

# Flowmon and Network Services

Flowmon is an appliance-based solution for network visibility, traffic monitoring, reporting, analysis and anomaly detection. Flowmon appliances provide and consume various network services to ensure maximal usability and benefits. To help configure network services, firewall rules or proxy servers properly we provide this summary of all network services that are being used by Flowmon.

<b>Flow Collection</b>	<b>1</b>
<b>User remote access</b>	<b>1</b>
<b>Flowmon APM</b>	<b>1</b>
<b>Flowmon Traffic Recorder</b>	<b>2</b>
<b>SNMP-based monitoring</b>	<b>2</b>
<b>Time synchronization</b>	<b>2</b>
<b>E-mails</b>	<b>2</b>
<b>Alerts</b>	<b>2</b>
<b>DNS</b>	<b>2</b>
<b>Flowmon Networks remote services portal</b>	<b>2</b>
<b>LDAP-based authentication</b>	<b>3</b>
<b>Distributed Architecture</b>	<b>3</b>
<b>Other network services</b>	<b>3</b>

## Flow Collection

Ensure that there are no firewall or ACL restrictions between flow sources (routers, Probes) and listening ports of Flowmon Collector. Default ports are UDP/2055 (NetFlow), UDP/3000 (NetFlow), UDP/9996 (NetFlow) and UDP/6343 (sFlow).

## User remote access

Flowmon provides HTTPS based web interface to access the system through a modern web browser. HTTP is redirected to HTTPS service. Ensure that TCP/443 is accessible. In addition to the web-based interface, Flowmon provides SSH console. Ensure that TCP/22 is accessible. Do not forget to change the default passwords and consider access restrictions by firewall or ACL.

## Flowmon APM

There are two TCP ports used for communication between APM collector and probe. TCP/20567 is used to send commands and TCP/20568 for data exchange.

## Flowmon Traffic Recorder

Both command and data channels between probes and collector are using TCP port range 7000-7999.

## SNMP-based monitoring

Flowmon includes standard SNMP monitoring through ports UDP/161 and UDP/162 and Zabbix client running on port TCP/10050. Both services might be disabled. We recommend changing the default SNMP community string when using SNMP monitoring.

## Time synchronization

For precise network traffic monitoring, it is necessary to ensure time synchronization using NTP service. Please ensure that Flowmon can access defined NTP servers on port UDP/123. For other configuration options (e.g. built-in NTP server) please consult Flowmon User Guide, chapter Flowmon Configuration Center, section System Settings.

## E-mails

E-mail notifications are available through user-configured SMTP server. SSL/TLS security is available as well as SMTP authentication or custom SMTP server port. Use “Send test email” feature to check your settings.

## Alerts

In addition to e-mail notifications, Flowmon can generate syslog messages in CEF (common event format) or SNMP traps. The default port for syslog is UDP/514 and SNMP traps operate on port UDP/162. Both ports are configurable. Use “Send testing syslog message” or “Send testing SNMP trap” to ensure that third-party system is able to receive alerts from Flowmon.

## DNS

Flowmon will use configured DNS servers to automatically translate IP address to corresponding DNS names. We recommend using internal DNS servers to ensure local IP addresses are translated correctly. Flowmon needs to have access to DNS server on port UDP/53.

## Flowmon Networks remote services portal

Flowmon Networks operates portal [services.invea.com](https://services.invea.com) to provide automatic software updates, IP reputation feeds and whois information. To take advantage of that services enable TCP/443 to [services.flowmon.com](https://services.flowmon.com) or enable usage of a proxy server in Flowmon.

## LDAP-based authentication

Flowmon supports external users defined in LDAP or Active Directory. Default ports are TCP/389 and TCP/636 when using LDAP over SSL. Both ports are configurable in the user interface. Use “Check Connection” to ensure that Flowmon can connect to LDAP identity source.

## Distributed Architecture

Distributed Architecture leverages ports TCP/2210 and TCP/4210. Port 2210 is used for configuration and control, port 4210 for queries/results. Make sure these ports are not being blocked on the firewall when using Distributed Architecture.

## Other network services

For more details about configuration of Flowmon Remote Access please consult Flowmon User Guide, chapter Flowmon Configuration Center, section Remote Access.