AKiPS™

Network Monitoring Software

Administrator 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 *Administrator guide* assists admin 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

Settings

2.1 Command console

To use the command console:

Go to **Admin** > **API** > **Command Console**.

Warning: for expert use only.

To run commands:

In the text field, enter your command/s.

Click **Run Commands**.

For detailed syntax, refer to the AKIPS API reference guide.

To view your command history:

Click **History**.

2.2 System settings

To configure the system settings:

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

To configure the hostname:

A hostname is a domain name assigned to the AKIPS system server. This is a combination of the server (host) local name and its parent domain name. The hostname must be an FQDN owned by your organisation.

In the **Hostname** text field, type your hostname, consisting of only:

- letters a through z (not case sensitive)
- digits 0 through 9
- - (hyphens).

A hostname cannot start or end with a hyphen.

To configure the interface vtnet0:

This setting refers to the network location of the vtnet0 interface, which links the system server to the network.

In the text fields, type either the:

- **IPv4 Address** and **IPv4 Netmask** or
- **IPv6 Address**.

To configure the gateway:

The default gateway is the IP address of the router which AKIPS uses to reach the network.

In the text fields, type either the:

- **IPv4 Gateway** or
- **IPv6 Gateway**.

To configure static routes:

Click **Show Routing Table** to see a list of all static route rules.

In the text fields, type the **Net** (subnet mask) and **Gateway** (IP address) details for each rule.

To configure the nameserver:

In either the **IPv4 Nameserver** or **IPv6 Nameserver** text field, type the IP address for your organisation's domain tree structure and domain name resolution.

To configure the NTP and timezone:

The NTP server and timezone keep accurate time across your network.

In the **NTP Server 1** and **NTP Server 2** text fields, type the IP address/es for your NTP server.

From the **Default Time Zone** drop-down list, select your closest location.

To configure the email server:

This setting enables AKIPS to send email alerts.

The default email address is akips@{hostname}.{yourdomain}

AKIPS will automatically populate the **From Address** text field. To change the outgoing email address, enter it in this text field.

If you have set up authentication for your mail server, type the hostname or IP address of your SMTP server, with the port number (optional), in the **SMTP Server** text field.

E.g. `smtp.mydomain.com:587`

Complete the **Username** and **Password** text fields.

To test these settings, type your email address in the **Test Email** text field.

Click **Send**.

Click **Save**.

Go to **Admin** > **System** > **System Shutdown**.

Rebooting the server will apply your changes.

Click **Reboot Server**.

2.3 Private AS numbers

Private AS numbers appear in BGP peer-state reports and NetFlow Reporter.

To rename a private AS number:

Go to **Admin** > **General** > **Private AS Numbers**.

In the text field, type the private AS number and name.

Use the following syntax:

```
{AS Number} {Name}
```

E.g. `64501 GnoEile_Philadelphia`

Click **Save**.

2.4 SSL certificate

SSL certificates in AKIPS must be in unencrypted PEM format.

If the files are in PKCS or PFX format, convert them before proceeding.

Example

```
openssl pkcs12
-in  <pkcs-12-certificate-and-key-file>
-out <pem-certificate-and-key-file>
```

2.4.1 SSL certificate templates

CSR

```
-----BEGIN CERTIFICATE-----

[primary certificate data]

-----END CERTIFICATE-----
```

External CA

Provide the private key and your host/domain certificate.

```
-----BEGIN RSA PRIVATE KEY-----

[private key data]

-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

[primary certificate data]

-----END CERTIFICATE-----
```

Internal CA

Provide the entire trust chain: private key, host certificate, intermediate certificates and root certificate.

```
-----BEGIN RSA PRIVATE KEY-----

[private key data]

-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

[primary certificate data]

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

[intermediate certificate data]

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

[root certificate data]

-----END CERTIFICATE-----
```

2.4.2 Installing

To generate a CSR:

Go to **Admin** > **General** > **SSL CSR**.

Using the following guidance, complete the text fields:

Text field	Details	Example
Common Name	The qualified hostname of your AKIPS server	`akips.example.com`
Organization	The name of your organisation	`AKIPS Pty Ltd`
Department	Your organisational unit name	`network operations`
City	The city in which your organisation is located. Do not abbreviate this	`Brisbane`
State / Province	The state or province in which your organisation is located. Do not abbreviate this	`Queensland`
Country	The two-letter code of the country in which your organisation is located	`AU`
Key Size	We recommend that you leave this as the default (2048 bits)	

Click **Generate**.

AKIPS will generate a CSR for you to provide to your organisation's security team. They will then issue you with a signed version of the certificate.

To install an SSL certificate:

Go to **Admin** > **General** > **SSL Settings**.

To install an SSL certificate with AKIPS's CSR:

You will need to provide *only* the signed certificate from your security team.

Use the template **AKIPS' CSR Example** which is provided on the right-hand side of the page.

To install an SSL certificate without AKIPS's CSR:

You will need to provide *both* the signed certificate and private key from your security team.

Use either **External CA Example** or **Internal CA Example**, provided on the right-hand side of the page.

Add your completed text to the **SSL Settings** text field.

Click **Save**.

If your SSL certificate does not work:

Click **Self-Signed Certificate** to generate a temporary one.

2.5 Service forwarding

Service forwarding (fanout) allows you to send the same information to several destinations at once.

To configure service forwarding:

Go to **Admin** > **General** > **Service Forwarding**.

In each text box, type the destination IPv4 addresses. You can define up to 10 addresses for each service.

Syslog Forwarding

AKIPS forwards all syslog messages it receives on UDP port 514 to the defined list of IPv4 addresses and optional port number (default 514).

E.g.

```
10.1.8.35

10.1.8.82 514

10.2.9.1 20514
```

Trap Forwarding

AKIPS forwards all SNMP trap messages to the defined list of IPv4 addresses on default port 162.

NetFlow Forwarding

AKIPS forwards all raw NetFlow packets to the defined list of IPv4 addresses on default port 514.

2.6 Miscellaneous settings

2.6.1 Adaptive polling

Because the majority of counters and gauges (e.g. interface errors and discards) rarely change value, adaptive polling is switched on, which significantly reduces the volume of SNMP network traffic.

To turn off adaptive polling:

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

Click the **Adaptive Polling** button **Off**.

Click **Save**.

2.6.2 CGI debugging

The default and recommended state is off.

Switch on *only* if directed by the AKIPS team.

2.6.3 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**.

2.6.4 Hiding unused reports

AKIPS displays all vendor reports in the **Reports** menu, including those which your network is not using.

To hide unused reports on your network:

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

Click the **Hide Unused Reports** button **On**.

Click **Save**.

2.6.5 Syslog and trap history

AKIPS stores the history for both the syslog and traps for 365 days.

To change the duration of the syslog and trap history:

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

In the **Syslog/Trap History** text field, type a value or use the arrows to increase or decrease the value (from one to 1000).

Click **Save**.

2.6.6 Temperature scale

AKIPS collects and displays the temperature from all devices in degrees Celsius.

To change the temperature scale:

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

In the **Temperature Scale** drop-down list, select **Fahrenheit**.

Click **Save**.

2.6.7 Tune interface speed

AKIPS retrieves and updates the speed for all interfaces every hour.

If switched off, AKIPS will not detect any changes until the next rewalk.

If a device with Wake-on-LAN enabled is powered down, its NIC will still be active in low-power mode (with its interface speed reduced to 10 Mbps).

To turn off tune interface speed:

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

Click the **Tune Interface Speed** button **Off**.

Click **Save**.

2.6.8 Tune interface state

When an interface is down, AKIPS stops polling it, which significantly reduces the amount of SNMP network traffic.

When its operational state is up again, AKIPS immediately restarts polling the interface and retrieves the new interface speed.

If tune interface state is switched off, AKIPS will continually poll interfaces which are down. This can increase SNMP traffic with little gain.

The IF-MIB.if OperStatus is always up for an interface connected to a device with Wake-on-LAN enabled. Even if the device is powered down, its interface statistics will continue to poll.

To turn off tune interface state:

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

Click the **Tune Interface State** button **Off**.

Click **Save**.

2.6.9 Tune interface title

AKIPS retrieves and updates the interface title (ifAlias) for all interfaces every hour.

If switched off, AKIPS will not detect any changes until the next discover or rewalk (see 3).

To turn off tune interface title:

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

Click the **Tune Interface Title** button **Off**.

Click **Save**.

2.6.10 Using HTTPS only

To allow only HTTPS connections:

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

Click the **Use HTTPS only** button **On**.

Click **Save**.

Chapter 3

Discover/rewalk

AKIPS performs daily scheduled ping and SNMP scans of your network (or specified IP address ranges) to:

- find and add new devices (**discover**)
- update the configuration for existing devices (**rewalk**).

Rewalk does not scan for new devices.

3.1 Settings

The **Discover / Rewalk** settings page has eight sections for setting up parameters. Not all apply to both discover and rewalk:

Section	Discover	Rewalk
Daily Discover Schedule (see 3.1.1)	Y	Y
Ping Scan Ranges (see 3.1.2)	Y	N
SNMP Parameters (see 3.1.3)	Y	Y
Device Match Rules (see 3.1.4)	Y	N
Device Naming Scheme (see 3.1.5)	Y	Y
Strip Domain Names (see 3.1.6)	Y	Y
Optional Features (see 3.1.7)	Y	Y
Interface Types (see 3.1.8)	Y	Y

To configure discover/rewalk settings:

Go to **Admin** > **Discover** > **Discover / Rewalk**.

Make any changes required, referring to the guidance on the right-hand side of the page and the following subsections.

Click **Save Changes**.

Click either **Discover** or **Rewalk** to finalise.

3.1.1 Daily Discover Schedule

You should schedule both a daily discover and a daily rewalk for a time when all devices on your network are most likely to be discoverable (e.g. during business hours).

If you schedule both the discover and the rewalk for the same time, AKIPS will run the rewalk first.

3.1.2 Ping Scan Ranges

AKIPS evaluates and executes each rule in order, one rule per line.

Parameter	Description	Examples
{IP range}	{address}/{mask}	10.1.0.0/16
	{address}.*	10.1.0.*
	{address}[{range}]	10.1.0.1-20
	{address}[{range}]/{mask}	10.1.0.200-210/24
	{address}[{range}].*	10.1.1-20.*
rate	The number of ping requests AKIPS sends per second. The default is 1000 and the maximum is 100,000	Scan the 10.1.0.0 subnet and limit the rate of ping requests to 2000 per second rate 2000 10.1.0.0/16
pass	The number of ping requests AKIPS sends to each IP address. The default is 2, which allows remote devices to wake up from sleep mode before responding	Increase the number of passes and ping requests per second pass 3 rate 10000

(continued)

Parameter	Description	Examples

limit	The maximum number of seconds a rule is allowed per pass. The default is 60 seconds and the maximum is 1800 seconds (30 minutes). If the calculated runtime of a rule exceeds the limit, AKIPS will skip the rule	Scan the 10.1.0.0 subnet and limit the runtime of the rule to 120 seconds
		
		`limit 120`
		
		`10.1.0.0/16`

wait	The number of seconds AKIPS will wait for a ping response. The default is three seconds and the maximum is 10 seconds	A small number of pings to a remote link, with a longer waiting period for the response and increased passes
		
		`rate 50`
		
		`wait 5`
		
		`pass`

Example

```
*** Starting Device Discovery ***
Fri, Jan 18, 2019 at 15:20
Performing Ping Scan
# Estimated runtime 6s
# Single IP rules:  total 1, found 1
# Total Found:  IP4 = 1, IP6 = 0
# Ping scan runtime 0s
Performing SNMP Scan.  This may take approximately 2 mins 30 secs
```

3.1.3 SNMP Parameters

AKIPS uses SNMP parameters when performing a discover/rewalk.

Use the following syntax:

```
version {1, 2, or 3}

community {community name}

context {context name}

user {username}

md5 | sha {password}

des | 3des | aes128 | aes192 | aes256 {password}
```

For optimal performance and security, use SNMPv3 SHA authentication and AES encryption. Avoid DES/3DES encryption.

Examples

SNMPv3 with no authentication and no encryption:

```
version 3 user mysnmpuser
```

SNMPv3 with authentication and no encryption:

```
version 3 user mysnmpuser sha myauthpasswd
```

SNMPv3 with authentication and encryption:

```
version 3 user mysnmpuser sha myauthpasswd aes256 mycryptpasswd
```

SNMPv1/2 devices:

```
version 1 community public version 2 community public
```

3.1.4 Device Match Rules

You can selectively import devices found during discover by matching them against values for various system attributes.

You can use device-match rules to either include or exclude a device.

Use the following syntax:

To ensure that your rules take precedence, place them before the vendor (default) rules.

```
include {mib}.{object} {regex}

exclude {mib}.{object} {regex}
```

AKIPS supports the following MIB objects:

- SNMPv2-MIB.sysName
- SNMPv2-MIB.sysDescr
- SNMPv2-MIB.sysObjectID
- SNMPv2-MIB.sysLocation

Examples

Wildcard entry to include all devices:

```
include SNMPv2-MIB.sysDescr .*
```

Exclude Cisco 366X models:

```
exclude SNMPv2-MIB.sysObjectID CISCO-PRODUCTS-MIB.cisco366.*
```

3.1.5 Device Naming Scheme

You can identify devices by:

- sysName
- IP address.

If you change the device-naming scheme, AKIPS will rename all devices accordingly.

3.1.6 Strip Domain Names

By default, strip domain names is switched on.

AKIPS adds device names it retrieves from the SNMPv2-MIB.sysName MIB object, after stripping the domain name up to the first . (full stop).

E.g.

SysName	**AKIPS will add the device as:**
`core1.its.mochomhlacht.com`	`core1`

If you define the domain name as:	**AKIPS will add the device as:**
`mochomhlacht.com`	`core1.its`

3.1.7 Optional Features

Optional features are MIB objects which AKIPS does not add by default during discover/rewalk because they may have a significant impact on the size of the configuration and polled data.

To include an optional feature, click its button **On**.

Cisco Access Points

AKIPS creates access points as ping only.

AKIPS assigns SNMP objects to the access point, but collects the data from the wireless LAN controller associated with each access point.

Cisco BFD

Due to the large number of Cisco devices which crash when walking the CISCO-IEFT-BFD-MIB, this is an opt-in feature.

Use auto grouping (see 4.1) or manual grouping (see 4.2) to include BFD collection for each required device in the tech_cisco_bfd device group.

E.g.

```
add device group tech_cisco_bfd

assign device router1 = tech_cisco_bfd
```

Ethernet Pause Frames

The default is 13 IF-MIB objects per interface.

When switched on, AKIPS adds two objects for each Ethernet interface.

Generic ISIS

Due to cases of denial of service on the Cisco ASR SNMP agent, you will need to opt in to this feature.

3.1.8 Interface Types

During discover, AKIPS selects the interface types to include and exclude from data collection and reporting. You can review the list and select or remove interface types for future discovers/rewalks.

In the **Discovered iftypes** column, AKIPS displays the interface types which it has discovered but will not include in data collection and reporting.

3.2 System logs

A number of logs and reports are available for you to review a discover, rewalk, component, or group of components.

AKIPS also produces network performance logs every hour, in the following order:

- interface speed
- interface title
- SNMPv3 engineIDs
- IP tables
- MAC tables.

3.2.1 Discover

The **Discover** log can assist you to troubleshoot discover issues.

The log includes the:

- **date and time**:

```
*** Starting Device Discovery
*** Mon, Nov 4, 2019 at 00:09
...
```

- results from the **ping scan**, including the potential number of IP addresses and the actual number found:

```
Performing Ping Scan
# Estimated runtime 31s
# ..........................
# 10.131.0.0/16        total 65536, rate 5000, passes 2:
                       1775 found
...
# Total Found:  IP4 = 1775, IP6 = 0
# Ping scan runtime 30s
...
```

- results from the **SNMP scan**, including devices which you have added/removed using include/exclude rules:

```
Performing SNMP Scan.  This may take approximately
3 mins 0 secs
.................................
SNMP Scan found:  588 devices
Pruning IP list by Include regex rules:  588 devices, 0 pruned
Pruning IP list by Exclude regex rules:  588 devices, 0 pruned
Pruning IP list using SNMPv3 Engine ID: 588 devices, 0 pruned
Pruning IP list using SNMPv2-MIB.sysName:
588 devices, 0 pruned
Retrieving MAC address tables:  588 walks completed in 26 secs
Processing MAC address tables:  575 devices, 43439 MAC entries
Pruning IP list by MAC address tables:  588 devices, 0 pruned
12345...
*** Starting Configuration Discovery ***
Loading configuration stats:  done
Performing SNMP walks:  ..................................
36209 walks completed in 11 mins 28 secs
Loading SNMP Walk results:  3218167 objects in 8 seconds
2 devices pruned:  failed
SNMPv2-MIB walk
Creating configuration:  ........  586 devices in 32 secs
```

- list of any **errors**:

```
ERROR: AKIPS does not support polling temperature sensors
configured in degrees Fahrenheit.  Configure the following
devices for Celsius:
     apc-131-0-150
     apc-131-0-160
     bitsight-131-1-102
```

- **auto grouping rules**, including the number of devices and technologies which you have assigned to each group:

```
Running Auto Grouping Rules:
add device group 3Com
add device group A10
add device group Accedian
add device group ADVA
add device group Aerohive
add device group Alcatel ...
...
(1) assign * * sys SNMPv2-MIB.sysObjectID value
/ECI-SMI/ = ECI
(2) assign * * sys SNMPv2-MIB.sysObjectID value
/EIP-(MON|STATS)-/ = EfficientIP
(3) assign * * sys SNMPv2-MIB.sysDescr value
/Sonoma/ = Endrun
(1) assign * * sys SNMPv2-MIB.sysDescr value
/Cabletron/ = Extreme
(9) assign * * sys SNMPv2-MIB.sysDescr value
/Enterasys/ = Extreme
(15) assign * * sys SNMPv2-MIB.sysDescr value
/Extreme/ = Extreme
(2) assign * * sys SNMPv2-MIB.sysObjectID value
/EXTREME/ = Extreme......
```

- **manual grouping rules**:

```
Running Manual Grouping Rules:
add report group Support_reports
(0) assign group APC = Support
(0) assign group Cisco = Support
(0) assign group PaloAlto = Support
(0) assign group Support_reports = Support
(1) assign report config_viewer = Support_reports
```

- **summary of devices** polled, including devices which AKIPS has newly discovered:

```
Building poller configuration:  done
Building discover summary:      done
1461 Devices
0 IPv4/IPv6 1
461 IPv4 only
0 IPv6 only
593 SNMP
0 SNMPv1
259 SNMPv2...
...
```

- totals for each **interface type**:

```
43239 Interfaces
3 adsl
2 atm
138 ds0
202 ds1
6 ds3
26621 ethernetCsmacd
15 fibreChannel
220 gigabitEthernet
106 mpls
8406 other
164 propPointToPointSerial
7357 propVirtual...
...
```

- totals for each **vendor technology** which AKIPS has discovered:

```
1 Aerohive Memory
8 Aerohive Radio
3 AKCP Humidity
3 AKCP Temperature
5 Alcatel CPU
5 Alcatel Memory
5 Alcatel Temperature
1 APC ATS
22 APC Battery Capacity
22 APC Battery Time...
...
```

- **total runtime**:

```
Total runtime:  17 mins 40 secs
Mon, Nov 4, 2019 at 00:27
*** Done ***
```

3.2.2 Rewalk

The **Rewalk** log contains details of the most recent rewalk.

It provides details in the same format as the discover log, and includes configuration changes to any monitored device.

3.2.3 Single Device

When you add a single SNMP device, AKIPS produces a **Single Device** log.

```
*** Starting Device Discovery ***
Fri, Nov 1, 2019 at 10:07

Using SNMP parameters:  version 3 maxrep 20 user fred
sha password aes256 password

Performing Ping Scan
# Estimated runtime6.1.7PING scan settings 6s
#
# Single IP rules:  total 1, found 1
# Total Found:  IP4 = 1, IP6 = 0
# Ping scan runtime 0s

Performing SNMP Scan.  This may take approximately 30 secs

SNMP Scan found:                              1 device
Pruning IP list by Include regex rules:       1 device, 0 pruned
Pruning IP list by Exclude regex rules:       1 device, 0 pruned
Pruning IP list using SNMPv3 Engine ID:       1 device, 0 pruned
Pruning IP list using SNMPv2-MIB.sysName:     1 device, 0 pruned
Retrieving MAC address tables:                1 walk completed
                                              in 0 secs
Processing MAC address tables:                1 devices,
                                              27 MAC entries
Pruning IP list by MAC address tables:        1 device, 0 pruned

*** Starting Configuration Discovery ***

Performing SNMP walks:
...
```

3.2.4 Hourly Interface Speed

The **Hourly Interface Speed** log provides details of the:

- devices AKIPS could not reach
- number of interface walks AKIPS completed and the time taken
- number of speeds updated.

```
*** Starting Discover Interface Speed ***
Mon, Nov 4, 2019 at 13:00
Skipping 4 unreachable devices:
     f5-131-1-212
     hp-131-2-15
     nortel-131-2-109
     trapeze-131-6-1
Retrieving interface tables:  2945 walks completed in 41 secs
Updating interface speeds:    85 updated
Total runtime:  43 secs
Mon, Nov 4, 2019 at 13:00
*** Done ***
```

3.2.5 Hourly Interface Title

The **Hourly Interface Title** log provides details of the:

- devices AKIPS could not reach
- number of interface walks AKIPS completed and the time taken
- number of speeds updated
- changes to the interface description, e.g. adding a router or switch.

```
*** Starting Discover Interface Title
*** Mon, Nov 4, 2019 at 13:00
Skipping 4 unreachable devices:
     f5-131-1-212
     hp-131-2-15
     nortel-131-2-109
     trapeze-131-6-1
Retrieving interface titles:  1767 walks completed in 8 secs
Updating interface titles:    12681 interfaces
Total runtime:  9 secs
Mon, Nov 4, 2019 at 13:00
*** Done ***
```

3.2.6 Hourly IP Tables

The **Hourly IP Tables** log provides details of the:

- devices AKIPS could not reach
- number of walks AKIPS completed and the time taken.

```
*** Starting Discover IP Tables ***
Mon, Nov 4, 2019 at 13:01
Skipping 3 unreachable devices:
     f5-131-1-212
     nortel-131-2-109
     trapeze-131-6-1
Retrieving IP v4/v6 Address tables:
2360 walks completed in 1 min 45 secs
Processing IP tables:  done
Total runtime:  1 min 46 secs
Mon, Nov 4, 2019 at 13:02
*** Done ***
```

3.2.7 Hourly MAC Tables

The **Hourly MAC Tables** log provides details of the:

- devices AKIPS could not reach
- number of walks AKIPS completed and the time taken
- number of devices AKIPS located and the count of MAC entries.

```
*** Starting Discover MAC Tables ***
Mon, Nov 4, 2019 at 13:02
Skipping 1 unreachable device:
     f5-131-1-212
Retrieving MAC address tables:  592 walks completed in 26 secs
Processing MAC address tables:  580 devices, 43678 MAC entries
Total runtime:  29 secs
Mon, Nov 4, 2019 at 13:03
*** Done ***
```

3.2.8 Hourly SNMPv3 EngineIDs

The **Hourly SNMPv3 EngineIDs** log provides details of the:

- devices AKIPS could not reach
- number of walks AKIPS completed using engineIDs and the time taken.

```
*** Starting Discover Engine IDs ***
Mon, Nov 4, 2019 at 13:00
Skipping 4 unreachable devices:
     f5-131-1-212
     hp-131-2-15
     nortel-131-2-109
     trapeze-131-6-1
Retrieving SNMPv3 Engine IDs:  332 walks completed in 6 secs
Processing SNMPv3 Engine IDs:  done
Total runtime:  6 secs
Mon, Nov 4, 2019 at 13:01 ***
Done ***
```

3.2.9 Discovered Devices

The **Discovered Devices** log displays details of devices which AKIPS found on the network during the previous discover, including sysObjectID, sysName and sysDescr for each device.

The SNMP version determines the other credentials shown.

```
IP Address  10.131.0.5
name        cisco-131-0-5
sysName     cisco-131-0-5
sysObjectID CISCO-PRODUCTS-MIB.ciscoASA5585Ssp20
sysDescr    Cisco Adaptive Security Appliance Version 9.1(7)4
version     2
community   public
maxrep      20
```

3.2.10 Ping Scan Results

The **Ping Scan Results** log contains a list of the IP addresses which successfully replied to AKIPS's ping requests during the most recent discover.

```
10.131.0.1
10.131.0.2
10.131.0.3
10.131.0.4
...
```

3.2.11 SNMP Scan Results

The **SNMP Scan Results** log checks all IP addresses against the SNMP credentials defined during the discover.

If this log fails, check the device configuration and IP address for errors.

It fails if the IP address does not match the device configuration.

```
10.131.1.161 SNMPv2-MIB sysDescr 0 DisplayString 3916
Service Delivery Switch
10.131.1.161 SNMPv2-MIB sysObjectID 0 ObjectIdentifier
WWP-RODUCTS-MIB.cn3916
10.131.1.161 SNMPv2-MIB sysUpTime 0 TimeTicks 9439803
10.131.1.161 SNMPv2-MIB sysContact 0 DisplayString demo@akips.com
10.131.1.161 SNMPv2-MIB sysName 0 DisplayString ciena-131-1-161
10.131.1.161 SNMPv2-MIB sysLocation 0 DisplayString Rm 287
#,tt=1572790222,runtime=0,ip=10.131.1.161,status=success,
reason=outside requested scope,object=SNMPv2-MIB.system,
packets=1,retries=0,bytes=432,oids=20,maxrep=20,rtt=10 10 10,
version=2,community=bne_hq
...
```

3.2.12 Excluded Devices

The **Excluded Devices** log contains a list of devices which were excluded from the last discover.

This report is most useful when troubleshooting issues that arise during discover/rewalk (see 3.4).

Devices may be excluded due to the parameters which you defined for discover/rewalk (see 3.1.4).

Devices may also be excluded because of potential conflicts arising from duplicates of the following:

- SNMPv2 sysNames
- SNMPv3 engineIDs
- MAC address tables.

```
10.1.0.6 no matching include rule
sysObjectID=BROTHER-MIB.net-printer
sysDescr=Brother NC-8500h Firmware Ver.1.16 (16.06.28)
MID 8CE-416FID 2
10.1.15.1 no matching include rule
sysObjectID=BEGEMOT-SNMPD-MIB.begemotSnmpd AgentFreeBSD
sysDescr=dev15.akips.com 3935255930 FreeBSD 11.1-RELEASE-p8
10.22.80.27 matching exclude rule SNMPv2-MIB.sysObjectID
CISCO-PRODUCTS-MIB.cisco366*
10.122.160.13 duplicate sysName swt0f5.mybiz.com
with 110.122.160.10
10.2.6.1 duplicate EngineID 800000090300a0e0afd20740
with 10.2.2.129*
10.122.160.20 duplicate MAC address table with 10.122.160.19 ...
```

3.2.13 MAC Address Table

The **MAC Address Table** log contains a list of all devices and their MAC addresses which AKIPS located and summarised in the most recent MAC tables log.

```
*** MAC Address Table ***
Mon, Nov 4, 2019 at 13:02
accedian-131-3-1 (10.131.3.1)
     00:15:ad:86:01:0a
     00:15:ad:86:01:0b
     00:15:ad:86:01:0c
     00:15:ad:86:01:0d
     00:15:ad:86:01:0e
     00:15:ad:86:01:0f
     00:15:ad:86:01:00
     00:15:ad:86:01:01
     00:15:ad:86:01:02
...
```

3.2.14 IP Address Table

The **IP Address Table** log contains a list of all IP addresses which AKIPS found on devices during the most recent discover.

The polling address is shown beside the device name, and the subsequent addresses are those which AKIPS found on the device.

```
swt9-3 (10.1.9.3)
     10.1.9.3
     fd00:10:1:8::250

cisco-131-0-1 (10.131.0.1)
     152.19.178.2
     152.2.252.58
     172.31.185.193
     172.31.185.161
     10.19.178.2
     152.2.207.142
     172.28.2.1
     10.131.0.1
...
```

3.2.15 IP Address to Name

The **IP Address to Name** log contains a list of all IP addresses and their related device names which AKIPS found during the most recent discover.

```
2021-01-20 11:00 10.1.0.2 swt2
2021-01-20 11:00 10.1.0.9 swt9
2021-01-20 11:00 10.19.178.2 cisco-150-0-1
2021-01-20 11:00 10.150.0.1 cisco-150-0-1
2021-01-20 11:00 152.2.207.142 cisco-150-0-1
2021-01-20 11:00 152.2.252.58 cisco-150-0-1
2021-01-20 11:00 152.19.178.2 cisco-150-0-1
2021-01-20 11:00 172.28.2.1 cisco-150-0-1
2021-01-20 11:00 172.31.185.161 cisco-150-0-1
2021-01-20 11:00 172.31.185.193 cisco-150-0-1
...
```

3.2.16 SNMP Walk Results

The **SNMP Walk Results** log contains a list of all SNMP devices, including:

- IP address
- version
- MIB object
- authorisation and authentication credentials.

```
tt=1572877002,runtime=0,ip=10.131.0.223,status=success,
reason=outside requested scope,
object=SYNOLOGY-DISK-MIB.disk Entry,packets=1,retries=0,
bytes=136,oids=1,maxrep=20,rtt=11 11 11,version=3,
engine=80000009030000550a8300df,boots=5,boottime=1571035111,
uptime=1841891,user=fred,auth=sha,auth_password=password,
priv=aes256,priv_password=password tt=1572877002,runtime=0,
ip=10.131.0.69,status=success,reason=outsiderequested scope,
object=ISIS-MIB.isisISAdj,packets=1,retries=0,bytes=493,oids=16,
maxrep=20,rtt=11 11 11,version=3,engine=80000009030000550a830045,
boots=839,boottime=1572876189,uptime=813,user=barney,auth=sha,
auth_password=password,priv=aes128,priv_password=password
...
```

3.2.17 SNMP Walk Failures

The **SNMP Walk Failures** log contains a list of SNMP devices that failed the most recent discover/rewalk.

The list contains device details, including:

- IP address
- MIB object
- authorisation and authentication credentials.

```
tt=1572877002,runtime=0,ip=10.131.0.223,status=success,
reason=outside requested scope,object=SYNOLOGY-DISK-IB.diskEntry,
packets=1,retries=0,bytes=136,oids=1,maxrep=20,rtt=11 11 11,
version=3,engine=80000009030000550a8300df,boots=5,
boottime=1571035111,uptime=1841891,user=fred,auth=sha,
auth_password=password,priv=aes256,
priv_password=password tt=1572877002,runtime=0,ip=10.131.0.69,
status=success,reason=outside requested scope,
object=ISIS-MIB.isisISAdj,packets=1,retries=0,bytes=493,oids=16,
maxrep=20,rtt=11 11 11,version=3,engine=80000009030000550a830045,
boots=839,boottime=1572876189,uptime=813,user=barney,auth=sha,
auth_password=password,priv=aes128,priv_password=password
```

3.3 Other reports and tools

3.3.1 Discover summary

The discover summary provides a high-level snapshot of all of the devices, interfaces and vendor technologies which AKIPS has located on your network.

To view the discover summary:

Go to **Admin** > **Discover** > **Discover Summary**.

3.3.2 SNMP walk statistics

SNMP walk statistics provides performance and error data from the most recent discover.

To view SNMP walk statistics:

Go to **Admin** > **Discover** > **SNMP Walk Statistics**.

3.3.3 Ping-only device

To collect data for a device which is vital to your network but is not under your direct control (e.g. a switch owned by a service provider), you can add it as a ping-only device without requiring SNMP authentication.

To add a ping-only device:

Go to **Admin** > **Discover** > **Add Ping Device**.

Complete the following text fields and then click **Save**.

Text field	Action
Name	(Mandatory) Type the device name (no spaces)
IPv4 or **IPv6**	(Mandatory) Type the IP address
Description	Type a description to appear on the **Device Dashboard**
Location	Type a physical location to appear on the **Device Dashboard**
Contact	Type contact details for the device
Group	Select from the list to assign the device to a group

3.3.4 Single SNMP device

Add a single SNMP device to AKIPS to avoid discovering the entire network.

To add several devices, run a discover with specified SNMP parameters (see 3.1.3).

To add a single SNMP device:

Go to **Admin** > **Discover** > **Add SNMP Device**.

Complete *only* the **IP Address** text field.

Click **Discover**.

3.4 Troubleshooting

AKIPS may exclude devices from discover/rewalk due to:

- exclusion rules (see 3.4.1)
- duplicate SNMPv3 engineIDs (see 3.4.2)
- duplicate SNMPv2-MIB sysNames (see 3.4.3).

3.4.1 Exclusion rules

Example

Excluded devices report:

```
10.22.80.27 matching exclude rule
SNMPv2-MIB.sysObjectIDCISCO-PRODUCTS-MIB.cisco366*
```

SNMP scan results from discover log:

```
Pruning IP list by Exclude regex rules:  588 devices, 1 pruned
```

To disable exclusion rules:

Go to **Admin** > **Discover** > **Discover / Rewalk**.

Review the exclusion rules defined in **5. Device Match Rules**.

To disable a rule, add a `#` as the first character.

E.g.

```
# exclude SNMPv2-MIB.sysObjectID CISCO-PRODUCTS-MIB.cisco366*
```

Click **Save**.

Disable (rather than delete) an exclusion rule for the option to easily restore it later.

3.4.2 Duplicate SNMPv3 engineIDs

Example

Excluded devices report:

```
10.2.6.1 duplicate EngineID 800000090300a0e0afd20740
with 10.2.2.129*
```

SNMP scan results from discover log:

```
Pruning IP list by SNMPv3 Engine ID: 588 devices, 1 pruned
```

To resolve duplicate SNMPv3 engineIDs:

Change the engineID on the excluded device to make it unique.

Run discover to add the device (see 3.3.4).

3.4.3 Duplicate SNMPv2-MIB sysNames

Example

Excluded devices report:

```
10.122.160.13 duplicate sysName swt0f5.mybiz.com
with 110.122.160.10
```

SNMP scan results from discover log:

```
Pruning IP list by SNMPv2-MIB.sysName:  588 devices, 1 pruned
```

To resolve duplicate SNMPv2-MIB sysNames:

Change the sysName on the excluded device to make it unique.

Run discover to add the device (see 3.3.4).

3.4.4 Locating missing devices

To ping a device:

Go to **Tools** > **Ping Tool**.

Select a device.

Alternatively, type the IP address in either the **IPv4 Address** or **IPv6 Address** text field.

Click **Ping**.

To walk a device:

Go to **Tools** > **Ping / SNMP Walk**.

From the **Version** drop-down list, select either **2** or **3**.

Complete the following parameters, based on your SNMP version:

- SNMPv2: **Community**
- SNMPv3: **Username**, **Auth** and **Priv**

Click **SNMP Walk**.

To rule out common reasons for missing devices:

Investigate if:

- a firewall is between the AKIPS server and the device
- AKIPS needs permission to access the device
- the device is offline or switched off.

If you still cannot locate the missing device, contact support@akips.com

Chapter 4

Grouping

AKIPS's grouping provides flexibility for monitoring, reporting and alerting.

Using grouping rules, you can:

- specify what to include/exclude from monitoring, reporting and alerting
- define a hierarchical structure for your organisation.

Examples of hierarchies include:

- location (floor, building, campus, city, state, country, etc)
- hardware/software (model, range, version, etc)
- business groups (sales, back office, manufacturing, etc).

AKIPS recommends that you take the time to design a structure and naming conventions before you create your groups and their interactions.

4.1 Auto grouping

Auto grouping enables you to:

- tailor a hierarchical structure to your organisation
- configure and manage events and alerts
- manage user access to data.

Auto grouping automatically creates groups for interface speed, type and VLANs.

Auto grouping maintains a comprehensive list of vendor rules (add and assign) which you should not change.

This means that when you add new devices, the vendor rules are already in place.

4.1.1 Super groups

To create a hierarchy of super groups:

Go to **Admin** > **Grouping** > **Auto Grouping**.

You can begin anywhere in the hierarchy, although starting at the highest level and working down often provides clarity.

(Optional) At the beginning of the rule, add a comment to identify it.

E.g. `#{Top Level Group}`

Add each super group on a new line. Group names cannot contain spaces: use an _ (underscore) or a - (hyphen).

E.g.

```
global_data_centre
```

```
global-data-centre
```

Use the following syntax:

```
add super group {supergroup_name}
```

Assign each super group to the higher-level super group where required.

Use the following syntax:

```
assign super group {lower_supergroup_name} =
{higher_supergroup_name}
```

Click **Save and Apply.**

To understand a super group report:

When you select a super group in a **device report**, the report will show only the devices in the super group's **device group**.

When you select a super group in an **interface report**, the report will show:

- all discovered interfaces on devices in the super group's **device group**
- all interfaces in the super group's **interface group**.

4.1.2 Adding groups

You should typically assign network entities to a group of the same type (devices, interfaces, systems, processors, memory, storage, temperature, NetFlow, etc).

To add and assign groups:

Go to **Admin** > **Grouping** > **Auto Grouping**.

Add each group on a new line.

Use the following syntax:

```
add {group_type} group {group_name}
```

```
add device group {devicegroup_name}
```

```
add interface group {interfacegroup_name}
```

Assign each group to an appropriate super group.

Use the following syntax:

```
assign group {group_name} = {super_group_name)
```

4.1.3 Renaming groups

To rename a group:

Go to **Admin** > **Grouping** > **Auto Grouping**.

Update the add and assign rules with the new name.

Click **Save and Apply.**

4.1.4 Assigning components

To assign a component to a device group:

Go to **Admin** > **Grouping** > **Auto Grouping**.

On a new line, assign each component to its respective group.

Use the following syntax:

```
assign device {device_name} = {devicegroup_name}
```

(device_name may be a * (wildcard) or regex)

```
assign interface {device_name} {interface_name} =
{interfacegroup_name}
```

(device_name and interface_name may be a * (wildcard) or regex)

```
assign system {device_name} {system_name} = {systemgroup_name}
```

```
assign processor {device_name} {processor_name} =
{processorgroup_name}
```

```
assign memory {device_name} {memory_name} = {memorygroup_name}
```

```
assign ipsla {device_name} {ipsla_name} = {ipslagroup_name}
```

```
assign temperature {device_name} {temperature_name} =
{temperaturegroup_name}
```

E.g.

```
assign device {*|name|/regex/} = {group}

assign device core-swt01 = core

assign device /^NW-/ = NorthWestCampus

assign device /rtr$/ = routers


assign interface {*|name|/regex/} {*|name|/regex/} = {group}

assign interface * /^Se/ = serial-links


assign * {*|name|/regex/} {*|name|/regex/} {*|name|/regex/}
[value|descr {match}] = {group}

assign * * * IF-MIB.ifDuplex value /half/ = Half-Duplex

assign * * sys SNMPv2-MIB.sysLocation value /bne/ = HeadOffice
```

Click **Save and Apply**.

AKIPS will display the components which match the assign rules.

4.1.5 Empty groups

AKIPS automatically removes any empty groups from menus during auto grouping.

To enable empty groups:

Go to **Admin** > **Grouping** > **Settings**.

Switch the required settings **Off**.

Click **Save**.

4.2 Manual grouping

Use manual grouping to:

- refine auto groups
- delete broken rules.

To view grouping rules:

Go to **Admin** > **Grouping** > **Manual Grouping**.

Select **Grouping Rules**.

To delete broken rules:

Go to **Admin** > **Grouping** > **Manual Grouping**.

Select **Delete Broken Rules**.

4.2.1 Adding groups

To add a manual group:

Go to **Admin** > **Grouping** > **Manual Grouping**.

Select the group type.

In the text field, type the name of the new group.

Click **Add**.

You can now assign components to the new group.

4.2.2 Renaming groups

To rename a group:

Go to **Admin** > **Grouping** > **Manual Grouping**.

Select the group type.

Select the group name.

Overtype the new name.

Click **Rename**.

AKIPS will also update the group's associated rules.

4.2.3 Assigning and removing devices

To assign or remove devices:

Go to **Admin** > **Grouping** > **Manual Grouping**.

Select the group type.

Select the group name.

Click **Edit**.

To assign devices to the group:

Select the checkbox next to a device.

To remove devices from the group:

Deselect the checkbox next to a device.

Click **Save**.

4.2.4 Deleting groups

You can delete obsolete groups, e.g. for decommissioned equipment.

To delete a group:

Go to **Admin** > **Grouping** > **Manual Grouping**.

Select the group type.

Select the group name.

Click **Delete**.

Chapter 5

Event handling

5.1 SNMP traps

Instead of waiting for AKIPS to poll devices, SNMP traps enable devices to send unsolicited SNMP messages to notify AKIPS of significant events.

To enable AKIPS to decode SNMP traps, ensure that you have:

- configured each device using either version 2 or 3
- defined the SNMP credentials.

To define SNMP trap credentials:

Go to **Admin** > **General** > **SNMP Traps**.

In the text field, type the SNMP credentials:

Version	Syntax
2	`community {community name}`

3	`version 3 user {username}`
	`version 3 user {username} md5|sha {auth password}`
	`version 3 user {username} md5|sha {auth password} des|3des|aes128|aes192|aes256 {priv password}`

Click **Save**.

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

Check the **Trap Reporter** to verify that AKIPS is collecting the data.

To troubleshoot SNMP traps:

Go to **Admin** > **System** > **System Log Viewer**.

From the **Log File** list, select **SNMP**.

In the **Filter** text field, type `trap`

Click **Search**.

Identify the error and take the corrective action:

Error	Action
`No SNMP trap credentials have been configured`	Define the additional **SNMP Trap Settings**
`Trap auth failed version 2 community...`	Check the **Discover** log and **SNMP Trap Settings** to locate and correct the credentials
`SNMPv1 traps are not supported`	Configure the device for version 2 or 3

5.2 Filtering syslog and SNMP traps

You can filter syslog data and SNMP traps so that AKIPS does not catch and store unwanted entries.

Entries that AKIPS caught before you added the filter will remain.

To add a syslog/trap filter:

Go to **Tools > Regex Checker**.

In the sample text field, paste some sample data.

Type your rule into the **Regex** text field.

Click **Test Regex**.

Rewrite and retest, if required.

Copy the tested rule.

To save the rule:

Go to **Admin > General > Syslog / Trap Filters**.

Paste your tested rule.

Click **Save**.

A short buffering delay will occur before the filter becomes active.

To remove a syslog/trap filter:

Go to **Admin > General > Syslog / Trap Filters**.

Select and delete the filter.

Click **Save**.

5.3 Filtering event notifications

5.3.1 Unwanted notifications

To remove unwanted event notifications:

Go to **Admin** > **Alerting** > **Status Alerts.**

Scroll to the **Status Attributes** list.

Copy the attribute.

Go to **Admin** > **Grouping** > **Auto Grouping**.

To modify existing Event Handling:

Scroll to the **Event Handling** section.

To add Event Handling:

Add an **Event Handling** section by typing the subheading

```
##### Event Handling ######
```

Create a rule to clear an event from the database.

E.g.

Type `* * *`

Paste the attribute.

Type `= warn_event`

Click **Save and Apply.**

5.3.2 Interface warnings

By default, interface events are not logged or shown in the **Events Dashboard** because the number of entries can be unnecessary (e.g. every time someone logs onto a computer).

However, several interfaces may have a significant impact if they are not operating, e.g. Uplinks.

To select interfaces to display in the Events Dashboard:

Go to **Admin** > **Grouping** > **Auto Grouping**.

To modify existing Event Handling:

Scroll to the **Event Handling** section.

To add Event Handling:

Add an **Event Handling** section by typing the subheading
`##### Event Handling ######`

Create a rule to include specific interface groups.

Use the following syntax:

```
assign * * * any group (group_name) = log_event

assign * * * any group (group_name) = warn_event
```

Click **Save and Apply**.

5.3.3 Network noise

Network noise can include:

- BGP flapping up and down (continuously switching from idle to active as the route is no longer valid)
- poor configuration of the spanning tree, e.g. someone turning a phone on and off
- vendor-specific noise, e.g. Juniper switching between states.

To identify network noise:

Go to **Tools** > **Events**.

Change the default duration (30 minutes) to 24 hours or longer.

Select **Summary**.

Review **Event** and **Count** to determine where to investigate further.

After you have identified the source of network noise, you can apply filters to either discard the events or mute them so that AKIPS logs them but does not display them in the **Events Dashboard**.

Chapter 6

Alerts

You can configure the following alerts:

- status (see 6.1)
- threshold (see 6.3)
- syslog (see 6.5)
- SNMP traps (see 6.6).

To create a rule, regardless of the type of alert, use the following syntax:

```
{filter} = {action}
```

To disable a rule, add a # as the first character.

6.1 Status alerts

You can view status alerts (changes in state) via the **Events Dashboard** or **Status Reporter**.

To add or edit a status alert:

Go to **Admin** > **Alerting** > **Status Alerts**.

Specify a filter.

Use the following syntax:

```
[wait {N}m|{N}h] [time {time filter}]
{type} {device regex} {child regex} {attribute regex}
[descr {/regex/}] [value {text|/regex/}]
[any|all|not group {group name} ...]
```

Specify an action.

Use the following syntax:

```
email * | {profile name} | {email address} [...]

mute [ {profile name} | {email address} [...]  ]

stop

call {function}
```

Assign to an alert group:

- log_event
- warn_event
- crit_event

Click **Save**.

6.2 Status attributes

You must select an attribute when defining a filter as part of a status alert rule.

AKIPS regularly updates the status attributes table as vendors release MIBs.

To select a status attribute:

Go to **Admin** > **Alerting** > **Status Alerts**.

Scroll to the **Status Attributes** table.

Copy and paste the required attribute into the rule.

Click **Save**.

6.3 Threshold alerts

You can create threshold rules for any attribute defined as a counter/gauge/meter.

AKIPS advises creating the rule and then assessing the quantity of alerts for seven to 14 days before you add the email alert.

To add or edit a threshold alert:

Go to **Admin** > **Alerting** > **Threshold Alerts**.

Specify a filter.

Use the following syntax:

```
{lastN} avg|total above|below {value}[%] [time {time filter}]
{type} {device regex} {child regex} {attribute name or regex}
[any|all|not group {group name} ...]
```

Specify an action.

Use the following syntax:

```
log discard flag warning|critical

email * | {profile name} | {email address} [...]

mute [ {profile name} | {email address} [...]  ]

call {function}
```

Select **Test**.

Modify and retest the rule, if necessary.

Click **Save**.

6.4 Threshold attributes

You must select an attribute when defining a filter as part of a threshold alert rule.

AKIPS regularly updates the threshold attributes table as vendors release MIBs.

To select a threshold attribute:

Go to **Admin** > **Alerting** > **Threshold Alerts**.

Scroll to the **Threshold Attributes** table.

Copy and paste the required attribute into the rule.

Click **Save**.

6.5 Syslog alerts

The filters in syslog alerts differ from those in status and threshold alerts because there are no configuration items (each vendor formats syslog messages differently).

Because part of the message is usually unique, AKIPS uses regex to filter syslog messages.

You can filter devices by:

- name
- group
- IP address.

To add or edit a syslog alert:

Go to **Admin** > **Alerting** > **Syslog Alerts**.

Specify a filter.

Use the following syntax:

```
/syslog regex/ [time {time filter}]

/syslog regex/ [time {time filter}] address {IP address}

/syslog regex/ [time {time filter}] device {device regex}
[any|all|not group {group name}]
```

Specify an action.

Use the following syntax:

```
email * | {profile name} | {email address} [...]

mute [ {profile name} | {email address} [...]  ]

forward {ip address}

call {function}
```

Click **Save**.

To check the regex:

Go to **Tools** > **Syslog**.

Review the log to identify text which is unique to the message.

Enter the text into the **Syslog Filter** text field.

Select **Table**.

6.6 SNMP trap alerts

To enable AKIPS to decode traps sent from an SNMP device:

AKIPS does not support SNMPv1 traps.

- configure the device using either version 2 or 3
- define the SNMP credentials.

To add or edit an SNMP trap alert:

Go to **Admin** > **Alerting** > **Trap Alerts**.

Specify a filter.

Use the following syntax:

```
/trap regex/ [time {time filter}]

/trap regex/ [time {time filter}] address {IP address}

/trap regex/ [time {time filter}] device {device regex}
[any|all|not group {groupname} ...]
```

Specify an action.

Use the following syntax:

```
email * | {profile name} | {email address} [...]

mute [ {profile name} | {email address} [...]  ]

call {function}
```

Click **Save**.

To access the system log viewer:

Go to **Admin** > **System** > **System Log Viewer.**

In the **Log File** drop-down list, select **SNMP**.

In the **Filter** text field, type `trap`

Click **Search**.

6.7 Troubleshooting

AKIPS will display a warning when an alert rule does not match anything in the ADB.

Alerts operate off events logged to the **Events Database**. If an event is not logged, it will not trigger an alert.

Interface events are not logged because a typical network constantly has interfaces going up and down. To create interface status alerts, configure auto grouping rules (see 4.1).

Chapter 7

Integration

You can integrate the following third-party applications into AKIPS:

- Opsgenie (see 7.1)
- PagerDuty (see 7.2)
- ServiceNow (see 7.3)
- Slack (see 7.4)
- Splunk (see 7.5).

AKIPS creates unique IDs for integration alerts and events using device_child_attribute

7.1 Opsgenie

To integrate Opsgenie:

For assistance when configuring Opsgenie, contact their support team.

Sign into your Opsgenie account.

Copy the API key.

In AKIPS, go to **Admin** > **API** > **Integration Settings**.

Paste the key into the Opsgenie **API key** text field.

Click **Save**.

In Opsgenie, configure a heartbeat.

Copy the heartbeat name.

Back in AKIPS, paste the name into the Opsgenie **Heartbeat Name** text field.

Click **On**.

Click **Save**.

Go to **Admin** > **Alerting** > **Status Alerts**.

Specify `call post_alert_opsgenie` on any rules you would like to send to Opsgenie.

E.g.

```
* * ping4 PING.icmpState = call post_alert_opsgenie

* * * * = call post_alert_opsgenie
```

7.2 PagerDuty

To integrate PagerDuty:

For assistance when configuring PagerDuty, contact their support team.

Sign into your PagerDuty account.

Copy the integration key.

In AKIPS, go to **Admin** > **API** > **Integration Settings**.

Paste the key into the PagerDuty **Integration key** text field.

Click **Save**.

Go to **Admin** > **Alerting** > **Status Alerts**.

Specify `call post_alert_pagerduty` on any rules you would like to send to PagerDuty.

E.g.

```
* * ping4 PING.icmpState = call post_alert_pagerduty

* * * * = call post_alert_pagerduty
```

7.3 ServiceNow

To integrate ServiceNow:

Sign into your ServiceNow account.

For assistance when configuring ServiceNow, contact their support team.

Create and copy the instance url.

In AKIPS, go to **Admin** > **API** > **Integration Settings**.

Paste the url into the ServiceNow **Instance URL** text field.

Enter your ServiceNow **Instance Username** and **Instance Password** into their corresponding text fields.

Click **Save**.

Go to **Admin** > **Alerting** > **Status Alerts**.

Specify `call post_alert_servicenow` on any rules you would like to send to ServiceNow.

E.g.

```
* * * * = call post_alert_servicenow

* * ping4 PING.icmpState = call post_alert_servicenow
```

7.4 Slack

To integrate Slack:

Sign into your Slack account.

For assistance when configuring Slack, contact their support team.

Create a webhook for your required Slack channel.

Copy the webhook.

In AKIPS, go to **Admin** > **API** > **Integration Settings**.

Paste the url into the Slack **Webhook URL** text field.

Click **Save**.

Go to **Admin** > **Alerting** > **Status Alerts**.

Specify `call post_alert_slack` on any rules you would like to send to Slack.

E.g.

```
* * ping4 PING.icmpState = call post_alert_slack

* * * * = call post_alert_slack
```

7.5 Splunk

To integrate Splunk:

Sign into your Splunk account.

For assistance when configuring Splunk, contact their support team.

Copy the HEC instance url and HEC token.

In AKIPS, go to **Admin** > **API** > **Integration Settings**.

Paste the url and token into the **Splunk HEC Instance URL** and **Splunk HEC Token** text fields.

Click **Save**.

In Splunk, configure the HTTP Event Collector.

Go to **Admin** > **Alerting** > **Status Alerts**.

Specify `call post_alert_splunk` on any rules you would like to send to Splunk.

E.g.

```
* * * * = call post_alert_splunk
```

```
* * ping4 PING.icmpState = call post_alert_splunk
```

Chapter 8

Availability

You can define availability settings in AKIPS for:

- IPv4/6 ping and SNMP reachability
- interface up status.

You can view the collected data (with target breaches highlighted) in the **Events Dashboard** and **Availability Reporter** graphs.

To add or edit availability settings:

Go to **Admin** > **General** > **Availability Settings**.

Next to the required device/interface group, define:

- an availability **Target**: between 95.00 and 100.00 (per cent)
- a **Time Filter**: leave blank for 24/7 coverage.

Click **Save and Test**.

Chapter 9

Scheduling a report

To schedule a report:

Go to **Admin > General > Scheduled Reports.**

Copy the syntax from the right-hand pane.

Paste the syntax into the text field.

In a new browser window, navigate to and customise the report.

Run the report.

Copy the report url, *without* akips.company.com

Return to **Scheduled Reports**.

Paste the url parameter.

Using the guidance on the right-hand side, complete the following parameters.

Click **Save**.

Chapter 10

Config crawler

Config crawler uses SSH to log in to network devices and collect the configuration data.

Warning: for expert use only.

AKIPS captures output from operations on devices and stores it in a revision-control system.

10.1 Config crawler settings

To set up config crawler:

Go to **Admin** > **Config Crawler** > **Settings**.

From the **Daily Crawl Schedule** drop-down list, choose your preferred schedule.

Using the guidance on the right-hand side, write rules in the **Script Rules** text field to determine the commands that config crawler will run.

Each script rule must have:

- a name
- a capture with start and end parameters.

This will generate the output which the AKIPS server will keep.

Using the guidance on the right-hand side, write rules in the **Device Rules** text field to run the scripts on specific groups of devices in your network.

To configure groups in AKIPS, see 4.

To save your rules, click **Save Changes**.

To run the config crawler, click **Run**.

10.2 Config viewer

Through config viewer, you can view, download and compare revisions of the config crawler logs.

Config viewer provides a list of scripts (directly linked to the script rules in 10.1) and their configurations.

To use config viewer:

Go to **Tools** > **Config Viewer**.

From the **Script** drop-down list, select the required script.

(Optional) From the **All Groups** drop-down list, filter the required group.

(Optional) In the **Device Filter** text field, you can further filter the devices.

From the device list, select a specific device to display its configuration.

To view the last config:

Click **Show Last Change**.

To view the current revision:

Click **View**.

To compare revisions:

Click **View**.

(Optional) Tick **All Revisions** to condense multiple runs in a single day into the last one for that day.

Select **Diff** beside the second revision which you would like to compare.

AKIPS will display the two revisions side by side and highlight the differences.

To download the output:

Click **Download**.

10.3 Crawler tool

While config crawler searches every device in your network each time it runs, the crawler tool searches only a single device.

This enables you to test/debug your config crawler configuration without affecting any other devices in your network.

To use the crawler tool:

Go to **Admin** > **Config Crawler** > **Crawler Tool**.

From the device list, select a specific device.

From the **Script** drop-down list, select the required script. This is directly linked to the script rules in 10.1.

In the **Script** text field, you can edit the script rules inline.

Click **Run**.

AKIPS will advise whether your edited script:

- succeeded
- failed (including details).

AKIPS will not save any script rules you test using the crawler tool. To update the script rules, see 10.1.

To download the output:

Click **Download Debug Log**.

Config crawler logs

When troubleshooting, AKIPS support may request the most recent config crawler logs.

To download config crawler logs:

Go to **Admin** > **Config Crawler** > **Log Viewer**.

From the drop-down list, select **Crawler Log**.

Click **Download Logs**.

Chapter 11

NetFlow

AKIPS collects and analyses NetFlow records and graphs network traffic (transmitted, received, packets discarded and lost, and overall volume).

Configure your router to send NetFlow records to AKIPS on port numbers 2055, 4739, 9995 or 9996 by completing the following mandatory text fields:

- source IP address
- destination IP address
- protocol
- bytes.

AKIPS will automatically collect the flows and display them in reports and graphs after approximately five minutes.

AKIPS supports:

- NetFlow v5/9
- J-Flow v5/9
- IPFIX Netstream.

AKIPS doesn't support index or AS numbers for NetFlow v5.

You can specify how long to retain the history for each meter.

Using service forwarding (fanout), you can specify up to 10 IPv4 destinations to receive NetFlow data.

11.1 Protocols

You can customise the protocols list by renaming, adding or deleting ports.

E.g. when deploying an in-house application in your environment, you may define a port number from which to run the application. Alternatively, when deploying an external application, you may customise the application to run from a port not designated by the vendor.

AKIPS bundles these customised ports into either TCP, UDP or GRE unknown.

You can label key ports or ports with high volumes (bytes and flow).

To reset the protocols list:

Go to **Admin** > **General** > **NetFlow Protocols**.

Select **Reset to Defaults**.

Click **OK**.

11.2 Managing ports

Use NetFlow protocols (see 11.1) in conjunction with NetFlow Reporter (**Unknown Ports** report) to configure individual ports.

To view unknown ports:

Go to **Tools** > **NetFlow** > **Unknown Ports**.

To change a port name:

Go to **Admin** > **General** > **NetFlow Protocols**.

Update the text fields.

Select **Add**.

To identify unknown ports:

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

From the **Exporter** drop-down list, select the required meter.

Select **Unknown Ports**.

To add ports to the protocols list:

From the list, select the **Port Number**.

The NetFlow protocols settings page will populate with the **Protocol** and **Port Number**.

Select **Add**.

To delete a port:

Go to **Admin** > **General** > **NetFlow Protocols**.

Tick **Delete** beside the port.

Click **Delete**.

Chapter 12

Switch port mapper

Switch port mapper enables you to find any IP or MAC address on your network and view its history for the past 60 days.

Switch port mapper completes SNMP walks to locate IP and MAC details and map them to their switch port.

By default, all switch port mapper options are switched on.

AKIPS collects switch port mapper data and ARP/bridge/VLAN tables data and caches it for 24 hours.

You can change the ping settings, or suspend data collection for:

- switch port mapper entirely
- specific tables (ARP/bridge/VLAN).

12.1 Switch port mapper collector

The switch port mapper collector runs every hour.

To turn off the switch port mapper collector:

Go to **Admin** > **General** > **Switch Port Mapper**.

Click the **Switch Port Mapper** button **Off**.

Click **Save**.

Collecting data from switches with large bridge forwarding tables (typically core switches) can cause CPU spikes on the switch.

To exclude a device from the switch port mapper collector:

Go to **Admin** > **Grouping** > **Auto Grouping**.

Create a rule to assign the device to an exclusion group.

Use the following syntax:

```
assign device {NameOfCoreSwitch} = spm_exclude
```

Click **Save and Apply**.

12.2 ARP tables collector

The ARP tables collector gathers data in routers and switch management interfaces.

To turn off the ARP tables collector:

Go to **Admin** > **General** > **Switch Port Mapper**.

Click the **ARP Tables** button **Off**.

Click **Save**.

If you turn this off, switch port mapper will not be able to provide information such as the IP addresses assigned to a MAC.

Switches often have broken SNMP implementations, which causes CPU spikes when AKIPS collects ARP table data from multiple contexts.

To exclude a device from the ARP tables collector:

Go to **Admin** > **Grouping** > **Auto Grouping**.

Create a rule to assign broken devices to an exclusion group.

Use the following syntax:

```
assign device {regex} = spm_exclude_arp_context
```

Click **Save and Apply**.

12.3 Bridge tables collector

The bridge tables collector gathers data from bridge tables in switches.

To turn off the bridge tables collector:

Go to **Admin** > **General** > **Switch Port Mapper**.

Click the **Bridge Tables** button **Off**.

Click **Save**.

12.4 VLAN tables collector

The VLAN tables collector gathers data from VLAN tables in switches.

To turn off the VLAN tables collector:

Go to **Admin** > **General** > **Switch Port Mapper**.

Click the **VLAN Tables** button **Off**.

Click **Save**.

To turn off VLAN auto grouping:

Go to **Admin** > **General** > **Switch Port Mapper**.

Click the **VLAN Auto Grouping** button **Off**.

Click **Save**.

To group and ungroup VLANs:

Go to **Admin** > **General** > **Switch Port Mapper**.

Use the **Include** and **Exclude** buttons to move VLANs between the **Discovered** and **Grouped** categories.

Click **Save**.

12.5 Ping-scan settings

Switch port mapper uses ping requests to scan the network and populate router ARP/NDP tables. This also populates the bridge forwarding tables for each switch port.

As a result, switch port mapper can map close to 100 per cent of your network in a single pass.

So that a single link/interface is not overwhelmed, AKIPS sends ping requests at random to IP addresses.

To configure ping-scan settings:

Go to **Admin** > **General** > **Switch Port Mapper**.

Ensure that **Ping Scan** is **On**.

In the text field, add the ping-scan ranges (see 3.1.2).

Click **Save**.

Chapter 13

Additional tools

13.1 Settings history

AKIPS keeps daily history snapshots of all important settings.

To view and compare history snapshots:

Go to **Admin** > **General** > **Settings History**.

Click on the setting you wish to view.

Click **View** next to any snapshot to view its details.

To compare the current snapshot with an earlier revision, select **Diff** beside the revision which you would like to compare.

AKIPS will display the two revisions side by side and highlight the differences.

To show the last change to a setting:

Go to **Admin** > **General** > **Settings History**.

Click on the setting you wish to view.

Click **Show Last Change**.

To download snapshot data:

Click **Download** next to the applicable snapshot.

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

Click **OK**.

To restore a previous revision of a config:

Click **Restore** next to the applicable snapshot.

Click **OK**.

13.2 Ping/SNMP walk features

To configure the ping/SNMP walk tool:

Go to **Tools > Ping / SNMP Walk**.

Complete the **IPv4 Address** or **IPv6 Address** text field.

For SNMP walks and OIDs, also complete the **MIB.Object** text field.

Click one of the following buttons to action:

Option	Action
Ping	AKIPS transmits 10 packets to a device and records the time taken for each transmission. It displays the min/avg/max/stddev for the 10 packets
Traceroute	AKIPS traces the route from the AKIPS server to the device (end point). It lists each hop and the time taken
SNMP Walk	AKIPS performs an SNMP walk of a MIB
SNMP OIDs	AKIPS performs an SNMP walk of a MIB and provides its OID number
Packet Capture	AKIPS provides a packet capture for the duration you select from the drop-down list

13.3 Editing a device

To edit the configuration for a device:

Go to **Tools** > **Device Editor**.

Select a device.

You cannot modify text fields shaded in grey as these are MIB objects specified on the device itself.

Editable properties may include:

Text field	Details
Device	The name of the device
IPv4/IPv6	The IPv4/6 address
SNMP IP	An IP address to receive SNMP requests. This is usually the same as the **IPv4/IPv6** text field
SNMP Version	1, 2 or 3
Max Repetitions	The maximum number of MIB objects to send in a walk response
Maintenance Mode	For network maintenance, suppress alerts by selecting **On**

Click **Save**.

Rewalk the device by clicking **Rewalk**.

13.4 Viewing devices' IP addresses

To view all devices and their IP addresses:

Go to **Tools > Device to IP Mapping**.

Click on any device to edit its configuration (see 13.3).

13.5 Resetting a password

To reset the root, akips or admin password:

Log into your hypervisor and access the console for your AKIPS server.

In AKIPS, go to **Admin** > **System** > **System Shutdown**.

You will have only a short amount of time to complete the next step.

Click **Reboot Server**.

Back in your hypervisor, at the boot menu, select **2: Boot Single user**.

At the **/bin/sh** prompt, select **Enter**.

Using the command `mount -a`, mount the file systems.

Run the following command to change the **root** or **akips** shell password, or the **admin** password for the AKIPS GUI:

Account	Command	Notes
root	`passwd root`	
akips	`passwd akips`	This account enables you to ssh into your server, i.e. ssh akips@{server}.com
admin	`passwd admin`	This account is for the AKIPS GUI and is used to manage most AKIPS functionality

At the prompt, type your new password.

Retype your new password.

To continue the normal boot process, type `exit`

13.6 Asset tables

You can add customisable asset tables to the **Device Dashboard** with asset tags, links to other systems, etc.

To add asset tables to the Device Dashboard:

Go to **Admin** > **API** > **Command Console**.

Using the attribute name (replacing underscores with spaces), generate the column headings.

E.g.

```
add child Atlanta-ro asset

add text Atlanta-ro asset Asset_Tag = 1234

add text Atlanta-ro asset SSH =
"<a href='ssh://10.1.2.3'>SSH</a>"

add text Atlanta-ro asset Wiki = "<a href='https://mywiki.
example.com/device/Atlanta-ro.html'>link</a>"
```

Click **Run Commands**.

13.7 IP firewall rules

To configure IP firewall rules:

Go to **Admin** > **General** > **IPFW Rules**.

Warning: for expert use only.

Refer to the warning notice and guidance on the right-hand side of the page.

Configure your rules in the text field.

Click **Save**.

13.8 Login banner

The login banner tool enables you to display a personalised message for users on your AKIPS login page.

To add a personalised login banner:

Go to **Admin** > **General** > **Login Banner**.

Type your message into the text field.

Click **Save**.

Chapter 14

Access control

14.1 Authentication settings

14.1.1 Local (Unix)

To configure authentication settings for Local (Unix):

Go to **Admin** > **Users / Profiles** > **Authentication**.

From the drop-down list, select **Local / Unix**.

Click **Save**.

14.1.2 LDAP

To configure authentication settings for LDAP:

Go to **Admin** > **Users / Profiles** > **Authentication**.

From the drop-down list, select **LDAP**.

Complete the following settings and then click **Save**.

Text field	Details
Server	Type the name or IP address of the LDAP server. You can also include the port number (optional). Use the following syntax: `{IP address}[:{port number}]` E.g. `10.2.78.20`
SSL/TLS	From the list, select the appropriate communication protocol: • none • SSL • STARTTLS
Base DN	Type the DN for the section of the directory where AKIPS should start searching for users and groups E.g. `dc=mydomain,dc=com`

(continued)

Text field	Details
Bind DN	(Optional) Type the full DN for the credential used to authenticate to the directory server. If left blank, AKIPS will use an anonymous bind E.g. `cn=admin1,cn=users,dc=mydomain,dc=com`
Bind Password	(Optional) Type the password for the bind DN
Scope	Select the appropriate search scope: • subtree • one-level
Login Attribute	Select the appropriate attribute to authenticate the user E.g. `uid`
SSL/TLS Certificate	Copy and paste your CA certificate for SSL/TLS authentication. It must be encrypted and in PEM format

14.1.3 RADIUS

To configure authentication settings for RADIUS:

Go to **Admin** > **Users / Profiles** > **Authentication**.

From the drop-down list, select **RADIUS**.

Complete the following settings:

Text field	Details
Server	Type the name or IP address of the RADIUS server. You can also include the port number (optional). Use the following syntax: `{IP address}[:{port number}]` E.g. `10.2.78.20`
Shared Secret	Add the shared secret text string, which serves as a password between hosts

Click **Save**.

14.1.4 TACACS+

To configure authentication settings for TACACS+:

Go to **Admin** > **Users / Profiles** > **Authentication**.

From the drop-down list, select **TACACS+**.

Complete the following settings:

Text field	Details
Server	Type the name or IP address of the TACACS+ server. You can also include the port number (optional). Use the following syntax: `{IP address}[:{port number}]` E.g. `10.2.78.20`
Shared Secret	Add the shared secret text string, which serves as a password between hosts

Click **Save**.

14.2 Profile groups

A profile group is a group of users (see 14.3) who all have the same access rights.

You can create, configure and delete profile groups at **Admin** > **Users / Profiles** > **Profile Settings**.

To create a profile group:

In the text field, type the name of the new profile group.

Click **Add**.

To configure a profile group:

Select the required profile group.

To allocate access to all groups:

Click the **All Groups** switch **On**.

To allocate access to all reports:

Click the **All Reports** switch **On**.

To allocate/remove access to selected groups:

Click **Edit Groups**.

From the list, select the required group.

Click **Include/Exclude**.

To allocate/remove access to selected reports:

Click **Edit Reports**.

From the list, select the required report.

Click **Include/Exclude**.

To delete a profile group:

Select the required profile group.

Click **Delete**.

Click **OK**.

14.3 User accounts

Admin users can view, create and delete accounts for any AKIPS user.

To view a user account:

Hover your cursor over **User** (on the right-hand side of the menu bar).

Select a profile.

You will still be logged in as the admin user but AKIPS will display menu items for the selected user account.

To create a user account:

Go to **Admin > Users / Profiles > User Settings**.

In the **Username** text field, type a unique username (without spaces or capital letters).

In the **Full Name** text field, type the user's name (with spaces and capital letters).

In the **Password** text field, type a password.

In the **Email** text field, type the user's email address.

Using the **Profile** drop-down list, allocate the user to a profile group (see 14.2).

Click **Add**.

To delete a user account:

Go to **Admin > Users / Profiles > User Settings**.

Select **Delete** beside the account.

Click **OK**.

Chapter 15

Requesting a MIB object

To request a MIB object:

Perform an SNMP walk of the required device:

Go to **Tools > Ping / SNMP Walk**.

Select the device.

AKIPS will display its configuration details.

In the **MIB Selector** drop-down list, select **All Objects**.

Click **SNMP Walk**.

After the walk has completed, click **Download Walk**.

If the walk is still progressing after 30 minutes, contact support@akips.com

Save the file without changing the default name.

Upload your SNMP walk file to https://www.akips.com/upload

Provide detailed notes regarding the MIB object you wish to monitor.
The AKIPS team will contact you if we require further information.

We will schedule your requested MIB object for a future AKIPS release.

Chapter 16

Sending data to AKIPS support

16.1 System logs

To send system logs to AKIPS support:

Go to **Admin** > **System** > **System Log Viewer.**

Next to **Download**, click **System Logs**.

AKIPS will provide a compressed archive txz file.

Upload the file to https://www.akips.com/upload

Complete the form with as much information as possible so the AKIPS support team can readily assist you.

Click **Upload**.

16.2 SNMP walk

To send an SNMP walk to AKIPS support:

Go to **Tools** > **Ping / SNMP Walk**.

Specify the device by either:

- typing an IP address and completing the SNMP credentials
- selecting a device.

In the **MIB Selector** drop-down list, select **All Objects**.

Click **SNMP Walk**.

The walk may take from a few seconds to several hours to complete, depending on the speed of the device.

If the walk times out, AKIPS will suggest alternative options.

Click **Download Walk**.

AKIPS will provide a compressed archive xz file.

If AKIPS support has also requested the packet capture:

Click **Download Packet Capture**.

AKIPS will provide a gzipped pcap file.

Upload the file/s to https://www.akips.com/upload

Complete the form with as much information as possible so the AKIPS support team can readily assist you.

Click **Upload**.

16.3 Packet capture

To send a packet capture to AKIPS support:

Go to **Tools** > **Ping / SNMP Walk**.

Specify the device by either:

- typing an IP address
- selecting a device.

Leave the duration as the default (**10m**).

Click **Packet Capture**.

A timer will count down the time left until the capture completes.

Click **Download Packet Capture**.

AKIPS will provide a gzipped pcap file.

Upload the file to https://www.akips.com/upload

Complete the form with as much information as possible so the AKIPS support team can readily assist you.

Click **Upload**.

You can review the packet capture via an app such as Wireshark.

16.4 Switch port mapper logs

To send switch port mapper logs to AKIPS support:

Go to **Admin** > **System** > **System Log Viewer**.

Click **Switch Port Mapper Logs**.

AKIPS will provide a compressed archive tgz file.

Upload the file to https://www.akips.com/upload

Complete the form with as much information as possible so the AKIPS support team can readily assist you.

Click **Upload**.

16.5 Discover logs

To send discover logs to AKIPS support:

Go to **Admin** > **Discover** > **Discover Log Viewer**.

Click **Download Logs**.

AKIPS will provide a compressed archive txz file.

Upload the file to https://www.akips.com/upload

Complete the form with as much information as possible so the AKIPS support team can readily assist you.

Click **Upload**.

Index

U

V