Kemp Flowmon ADS Quick Start Guide

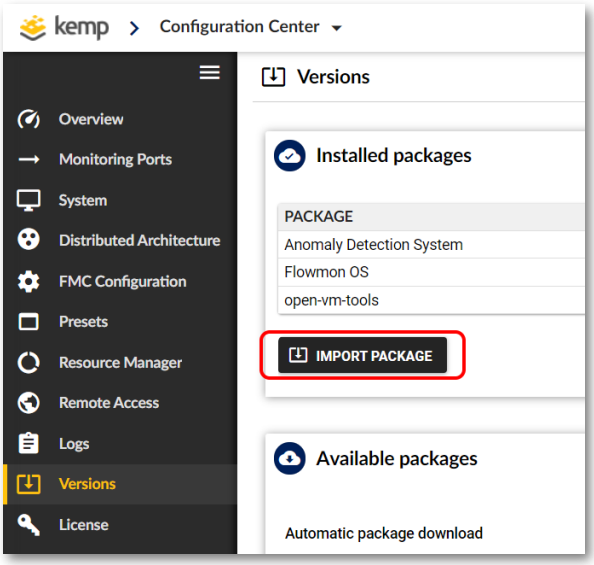
This document describes installation steps and configuration of Kemp Flowmon ADS module.

Requirements

- **Kemp Flowmon ADS module** detects suspicious network traffic patterns and anomalies using flow statistics. Flow statistics can be generated from various sources (routers, switches, firewalls etc., or Kemp Flowmon Probes). Module supports NetFlow v5 / v9 and IPFIX and other compatible flow data formats. Using sFlow is not recommended as an effectiveness of some detection methods might be affected due to insufficient quality of source data.
- **Kemp Flowmon ADS** can be deployed on:
  - **Kemp Flowmon Collector** – storage and analysis of flow statistics in all major industrial formats (NetFlow v5/v9, IPFIX, sFlow and other technologies compatible with NetFlow) from thousands of sources.
  - **Kemp Flowmon Probe** – hardware probe includes build-in collector and enables to deploy Kemp Flowmon ADS. Build-in collector can process only flow statistics from probe itself and cannot be destination of other flow exporters.

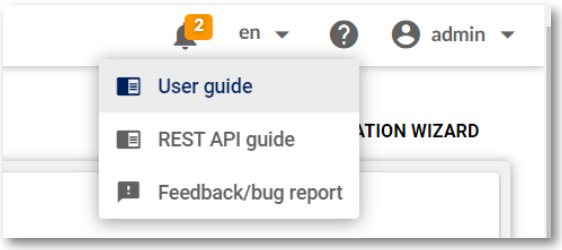
Installation

- Download **Kemp Flowmon ADS** installation package from **Kemp Support Portal** (https://support.kemptechnologies.com).
- Log into **Configuration Center.**
- Make sure that appliance is correctly licensed for **Kemp Flowmon ADS**, if not, click on **License** tab and upload appropriate license file.
- Click on **Versions** in the left menu.



- Click on **Import Package**.
- Select downloaded **Kemp Flowmon ADS** installation package.
- Click on **Upload.**
- **Kemp Flowmon ADS** will be now installed with no system restart required.

For detailed information about the Kemp Flowmon ADS see the user guide available after the installation from GUI top right corner.



Configuration

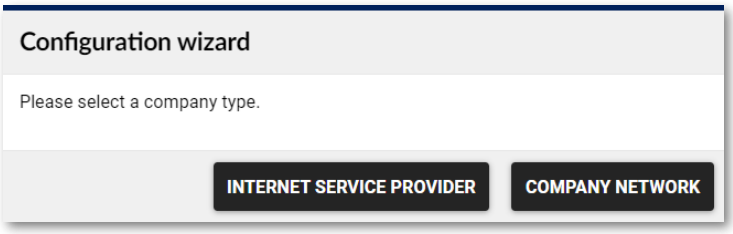
Kemp Flowmon ADS configuration is done in three steps:

1. Configuration wizard to apply basic configuration.
2. Flow data sources definition to define processed data.
3. Tuning up to improve overall module detection capability and creating exceptions to reduce false positives.

Configuration wizard

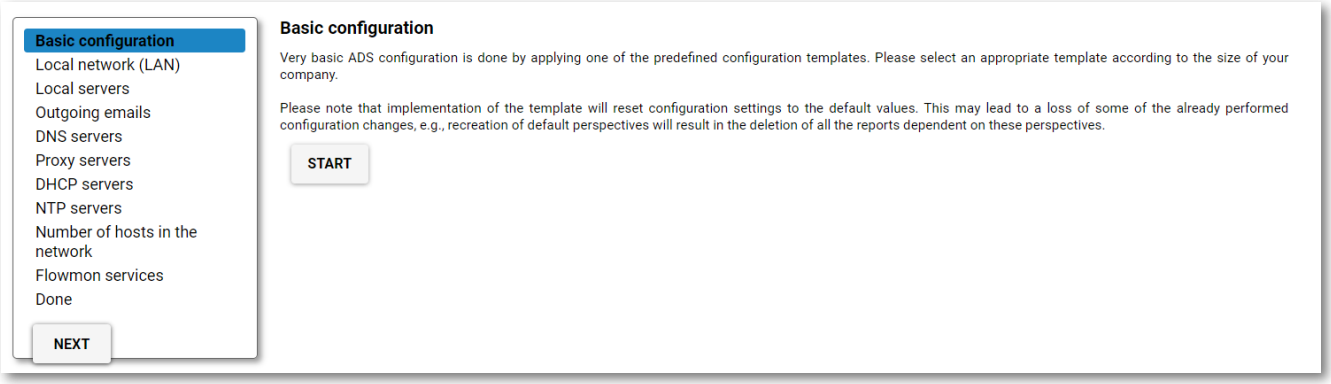
After first logging into the Kemp Flowmon ADS, welcome window will be showed with the link to configuration wizard. Configuration wizard will guide you through the configuration of Kemp Flowmon ADS. In case configuration wizard is not showed or you need to run wizard again, click on **Settings** in left menu, then click on **Configuration wizard** on top right of the screen.

The first step of the configuration wizard is to apply the configuration template. Select the template that suites your environment.



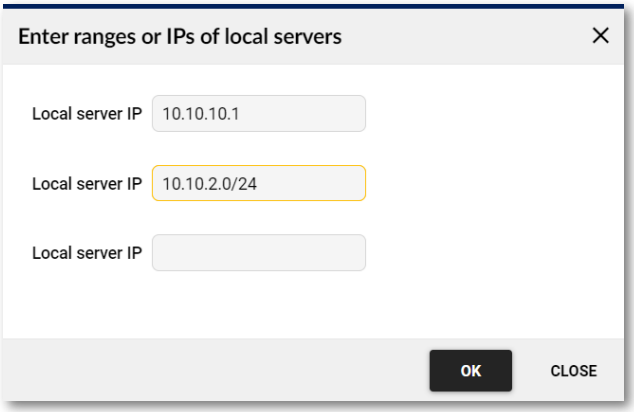
Configuration wizard – Company Network

After selecting the Company Network template, the wizard will guide you through all necessary initial settings. All set values are used for relevant detection method parameters. Please follow the instruction provided by the wizard to ensure correct system configuration and more precise anomaly detection.



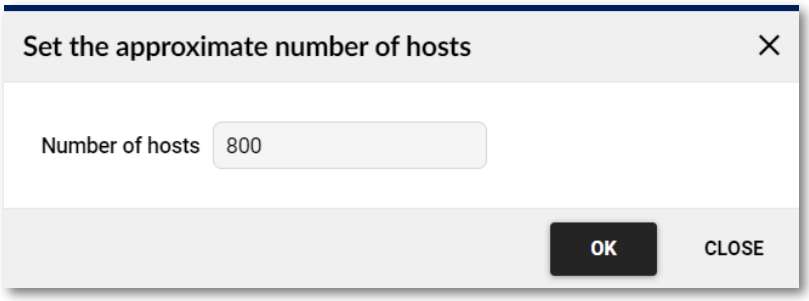
Click on **Start** button to begin with the configuration by selecting the approximate size of the company. After that it is necessary to enter IP addresses of your LAN (other than general private ranges that are added automatically) together with public IP ranges, then IP addresses of local servers and separately the IP addresses of SMTP, DNS, DHCP, NTP and proxy servers. It is possible to enter individual IP addresses or ranges using notation described in the user guide in chapter 2.3.11 Filters (e.g., 10.0.0.0/24, 10.0.0.[1-10], 172.16.*.1, 192.168.{1,3,20}.1).

When entering local servers, be sure to add IP addresses of **all servers** in the network – all DHCP, DNS, SMTP, NTP servers, Zabbix and other monitoring systems, database servers, proxies, etc. Individual types of servers will be defined again in the next steps.

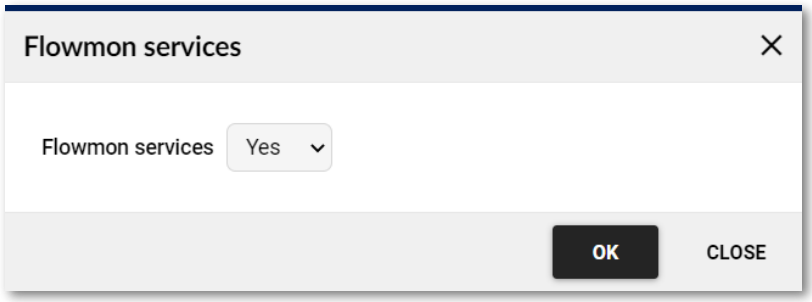


When entering specific server (SMTP, DNS, Proxy, DHCP or NTP) IP addresses, enter the addresses of servers that can be used by users (e.g., public DNS servers like 8.8.8.8 if the company policy allows to use them).

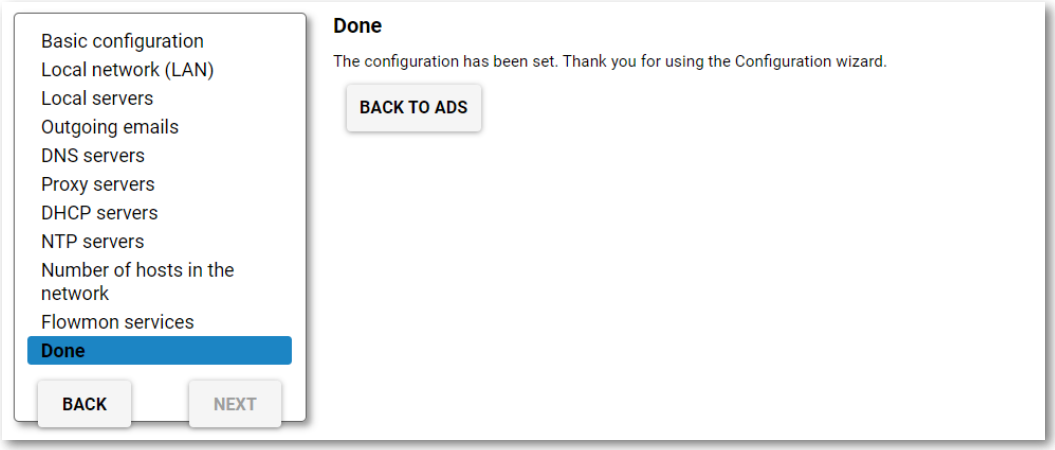
When entering approximate number of hosts, include all end devices in your network (hosts, printers, etc.). The ADS sets threshold values for detection methods based on this number.



External services include update of blacklist and behavior patterns used for detecting malicious network communications and anomalies. It also includes public services to look up for additional information., whoiis, ipvoid and others. Select **Yes**, if the system has access to the Internet.

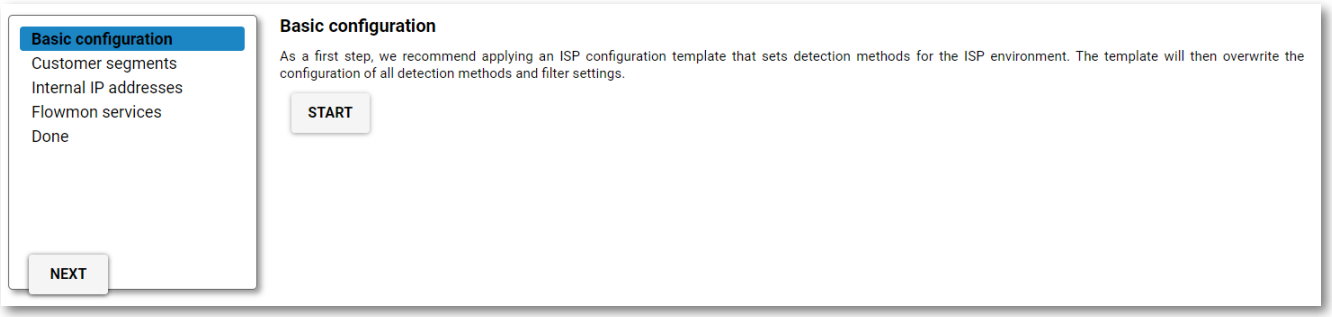


Kemp Flowmon ADS is now configured. All entered data have been loaded into the filters and methods for event detection. Click on **Back to ADS** to finish the configuration wizard. The next step is to configure the data feeds.



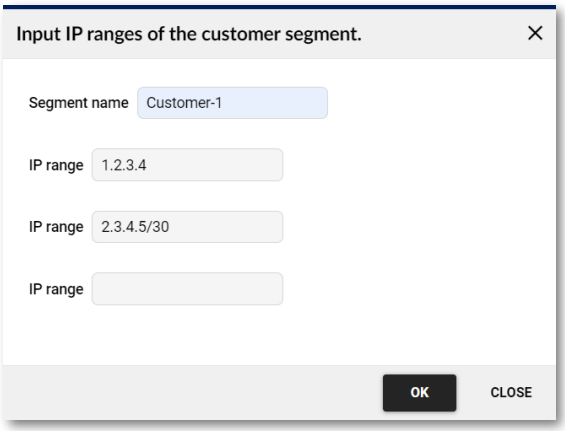
Configuration wizard – Internet Service Provider

After selecting the Internet Service Provider template, the wizard will guide you through all necessary initial settings. All set values are used for relevant detection method parameters. Please follow the instruction provided by the wizard to ensure correct system configuration and more precise anomaly detection.



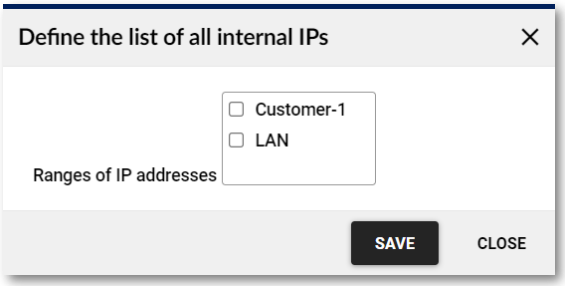
Click on **Start** button to begin with the configuration to select and apply configuration template for Internet Service Provider environment.

After the template is applied, enter customer segments (IP ranges/subnets or IP addresses). It is possible to enter individual IP addresses or ranges using notation described in the user guide in chapter 2.3.11 Filters (e.g., 10.0.0.0/24, 10.0.0.[1-10], 172.16.*.1, 192.168.{1,3,20}.1).

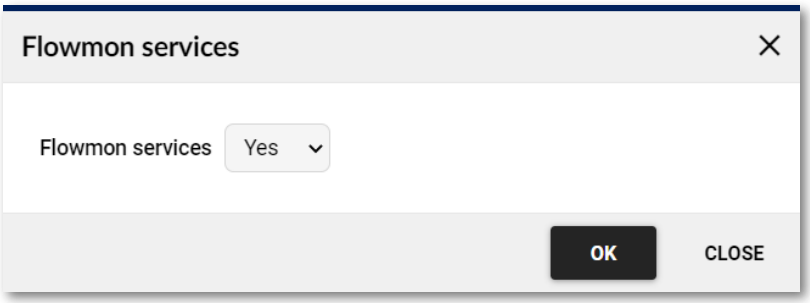


It is possible to edit the list of segments anytime later using configuration wizard or directly in the ADS configuration section (Settings – Processing – Filters).

After all segments are entered, define internal IP ranges/subnets or IP addresses by selecting displayed filters (named groups of IP ranges). In case there arer any IP ranges missing add them using the previous wizard step or in the ADS configuration section (Settings – Processing – Filters).



The next step is to enable external services. External services include update of blacklist and behavior patterns used for detecting malicious network communications and anomalies. It also includes public services to look up for additional information., whoiis, ipvoid and others. Select **Yes**, if the system has access to the Internet.



Kemp Flowmon ADS is now configured. All entered data have been loaded into the filters and methods for event detection. Click on **Back to ADS** to finish the configuration wizard. The next step is to configure the data feeds.

Kemp Flowmon ADS Configuration – Data Feeds

Data feeds are the flow data that will be processed by the Kemp Flowmon ADS. Data feeds are bound to the profiles created in Flowmon Monitoring Center (FMC). To process all data in ADS you can use the default data feed that uses “All sources” profile as defined in FMC. If you want to process only part of flow data in Kemp Flowmon ADS, create corresponding profile in FMC. Data feeds can be customized by clicking in **Settings – Processing – Data Feeds** tab. For each data feeds:

- Enter a unique name.
- Select the profile (defined in FMC) and the appropriate channels that should be used as an input.
- After the new data feed is saved, set it as active to start processing of flow data. Data feed needs to be assigned to detection methods. That can be done for all methods in additional menu in **Settings – Processing – Data Feeds** or individually for each method in **Settings – Processing – Methods**.

Kemp Flowmon ADS Configuration – Tune Up

Correct settings of flow data sources and filters affects the results of the detection methods and the overall module predictive capability. To tune up the Kemp Flowmon ADS and its detection, you can add IP ranges/subnets or IP addresses into filters created by configuration wizard or create new filters in **Settings – Processing – Filters**. The detection can be also tuned up by creating false positive rules. Every event can be marked as false positive creating a rule so the event of given type caused by given IP address will no longer be reported. You can also create false positive rules in **Settings – Processing – Data Feeds – False positives** to create exceptions for various known patterns in your network traffic (for example backups, SNMP monitoring, etc.). For more information consult the user guide or contact us at support@flowmon.com.