector Performance service
`/etc/init.d/mgnetflowd`	MG-SOFT Net Inspector NetFlow service
`/etc/init.d/mgtrapd`	MG-SOFT SNMP Trap Listening service (mgtrapd package)
`/etc/init.d/mgniwatchdogd`	MG-SOFT Net Inspector Daemon Watchdog service

3.3.2 Apache HTTPD Integration File

Integration files	Comment
`/etc/httpd/conf.d/mgnetinspector.conf`	Apache HTTPD PHP integration

3.4 Server TCP and UDP Listening Ports

MG-SOFT Net Inspector services listen on several ports that need to be open in the firewall where Net Inspector Server is running (for example, `firewalld` on Linux or `Windows Firewall` on Windows). In addition, Web server (HTTPS or HTTP) port needs to be open. The following are the default listening ports:

	Port	Protocol	Interface	Service	Comment
1	5223	TCP	all	`mgniengined`	MG-SOFT Net Inspector distributed modules connection listening port
2	5225	TCP	localhost	`mgnipostmaster`	PostgreSQL database connection listening port
3	162	UDP	all	`mgtrapd`	MG-SOFT SNMP Trap daemon listening port
4	9991	UDP	all	`mgnetflowd`	MG-SOFT Net Inspector NetFlow router flows listening port
5	80/443	TCP	all	`Web server (Apache)`	Web server listening port (443 - HTTPS, 80 - HTTP)

The MG-SOFT Net Inspector services ports are configured in the following configuration files:

	Port	INI File	INI File Section	Parameter Name
1	5223	niengine.ini pollingengine.ini	[connection] [net inspector]	extension_port port
2	5225	N/A	N/A	N/A
3	162	niengine.ini	[snmp notifications]	port, port1, port2, … portN
4	9991	N/A – configur. through Client	N/A	Settings/NetFlow/Ports

4 INSTALLING NET INSPECTOR ON WINDOWS

4.1 System Requirements

In order to install MG-SOFT Net Inspector 2017 for Windows (version 11.x), your computer needs to meet the following requirements:

Net Inspector Edition	CPU (Intel x86_64)	Memory	Hard Disk[1]	OS (64 bit only)[2, 3]
Lite	Quad-Core @ 2.4 GHz	4 GB	>= 25 GB	Windows Server 2008 R2, Windows 7, Windows Server 2012, Windows 8.x, Windows 10, Windows Server 2016
WorkGroup	Quad-Core @ 2.4 GHz	8 GB	>= 50 GB	
Enterprise	Quad-Core @ 3 GHz	8 GB (16 GB recommended)	>= 100 GB[4]	

[1] Using an SSD disk improves the performance of the database and thus also the performance of Net Inspector web-based user interface.

[2] Net Inspector 2017 is available only for 64-bit version of Windows (x64).

[3] Windows Server operating system is strongly recommended for using the WorkGroup and Enterprise Edition of Net Inspector

[4] At least 250 GB free disk space is required for the NetFlow database if the Net Inspector NetFlow module is used for actively collecting and analyzing NetFlow and/or sFlow packets.

Additional requirements:

- Administrative user privileges are required to install Net Inspector.
- IP address(es) of the host(s) running Net Inspector Server and polling engines should not change after the software has been installed.
- MS Internet Information Services (IIS), with enabled Web server (WWW services) and at least the following features (Figure 5):
  - Common HTTP features (Directory Browsing, HTTP Errors, Static Content),
  - Application Development features (ISAPI Extensions and (Fast)CGI)

  Please consult your Windows documentation for instructions on installing IIS.

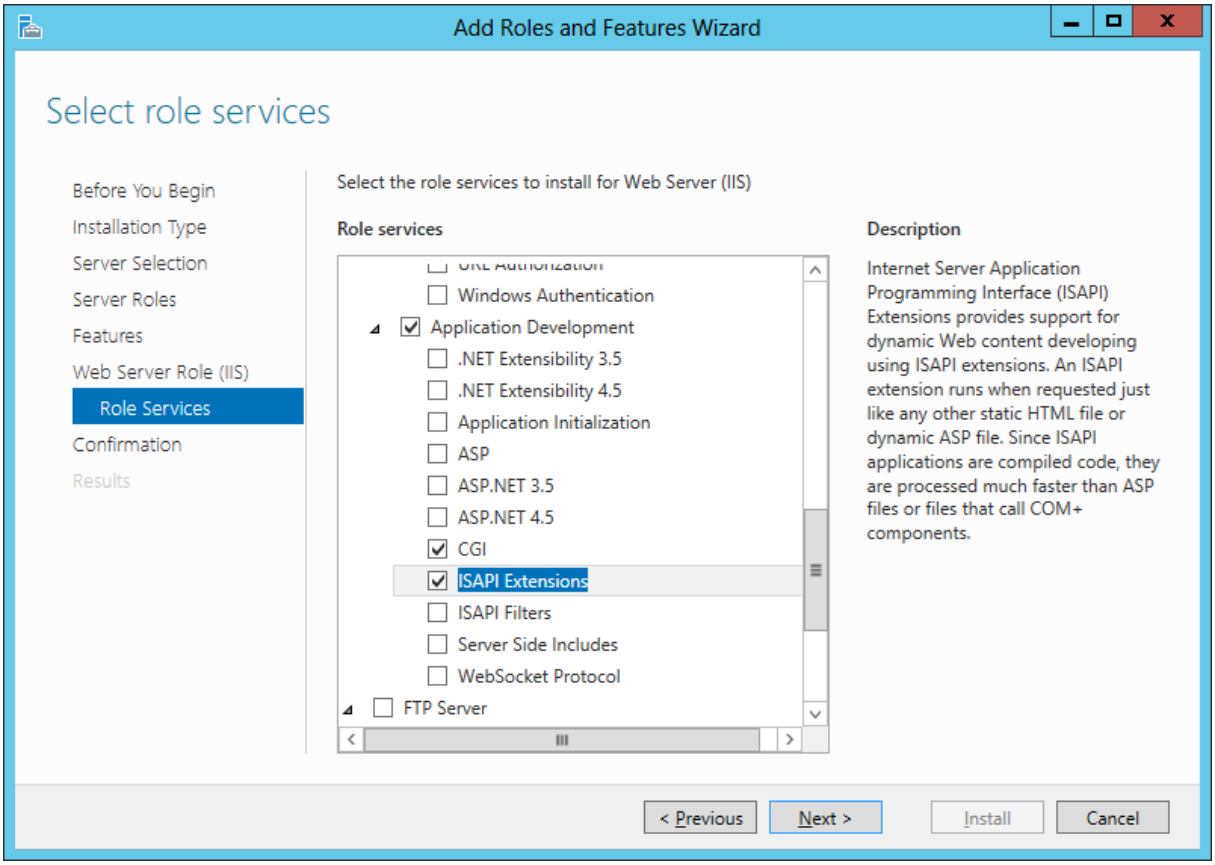


Figure 5: Example of installing the required IIS components (Windows Server 2012 R2)

- One of the following Web browsers for presenting Net Inspector web-based user interface: Chrome v65+ (recommended), Firefox v53+, Safari v10+, Edge v38+.
- Minimal screen resolution is 1280x1024 pixels (recommended 1920x1080 or higher).

4.2 Installing Net Inspector for Windows

Net Inspector 2017 is available only in 64-bit build (x64).

This section describes the procedure of creating a **fresh installation** of Net Inspector and the procedure of **upgrading previous version** of Net Inspector on Windows.

These procedures may be identical or different, depending on the version of Windows used and, in case of an upgrade, on whether the existing (old) machine meets the new system requirements or not.

4.2.1 Fresh Installation on Windows

Before installing the software, please make sure your computer and operating system meets the system requirements.

Note: This manual describes only those installation steps that are specific to the MG-SOFT Net Inspector installation procedure.

1. In Windows Explorer open the folder that contains MG-SOFT Net Inspector setup executable and double-click the **`setup-64.exe`** file to run the installer.

   Note: Administrative user privileges are required to install MG-SOFT Net Inspector.

2. MG-SOFT Net Inspector 2017 installer Welcome screen appears (Figure 6). The installer lets you install either all components of the package or only Net Inspector Performance Manager (and corresponding databases). Click the ***Next*** button at the bottom of the installation wizard screen to proceed with the installation and pass from one screen to another.

Figure 6: Net Inspector installer - Welcome screen

3. Net Inspector installer then verifies if all the required MS Internet Information Services (IIS) components are properly installed on the system. If one or more required IIS components are missing, the "Required IIS Components Not Installed" screen is displayed (Figure 7). Clock the ***Finish*** button to quit the installer without installing the Net Inspector software. Then, install the required IIS components and run the Net Inspector setup again.

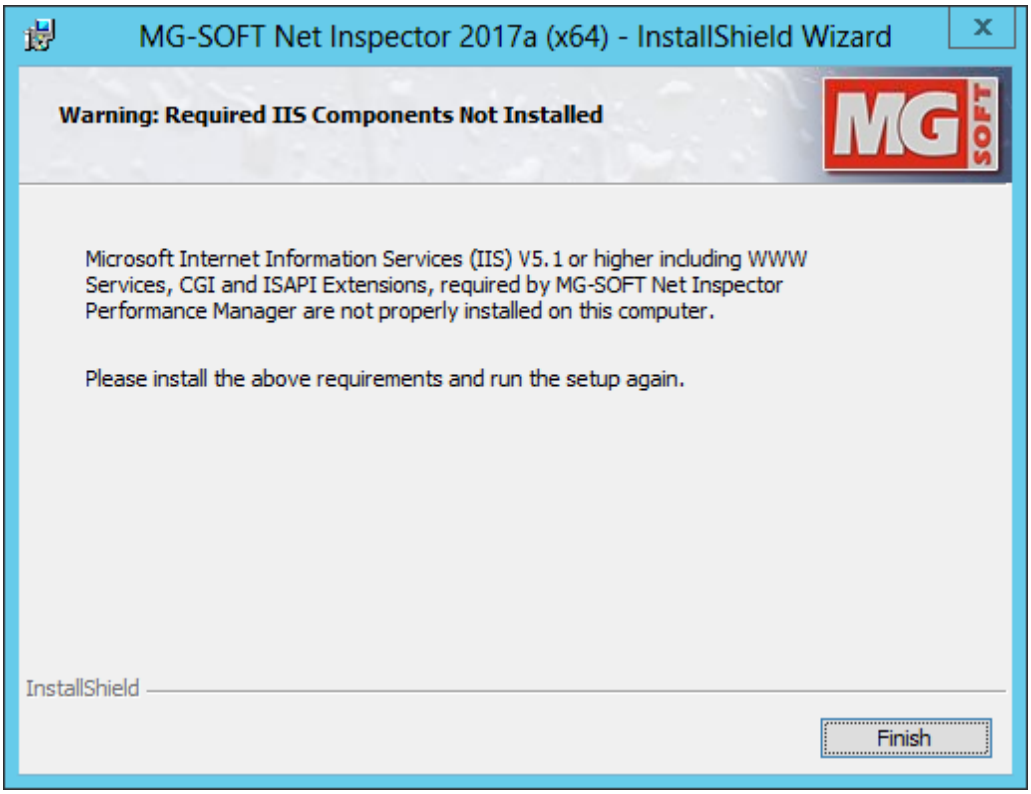


Figure 7: Net Inspector installer – missing IIS components screen

4. After passing the standard installation steps of accepting the license agreement, specifying the license key file location, providing the user information, and specifying the installation destination folder, the "Program Features" screen appears (Figure 8), where you can select which main components of the package will be installed:

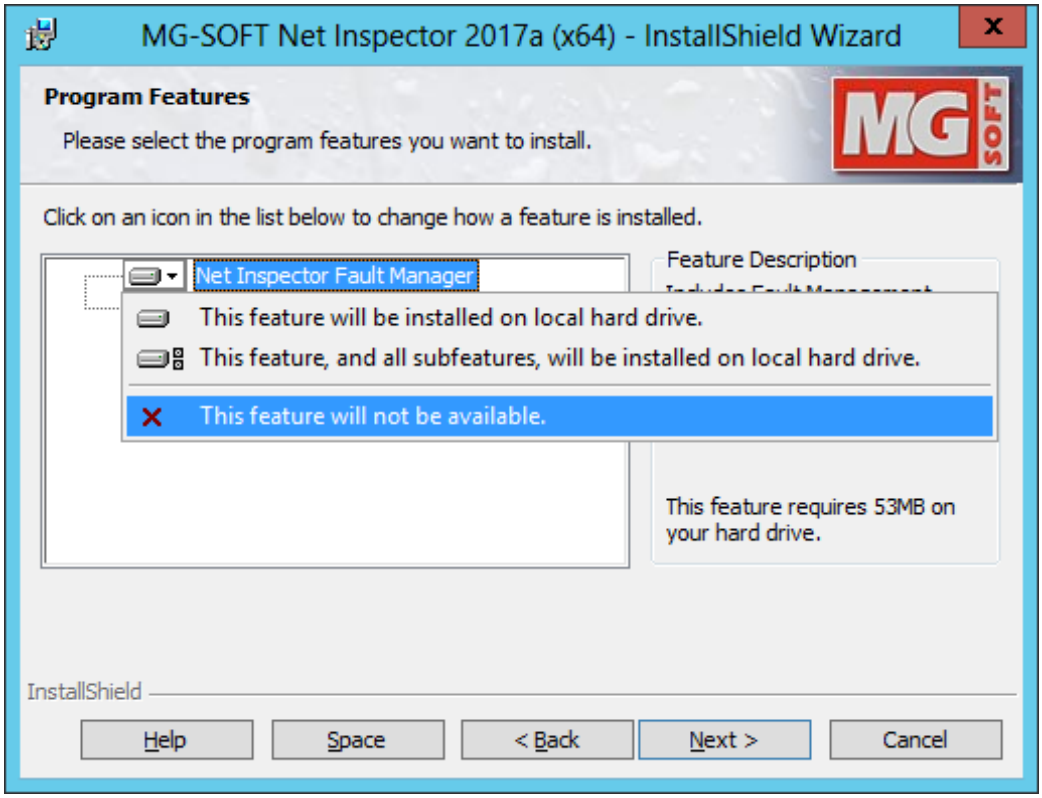


Figure 8: Net Inspector installer – Program Features screen

- Typical configuration (Fault and Performance Manager installed on the same host)

  To install all components of the package to the same computer, select both options in the Program Features screen and click the ***Next*** button. The installer continues as described in step 8 below.

- Distributed configuration (Performance Manager remote polling engines can be installed)

  To install only Net Inspector Performance Manager application to the local computer, select the corresponding option in the Program Features screen and deselect the other option (click the disk drive icon in front of the application's name and select the "This feature will not be available" entry from the drop-down menu). Then, click the ***Next*** button.

  - If you have selected to install only Net Inspector Performance Manager, the "Information About Remote Net Inspector Installation" screen appears (Figure 9). Into the ***IP address*** input line enter the IP address of the computer that runs or will run Net Inspector Fault Manager. If you specify this address now, the Performance Manager polling engine you are installing will automatically connect to the remote Net Inspector server and receive configuration from it. If you leave the ***IP address*** input line empty, you need to specify the relevant IP address later in the `pollingengine.ini` file. After Performance Manager installation finishes, run the setup again on a different computer to install Net Inspector Fault Manager.

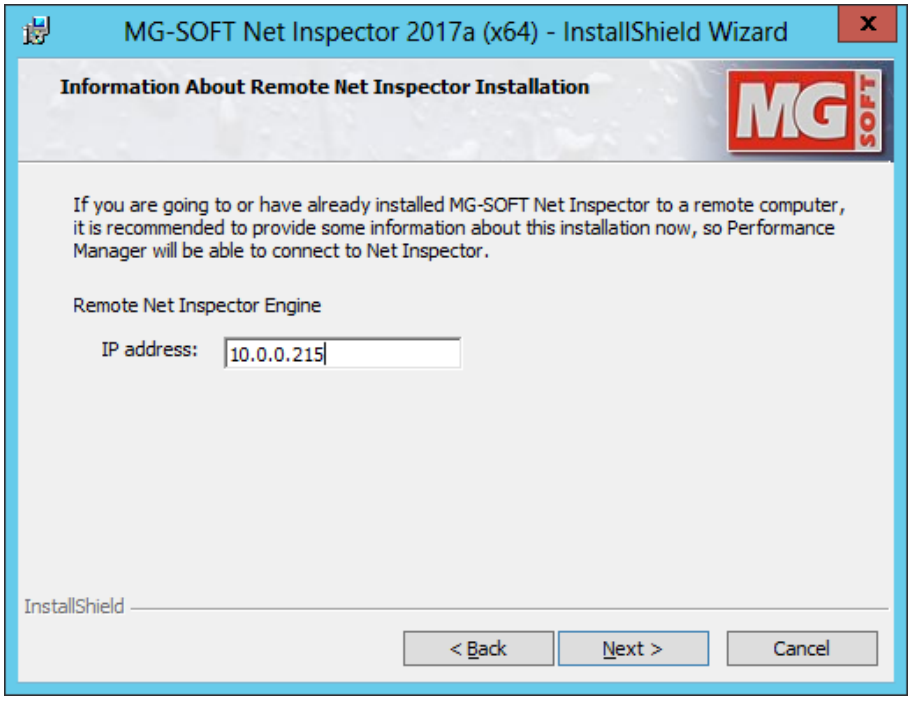


Figure 9: Net Inspector installer – entering the address of Net Inspector Server

5. Click the ***Next*** button to proceed to the "Ready to Install the Program" screen (Figure 10).

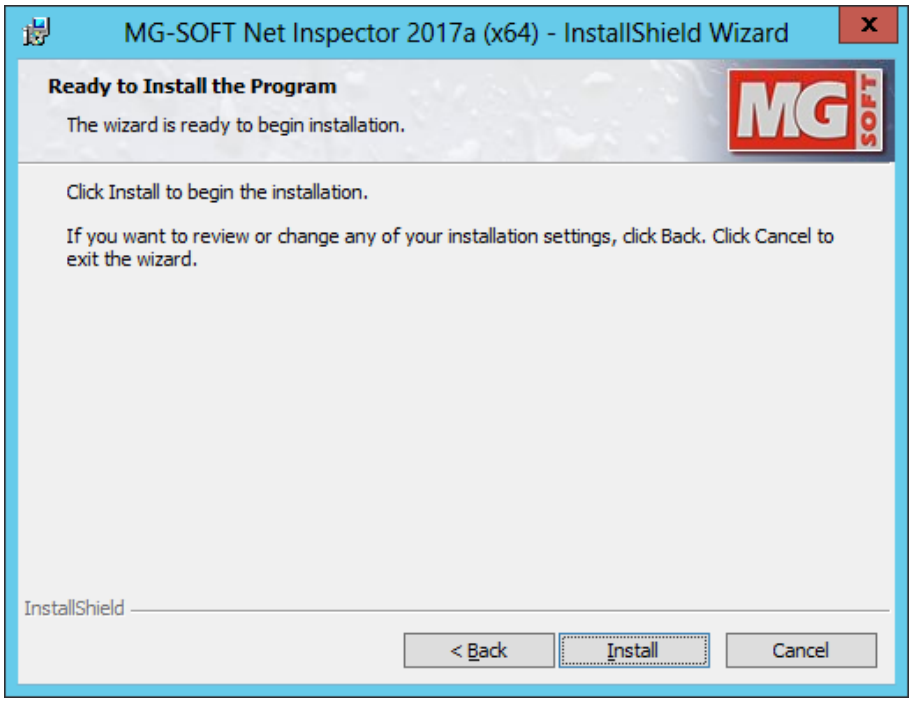


Figure 10: Net Inspector installer – Ready to Install screen

6. Click the ***Install*** button to install the software according to the settings specified in previous steps. If HTTPS is not configured in your IIS Web server, the HTTPS Configuration dialog appears (Figure 11).

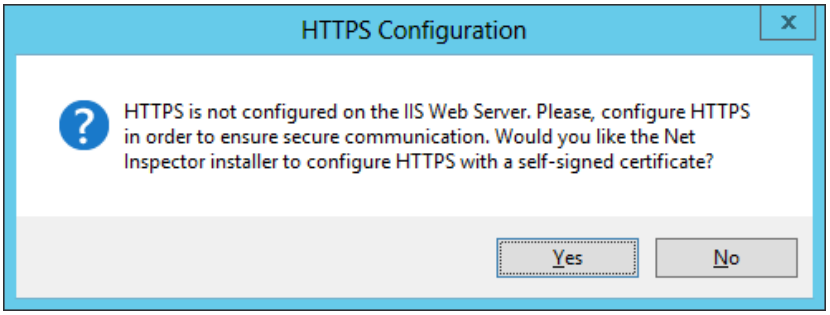


Figure 11: Net Inspector installer - HTTPS Configuration option

7. Click the ***Yes*** button if you want the Net Inspector installer to create a self-signed certificate and enable secure HTTPS protocol with this certificate on your IIS Web server. If you don't want the Net Inspector to configure HTTPS on your Web server, click the ***No*** button. After copying the required files and setting up necessary registry entries, the final screen of the Net Inspector Installation Wizard appears (Figure 12).

Figure 12: Net Inspector installer – final screen

8. Click the ***Finish*** button to end the Net Inspector Installation Wizard. If you check the ***Launch MG-SOFT Net Inspector*** checkbox, this operation also displays the Net Inspector Login page in the default Web browser application, which lets you log into the Net Inspector application.

Note 1: Please refer the **Net Inspector Online Help** in HTML format for more information on using Net Inspector.

Note 2: If you received a valid license key file after you had installed the software, you need to copy the `license.key` file to the Net Inspector's Bin folder (i.e., `C:\Program Files\MG-SOFT\Net Inspector 11\Bin`) and restart the MG-SOFT Net Inspector Server service in the Services window (***Start / Settings / Control Panel / Administrative Tools / Services***).

4.2.2 Upgrading From Previous Version on Windows

Net Inspector 2017 is available only in 64-bit build (x64).

The procedure of **upgrading from previous version of Net Inspector** depends on the version of Windows used and on whether the existing (old) machine meets the new system requirements or not:

On a machine that runs a supported **64-bit** version of Windows and meets other system requirements, the procedure of fresh installation and upgrade from previous version is identical - simply run the latest Net Inspector setup wizard to install or upgrade previous version to the latest one. During the upgrade, the data and configuration is automatically imported into the new version. For detailed instructions, please refer to the Fresh Installation on Windows section.

To upgrade from previous version of Net Inspector running on a **32-bit** version of Windows or on a computer that does not meet the new system requirements, a fresh installation is required with some additional steps in order to backup and import the old data and configuration into the new version of Net Inspector. The latter procedure is described below:

1. Create a backup of the workspace and databases in existing (old) version of Net Inspector, for example (run all commands with administrator privileges):

   ```
   cd "C:\Program Files\MG-SOFT\Net Inspector 10\Bin"
   mg_ni_backup -w -d -f C:\tmp\nibackup
   ```

   The above command creates a backup in the "date&time" subfolder of the above specified path, e.g.: `C:\tmp\nibackup\YYYY-MM-DD_HH-mm-ss`.

2. Create a fresh installation of Net Inspector 2017 on one of the supported 64-bit Windows operating systems.

3. Restore the workspace and databases from a backup using the new version of Net Inspector, for example:

   ```
   cd "C:\Program Files\MG-SOFT\Net Inspector 11\Bin"
   mg_ni_restore C:\tmp\nibackup\YYYY-MM-DD_HH-mm-ss
   ```

Note: In case of a distributed configuration (i.e., if you have one or more polling engines installed on remote machine(s)), perform the above steps on all machines involved.

5 INSTALLING NET INSPECTOR ON LINUX

5.1 System Requirements

In order to install MG-SOFT Net Inspector 2017 for Linux (version 11.x), your computer needs to meet the following requirements:

Net Inspector Edition	CPU (Intel x86_64)	Memory	Hard Disk[1]	OS (64 bit only)[2]
Lite	Quad-Core @ 2.4 GHz	4 GB	>= 25 GB	RHEL/CentOS 7 or higher Debian 8 or higher
WorkGroup	Quad-Core @ 2.4 GHz	8 GB	>= 50 GB	RHEL/CentOS 7 or higher Debian 8 or higher
Enterprise	Quad-Core @ 3 GHz	8 GB (16 GB recommended)	>= 100 GB[3]	RHEL/CentOS 7 or higher Debian 8 or higher

[1] The usage of SSD disk improves the performance of the database and thus also the performance of the Net Inspector web-based user interface.

[2] Net Inspector 2017 is available only in 64-bit build (for Intel x86_64 architecture).

[3] At least 250 GB free disk space on `/var/mg-soft/` is required for the NetFlow database if the Net Inspector NetFlow module is used for actively collecting and analyzing NetFlow and/or sFlow packets.

Additional requirements:

- Apache HTTP server (httpd) version 2.0 or greater
- PHP version 5.4 or greater (php, php-common, php-cli, php-pdo, php-pgsql)
- One of the following Web browsers for using Net Inspector web-based user interface: Chrome v65+ (recommended), Firefox v53+, Safari v10+, Edge v38+. Minimal screen resolution is 1280x1024 pixels (recommended 1920x1080 or higher).
- xterm
- en_US.UTF-8 locale
- Administrative (root) privileges are required to successfully install or update Net Inspector.

The procedure of installing Net Inspector on a Linux operating system includes several steps, as described in this section. Throughout this guide it is presumed that the contents of the Net Inspector installation tarball is accessible in the temporary directory `/install_niv11`. The entire installation procedure is carried out from this temporary directory. To create the temporary directory, execute the following command at a command prompt:

```
mkdir /install_niv11
```

5.2 Installing Net Inspector on RHEL 7 or CentOS 7

NOTE: Net Inspector requires the presence of **en_US.UTF-8 locale** in the system locale setting. If your locale does not include this item (run `locale -a | grep "en_US.utf8"` to check it), you can add it as follows:

Add the required locale by using the following command:

```
/usr/bin/localedef -c -f UTF-8 -i en_US en_US.UTF-8
```

5.2.1 Fresh Installation on RHEL/CentOS 7

A) Using Yum RPM Installer:

If you have access to the Internet, use the Yum RPM installer/updater facility to install the required modules (Apache, PHP, xterm). To do this, run the following commands with **root** user privileges in a terminal window:

1. Install required modules: Apache v2+, PHP v5.4+,..:

```
yum install httpd
yum install php
yum install php-pdo
yum install php-pgsql
yum install php-common
yum install php-cli
yum install xterm
```

2. Set the auto startup for Apache service for runlevels 2, 3, 4, 5:

```
/sbin/chkconfig --level 2345 httpd on
```

3. Change to temporary directory where Net Inspector v11 RPM packages are (e.g.: `cd /install_niv11`) and install MG-SOFT SNMP Trap service:

```
rpm -ivh mgtrapd-8.x-x.x86_64.rpm
```

Note: Net Inspector Enterprise Edition supports distributed setup that supports also distributed SNMP Trap collection. More specifically, remote Net Inspector Performance Manager modules can be configured to receive SNMP Trap and Inform notification messages and pass them to Net Inspector Server, which acts as a central station that displays all alarms. In such configuration, MG-SOFT SNMP Trap service needs to be installed on every computer that runs Net Inspector distributed modules.

4. **Install Net Inspector:**

Option 1: Install the complete package of Net Inspector v11.x

```
rpm -ivh mgNetInspector_2017-11.x-x.x86_64.rpm
```

Option 2: Install Net Inspector v11.x distributed modules

This option may be used if the main Net Inspector v11.x package is or will be installed on another computer (see the Distributed Setup section of this manual). To install Net Inspector distributed modules, install the Net Inspector RPM package as described above, and run the following commands to update the necessary configuration files and connect this instance of Performance Manager polling engine to the main Net Inspector server:

```
cd /usr/local/mg-soft/mgnetinspector/.data/
./mg_ni_configure_remote_pm.sh enable_remote IP.IP.IP.IP
```

where `IP.IP.IP.IP` is the IP address of the main Net Inspector server.

Note: After installing Net Inspector v11 distributed modules, you should assign this remote polling engine to some devices, as described in Assigning Performance Manager Polling Engine to Devices section.

Note: If **firewalld firewall** is running, Net Inspector installation script automatically opens the relevant TCP and UDP ports which Net Inspector services listen to.

5. Copy your `license.key` file to proper directories:

```
cp license.key /usr/local/mg-soft/mgtrapd/bin
cp license.key /usr/local/mg-soft/mgnetinspector/bin
```

6. Restart Net Inspector services to read the license key:

```
/usr/local/mg-soft/mgnetinspector/bin/mg_ni_restart_services.sh
```

7. Once the entire installation process is completed, you can delete the temporary directory from which you installed the software by issuing the following commands:

```
cd ..
rm –Rf /install_niv11
```

After successfully installing Net Inspector, you can launch a supported web browser application and enter the following URL into the URL/address input line to display the Net Inspector Login page:

```
https://IP.IP.IP.IP
```

where `IP.IP.IP.IP` is the IP address of the main Net Inspector server.

NOTE: If your web server does not support the secure HTTPS protocol, use HTTP protocol instead in the URL above. For instructions on enabling HTTPS, please refer to the section Enabling HTTPS with a Self-Signed Certificate (on RHEL/CentOS).

For detailed instructions, please refer to the Net Inspector Online Help (HTML).

Note: To be able to effectively monitor alarms on managed objects, you should configure the SNMP agents on managed devices to send SNMP notifications to Net Inspector Server. Otherwise, Net Inspector will not receive those notifications and consequently will not display and notify you about the corresponding alarms.

B) Manually Installing RPM Packages:

Instead of using the Yum updater/installer, you can install the required modules manually from the RHEL/CentOS DVD medium using the RPM Package Manager. This option requires no Internet connection. To do this, insert the RHEL7/CentOS DVD medium into the DVD drive, mount the DVD drive (e.g., `mount /dev/sr0 /media/dvdrom`) and use the following commands in a Terminal window to install all the required modules and MG-SOFT Net Inspector v11.x for Linux (root privileges are required):

1. Change current directory to directory with RPM modules on RHEL7 DVD:

> **Note:** Versions in RPM file names in the examples below are for **RHEL_7.2 x86_64 Server** DVD. For other RHEL 7 or CentOS 7 releases, please use the corresponding versions of RPM packages available in the used release.

```
cd /media/dvdrom/RHEL-7.2 Server.x86_64/Packages
```

2. Install Apache HTTP server v2.x and dependencies:

```
rpm -Uvh mailcap-2.1.41-2.el7.noarch.rpm
rpm -Uvh apr-1.4.8-3.el7.x86_64.rpm
rpm -Uvh apr-util-1.5.2-6.el7.x86_64.rpm
rpm -Uvh httpd-tools-2.4.6-40.el7.x86_64.rpm
rpm -Uvh httpd-2.4.6-40.el7.x86_64.rpm
```

3. Set the auto startup for httpd service for runlevels 2, 3, 4, 5:

```
/sbin/chkconfig --level 2345 httpd on
```

4. Install PHP v5.4+ and the required PHP components:

```
rpm -Uvh libzip-0.10.1-8.el7.x86_64.rpm
rpm -Uvh php-common-5.4.16-36.el7_1.x86_64.rpm
rpm -Uvh php-cli-5.4.16-36.el7_1.x86_64.rpm
rpm -Uvh php-5.4.16-36.el7_1.x86_64.rpm
rpm -Uvh t1lib-5.1.2-14.el7.x86_64.rpm
rpm -Uvh php-gd-5.4.16-36.el7_1.x86_64.rpm
rpm -Uvh php-pdo-5.4.16-36.el7_1.x86_64.rpm
rpm -Uvh postgresql-libs-9.2.13-1.el7_1.x86_64.rpm
rpm -Uvh php-pgsql-5.4.16-36.el7_1.x86_64.rpm
```

5. Change to temporary directory where the Net Inspector v11 RPM packages are (e.g.: `cd /install_niv11`) and install MG-SOFT SNMP Trap service:

```
rpm -ivh mgtrapd-8.x-x.x86_64.rpm
```

> **Note:** Net Inspector Enterprise Edition supports distributed setup that supports also distributed SNMP Trap collection. More specifically, remote Net Inspector Performance Manager modules can be configured to receive SNMP Trap and Inform notification messages and pass them to Net Inspector Server, which acts as a central station that displays all alarms. In such configuration, MG-SOFT SNMP Trap service needs to be installed on every computer that runs Net Inspector distributed modules.

6. **Install Net Inspector:**

Option 1: Install the complete package of Net Inspector v11.x

```
rpm -ivh mgNetInspector_2017-11.x-x.x86_64.rpm
```

Option 2: Install Net Inspector v11.x distributed modules

This option may be used if the main Net Inspector v11.x package is or will be installed on another computer (see the Distributed Setup section of this manual). To install Net Inspector distributed modules, install the Net Inspector RPM package as described above, and run the following commands to update the necessary configuration files and connect this instance of Performance Manager polling engine to the main Net Inspector server:

```
cd /usr/local/mg-soft/mgnetinspector/.data/
./mg_ni_configure_remote_pm.sh enable_remote IP.IP.IP.IP
```

where `IP.IP.IP.IP` is the IP address of the main Net Inspector server.

Note: After installing Net Inspector v11 distributed modules, you should assign this remote polling engine to some devices in order to poll them, as described in Assigning Performance Manager Polling Engine to Devices section.

Note: If **firewalld firewall** is running, Net Inspector installation script automatically opens the relevant TCP and UDP ports which Net Inspector services listen to. If needed, you can manually run the scripts to open ports in the local firewall (firewalld or iptables), as follows:

/usr/local/mg-soft/mgnetinspector/bin/mg_ni_iptables_open_ports.sh

/usr/local/mg-soft/mgnetinspector/bin/mg_ni_firewalld_open_ports.sh

7. Copy your `license.key` file to proper directories:

```
cp license.key /usr/local/mg-soft/mgtrapd/bin
cp license.key /usr/local/mg-soft/mgnetinspector/bin
```

8. Restart Net Inspector services to read the license key:

```
/usr/local/mg-soft/mgnetinspector/bin/mg_ni_restart_services.sh
```

9. Once the entire installation process is completed, you can delete the temporary directory from which you installed the software by issuing the following commands:

```
cd ..
rm –Rf /install_niv11
```

After successfully installing Net Inspector, you can launch a supported web browser application and enter the following URL into the URL/address input line to display the Net Inspector Login page:

```
https://IP.IP.IP.IP
```

where `IP.IP.IP.IP` is the IP address of the main Net Inspector server.

NOTE: If your web server does not support the secure HTTPS protocol, use HTTP protocol instead in the URL above. For instructions on enabling HTTPS, please refer to the section Enabling HTTPS with a Self-Signed Certificate (on RHEL/CentOS).

For detailed instructions, please refer to the Net Inspector Online Help (HTML).

Note: To be able to effectively monitor alarms on managed objects, you should configure the SNMP agents on managed devices to send SNMP notifications to Net Inspector Server. Otherwise, Net Inspector will not receive those notifications and consequently will not display and notify you about the corresponding alarms.

5.2.2 Upgrading From Previous Version on RHEL/CentOS

On Linux, a direct upgrade from previous versions of Net Inspector is **NOT** possible.

In order to use the latest version of Net Inspector and preserve the configuration and collected data from previous version, please proceed as follows:

10. Create a backup of the workspace and databases in existing (old) version of Net Inspector, for example (run all commands with root privileges):

```
cd /usr/local/mg-soft/mgnetinspector/bin
./mg_ni_backup.sh -w -d -f /root/nibackup.tar.gz
```

11. Create a fresh installation of Net Inspector 2017 on one of the supported 64-bit Linux distributions.

12. Restore the workspace and databases from a backup using the new version of Net Inspector, for example:

```
cd /usr/local/mg-soft/mgnetinspector/bin
./mg_ni_restore /root/nibackup.tar.gz
```

Note: In case of a distributed configuration (i.e., if you have one or more polling engines installed on remote machine(s)), perform the above steps on all machines involved.

5.2.3 Enabling HTTPS with a Self-Signed Certificate (on RHEL/CentOS)

It is highly recommended to have secure HTTPS protocol configured and enabled on the web server (Apache) hosting Net Inspector pages. HTTPS protocol enables web server authentication and encryption of communication between web browser and web server. If you wish to enable HTTPS with a self-signed certificate, you can run the bundled Net Inspector script that will help you generate a self-signed digital certificate (X.509) and configure local Apache web server to use it for HTTPS communication.

1. Install the prerequisite **mod_ssl** package with the following command:

```
yum install mod_ssl
```

2. To generate a certificate and enable HTTPS with it, run the following commands:

```
cd /usr/local/mg-soft/mgnetinspector/.data/
./mg_ni_configure_httpd_certificate_rhel.sh create_new
```

3. The script will prompt you to specify the certificate Distinguished Name details, like the Country, Locality, Organization, Common Name, etc. Make sure to enter the fully qualified domain name of the server or its IP address into the **Common Name** field, for example:

```
Country Name (2 letter code) [XX]:SI
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:Maribor
Organization Name (eg, company) [Default Company Ltd]:MG-SOFT
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname)[]:ni.mg-soft.si
Email Address []:nidmin@mg-soft.si

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Signature ok
subject=/C=SI/L=Maribor/O=MG-SOFT/OU=IT/CN=ni.mg-
soft.si/emailAddress=niadmin@mg-soft.si
Getting Private key
Stopping httpd service: httpd is inactive (dead)
Starting httpd service: httpd (pid=9760) is active (running)
```

4. After specifying the certificate Distinguished Name details, the script generates the digital certificate (with 10 years validity by default) and the corresponding private key, copies them to proper locations and restarts the Apache web server to read the new configuration and enable HTTPS with the given certificate.

> **Note:** After enabling the HTTPS with the above script, you will be able to connect to this web server by using HTTPS protocol, but will need to **add an exception** in your web browser to accept this self-signed certificate as trusted.

5.2.4 Uninstalling Net Inspector (RPM Package)

To uninstall Net Inspector for Linux (2013 or newer), first stop the Net Inspector services and uninstall the existing Net Inspector RPM package and MG-SOFT SNMP Trap daemon (if not needed by other MG-SOFT applications on the same computer).

1. Stop MG-SOFT Net Inspector services and MG-SOFT SNMP Trap daemon (mgtrapd), using the following commands:

```
/usr/local/mg-soft/mgnetinspector/bin/mg_ni_stop_services.sh
/etc/init.d/mgtrapd stop
```

2. Remove the existing Net Inspector installation by running the following command:

   ```
   rpm –e mgNetInspector_XXXX
   ```

   where XXXX is the version of Net Inspector, e.g. `2013`, `2014`, `2015`, or `2017`.

3. Uninstall the existing version of MG-SOFT SNMP Trap daemon (mgtrapd) <if not needed by other MG-SOFT applications on the same machine> by using the following command:

   ```
   rpm -e mgtrapd
   ```

5.3 Installing Net Inspector on Debian 8 or 9

NOTE: Net Inspector requires the presence of **en_US.UTF-8 locale** in the system locale setting. If your locale does not include this item (run `locale -a | grep "en_US.utf8"` to check it), you can add it as follows:

1. Edit the following file (using vi, nano, gedit, etc.): `/etc/locale.gen`
2. Add the following line to the file above: `en_US.UTF-8 UTF-8`
3. Run this command to generate new locale: `/usr/sbin/locale-gen`

5.3.1 Fresh Installation on Debian 8

Use the **apt-get** installer/updater facility to install the required modules (Apache, PHP, sudo, xterm, etc.). To do this, run the following commands with **root** user privileges in a terminal window:

1. Install required modules: Apache v2+, PHP v5.4+,..:

   ```
   apt-get install sudo
   apt-get install apache2
   apt-get install php5
   apt-get install php5-common
   apt-get install libapache2-mod-php5
   apt-get install php5-cli
   apt-get install php5-pgsql
   apt-get install php5-gd
   apt-get install php5-curl
   apt-get install xterm
   ```

2. Change to temporary directory where Net Inspector v11 DEB packages are (e.g.: `cd /install_niv11`) and install MG-SOFT SNMP Trap service:

```
dpkg -i mgtrapd_8.x-x_x86_64.deb
```

Note: Net Inspector Enterprise Edition supports distributed setup that supports also distributed SNMP Trap collection. More specifically, remote Net Inspector Performance Manager modules can be configured to receive SNMP Trap and Inform notification messages and pass them to Net Inspector Server, which acts as a central station that displays all alarms. In such configuration, MG-SOFT SNMP Trap service needs to be installed on every computer that runs Net Inspector distributed modules.

3. **Install Net Inspector:**

Option 1: Install the complete package of Net Inspector v11.x

```
dpkg -i mgNetInspector-2017_11.x-x_x86_64.deb
```

Option 2: Install Net Inspector v11.x distributed modules

This option may be used if the main Net Inspector v11.x package is or will be installed on another computer (see the Distributed Setup section of this manual). To install Net Inspector distributed modules, install the Net Inspector DEB package as described above, and run the following commands to update the necessary configuration files and connect this instance of Performance Manager polling engine to the main Net Inspector server:

```
cd /usr/local/mg-soft/mgnetinspector/.data/
./mg_ni_configure_remote_pm.sh enable_remote IP.IP.IP.IP
```

where `IP.IP.IP.IP` is the IP address of the main Net Inspector server.

Note: After installing Net Inspector v11 distributed modules, you should assign this remote polling engine to some devices, as described in Assigning Performance Manager Polling Engine to Devices section.

Note: If **iptables** firewall is running, Net Inspector installation script automatically opens the relevant TCP and UDP ports which Net Inspector services listen to.

4. Copy your `license.key` file to proper directories:

```
cp license.key /usr/local/mg-soft/mgtrapd/bin
cp license.key /usr/local/mg-soft/mgnetinspector/bin
```

5. Restart Net Inspector services to read the license key:

```
/usr/local/mg-soft/mgnetinspector/bin/mg_ni_restart_services.sh
```

6. Once the entire installation process is completed, you can delete the temporary directory from which you installed the software by issuing the following commands:

```
cd ..
rm –Rf /install_niv11
```

After successfully installing Net Inspector, you can launch a supported web browser application and enter the following URL into the URL/address input line to display the Net Inspector Login page:

```
https://IP.IP.IP.IP
```

where `IP.IP.IP.IP` is the IP address of the main Net Inspector server.

NOTE: If your web server does not support the secure HTTPS protocol, use HTTP protocol instead in the URL above. For instructions on enabling HTTPS, please refer to the section Enabling HTTPS with a Self-Signed Certificate (on Debian).

For detailed instructions, please refer to the Net Inspector Online Help (HTML).

Note: To be able to effectively monitor alarms on managed objects, you need to configure the SNMP agents on managed devices to send SNMP notifications to Net Inspector Server. Otherwise, Net Inspector will not receive those notifications and consequently will not display and notify you about the corresponding alarms.

5.3.2 Fresh Installation on Debian 9

Use the **apt-get** installer/updater facility to install the required modules (Apache, PHP, sudo, xterm, etc.). To do this, run the following commands with **root** user privileges in a terminal window:

7. Install required modules: Apache v2+, PHP v7+,..:

```
apt-get install sudo
apt-get install apache2
apt-get install php7.0
apt-get install libapache2-mod-php7.0
apt-get install php7.0-common
apt-get install php7.0-cli
apt-get install php7.0-pgsql
apt-get install php7.0-gd
apt-get install libxml2
apt-get install php7.0-xml
apt-get install xterm
apt-get install php7.0-curl
```

8. Change to temporary directory where Net Inspector v11 DEB packages are (e.g.: `cd /install_niv11`) and install MG-SOFT SNMP Trap service:

```
dpkg -i mgtrapd_8.x-x_x86_64.deb
```

Note: Net Inspector Enterprise Edition supports distributed setup that supports also distributed SNMP Trap collection. More specifically, remote Net Inspector Performance Manager modules can be configured to receive SNMP Trap and Inform notification messages and pass them to Net Inspector Server, which acts as a central station that displays all alarms. In such configuration, MG-SOFT SNMP Trap service needs to be installed on every computer that runs Net Inspector distributed modules.

9. **Install Net Inspector:**

   Option 1: Install the complete package of Net Inspector v11.x

   ```
   dpkg -i mgNetInspector-2017_11.x-x_x86_64.deb
   ```

   Option 2: Install Net Inspector v11.x distributed modules

   This option may be used if the main Net Inspector v11.x package is or will be installed on another computer (see the Distributed Setup section of this manual). To install Net Inspector distributed modules, install the Net Inspector DEB package as described above, and run the following commands to update the necessary configuration files and connect this instance of Performance Manager polling engine to the main Net Inspector server:

   ```
   cd /usr/local/mg-soft/mgnetinspector/.data/
   ./mg_ni_configure_remote_pm.sh enable_remote IP.IP.IP.IP
   ```

   where `IP.IP.IP.IP` is the IP address of the main Net Inspector server.

   Note: After installing Net Inspector v11 distributed modules, you should assign this remote polling engine to some devices, as described in Assigning Performance Manager Polling Engine to Devices section.

   Note: If **iptables** firewall is running, Net Inspector installation script automatically opens the relevant TCP and UDP ports which Net Inspector services listen to.

10. Copy your `license.key` file to proper directories:

    ```
    cp license.key /usr/local/mg-soft/mgtrapd/bin
    cp license.key /usr/local/mg-soft/mgnetinspector/bin
    ```

11. Restart Net Inspector services to read the license key:

    ```
    /usr/local/mg-soft/mgnetinspector/bin/mg_ni_restart_services.sh
    ```

12. Once the entire installation process is completed, you can delete the temporary directory from which you installed the software by issuing the following commands:

    ```
    cd ..
    rm –Rf /install_niv11
    ```

After successfully installing Net Inspector, you can launch a supported web browser application and enter the following URL into the URL/address input line to display the Net Inspector Login page:

```
https://IP.IP.IP.IP
```

where `IP.IP.IP.IP` is the IP address of the main Net Inspector server.

NOTE: If your web server does not support the secure HTTPS protocol, use HTTP protocol instead in the URL above. For instructions on enabling HTTPS, please refer to the section Enabling HTTPS with a Self-Signed Certificate (on Debian).

For detailed instructions, please refer to the Net Inspector Online Help (HTML).

> **Note:** To be able to effectively monitor alarms on managed objects, you need to configure the SNMP agents on managed devices to send SNMP notifications to Net Inspector Server. Otherwise, Net Inspector will not receive those notifications and consequently will not display and notify you about the corresponding alarms.

5.3.3 Enabling HTTPS with a Self-Signed Certificate (on Debian)

It is highly recommended to have secure HTTPS protocol configured and enabled on the web server (Apache) hosting Net Inspector pages. HTTPS protocol enables web server authentication and encryption of communication between web browser and web server. If you wish to enable HTTPS with a self-signed certificate, you can run the bundled Net Inspector script that will help you generate a self-signed digital certificate (X.509) and configure local Apache web server to use it for HTTPS communication.

1. Run the following prerequisite commands:

   Enable apache SSL module:
   ```
   sudo a2enmod ssl
   ```

   Enable SSL default site:
   ```
   sudo a2ensite default-ssl
   ```

2. To generate a certificate and enable HTTPS with it, run the following commands:
   ```
   cd /usr/local/mg-soft/mgnetinspector/.data/
   ./mg_ni_configure_apache2_certificate_deb.sh create_new
   ```

3. The script will prompt you to specify the certificate Distinguished Name details, like the Country, Locality, Organization, Common Name, etc. Make sure to enter the fully qualified domain name of the server or its IP address into the **Common Name** field, for example:
   ```
   Country Name (2 letter code) [XX]:SI
   State or Province Name (full name) []:
   Locality Name (eg, city) [Default City]:Maribor
   Organization Name (eg, company) [Default Company Ltd]:MG-SOFT
   Organizational Unit Name (eg, section) []:IT
   Common Name (eg, your name or your server's hostname)[]:ni.mg-soft.si
   Email Address []:nidmin@mg-soft.si

   Please enter the following 'extra' attributes
   to be sent with your certificate request
   A challenge password []:
   An optional company name []:
   Signature ok
   ```

```
subject=/C=SI/L=Maribor/O=MG-SOFT/OU=IT/CN=ni.mg-
soft.si/emailAddress=niadmin@mg-soft.si
Getting Private key
Stopping httpd service: httpd is inactive (dead)
Starting httpd service: httpd (pid=9760) is active (running)
```

4. After specifying the certificate Distinguished Name details, the script generates the digital certificate (with 10 years validity by default) and the corresponding private key, copies them to proper locations and restarts the Apache web server to read the new configuration and enable HTTPS with the given certificate.

> **Note:** After enabling the HTTPS with the above script, you will be able to connect to this web server by using HTTPS protocol, but will need to **add an exception** in your web browser to accept this self-signed certificate as trusted.

5.3.4 Uninstalling Net Inspector (DEB Package)

To uninstall Net Inspector for Linux (2017 or newer), first stop the Net Inspector services and uninstall the existing Net Inspector DEB package MG-SOFT SNMP Trap daemon package.

1. Stop MG-SOFT Net Inspector services and MG-SOFT SNMP Trap daemon (mgtrapd), using the following commands:

```
/usr/local/mg-soft/mgnetinspector/bin/mg_ni_stop_services.sh
/etc/init.d/mgtrapd stop
```

2. Remove the existing Net Inspector installation by running the following command:

```
dpkg -r mgNetInspector-XXXX
```

   where XXXX is the version of Net Inspector, e.g. `2013`, `2014`, `2015`, or `2017`.

3. Uninstall the existing version of MG-SOFT SNMP Trap daemon (mgtrapd) <if not needed by other MG-SOFT applications on the same machine> by using the following command:

```
dpkg -r mgtrapd
```

5.4 Starting and Stopping Net Inspector Server from Command Prompt

If you would like to configure any parameters in the Net Inspector Server initialization file or the Net Inspector Performance Manager initialization file, you first need to stop the Net Inspector Server daemon (`mgniengined`) or the Performance Manager daemon (`mgperfmngd`), respectively. Then, edit the configuration (.ini) file(s) and then start the corresponding daemons again, as described in this section.

You need the root user privileges to successfully start and stop Net Inspector Server from a command prompt (terminal).

- To stop the Net Inspector Performance Manager and Net Inspector Server daemon, run the following commands:

```
/etc/init.d/mgperfmngd stop
/etc/init.d/mgniengined stop
```

- To start the Net Inspector Server and Performance Manager daemon, run the following commands:

```
/etc/init.d/mgniengined start
/etc/init.d/mgperfmngd start
```

Note: If using Net Inspector in a clustered environment, you must start and stop Net Inspector Server from the cluster management software.

6 NET INSPECTOR SERVER INITIALIZATION FILE

Net Inspector Server initialization parameters are specified in the **niengine.ini** file. This initialization file should be located in the **workspace** directory. When Net Inspector Server starts up, it reads the initialization parameters from the niengine.ini file, and initializes itself accordingly. If the niengine.ini file is not present in the workspace directory, the default initialization parameters are used.

The Net Inspector Server initialization file (niengine.ini) is a plain ASCII file that can be edited in any text editor. It has the following format:

```
[section1]
; optional comment
parameter1 = value1
parameter2 = value2
parameter3 = value3

[section2]
; optional comment
parameter1 = value1
parameter2 = value2

...
```

The initialization file contains several sections. Every section contains one or more parameter. Not all sections of niengine.ini file are described here, only those sections that may be potentially edited by users are described below.

6.1 Section [log]

The [log] section contains parameters that control the Net Inspector Server logging behavior.

Net Inspector Server logs messages to the following log files located in the //**workspace**/log directory:

- niengine.log,
- niengine_action.log,
- niengine_stat.log,
- niengine_trap.log.

The system parameter controls what messages related to Net Inspector Server functioning are logged. Valid values are:

- debug – all messages are logged,

- `notice` – all normal (but relevant) messages, warning and error messages are logged,
- `warning` – only warning and error messages are logged,
- `error` – only error messages are logged.

The `system_size` parameter controls the size of the `niengine.log` file. The maximum value of this parameter is 2 GB, while the default value is 10 MB. The value of this parameter must be specified in bytes; for example, 10 MB (=10485760 bytes) needs to be entered as 10485760.

The `action` parameter controls the logging of Net Inspector Server actions. Valid values are:

- `admin` – all actions performed by the users with admin access rights are logged,
- `none` – actions are not logged.

The `default_size` parameter controls the size of the `niengine_action.log` and `niengine_stat.log` log files. The maximum and default value of this parameter is 2 MB. The value must be specified in bytes.

The `stat` parameter controls the logging of Net Inspector Server operating statistics. Valid values are:

- `all` – statistics on Net Inspector Server functioning is logged,
- `none` – statistics on Net Inspector Server functioning is not logged.

The `stat_interval` parameter value (in minutes) specifies the interval for statistics logging.

The `trap` parameter controls the logging of received SNMP notifications. Valid values are:

- `all` – all received SNMP notifications are logged,
- `none` – SNMP notifications are not logged.

The `trap_size` parameter controls the size of the `niengine_trap.log` file. The maximum value of this parameter is 2 GB, while the default value is 10 MB. The value must be specified in bytes.

The `trap_format` parameters specifies which details of SNMP notifications are logged and in what format. This is achieved by using the reserved words, which are:

```
$NOTIFICATION       The identity (name) of the SNMP notification
$TIME_STAMP         The notification's time stamp value
$AGENT_ADDRESS      The address of the notification sender
$V1AGENT_ADDRESS    The SNMPv1 agent address from the SNMPv1 Trap
$PROTOCOL           The SNMP protocol version of the notification
$ENTERPRISE         The enterprise associated with notification
$COMMUNITY          The SNMPv1/v2c community string
$TRANSPORT          The notification's transport protocol
```

```
$PORT               The UDP port of notification receiver
$VBCOUNT            The total number of variable bindings in the
                    notification
$VB(E)              Log E bindings. E can be individual bindings
                    from the variable bindings list (1,3,19),
                    ranges of bindings (3-6), or both (1,3-6,19).
$VBALL              Log all bindings
$SEC_USER_NAME      SNMPv3 security user name
$SEC_AUTH_PROTOCOL  SNMPv3 authentication protocol
$SEC_PRIV_PROTOCOL  SNMPv3 privacy protocol
$SEC_CONTEXT        SNMPv3 context name
```

Example:

```
[log]
; system log types are: debug, notice, warning, error
system = notice
system_size = 50000000
; action log types are: admin, none
action = admin
default_size = 1200000
; trap types are: all, none
trap = all
trap_size = 70000000
trap_format = $NOTIFICATION($PROTOCOL) $AGENT_ADDRESS $COMMUNITY
$VB(1-3)
; stat types are: all, none
stat = all
; interval is in minutes
stat_interval = 5
```

6.2 Section [snmp notifications]

The `[snmp notifications]` section controls the SNMP notification reception.

The `port` parameter specifies on which UDP port(s) Net Inspector Server listens to for incoming SNMP notifications. More than one port can be specified, using the following notation:

```
port = 162
port1 = 7000
...
portN = 8000
```

The `assign_to_object` parameter controls whether the received SNMP notification messages are assigned to managed objects or not.
Valid values of this parameter are `true` and `false`. If the value of this parameter is `true`, Net Inspector Server checks the address from which the generic SNMP notification has been sent and tries to assign the received SNMP notification to the

managed object with the same address. If the managed object with the matching address exists in Net inspector, its name is displayed in the “Source” field of the alarm or event that has been created from the notification. If the managed object with the matching address does not exist in Net inspector, the generic SNMP notification is either assigned to the `SNMP notification` system object or silently discarded, depending on the value of the `ignore_unassigned` parameter. If the value of this parameter is `false`, Net Inspector Server does not assign received SNMP notifications to managed objects. Whether notifications in this case will be discarded or converted to events/alarms and displayed depends on the value of the `ignore_unassigned` parameter.

The `ignore_unassigned` parameter controls whether the received SNMP notification messages that were not assigned to managed objects (because no such managed objects exist in Net Inspector or because the `assign_to_object` value is set to `false`) are ignored or not. Valid values are `true` and `false`.

The `unknown_to_alarm` parameter controls whether the “unknown” SNMP notifications are mapped to alarms and thus logged and displayed by Net Inspector or not. “Unknown” notifications are those SNMP notifications for which neither built-in nor user-defined trap-to-alarm rules exist in Net Inspector. Note that Net Inspector comes with a built-in set of rules for mapping the generic SNMP notifications (coldStart, warmStart, linkDown, linkUp, authenticationFailure, egpNeighborLoss) to alarms/events. Therefore, the generic SNMP notifications are “known” notifications. Additionally, users can define their own trap-to-alarm mapping rules for enterprise specific SNMP notifications and thus make those types of notifications “known” to Net Inspector.

The `unknown_to_event` parameters controls whether the “unknown” SNMP notifications are mapped to events or not. If the value of the `unknown_to_alarm` parameter is `true`, then the value of this parameter must also be `true`.

The `unknown_ignore_duplicate` parameters controls whether the duplicate “unknown” SNMP notifications are ignored or not. The default value is `true`, meaning that only the first “unknown” SNMP notification of a certain type, coming from a certain source, will be mapped to a new alarm and event (if the `unknown_to_alarm` parameter is `true`), while all subsequently sent “unknown” SNMP notifications of the same type (timestamps are ignored) and coming from the same source will not generate new alarms or events in Net Inspector.

The `check_community` parameter controls if the community names included in received SNMP notification messages should be compared with the trap community names configured for the managed objects the notifications are being assigned to. Valid values are `true` and `false`.

Example:

```
[snmp notifications]
port = 162
port1 = 7000
unknown_to_alarm = true
```

```
unknown_to_event = true
unknown_ignore_duplicate = true
assign_to_object = true
ignore_unassigned = false
check_community = false
```

7 NET INSPECTOR PERFORMANCE MANAGER INITIALIZATION FILE

Net Inspector Performance Manager initialization parameters are specified in the **`pollingengine.ini`** file. When Net Inspector Performance Manager Engine starts up, it reads the initialization parameters from the `pollingengine.ini` file, and initializes itself accordingly.

The `pollingengine.ini` is a plain ASCII file that can be edited in any text editor. Before editing the file, you need to stop the Net Inspector Performance Manager Engine service (in Linux use the `/etc/init.d/mgperfmngd stop` command).

The `pollingengine.ini` is located in the following directory:

In Linux:

`/var/mg-soft/mgnetinspector/mgperfmng`

In Windows:

`C:\ProgramData\MG-SOFT\Net Inspector\mgperfmng`

The initialization file contains several sections containing one or more parameters. Not all sections of the `pollingengine.ini` file are documented, only those sections that may be edited by users are described below.

7.1 Section [net inspector]

The `[net inspector]` section contains parameters used by Net Inspector Performance Manager Engine to connect to the Net Inspector Server Engine.

the `ipaddress` parameter specifies the IP address of the computer running Net Inspector Server.

The `port` parameter specifies the TCP port number on which Net Inspector Server listens to for incoming Performance Manager connections (by default: 5223).

The `local_ipaddress` parameter specifies the IP address that will be used by the Performance Manager Engine to connect to Net Inspector Server. This parameter needs to be configured only when running Performance Manager Engine in a high availability cluster in order to instruct both (all) instances of Performance Manager Engine to connect from the cluster's floating IP address (e.g., in case of a failover event). This parameter can also be used in non-clustered environments on computers that have two or more network interfaces or IP addresses assigned in order for the Performance Manager Engine to always use the specified IP address to connect to Net Inspector Server.

Example:

```
[net inspector]
ipaddress = 10.0.3.151
port = 5223
local_ipaddress = 10.0.0.123
```

7.2 Section [system]

The `[system]` section controls whether the Performance Manager Engine should receive SNMP notifications or not (if not, Net Inspector Server can receive them).

the `receive_traps` parameter specifies if Performance Manager should receive SNMP Trap and Inform notification messages or not. The default value in a simple installation (all components of Net Inspector installed on one computer) is `false`, while the default value in a distributed setup is `true`.

> **Note:** For Performance Manager Engine or Net Inspector Server to be able to receive SNMP Trap and Inform messages, MG-SOFT SNMP Trap service must be installed and running on the same computer. Net Inspector installer for Windows installs this service automatically, however, on Linux, you need to install it from a separate RPM package (`mgtrapd-x.x-x.AAA.rpm`), as described in the Installing Net Inspector on Linux section.

Example:

```
[system]
receive_traps = true
```

8 NET INSPECTOR NETFLOW MODULE KNOWN PORTS FILE

By default, Net Inspector NetFlow engine ignores the source and destination TCP and UDP ports above 1024 in collected flows and replaces those ports with the value 0 when storing flow records in the NetFlow database (to prevent excessive database growth). As a consequence, NetFlow Conversation Details web pages generated by Net Inspector Performance Manager show the “random high port” label for port numbers above 1024 (instead of displaying the actual port numbers). To enable storing and displaying source and destination TCP and UDP ports greater than 1024, one needs to edit the `known_ports.dat` file in the following location:

In Linux:

```
/var/mg-soft/mgnetinspector/mgnetflow/
```

In Windows:

```
C:\ProgramData\MG-SOFT\Net Inspector\mgnetflow
```

When Net Inspector NetFlow module starts up, it reads the `known_ports.dat` file and initializes itself accordingly. If this file is not present in the `above path`, the default behavior described above is applied.

The `known_ports.dat` is a plain ASCII file that can be edited in any text editor. It lists ports and port ranges above 1024 that are not ignored (each port or port range is specified in one line), as follows:

To name a port or a port range, use a colon (:) and specify the name of the port or port range as it will appear in the NetFlow reports (Top N Applications), e.g.;

```
9991: NetFlow Engine
5223-5225: Net Inspector
```

If the name is omitted, the port number will appear in the NetFlow reports instead.

Use '#' or ';' for comments.

Example of the `known_ports.dat` file contents:

```
5223: NI Ext       # MG-SOFT Net Inspector Server (listening for extensions)
16384-16386: XY    # Port range used by XY application
```

After editing the `known_ports.dat` file, apply the changes by restarting the NetFlow engine, as follows:

In Linux:

```
/etc/init.d/mgnetflowd restart
```

In Windows:

```
net stop “MG-SOFT Net Inspector NetFlow Manager”
net start “MG-SOFT Net Inspector NetFlow Manager”
```

9 NET INSPECTOR NETFLOW MODULE KNOWN URLS FILE

By default, when the Net Inspector NetFlow engine starts up, it reads the `known_urls.dat` file and resolves the domain names listed in this file to IP addresses and stores this information in the NetFlow database. The `known_urls.dat` file contains a list of domain names of the 200 world's most important Internet sites (e.g., google.com, youtube.com, etc.). By default, Net Inspector NetFlow Engine resolves each of these domain names to (a list of) IP addresses via DNS or NBNS in order to 'identify' and tag the IP addresses found in the received NetFlow packets more accurately and quickly with names (NetFlow reports generated by Net Inspector display the names of endpoints if possible). This behavior (resolving well known domains to IP addresses) is controlled by the `resolve_url_file` parameter in the `netflowengine.ini` file.

The `known_urls.dat` file is located in the following directory:

In Linux:

`/var/mg-soft/mgnetinspector/mgnetflow/`

In Windows:

`C:\ProgramData\MG-SOFT\Net Inspector\mgnetflow`

The `known_urls.dat` is a plain ASCII file that can be edited in any text editor.

10 BACK UP AND RESTORE NET INSPECTOR CONFIGURATION AND DATABASE

Net Inspector comes with the **mg_ni_backup** script that lets you create a backup copy of the entire Net Inspector configuration (i.e., workspace and related files) and optionally a backup copy of all Net Inspector databases (event, performance and NetFlow databases) and save it to a disk archive. The back up operation can be performed during runtime, i.e., while Net Inspector system is running.

Furthermore, the bundled **mg_ni_restore** script can restore the entire Net Inspector configuration and databases from a backup archive.

10.1 Back Up Procedure

The mg_ni_backup script supports several command line switches, as follows:

```
Usage: mg_ni_backup [-w][-d][-f path*/file.tar.gz][-s][-h][-?]

Options:
   -h      Show the usage
   -w      Archive Net Inspector workspace (configuration)
   -d      Archive Net Inspector database(s)
   -f      Save archive to user-specified path*
   -s      Silent mode
```

* The path may contain only US-ASCII characters and must follow the operating system rules for specifying a valid path.

The default backup archive location is:

Windows:

```
C:\ProgramData\MG-SOFT\Net Inspector\archive\date_time\
```

Note: date_time is the date and time of archive creation in YYYY-MM-DD_hh-mm-ss format

Linux:

```
/var/mg-soft/mgnetinspector/archive/mg_ni_archive_date_time.tar.gz
```

Note: date_time is the date and time of archive creation in YYYY-MM-DD_hh-mm-ss format

10.1.1 On Windows

Open a command prompt (CMD) window as administrator.

Change directory to the //Engine/bin, i.e.:

```
cd "C:\Program Files\MG-SOFT\Net Inspector 11\Bin"
```

Run the following command to back up the Net Inspector configuration (workspace) and databases to the default location:

```
mg_ni_backup –w –d
```

The above command creates a backup archive in the default folder (exact location depends on the Windows version used).

10.1.2 On Linux

Root user privileges are required.

Change directory to the //Engine/bin, i.e.:

```
cd /usr/local/mg-soft/mgnetinspector/bin
```

Run the following command to back up the Net Inspector configuration (workspace) and databases to the default location:

```
./mg_ni_backup.sh –w –d
```

The backup script creates a backup archive in the default folder. The archive is stored in a compressed tarball (.tar.gz) file. The archive files are named according to the following scheme:

`mg_ni_archive`	prefix indicating that this is a Net Inspector backup archive
`ws`	if present, the archive contains Net Inspector configuration files (workspace)
`db`	if present, the archive contains a backup of Net Inspector database(s)
`date_time`	the date and time of archive creation in YYYY-MM-DD_hh-mm-ss format

Example:

```
mg_ni_archive_ws_db_2017-05-16_15-01-35.tar.gz
```

Note that it is not necessary to stop Net Inspector services while creating a backup.

10.2 Restore Procedure

The **`mg_ni_restore`** script restores the Net Inspector configuration and databases (if present in the archive) from a backup archive.

```
Usage: mg_ni_restore [-s] [-h] path*/mg_ni_archive_file.tar.gz

Options:
-h      Show the usage
-s      Silent mode
```

* The path may contain only US-ASCII characters

The script stops all relevant Net Inspector services, restores the configuration and database(s) from the backup archive (if present in the archive), and restarts Net Inspector services.

10.2.1 On Windows

Open a command prompt (CMD) window as administrator.

Change directory to the //Engine/bin, i.e.:

```
cd "C:\Program Files\MG-SOFT\Net Inspector 11\Bin"
```

Example of a command that restores the Net Inspector configuration (workspace) and databases from a backup:

```
mg_ni_restore "C:\ProgramData\MG-SOFT\Net Inspector\archive\2017-05-16_15-01-35"
```

10.2.2 On Linux

Root user privileges are required.

Change directory to the //Engine/bin, i.e.:

```
cd /usr/local/mg-soft/mgnetinspector/bin
```

Example of a command that restores the Net Inspector configuration (workspace) and databases from a backup archive:

```
./mg_ni_restore.sh /var/mg-soft/mgnetinspector/archive/mg_ni_archive_ws
_db_2017-05-16_15-01-35.tar.gz
```

11 CONFIGURING SNMP NOTIFICATION DESTINATION ON SNMP AGENTS

To be able to discover devices based on SNMP Trap or Inform notifications received from them (using the auto configuration feature) and to effectively monitor alarms on managed objects with Net Inspector, you need to configure the SNMP agents on managed devices to send SNMP notifications to the computer (IP address) running Net Inspector Server (simple setup scenario) or a Net Inspector Performance Manager engine (distributed setup scenario). Otherwise, Net Inspector will not receive those notifications and consequently will not display and notify you about the corresponding alarms. For details on configuring SNMP agents on managed objects, kindly refer to user manuals of the relevant network elements.