AKiPS™

Network Monitoring Software

User guide

Disclaimer

While the publisher (AKIPS Pty Ltd) has taken every precaution in the preparation of this guide to ensure that the information and instructions contained herein are accurate at the date of publication, it makes no expressed or implied warranty of any kind, and disclaims all responsibility for errors or omissions. The publisher assumes no liability for incidental or consequential losses or damages in connection with, or arising out of, the use of the information contained herein.

Publisher

AKIPS, PO Box 3422, Shailer Park, Queensland, 4128, Australia

Email: info@akips.com

Website: https://www.akips.com

Edition	Software release	Date
15	21.7	September 2021

Contents

Chapter 1

About this guide

The AKIPS *User guide* introduces the features available to users of AKIPS Network Monitoring Software.

The following **Abbreviations** (see 1.1), **Text conventions** (see 1.2) and **Syntax** (see 1.3) are used throughout AKIPS's guides.

1.1 Abbreviations

3DES	triple data encryption standard
ADB	AKIPS database
AES	advanced encryption standard
AKIPS	Always Keep It Purely Simple :)
API	application programming interface
ARP	address resolution protocol
AS	autonomous system
BFD	bidirectional forwarding detection
BGP	border gateway protocol
CA	certificate authority
CBQoS	class-based quality of service
CGI	computer gateway interface
CIDR	classless inter-domain routing
CLI	command line interface
CPU	central processing unit
CSR	certificate signing request
CSV	comma-separated values
cURL	client url
DHCP	dynamic host configuration protocol
DN	distinguished name
DNS	domain name system
FQDN	fully qualified domain name
GB	gigabyte
GRE	generic routing encapsulation
GUI	graphical user interface
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol secure
IF-MIB	interface MIB
IP	internet protocol
IPFIX	internet protocol flow information export
ipsla	internet protocol service level agreement
IS-IS	intermediate system to intermediate system
LAN	local area network
LDAP	lightweight directory access protocol

MAC	media access control
MIB	management information base
NAS	network-attached storage
NDP	neighbour discovery protocol
NIC	network interface card
NMS	network-monitoring software
NTP	network time protocol
OID	object identifier
OS	operating system
PCRE	Perl-compatible regular expressions
PEM	privacy-enhanced mail
PFX	personal information exchange format
PKCS	public key cryptography standards
png	portable network graphics
POSIX	portable operating system interface
PSSH	parallel secure shell
QoS	quality of service
RADIUS	remote authentication dial-in user service
RAID	redundant array of independent disks
RAM	random-access memory
RTT	round-trip time
SAN	storage area network
SCSI	small computer system interface
SHA	secure hash algorithm
SMI	structure of management information
SMTP	simple mail transfer protocol
SNMP	simple network management protocol
SSH	secure shell
SSL	secure sockets layer
STARTTLS	start transport layer security
stderr	standard error
sysadmin	system administrator
TACACS+	terminal access controller access-control system plus
TCP	transmission control protocol
TLS	transport layer security
TOS	type of service

UID	user identifier
UDP	user datagram protocol
UTC	coordinated universal time
VLAN	virtual local area network
VM	virtual machine
WAN	wide area network

1.2 Text conventions

Menu names and options are in **bold**.

E.g. **Go to Admin > System > System Settings**

Bold is also used for emphasis or clarity.

E.g. The **backup server** must have double the disk space of the **production server**.

Bookmarks (active links to Contents, Index and shortcut items) are depicted as red boxes.

E.g. The following **Abbreviations** (see 1.1), **Text conventions** (see 1.2) and **Syntax** (see 1.3) are used throughout AKIPS's guides.

Bookmarks display (as red boxes) in pdfs but not hard copies.

Websites and email addresses are in blue.

If they have an active hyperlink, they will also be in a cyan box.

E.g. https://www.akips.com

Hyperlinks display (as cyan boxes) in pdfs but not hard copies.

Code is in `monospace`.

Further:

Command syntax is in `red`.

E.g. `{ddd} {hh:mm} to {hh:mm}`

Input (user) is in `blue`.

E.g. `tf dump last7d`

Output (AKIPS) is in `cyan`.

E.g. `cisco-74-1-1 sys ip4addr = 10.74.1.1`

1.3 Syntax

Syntax may be formatted across multiple lines due to layout constraints. You will need to run commands in a single line.

Parameters (fields expecting a substituted value) are contained within { } (braces).

E.g. `{type} {value}`

Optional parameters are contained within [ ] (square brackets).

E.g. `[index,{description}]`

Optional parameters may be nested.

E.g.

```
mlist {type} [{parent regex} [{child regex} [{attribute regex}]]]
```

For values separated by a | (pipe), choose one option only.

E.g. `[any|all|not group {group name} ...]`

Multiple parameters will have an ... (ellipsis).

E.g. `not group {group name} ...`

Chapter 2

Dashboards

The following are available under **Dashboards** on the toolbar:

Events Dashboard

The **Events Dashboard** (see 2.1) provides an immediate view of your network, including availability, unreachable devices, and any devices not hitting your defined targets.

Device Dashboard

The **Device Dashboard** (see 2.2) displays vitals and interface and syslog information for an individual device.

Interface Dashboard

The **Interface Dashboard** (see 2.3) provides usage and traffic details for interfaces, including transmit receipts, errors and discards.

NetFlow Dashboard

The **NetFlow Dashboard** displays protocols, talkers (source) and listeners (destination).

2.1 Events Dashboard

The **Events Dashboard** displays key information relating to events on your network.

AKIPS will not display events which you have discarded through muting (see 5) or auto grouping (refer to the Grouping chapter in the AKIPS Administrator guide*).*

2.1.1 Impact Assessment

The **Impact Assessment** table shows details of any unreachable devices, so you can assess the impact of these on your organisation.

2.1.2 Status Exceptions

AKIPS populates the **Status Exceptions** table from status alerts and attributes which you can configure through auto grouping.

Refer to the Alerts chapter in the AKIPS Administrator guide.

2.1.3 Graphs

AKIPS collects data every 60 seconds and plots graphs according to your selected timeframe.

When you point to a position on a graph, it highlights an interval. You can drill down to 60-second intervals.

Critical Events

The **Critical Events** graph plots events which you have defined as critical, e.g. core interfaces failing.

Refer to the Alerts chapter in the AKIPS Administrator guide.

Critical Thresholds

The **Critical Thresholds** graph displays counters/gauges/meters which have failed to meet thresholds which you have defined as critical.

Events

The **Events** graph plots the results of outages and changes, including for ping, SNMP, Cisco IPSLA and spanning tree.

Thresholds

The **Thresholds** graph charts any events in breach of threshold rules which you have defined.

Syslog

The **Syslog** graph displays syslog entries which AKIPS has received according to your selected timeframe.

Traps

The **Traps** graph charts the number of trap messages from devices which you have configured to send messages to AKIPS.

Although AKIPS catches traps immediately, the dashboard takes 60 seconds to refresh.

2.1.4 IPv4 Ping Availability

The **IPv4 Ping Availability** chart displays the ping results for the previous 24 hours with availability targets which you have set (between 95 and 100 per cent).

Refer to the Availability chapter in the AKIPS Administrator guide.

2.1.5 SNMP Availability

The **SNMP Availability** chart displays the SNMP results for the previous 24 hours with availability targets which you have set (between 95 and 100 per cent).

2.1.6 Interface Status Availability

The **Interface Status Availability** chart displays the interface results for the previous 24 hours with availability targets which you have set.

2.2 Device Dashboard

The **Device Dashboard** provides reports on an individual device and its related interfaces.

You can access the **Device Dashboard** either via the main menu, or by clicking a specific device on the **Events Dashboard**.

The Device and Events Dashboards share many of the same graphs and charts.

2.2.1 Graphs

AKIPS collects data every 60 seconds and plots graphs according to your selected timeframe.

When you point to a position on a graph, it highlights an interval. You can drill down to 60-second intervals.

Events

The **Events** graph plots the status alerts for the device, which include events such as ping and SNMP down, Cisco IPSLA operational status, and spanning tree changes.

Thresholds

The **Thresholds** graph charts any events in breach of threshold rules which you have defined.

Refer to the Alerts chapter in the AKIPS Administrator guide.

Syslog

The **Syslog** graph displays syslog entries which AKIPS has received according to your selected timeframe.

Traps

The **Traps** graph charts the number of trap messages from devices which you have configured to send messages to AKIPS.

Although AKIPS catches traps immediately, the dashboard takes 60 seconds to refresh.

2.2.2 Status Exceptions

AKIPS populates the **Status Exceptions** table from status alerts and attributes which you can configure through auto grouping.

Refer to the Alerts chapter in the AKIPS Administrator guide.

2.2.3 Device Groups

The **Device Groups** table lists the groups to which you have assigned a device.

Refer to the Grouping chapter in the AKIPS Administrator guide.

2.2.4 Availability

The **Availability** chart displays the ping and SNMP reachability over time, graphed between 95 and 100 per cent.

Refer to the Availability chapter in the AKIPS Administrator guide.

2.2.5 Vitals

The **Vitals** chart shows vital statistics for a device according to your selected timeframe.

2.2.6 Interfaces

The **Interfaces** table displays all interfaces relating to a device, showing what is up and down, their speeds and traffic:

- the **Config** button opens the interface configuration report for the device
- the **Statistics** button provides traffic data (bits/bytes/packets) and graphs for each interface on the device, along with any errors and discards
- the **Port Mapper** button opens the switch port mapper for the device. It includes ARP and VLAN tables as well as a list of all of the addresses that appear on each interface
- the **Unused** button provides the speed of each interface, details of any free interfaces, and the date of the last change.

2.2.7 Syslog

The **Syslog** table shows all syslog messages for a selected duration.

2.3 Interface Dashboard

The **Interface Dashboard** shows:

- device details, which link to the **Device Dashboard** (see 2.2)
- state, speed, usage and traffic
- group details.

You can access the **Interface Dashboard** either via the main menu, or by clicking a specific interface on the **Device Dashboard**.

When you point to a position on a graph, it highlights an interval. You can drill down to 60-second intervals.

2.3.1 Interface Groups

The **Interface Groups** table lists the interface groups which you have configured.

Refer to the Grouping chapter in the AKIPS Administrator guide.

2.3.2 Address

The **Address** parameter shows the addresses that appear on this interface.

AKIPS will display this only if you have configured the interface in the switch port mapper settings (see 3.2).

Chapter 3

Reports

3.1 Unreachable Devices

The **Unreachable Devices** report lists any devices which AKIPS cannot presently reach.

Details include the device's IP address, date of its last change, location and description.

To determine reachability, AKIPS sends ping and SNMP (sysUpTime) requests according to the following:

Request	**Interval**	**Considered down when unresponsive for**
Ping	15 seconds	45 seconds
SNMP	60 seconds	120 seconds

To display unreachable devices:

Go to **Reports** > **Device** > **Unreachable**.

From the drop-down list, select the number of devices to display.

Define which results to display by checking or unchecking **Ping IPv4**, **Ping IPv6** and **SNMP**.

From the drop-down list, select the devices to display.

To display only devices in maintenance mode:

Select the **Maintenance** checkbox.

From the **All Groups** drop-down list, select **maintenance_mode**.

Complete the **Group Filter** and **Device Filter** to further filter the report.

To delete unreachable devices:

To delete all unreachable devices:

In the table, click **Select All**.

To delete individual unreachable devices:

In the table, select the checkboxes next to specific devices.

Select **Delete**.

Click **OK**.

3.2 Switch port mapper

Every hour, switch port mapper walks the ARP and bridge tables and IP and MAC addresses.

To use switch port mapper:

Go to **Tools** > **Switch Port Mapper**.

In the **Address Locator** text field, enter an IPv4/6 or MAC address.

Click either **Search** or **History**.

Use the **Group Filter** and **Device Filter** to generate mapping details.

3.3 Availability Reporter

To view Availability Reporter:

Go to **Tools** > **Availability**.

Using the drop-down lists, complete the following parameters:

Option	Action
Time range	Defines the time range of the report
Report	Charts one or all of the following: **IPv4 Ping**, **IPv6 Ping**, **Interface Status**, **SNMP**
Sort	Sorts devices either alphabetically (**Sort Name**), or from least used to most used (**Sort Availability**)
Show	Shows either all devices (**Show All**), or only those which have not met their target (**Show Failed**)

To include devices in maintenance mode:

Select the **Maintenance Mode Devices** checkbox.

3.4 NetFlow Reporter

Use **NetFlow Reporter** to define tables and graphs to monitor your traffic.

Table

The **Table** button generates a sorted table with fields matching the filters and checkboxes.

Bar Graph

The **Bar Graph** button generates a sorted bar graph for the number of bytes matching the filters and checkboxes.

Disk Usage

The **Disk Usage** button reports the disk space used for each exporter.

Unknown Ports

The **Unknown Ports** button reports on each exporter for the past five minutes, which IP address last used them, and the number of bytes sent.

To use NetFlow Reporter:

Go to **Tools** > **NetFlow**.

To view a table or bar graph:

Using the text fields and drop-down lists, select your date and time parameters.

Start typing the IP address into the **Exporter** text field and select the address.

Set filters using the **Address**, **AS Filter** and **Interface** text fields:

- select **both** to display the matches for both filters
- select **any** to display the matches for either one filter or both filters.

From the drop-down lists, select the protocol, limit and sort options.

Further refine by selecting or deselecting the checkboxes.

Click either **Table** or **Bar Graph**.

To view the usage for the NetFlow Exporter database:

Click **Disk Usage**.

To view unknown ports located during the past 24 hours:

Click **Unknown Ports**.

3.4.1 NetFlow performance

To generate NetFlow performance graphs:

Go to **Admin** > **Performance** > **NetFlow**.

AKIPS will automatically display the graph for the past hour.

3.4.2 DNS cache

DNS cache automatically lists, resolves and caches hostnames for fast reporting.

It uses conservative rate limiting to avoid overrunning your DNS, and automatically deletes expired entries.

DNS cache is in its prototype phase and is currently used only in NetFlow Reporter.

To view DNS performance graphs:

Go to **Admin** > **Performance** > **DNS**.

AKIPS will automatically display the graph for the past hour.

To disable DNS cache:

Go to **Admin** > **General** > **Miscellaneous**.

Click the **DNS Resolution** button **Off**.

Click **Save**.

3.5 Trap Reporter

To use Trap Reporter:

Go to **Tools** > **SNMP Traps**.

Using the text fields and drop-down lists, set the time and device filters.

To display a list of messages:

Click **Table**.

To display the device name, IP address and count:

Click **Top Talkers**.

3.6 CSV output

To export reports in CSV format:

On the toolbar, click **CSV**.

When prompted, either open the file by selecting a program, or save it by clicking **Save File**.

Click **OK**.

Chapter 4

Filter and display options

4.1 Filters

The following filters are available to filter the data in **Dashboards** (see 2) and **Reports** (see 3):

- date and time (see 4.1.1)
- IP address (see 4.1.2)
- group (see 4.1.3).

4.1.1 Date and time

Use date and time filters to search any 60-second interval.

The default time range is the past 30 minutes.

To view historical intervals, select a date from the calendar and navigate with the arrows.

To further refine your search, specify a start time and duration.

AKIPS displays the results according to your allocated timezone. Refer to the Settings chapter in the AKIPS Administrator guide.

4.1.2 IP address

Create IPv4/6 address filters using the following:

Metacharacter	Description	Example
*	wildcard	`10.1.11.*`
-	range	`10.1.11.0-9`
!	negate rule	`!10.1.11.7`
/	CIDR notation to apply Netmask to the IP address	`10.1.11.7/16`

Use the negate rule only for NetFlow, trap and syslog reports.

4.1.3 Group

Use group filters by typing a group name into the **Group** text field or by using the following regex:

For more information on regex, refer to Regular Expressions Cookbook *(Goyvaerts & Levithan, 2012).*

Metacharacter	Description
/	(Mandatory) Binds all expressions
*	Matches the preceding element zero or more times
+	Matches the preceding element one or more times
^	Start with
.	Matches a single character
$	End with
[ ]	Matches a single character contained within
[^]	Matches a single character not contained within
( )	A marked subexpression
|	Or

To check your regex:

Go to **Tools** > **Regex Checker**.

Paste sample text into the text field.

Type the regex you want to check, *without* / / (forward slashes), into the **Regex** text field.

Click **Test Regex**.

Examples

Must match akips09 or akips134:

```
/akips09|akips134/
```

Must match AKDSQ, AKDSI, AKDPR, MSD or EIA:

```
/AKDSQ|AKDSI|AKDPR|MSD|EIA/
```

Match anything with SD followed by any number from four to nine:

```
/SD[4-9]/
```

Match anything that starts with fa or gi and only those from zero through to five:

```
/^(fa|gi)[0-5]/
```

4.2 Graphs

The following display options are available when viewing graphs in **Dashboards** (see 2) and **Reports** (see 3).

Individual commands in the url are separated by a `;` (semicolon).

To remove the title from a graph:

In the url, delete the text in the title component following `title=`

E.g. for `title=cisco-131-16-137`, delete `cisco-131-16-137`

If the url does not include a title component, add the following: `title=;`

Click **Enter**.

To remove the subtitle from a graph:

In the url, delete the text in the subtitle component following `subtitle=`

E.g. for `subtitle=cisco-cpu`, delete `cisco-cpu`

If the url does not include a subtitle component, add the following: `subtitle=;`

Click **Enter**.

To remove the date from a graph:

In the url, add the following: `date=0;`

Click **Enter**.

To remove the navigation controls from a graph:

In the url, add the following: `nav=0;`

Click **Enter**.

To remove the statistics from a graph:

In the url, add the following: `legend_stat=0;`

Click **Enter**.

To change the height of a graph:

If the url includes a height component:

In the url, replace the height with your required height in pixels (maximum 1469).

If the url does not include a height component:

In the graph navigation controls, click either - (minus) or + (plus) next to **Height**. This will change the graph height and display it in the url.

Replace the height with your required height in pixels (maximum 1469).

Click **Enter**.

To change the width of a graph:

If the url includes a width component:

In the url, replace the width with your required width in pixels.

If the url does not include a width component:

In the graph navigation controls, click either - (minus) or + (plus) next to **Width**. This will change the graph width and display it in the url.

Replace the width with your required width in pixels.

Click **Enter**.

To output the graph as a png file:

In the url, add the following: `filetype=png;`

Click **Enter**.

Chapter 5

Muting alerts

It is quick and simple to mute alerts which you previously configured in AKIPS.

Refer to the Alerts chapter in the AKIPS Administrator guide.

To mute alerts:

Hover your cursor over **User**.

Select **Mute Alerts**.

Click the button for the duration (from **1h** to **forever**) for which you would like to mute alerts.

To resume alerts:

Hover your cursor over **User**.

Select **Mute Alerts**.

Click **Cancel Mute**.

Chapter 6

User settings

6.1 Changing your profile

Admin users can change to a different profile with different settings. Users who do not have admin access cannot change their profile.

Refer to the Access control chapter in the AKIPS Administrator guide.

To change your profile:

Hover your cursor over **User**.

Select a profile.

This is located on the right-hand side of the menu bar.

6.2 Changing your password

To change your password:

Hover your cursor over **User**.

This is located on the right-hand side of the menu bar.

Select **Change Password**.

Complete the text fields.

Click **Change Password**.

Index