NGMEDIA
innovation to the core

Quick Start

NG Media Server 6.1.6

Last updated: 2021.08.02

NG MEDIA

21 Avenue de Canteranne / F-33600 Pessac – France
Tel +33 5 56 21 55 51

www.n-g-media.com

NGMEDIA
innovation to the core

Contents

Installation

Linux

NG Media Server 6.1.6 supports the Ubuntu 20.04 LTS and 18.04 LTS Distributions.

You can install NG Media Server using a Debian Package (ngms-6.1.6-lin.deb) or using the installation program (ngms-6.1.6-lin.run). The Debian Package is the recommended method.

Debian Package installation

The reference Debian Package can be built using ngms-6.1.6-lin.run:

```
sudo ./ngms-6.1.6-lin.run -deb:path
```

Setting your login credentials:
Under /etc/ngms/config, open or create the file **general.json**, then set the AdministratorUsername and AdministratorPassword values (see below).

Minimal general.json file:

```
{
   "AdministratorUsername":"admin",
   "AdministratorPassword":"pass"
}
```

Warning: you must set your own username and password.

Installing NG Media Server:
Go in the folder containing the ngms-6.1.6-lin.deb package and run the following commands:

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get ./ngms-6.1.6-lin.deb
```

Running NG Media Server:
By default, NG Media Server is installed as a systemd service and will start automatically.

Installation Program

Setting your login credentials:
Under /etc/ngms/config, open or create the file **general.json**, then set the AdministratorUsername and AdministratorPassword values (see below).

Minimal general.json file:

```
{
   "AdministratorUsername":"admin",
   "AdministratorPassword":"pass"
}
```

Warning: you must set your own username and password.

Installing NG Media Server:
Go in the folder containing the ngms-6.1.6-lin.run program and run the following commands:

```
sudo chmod +x ngms-6.1.6-lin.run
sudo ./ngms-6.1.6-lin.run
```

Running NG Media Server:
By default, NG Media Server is installed as a systemd service and will start automatically.

Windows

NG Media Server ships with an installation program under Windows.

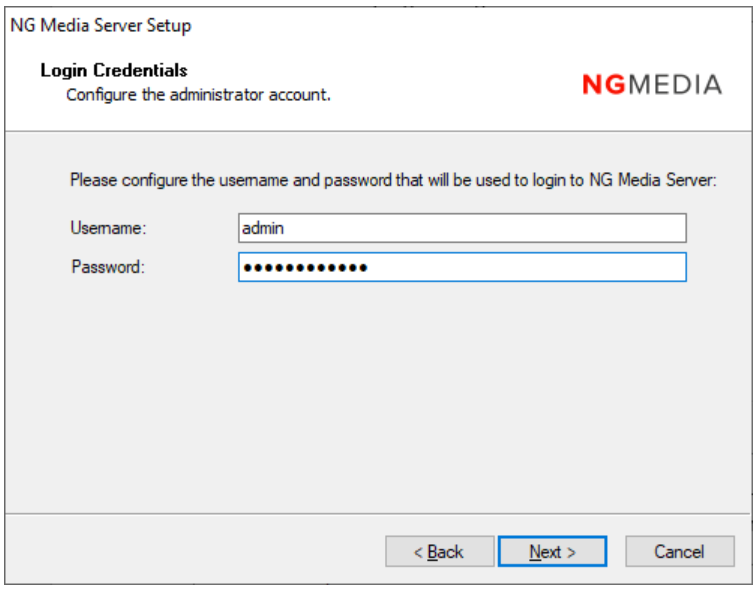
Installation Wizard

Installing NG Media Server

Run the installation program **ngms-xxx.exe** and follow the Installation Wizard.

Setting your login credentials:

During the installation, you will be prompted to configure your Login Credentials.
The Username and Password provided will be required to login to NG Media Server.



Running NG Media Server:

NG Media Server is installed as a Windows service and will start automatically.

Docker

NG Media Server 6.1.6 supports Docker 18.09 and higher.

You must install a Linux with the Docker feature installed.

The Linux distribution and version you are using to run Docker is not important because the NG Media Server Docker image will automatically install a container with an Ubuntu Server 20.04 LTS or 18.04 LTS.

The reference Docker image can be built using ngms-6.1.6-lin.run:

```
sudo ./ngms-6.1.6-lin.run -docker:path
```

The NG Media Server Docker image can be deployed as a container using one of the following network modes: host, macvlan, proxy. By default, we suggest using the host network mode.

Container Installation

Installing NG Media Server:

```
sudo docker load < ngms-6.1.6-lin-docker.tar.gz
```

Setting your login credentials:

Under /etc/ngms/config, open or create the file **general.json**, then set the AdministratorUsername and AdministratorPassword values (see above).

Minimal general.json file:

```
{
   "AdministratorUsername":"admin",
   "AdministratorPassword":"pass"
}
```

Warning: you must set your own username and password.

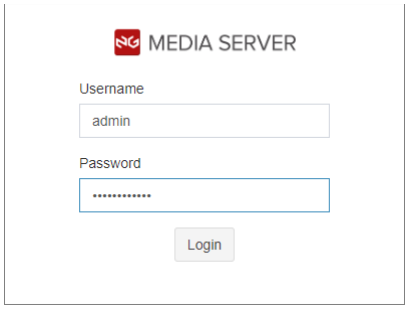
Running NG Media Server:

```
sudo docker run -d --network host --name ngms-container ngms
sudo docker attach ngms-container
```

Configuration

Log into NG Media Server

1. Start your preferred web Browser (Firefox, Chrome, Opera, Safari, Edge, Internet Explorer 11)
2. In the address bar, enter the following URL and press Enter:
   https://<ng-media-server-name>:5081/ngms
   where <ng-media-server-name> is the name or IP address of the server.
3. A security warning shows in the web browser. Click the appropriate action (see the HTTPS and Certificates section below).
4. The login page shows. Enter the **Username** and **Password** that you configured during the installation process and click on **Login**.



HTTPS and Certificates

NG Media Server uses Security Certificates (SSL) with HTTPS and other protocols (SIPS, …).

To be accessible using HTTPS, a self-signed certificate is generated by default by NG Media Server.

Your web browser will typically show a security warning when using a self-signed certificate.

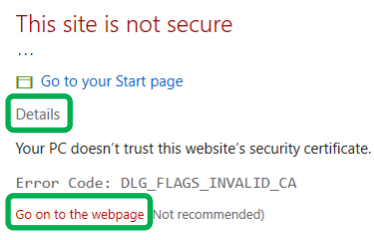
To proceed to NG Media Server:

- replace the self-signed certificate by a certificate signed by a trusted Certificate Authority, as described in section Certificates Replacement.
- or import the self-signed certificate in the **Trusted Root Certification Authorities** of your web browser.
- or simply select to continue to the website in your web browser, as in the following examples:

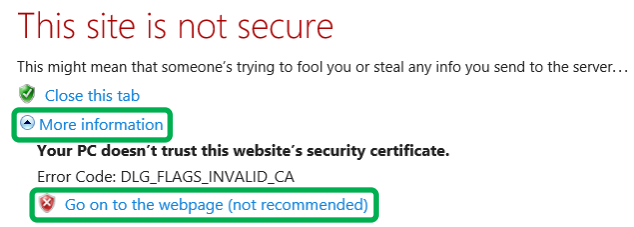
Mozilla Firefox: select **Advanced…**, then **Accept the Risk and Continue**

Google Chrome: select **Advanced** and then **Proceed to …**

Microsoft Edge: select **Details** and then **Go on to the webpage**

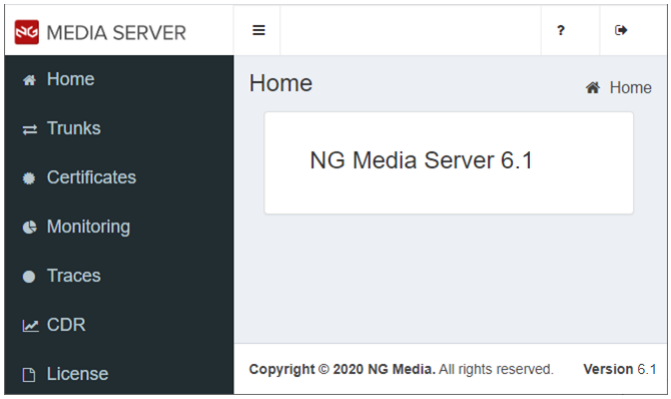


Microsoft Internet Explorer: select **More information** and then **Go on to the webpage**



Overview

From the **Menu** (left side), you get access to the different monitoring and configuration options of NG Media Server.

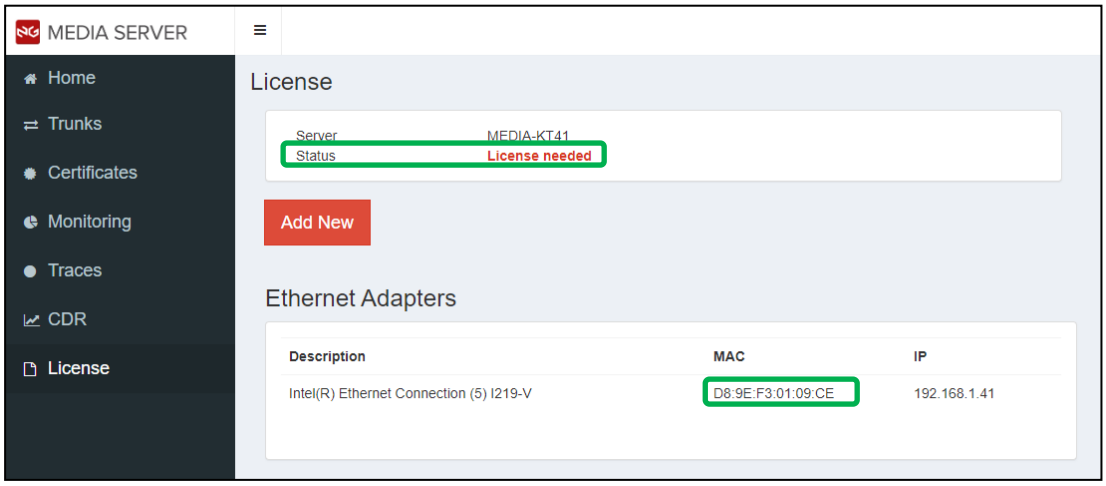


Menu	Description
Home	General information
Trunks	**Communication** services management (SIP Trunks, Media Profile, SIP Profile)
Certificates	SSL Security Certificates management (HTTPS and SIPS)
Monitoring	Statistics (Traffic, Disconnect Causes)
Traces	Traces (Display, Record to Disk)
CDR	Call Details Records
License	License (Display, Set, Upgrade)

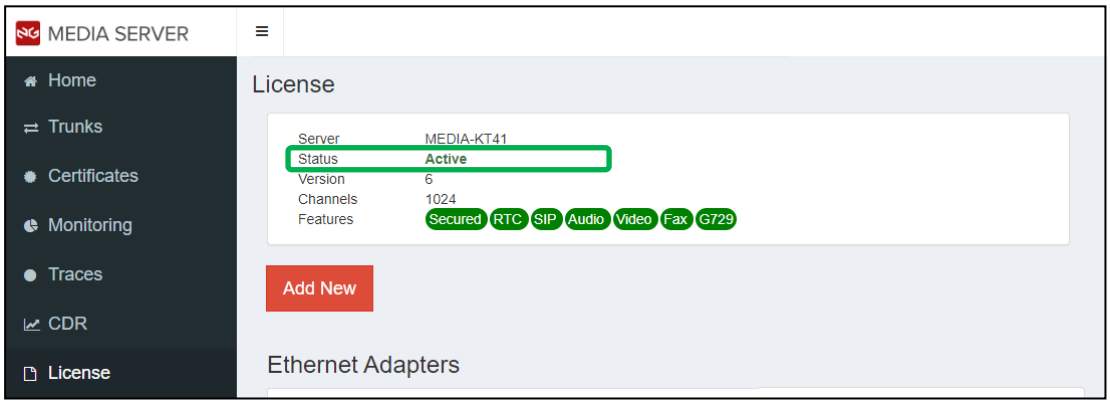
License

NG Media Server requires a valid license file in order to start communications.

To get a license file, go in the **License** page and collect the **MAC** address of your **Ethernet Adapter**, then provide this information to your NG Media Partner.



Once you received your license file, click on **Add License**, and then select your license file.



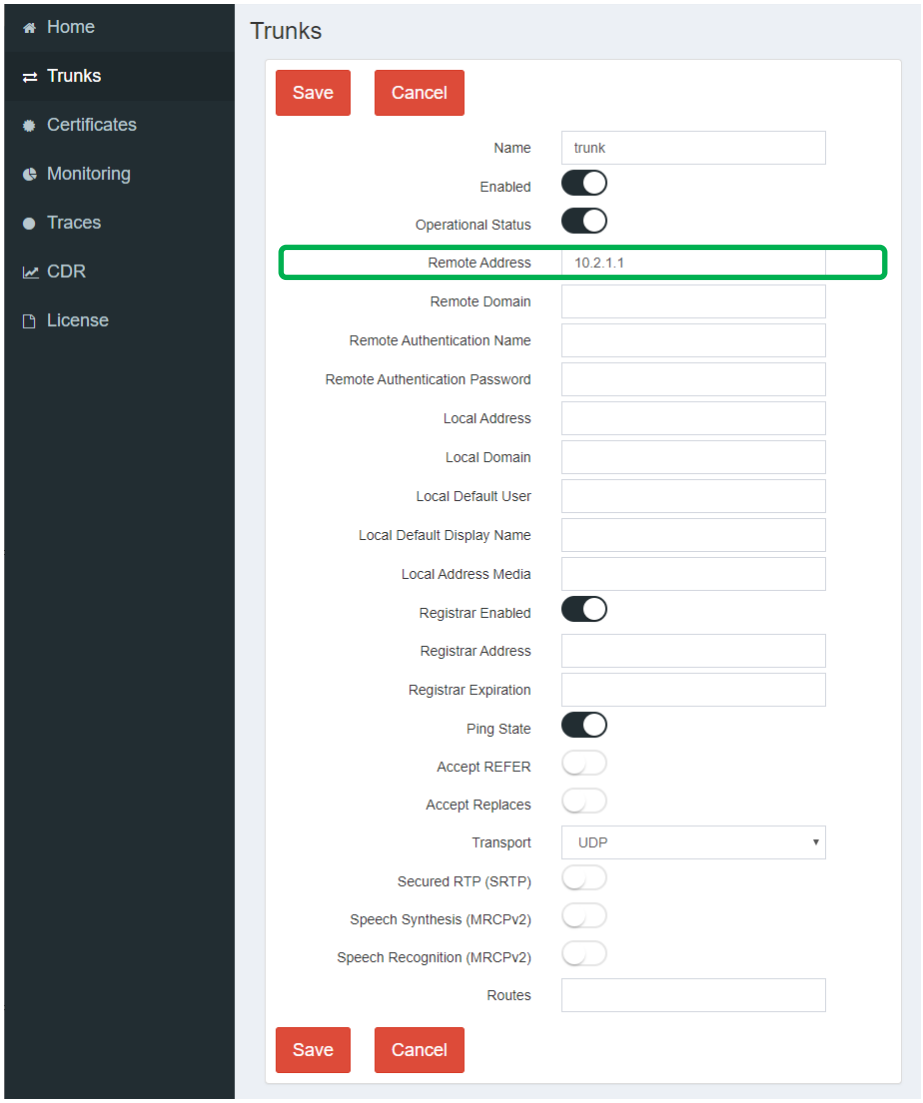
Trunks

To create a SIP trunk, go in the **Trunks** page and click on **Add New**.

Under **Remote Address**, enter the address (DNS or IP Address) of your SIP equipment or provider.

Additional configuration may be required according to your remote equipment.

Click on **Apply** to create your SIP trunk.

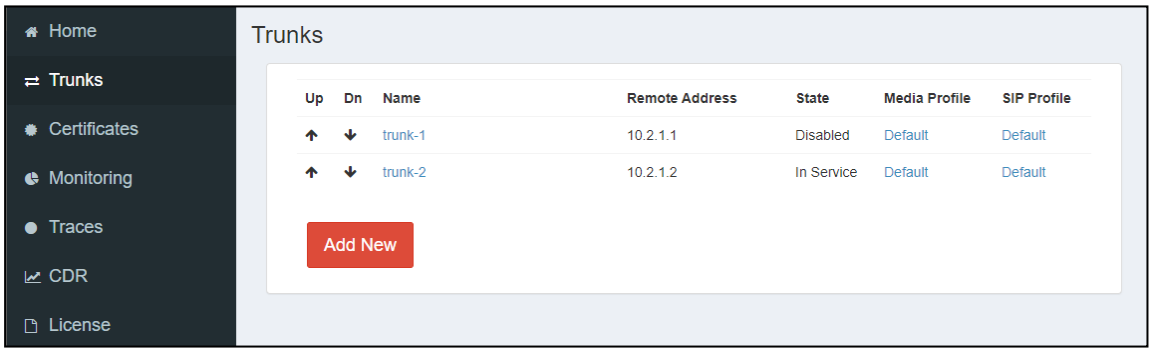


Name	Description
Name	Friendly name. Must be unique for each sip trunk.
Enabled	Enable this trunk. When disabled, no outgoing calls will be attempted on this trunk.
Operational Status	Define the operational status to return when receiving OPTIONS ping. When enabled, the remote will get a trunk status as in service. When disabled, the remote will get a trunk status as out of service.
Remote Address	Remote address of the trunk. **This information is required**. This can be a host domain name or one or more (.254) IP addresses space-separated. Failover is available when several IP addresses are configured (or returned by DNS). Each address can contain an optional port (column-separated, eg : "1.2.3.4:5060")
Remote domain	Remote domain of the trunk. When not provisioned, the RemoteAddress is used
Remote Authentication Name	Authentication name to use on this trunk. When registering a phone extension, this information is often the LocalUser.
Remote Authentication Password	Authentication password to use on this trunk
Local Address	Local address to use on this trunk. When not provisioned, the best local address matching the remote address is used.
Local Domain	Local domain of the trunk. When not provisioned, the LocalAddress is used
Local Default User	Default local user to use with Registration and when placing an outgoing Call. With telephony systems, the local user typically represents the phone number or extension, also known as CallerID. With system requiring an account (in the format [sip[s]:]user@domain), the local user represents the user part of the account. Application-provided CallerID overrides the default local user information.
Local Default Display Name	Default local display name to use in association with the LocalUser.
Local Address Media	Local address to use on this trunk for the Media (RTP / UDPTL). When not provisioned, the LocalAddress is used.
Registrar Enabled	Enable registration on this trunk. When disabled, no registration will be attempted on this trunk.
Registrar Address	Address where to register this trunk (or default local user). When not provisioned, the RemoteAddress is used.
Registrar Expiration	Registration duration as proposed to the registrar server When not provisioned, 1 hour (3600 seconds) is used.
Ping State	Enable OPTIONS ping, to automatically test the IP Addresses of the RemoteAddress
Accept REFER	Process REFER request received, as part of call transfer requested by the remote. **Warning:** This feature must be enabled only on trusted Trunks, as new outgoing calls can be initiated on remote request.
Accept Replaces	Process INVITE Replaces header received, as part of call transfer requested by the remote. **Warning:** This feature must be enabled only on trusted Trunks, as new incoming calls can replace the remote participant of an existing call.
Transport	Transport layer for outbound SIP transactions
Secured RTP (SRTP)	Enable Secure RTP (SRTP). When disabled, the Secured RTP (SRTP) setting of the Media Profile is used.
Speech Synthesis (MRCPv2)	Activate this option if this Trunk is used to connect to an MRCP Speech Synthesis server.
Speech recognition (MRCPv2)	Activate this option if this Trunk is used to connect to an MRCP Speech Recognition server.
Routes	Route pattern associated with this trunk. See section Route Pattern.

Configuration examples:

	SIP Trunk *Gateway at 10.2.1.1*	**SIP Extension** *Phone extension 2001*	**SIP Account** *Account bob@biloxi.com*
Remote Address	10.2.1.1 (Gateway Address)	10.2.1.1 (PBX Address)	biloxi.com (Service Address)
Remote Auth. Name	Your trunk login (if any)	Your extension login (typically 2001)	Your account login (typically bob)
Remote Auth. Password	Your trunk password (if any)	Your extension password	Your account password
Local Domain	Leave empty (Local Address)	10.2.1.1	biloxi.com
Local Default User	Default trunk CallerID (if needed)	2001	bob

The **Trunks** page displays all the available SIP trunks and their corresponding state.



When one or more trunks are created, access to the **Media Profile** and **SIP Profile** configuration is available, by clicking under **Default** under the column of interest.

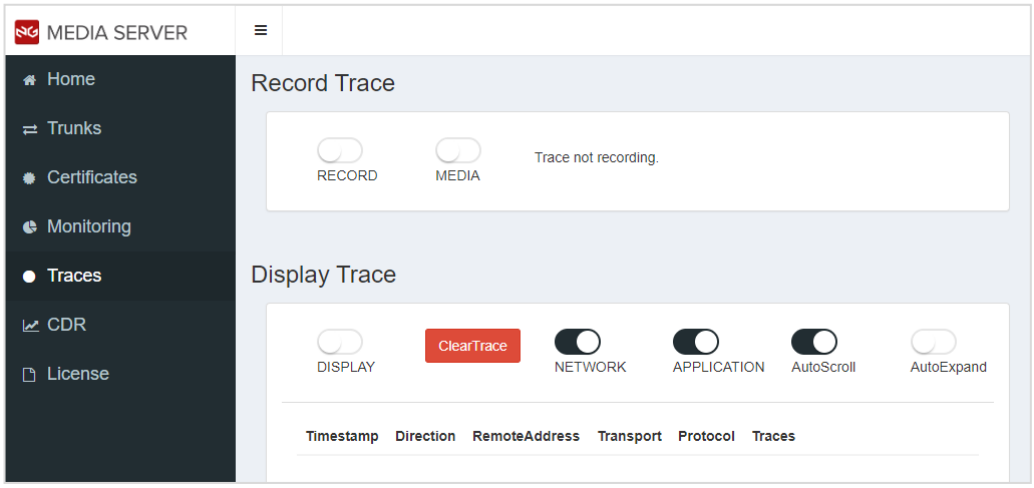
Traces

NG Media Server provides full traceability of all messages exchanged with Applications and Networks.

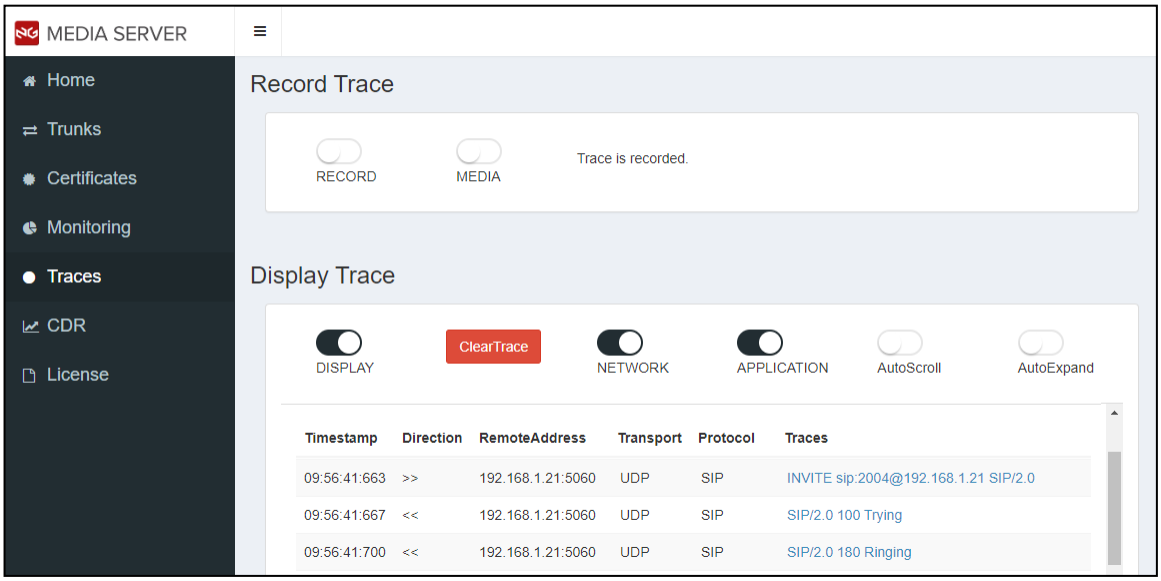
Traces can be displayed in real time, enabling quick diagnosis during low traffic.

Traces can also be recored to disk, enabling in depth analysis and diagnosis during high traffic.

To display and record traces, go in the **Traces** page.



To display the main messages exchanged, select **Display** in the **Display Trace** section.



The display will show the main messages exchanged, with colors helping to quickly locate potential issues.

By default, a summary of each trace is displayed. You can click on a trace to toggle between the display of the message summary and the full message.

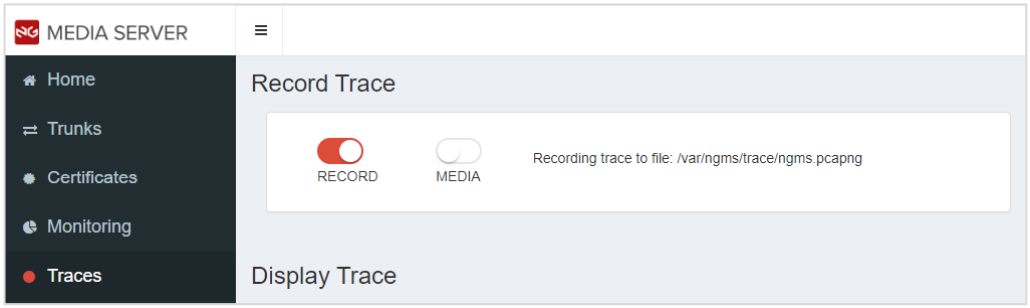
Network and **Application** enable to select which messages should be displayed. At least one option should be selected.

Filter	Shows
Network	Network signaling (WebRTC, SIP, ISDN, T30)
Application	API calls and notifications (NG Media Server UCS, CAPI, TAPI)

AutoScroll enables to control the automatic scrolling of traces. It is enabled by default. Clicking on a trace automatically disable the AutoScroll mode for convenience.

AutoExpand enables to select if new traces should display the message summary (collapsed messaged) or the full message (expanded message).

To record traces to disk, select **Record** in the **Record Trace** section.



The generated trace file **ngms.pcapng** is stored in the default trace folder:

OS	Default trace folder
Linux	/var/ngms/trace
Windows	C:\Program Files\NG Media Server\trace

Recording the media content (Audio, Video, Fax, Data) is typically unnecessary to diagnose most issues and should be avoided (see the Warning section below).
If you are instructed to record the media content, select **Media**.

Traces are recorded using the PCAPNG (PCAP Next Generation) file format.
This format is supported by most network packet analyzers tools, including **Wireshark**.

Warning: traces recorded to disk can consume a large amount of disk space, especially:

- with the Media option selected (throughput may be up to 40 kB per second per SIP call).
  You should avoid the Media option unless necessary.
- with High-Density productions (several hundred simultaneous calls).
  You should reproduce an issue and generate a trace outside of the production/peak hours.
- with small disk sizes (virtual machines are typically assigned reduced disk space).
  You may use higher disk size or pay attention to the time recorded.
- when recording for a long time (several hours or days).
  You should stop the trace once no more needed, or you should restart the trace frequently.

To analyze traces using **Wireshark**

Starting with NG Media Server 6, traces recorded by NG Media Server can be analyzed directly using **Wireshark**. You can download Wireshark from https://www.wireshark.org/.

To view secured network traffics in clear (UCS, …), API function calls (CAPI, TAPI, …) and extra logging info (CDR, Text, …), you will need to install the **NG Media Server dissector for Wireshark**.

What about capturing traces directly using Wireshark?!

Warning: generating traces using Wireshark is not recommended:

- traces captured by Wireshark will not enable to show in clear most secured protocols.
- traces captured by Wireshark will not include all usable information.
- traces captured by Wireshark may contain unrelated sensible network traffic.
- capturing traces using Wireshark may significantly degrade system performance

However, generating traces directly using Wireshark can be helpful to diagnose low level network issues, like with packet routing (ARP, ICMP, …), TCP connections and TLS handshake.

Indeed, whereas NG Media Server captures traffic on top of the UDP/TCP socket stacks (high level), Wireshark captures real Ethernet/IP/TCP/UDP packets (low level), so Wireshark captures real QoS (DSCP) tagging contents, real packet fragmentation, TCP packets retransmissions, sublayer protocols, …

Here is a comparison:

Feature	traces generated by **NG Media Server**	traces generated by **Wireshark**
Enable to View unsecured Network traffics	Yes	Yes
Enable to View secured Network traffics in clear	Yes	No (most of the time)
Enable to View API function calls (CAPI, TAPI, …)	Yes	No
Enable to View extra logging info (CDR, Text, …)	Yes	No
Capture NG Media Server traffic only	Yes	No (requires filtering)
Enable full support by NG Media Analyzer	Yes	Limited
Enable to Diagnose Low level network issues	Partially	Yes

Collecting traces during High-Density Production:

Generating traces may involve extra Disk and CPU consumption, especially with the Media option enabled. Recording traces under heavy activity should be performed only when necessary and with extra care.