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 |
|---|---|---|
| 17 | 22.1 | January 2022 |

# 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 |
| CDP | Cisco discovery protocol |
| 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 |
| LLDP | link layer discovery 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 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**.

Links to other parts of this guide are shown 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.

Websites and email addresses are in blue.

If they are also hyperlinks, they are shown as cyan boxes.

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

Code is in `monospace`.

Further:

> Command syntax is in `red monospace`.
>
> E.g. `{ddd} {hh:mm} to {hh:mm}`
>
> Input (by the user) is in `blue monospace`.
>
> E.g. `tf dump last7d`
>
> Output (by AKIPS) is in `cyan monospace`.
>
> E.g. `cisco-74-1-1 sys ip4addr = 10.74.1.1`

## 1.3 Syntax

Syntax may be presented in this guide across multiple lines due to layout constraints. When using AKIPS, 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

Warning: for expert use only.

Only admin users may access the command console.

### To use the command console:

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

#### To run commands:

In the text field, enter your command/s. (For detailed syntax, refer to the AKIPS *API reference guide*.)

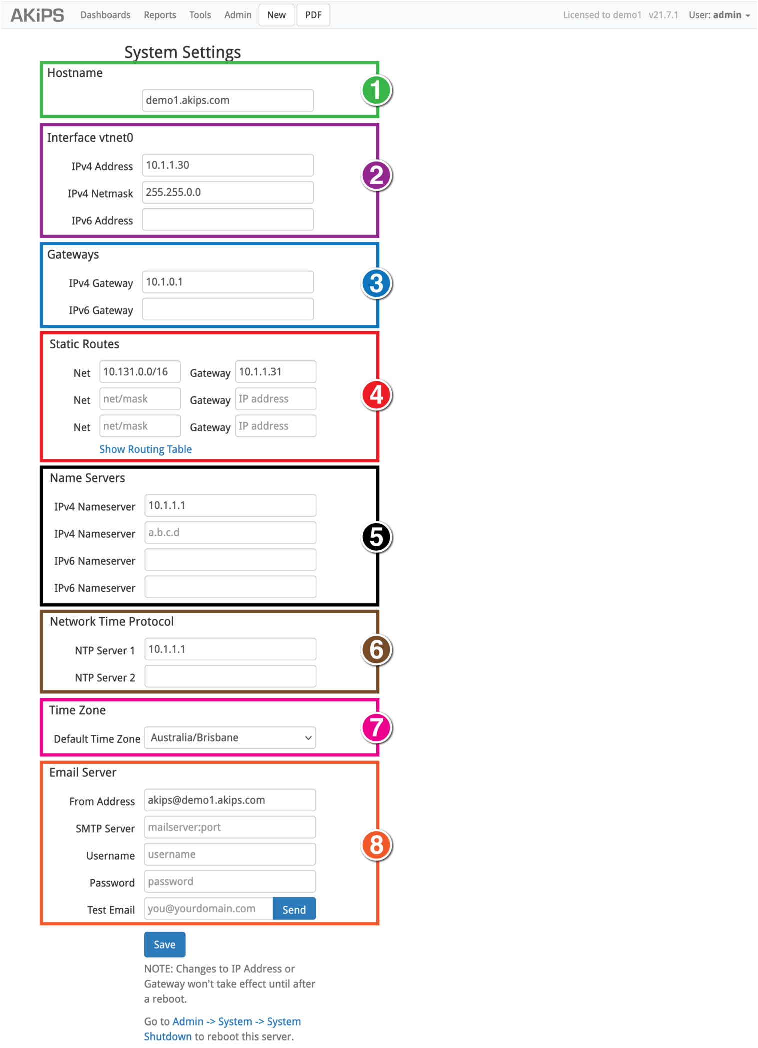
Click **Run Commands**.

#### To view your command history:

Click **History**.

## 2.2 System settings

To view the video *AKIPS system settings*,
visit https://vimeo.com/manage/videos/603622131



System Settings

Hostname
demo1.akips.com

Interface vtnet0
IPv4 Address: 10.1.1.30
IPv4 Netmask: 255.255.0.0
IPv6 Address:

Gateways
IPv4 Gateway: 10.1.0.1
IPv6 Gateway:

Static Routes
Net: 10.131.0.0/16 Gateway: 10.1.1.31
Net: net/mask Gateway: IP address
Net: net/mask Gateway: IP address
Show Routing Table

Name Servers
IPv4 Nameserver: 10.1.1.1
IPv4 Nameserver: a.b.c.d
IPv6 Nameserver:
IPv6 Nameserver:

Network Time Protocol
NTP Server 1: 10.1.1.1
NTP Server 2:

Time Zone
Default Time Zone: Australia/Brisbane

Email Server
From Address: akips@demo1.akips.com
SMTP Server: mailserver:port
Username: username
Password: password
Test Email: you@yourdomain.com

NOTE: Changes to IP Address or Gateway won't take effect until after a reboot.

Go to Admin -> System -> System Shutdown to reboot this server.

*Graphic 1: navigating the AKIPS system settings*

*1. hostname (see 2.2.1); 2. interface vtnet0 (see 2.2.2);*
*3. gateways (see 2.2.3); 4. static routes (see 2.2.4);*
*5. name servers (see 2.2.5); 6. network time protocol (see 2.2.6);*
*7. timezone (see 2.2.7); 8. email server (see 2.2.8).*

### 2.2.1 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.

#### To configure the hostname:

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

In the **Hostname** text field (see 2.2), type your hostname, consisting of only:

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

Click **Save**.

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

Click **Reboot Server**.

### 2.2.2 Interface vtnet0

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

## To configure the interface vtnet0:

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

Scroll to the **Interface vtnet0** section (see 2.2).

In the applicable text fields, type either the:

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

Click **Save**.

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

Click **Reboot Server**.

### 2.2.3 Gateways

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

#### To configure the gateways:

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

Scroll to the **Gateways** section (see 2.2).

In the applicable text field, type either the:

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

Click **Save**.

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

Click **Reboot Server**.

### 2.2.4 Static routes

#### To configure the static routes:

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

Scroll to the **Static Routes** section (see 2.2).

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

To configure each rule:

- in the **Net** text field, type the subnet mask
- in the corresponding **Gateway** text field, type the IP address.

Click **Save**.

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

Click **Reboot Server**.

### 2.2.5 Name servers

#### To configure the name servers:

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

Scroll to the **Name Servers** section (see 2.2).

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

Click **Save**.

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

Click **Reboot Server**.

### 2.2.6 Network time protocol

The network time protocol server helps keep accurate time across your network.

#### To configure the network time protocol:

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

Scroll to the **Network Time Protocol** section (see 2.2).

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

Click **Save**.

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

Click **Reboot Server**.

### 2.2.7 Timezone

The timezone helps keep accurate time across your network.

#### To configure the timezone:

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

Scroll to the **Time Zone** section (see 2.2).

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

Click **Save**.

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

Click **Reboot Server**.

### 2.2.8 Email server

This setting enables AKIPS to send email alerts (see 6).

#### To configure the email server:

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

Scroll to the **Email Server** section (see 2.2).

To change the default email address, enter it in the **From Address** text field.

In the **SMTP Server** text field, type the hostname or IP address of your SMTP server. The port number is optional.

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

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

To test, type your email address in the **Test Email** text field and click **Send**.

Click **Save**.

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

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** | your organisation name | `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 view the video *Forwarding NetFlow, syslog & SNMP traps in AKIPS*, visit https://vimeo.com/manage/videos/527555899

### 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 it receives on UDP port 162 to the defined list of IPv4 addresses on default port 162.

E.g.

```
10.1.8.35

10.1.8.82

10.2.9.1
```

### NetFlow Forwarding

AKIPS forwards all raw NetFlow packets it receives via either SCTP or UDP ports 2055, 4739, 9995, or 9996 to the defined list of IPv4 addresses and port numbers.

E.g.

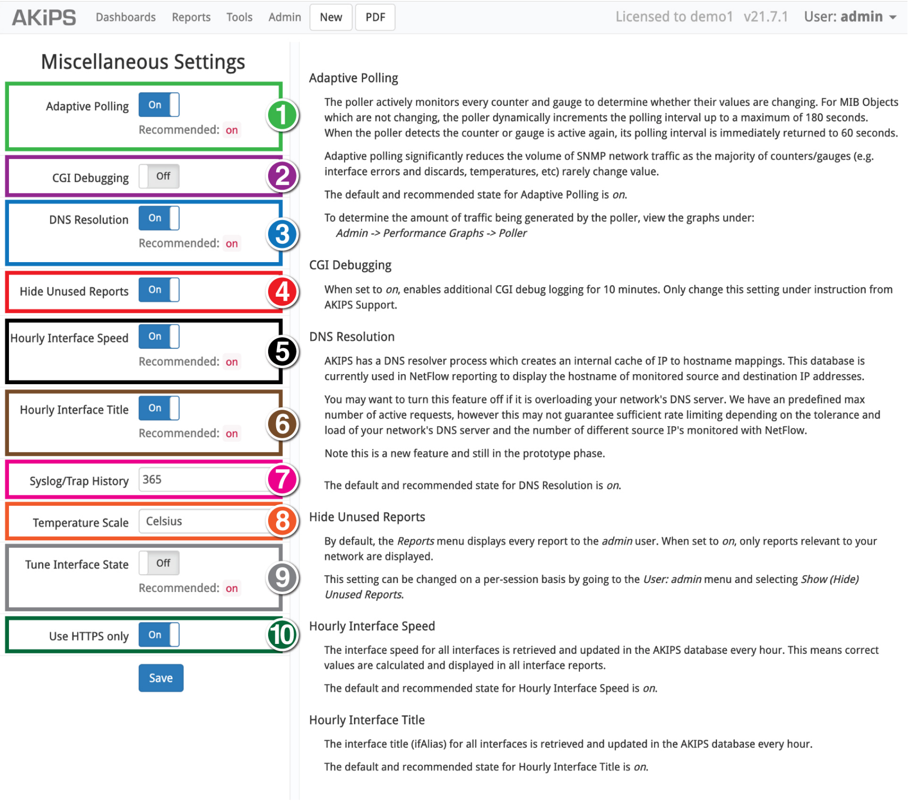
```
10.1.8.35 9995

10.1.8.82 9996

10.2.9.1 2055
```

## 2.6 Miscellaneous settings

To view the video *AKIPS miscellaneous settings*,
visit https://vimeo.com/manage/videos/542993281



Miscellaneous Settings

Adaptive Polling: On — Recommended: on

CGI Debugging: Off

DNS Resolution: On — Recommended: on

Hide Unused Reports: On

Hourly Interface Speed: On — Recommended: on

Hourly Interface Title: On — Recommended: on

Syslog/Trap History: 365

Temperature Scale: Celsius

Tune Interface State: Off — Recommended: on

Use HTTPS only: On

Adaptive Polling

The poller actively monitors every counter and gauge to determine whether their values are changing. For MIB Objects which are not changing, the poller dynamically increments the polling interval up to a maximum of 180 seconds. When the poller detects the counter or gauge is active again, its polling interval is immediately returned to 60 seconds.

Adaptive polling significantly reduces the volume of SNMP network traffic as the majority of counters/gauges (e.g. interface errors and discards, temperatures, etc) rarely change value.

The default and recommended state for Adaptive Polling is *on*.

To determine the amount of traffic being generated by the poller, view the graphs under:
*Admin -> Performance Graphs -> Poller*

CGI Debugging

When set to *on*, enables additional CGI debug logging for 10 minutes. Only change this setting under instruction from AKIPS Support.

DNS Resolution

AKIPS has a DNS resolver process which creates an internal cache of IP to hostname mappings. This database is currently used in NetFlow reporting to display the hostname of monitored source and destination IP addresses.

You may want to turn this feature off if it is overloading your network's DNS server. We have an predefined max number of active requests, however this may not guarantee sufficient rate limiting depending on the tolerance and load of your network's DNS server and the number of different source IP's monitored with NetFlow.

Note this is a new feature and still in the prototype phase.

The default and recommended state for DNS Resolution is *on*.

Hide Unused Reports

By default, the *Reports* menu displays every report to the *admin* user. When set to *on*, only reports relevant to your network are displayed.

This setting can be changed on a per-session basis by going to the *User: admin* menu and selecting *Show (Hide) Unused Reports*.

Hourly Interface Speed

The interface speed for all interfaces is retrieved and updated in the AKIPS database every hour. This means correct values are calculated and displayed in all interface reports.

The default and recommended state for Hourly Interface Speed is *on*.

Hourly Interface Title

The interface title (ifAlias) for all interfaces is retrieved and updated in the AKIPS database every hour.

The default and recommended state for Hourly Interface Title is *on*.

*Graphic 2: navigating the AKIPS miscellaneous settings*

*1. adaptive polling (see 2.6.1); 2. CGI debugging (see 2.6.2);*
*3. DNS resolution (see 2.6.3); 4. hide unused reports (see 2.6.4);*
*5. hourly interface speed (see 2.6.5); 6. hourly interface title (see 2.6.6);*
*7. syslog/trap history (see 2.6.7); 8. temperature scale (see 2.6.8);*
*9. tune interface state (see 2.6.9); 10. use HTTPS only (see 2.6.10).*

### 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 view the video *AKIPS intelligent polling*,
visit https://vimeo.com/manage/videos/460367808

#### To turn off adaptive polling:

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

Click the **Adaptive Polling** button **Off** (see 2.6).

Click **Save**.

### 2.6.2 CGI debugging

The default and recommended state is off.

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

#### To turn on CGI debugging:

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

Click the **CGI Debugging** button **On** (see 2.6).

Click **Save**.

### 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.

#### 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** (see 2.6).

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** (see 2.6).

Click **Save**.

### 2.6.5 Hourly interface speed

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

AKIPS then calculates and displays correct values in all interface reports.

### To turn off hourly interface speed:

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

Click the **Hourly Interface Speed** button **Off** (see 2.6).

Click **Save**.

### 2.6.6 Hourly interface title

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

### To turn off hourly interface title:

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

Click the **Hourly Interface Title** button **Off** (see 2.6).

Click **Save**.

### 2.6.7 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 (see 2.6), type a value or use the arrows to increase or decrease the value (from 1 to 1000).

Click **Save**.

### 2.6.8 Temperature scale

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

#### To change the temperature scale to Fahrenheit:

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

In the **Temperature Scale** drop-down list, select **Fahrenheit** (see 2.6).

Click **Save**.

### 2.6.9 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.

#### To turn off tune interface state:

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

Click the **Tune Interface State** button **Off** (see 2.6).

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** (see 2.6).

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**).

## 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 |
| existing SNMP parameters (see 3.1.4) | n/a | n/a |
| device-match rules (see 3.1.5) | Y | N |
| device-naming scheme (see 3.1.6) | Y | Y |
| strip domain names (see 3.1.7) | Y | Y |
| optional features (see 3.1.8) | Y | Y |
| interface types (see 3.1.9) | 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<br>rate 2000<br>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<br>pass 3<br>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<br>`limit 120`<br>`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<br>`rate 50`<br>`wait 5`<br>`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.

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

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}
```

#### 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
```

### 3.1.4 Existing SNMP parameters

This lists the SNMP parameters of devices which AKIPS has already discovered, for informational purposes.

### 3.1.5 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.

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

Use the following syntax:

```
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.*
```

### 3.1.6 Device-naming scheme

You can identify devices by:

- sysName
- IP address.

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

### 3.1.7 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` |

### 3.1.8 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**.

The optional features are:

#### 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
```

#### Cisco Error-Disable

The error-disable feature in Cisco switches automatically disables a switch port when it detects an error.

AKIPS dynamically creates the MIB objects for error-disable ports in a conceptual MIB table.

AKIPS cannot collect the error-disable state via the normal polling process, but only during a discover/rewalk.

### Cisco Class-Based QoS

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

E.g.

```
add device group tech_cisco_qos

assign device router1 = tech_cisco_qos
```

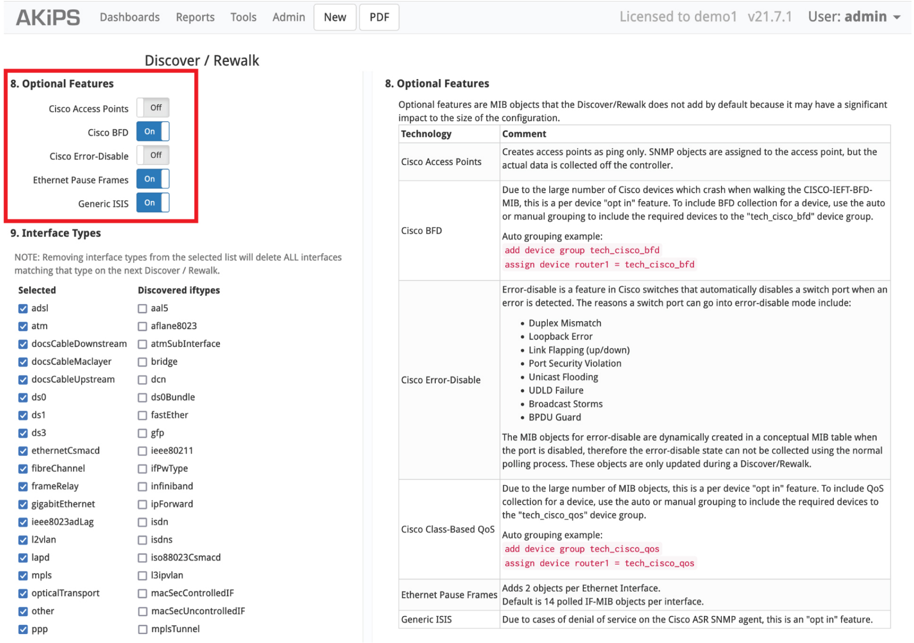
### Ethernet Pause Frames

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.



Discover / Rewalk

**8. Optional Features**

| | |
|---|---|
| Cisco Access Points | Off |
| Cisco BFD | On |
| Cisco Error-Disable | Off |
| Ethernet Pause Frames | On |
| Generic ISIS | On |

**9. Interface Types**

NOTE: Removing interface types from the selected list will delete ALL interfaces matching that type on the next Discover / Rewalk.

**Selected**

☑ adsl
☑ atm
☑ docsCableDownstream
☑ docsCableMaclayer
☑ docsCableUpstream
☑ ds0
☑ ds1
☑ ds3
☑ ethernetCsmacd
☑ fibreChannel
☑ frameRelay
☑ gigabitEthernet
☑ ieee8023adLag
☑ l2vlan
☑ lapd
☑ mpls
☑ opticalTransport
☑ other
☑ ppp

**Discovered iftypes**

□ aal5
□ aflane8023
□ atmSubInterface
□ bridge
□ dcn
□ ds0Bundle
□ fastEther
□ gfp
□ ieee80211
□ ifPwType
□ infiniband
□ ipForward
□ isdn
□ isdns
□ iso88023Csmacd
□ l3ipvlan
□ macSecControlledIF
□ macSecUncontrolledIF
□ mplsTunnel

**8. Optional Features**

Optional features are MIB objects that the Discover/Rewalk does not add by default because it may have a significant impact to the size of the configuration.

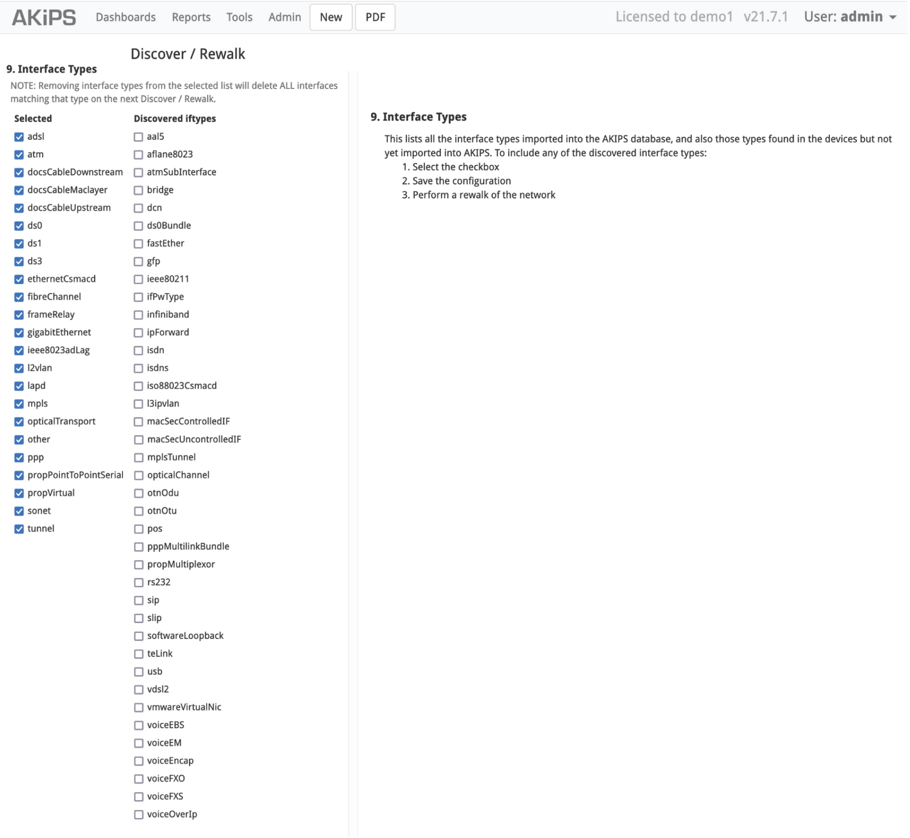
| Technology | Comment |
|---|---|
| Cisco Access Points | Creates access points as ping only. SNMP objects are assigned to the access point, but the actual data is collected off the controller. |
| Cisco BFD | Due to the large number of Cisco devices which crash when walking the CISCO-IEFT-BFD-MIB, this is a per device "opt in" feature. To include BFD collection for a device, use the auto or manual grouping to include the required devices to the "tech_cisco_bfd" device group.<br>Auto grouping example:<br>`add device group tech_cisco_bfd`<br>`assign device router1 = tech_cisco_bfd` |
| Cisco Error-Disable | Error-disable is a feature in Cisco switches that automatically disables a switch port when an error is detected. The reasons a switch port can go into error-disable mode include:<br>• Duplex Mismatch<br>• Loopback Error<br>• Link Flapping (up/down)<br>• Port Security Violation<br>• Unicast Flooding<br>• UDLD Failure<br>• Broadcast Storms<br>• BPDU Guard<br>The MIB objects for error-disable are dynamically created in a conceptual MIB table when the port is disabled, therefore the error-disable state can not be collected using the normal polling process. These objects are only updated during a Discover/Rewalk. |
| Cisco Class-Based QoS | Due to the large number of MIB objects, this is a per device "opt in" feature. To include QoS collection for a device, use the auto or manual grouping to include the required devices to the "tech_cisco_qos" device group.<br>Auto grouping example:<br>`add device group tech_cisco_qos`<br>`assign device router1 = tech_cisco_qos` |
| Ethernet Pause Frames | Adds 2 objects per Ethernet Interface.<br>Default is 14 polled IF-MIB objects per interface. |
| Generic ISIS | Due to cases of denial of service on the Cisco ASR SNMP agent, this is an "opt in" feature. |

*Graphic 3: configuring optional features*

### 3.1.9 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/remove interface types for/from 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.



Discover / Rewalk

**9. Interface Types**

NOTE: Removing interface types from the selected list will delete ALL interfaces matching that type on the next Discover / Rewalk.

**Selected**

☑ adsl
☑ atm
☑ docsCableDownstream
☑ docsCableMaclayer
☑ docsCableUpstream
☑ ds0
☑ ds1
☑ ds3
☑ ethernetCsmacd
☑ fibreChannel
☑ frameRelay
☑ gigabitEthernet
☑ ieee8023adLag
☑ l2vlan
☑ lapd
☑ mpls
☑ opticalTransport
☑ other
☑ ppp
☑ propPointToPointSerial
☑ propVirtual
☑ sonet
☑ tunnel

**Discovered iftypes**

□ aal5
□ aflane8023
□ atmSubInterface
□ bridge
□ dcn
□ ds0Bundle
□ fastEther
□ gfp
□ ieee80211
□ ifPwType
□ infiniband
□ ipForward
□ isdn
□ isdns
□ iso88023Csmacd
□ l3ipvlan
□ macSecControlledIF
□ macSecUncontrolledIF
□ mplsTunnel
□ opticalChannel
□ otnOdu
□ otnOtu
□ pos
□ pppMultilinkBundle
□ propMultiplexor
□ rs232
□ sip
□ slip
□ softwareLoopback
□ teLink
□ usb
□ vdsl2
□ vmwareVirtualNic
□ voiceEBS
□ voiceEM
□ voiceEncap
□ voiceFXO
□ voiceFXS
□ voiceOverIp

**9. Interface Types**

This lists all the interface types imported into the AKIPS database, and also those types found in the devices but not yet imported into AKIPS. To include any of the discovered interface types:

1. Select the checkbox
2. Save the configuration
3. Perform a rewalk of the network

*Graphic 4: configuring interface types*

## Case study

A customer noticed that AKIPS was displaying statistics for his Cisco ASR and ISR routers, but not for their routed sub interfaces.

He resolved this by going to **Admin > Discover > Discover / Rewalk**, scrolling to the **Interface Types** section, and selecting the checkboxes for **l2vlan** and **l3ipvlan**.

## 3.2 Discover logs

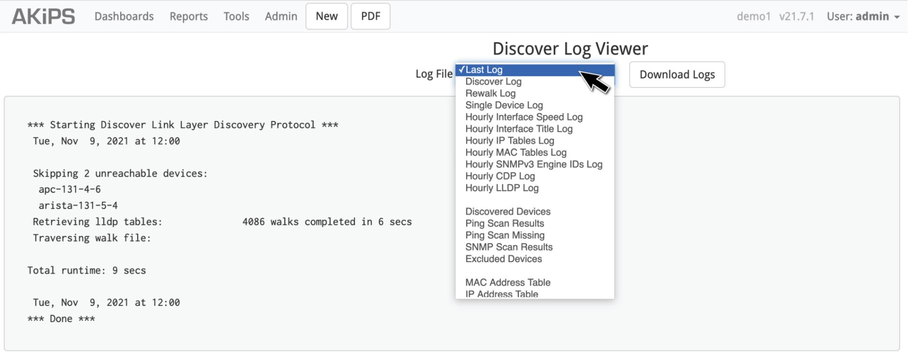
A number of logs and reports are available for you to review a discover, rewalk, component, or group of components.

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

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

### To view the discover logs:

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



```
*** Starting Discover Link Layer Discovery Protocol ***
 Tue, Nov  9, 2021 at 12:00

 Skipping 2 unreachable devices:
  apc-131-4-6
  arista-131-5-4
 Retrieving lldp tables:             4086 walks completed in 6 secs
 Traversing walk file:

Total runtime: 9 secs

 Tue, Nov  9, 2021 at 12:00
*** Done ***
```

*Graphic 5: viewing the discover logs*

### 3.2.1 Last log

The last log contains details of the most recent discover/rewalk.

#### To view the last log:

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

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

### 3.2.2 Discover log

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 ***
  ```

### To view the discover log:

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

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

### 3.2.3 Rewalk log

The rewalk log contains details of the most recent rewalk.

It provides details in the same format as the discover log (see 3.2.2), and includes configuration changes to any monitored device.

### To view the rewalk log:

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

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

### 3.2.4 Single-device log

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:
...
```

## To view the single-device log:

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

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

### 3.2.5 Hourly interface-speed log

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 ***
```

#### To view the hourly interface-speed log:

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

In the **Log File** drop-down list, select **Hourly Interface Speed Log**.

### 3.2.6 Hourly interface-title log

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 ***
```

## To view the hourly interface-title log:

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

In the **Log File** drop-down list, select **Hourly Interface Title Log**.

### 3.2.7 Hourly IP tables log

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 ***
```

#### To view the hourly IP tables log:

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

In the **Log File** drop-down list, select **Hourly IP Tables Log**.

### 3.2.8 Hourly MAC tables log

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 ***
```

## To view the hourly MAC tables log:

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

In the **Log File** drop-down list, select **Hourly MAC Tables Log**.

### 3.2.9 Hourly SNMPv3 engine IDs log

The hourly SNMPv3 engine IDs 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 ***
```

#### To view the hourly SNMPv3 engine IDs log:

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

In the **Log File** drop-down list, select **Hourly SNMPv3 Engine IDs Log**.

### 3.2.10 Hourly CDP log

The hourly CDP log displays details of the hourly Cisco discovery protocol.

#### To view the hourly CDP log:

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

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

### 3.2.11 Hourly LLDP log

The hourly LLDP log displays details of the hourly link layer discovery protocol.

#### To view the hourly LLDP log:

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

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

### 3.2.12 Discovered-devices log

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
```

#### To view the discovered-devices log:

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

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

### 3.2.13 Ping-scan results log

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
...
```

#### To view the ping-scan results log:

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

In the **Log File** drop-down list, select **Ping Scan Results**.

### 3.2.14 Ping-scan missing log

The ping-scan missing log contains a list of the IP addresses which did not reply to AKIPS's ping requests during the most recent discover.

#### To view the ping-scan missing log:

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

In the **Log File** drop-down list, select **Ping Scan Missing**.

### 3.2.15 SNMP-scan results log

The SNMP-scan results log checks all IP addresses against the SNMP credentials defined during the discover.

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
...
```

### To view the SNMP-scan results log:

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

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

### 3.2.16 Excluded-devices log

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 3.1.5).

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 ...
```

### To view the excluded-devices log:

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

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

### 3.2.17 MAC address table report

The MAC address table report 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
...
```

## To view the MAC address table report:

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

In the **Log File** drop-down list, select **MAC Address Table**.

### 3.2.18 IP address table report

The IP address table report 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
...
```

## To view the IP address table report:

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

In the **Log File** drop-down list, select **IP Address Table**.

### 3.2.19 IP address to name report

The IP address to name report 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
...
```

## To view the IP address to name report:

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

In the **Log File** drop-down list, select **IP Address To Name**.

### 3.2.20 SNMP walk results report

The SNMP walk results report 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
...
```

### To view the SNMP walk results report:

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

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

### 3.2.21 SNMP walk failures report

The SNMP walk failures report 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
```

### To view the SNMP walk failures report:

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

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

## 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.

| **Text field** | **Description** |
|---|---|
| **Name** | (mandatory) the device name (no spaces) |
| **IPv4** or **IPv6** | (mandatory) the IP address |
| **Description** | the description to appear on the **Device Dashboard** |
| **Location** | the physical location to appear on the **Device Dashboard** |
| **Contact** | contact details for the device |
| **Group** | the device group |

Click **Save**.

### 3.3.4 Single SNMP device

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

### To add a single SNMP device:

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

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

Click **Discover**.

## 3.4 Locating missing devices

### 3.4.1 Disabling exclusion rules

AKIPS may exclude devices from discover/rewalk due to exclusion rules.

E.g.

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**.

### 3.4.2 Resolving duplicate SNMPv2-MIB sysNames

AKIPS may exclude devices from discover/rewalk due to duplicate SNMPv2-MIB sysNames.

E.g.

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:

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

Select the device.

In the sysName text field, change the name to make it unique.

Click **Save**.

Run discover to add the device (see 3.3.4).

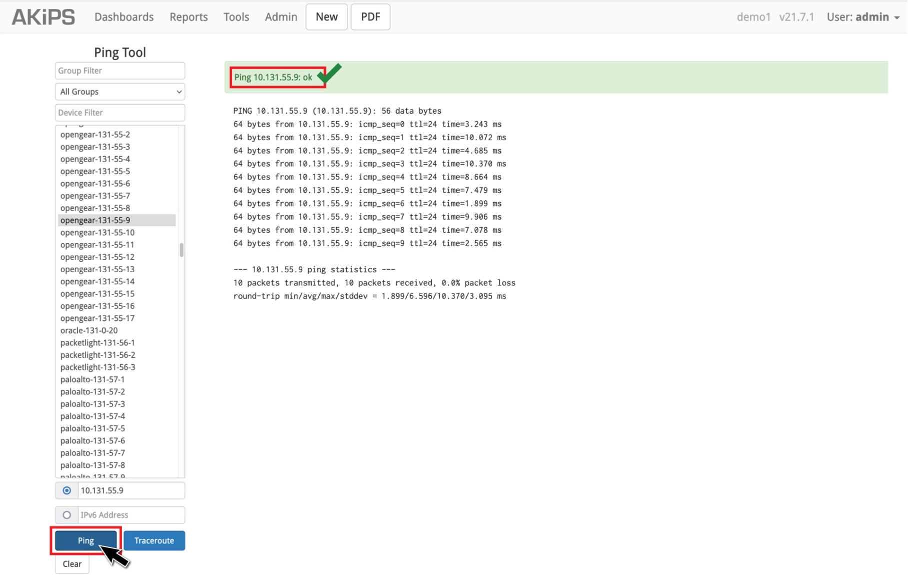
### 3.4.3 Pinging a device

## To ping a device:

Go to **Tools > Ping Tool**.

Select a device.

Click **Ping**.



● 10.131.55.9

Ping 10.131.55.9: ok ✓

```
PING 10.131.55.9 (10.131.55.9): 56 data bytes
64 bytes from 10.131.55.9: icmp_seq=0 ttl=24 time=3.243 ms
64 bytes from 10.131.55.9: icmp_seq=1 ttl=24 time=10.072 ms
64 bytes from 10.131.55.9: icmp_seq=2 ttl=24 time=4.685 ms
64 bytes from 10.131.55.9: icmp_seq=3 ttl=24 time=10.370 ms
64 bytes from 10.131.55.9: icmp_seq=4 ttl=24 time=8.664 ms
64 bytes from 10.131.55.9: icmp_seq=5 ttl=24 time=7.479 ms
64 bytes from 10.131.55.9: icmp_seq=6 ttl=24 time=1.899 ms
64 bytes from 10.131.55.9: icmp_seq=7 ttl=24 time=9.906 ms
64 bytes from 10.131.55.9: icmp_seq=8 ttl=24 time=7.078 ms
64 bytes from 10.131.55.9: icmp_seq=9 ttl=24 time=2.565 ms

--- 10.131.55.9 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.899/6.596/10.370/3.095 ms
```

*Graphic 6: pinging a device*

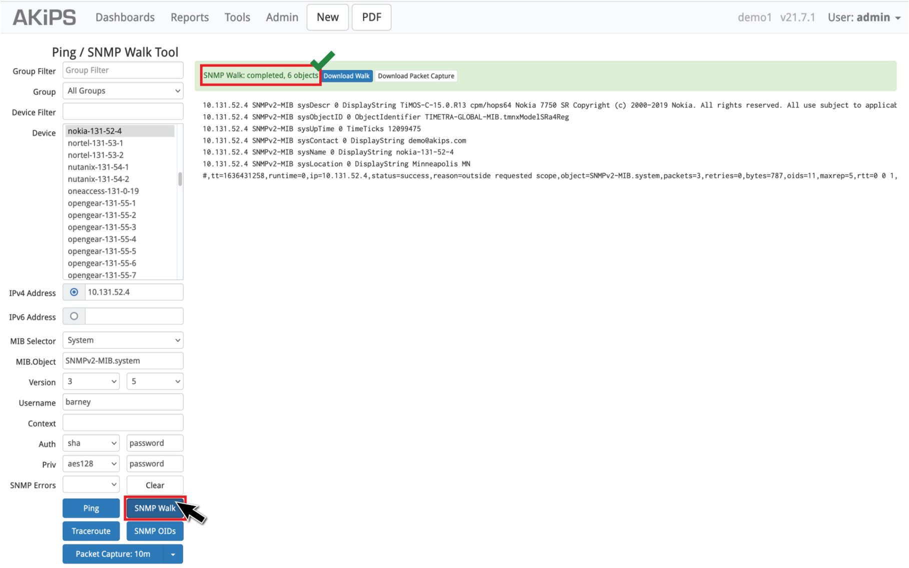
### 3.4.4 Walking a device

## To walk a device:

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

Select a device.

Click **SNMP Walk**.



Ping / SNMP Walk Tool

SNMP Walk: completed, 6 objects

```
10.131.52.4 SNMPv2-MIB sysDescr 0 DisplayString TiMOS-C-15.0.R13 cpm/hops64 Nokia 7750 SR Copyright (c) 2000-2019 Nokia. All rights reserved. All use subject to applicat
10.131.52.4 SNMPv2-MIB sysObjectID 0 ObjectIdentifier TIMETRA-GLOBAL-MIB.tmnxModelSRa4Reg
10.131.52.4 SNMPv2-MIB sysUpTime 0 TimeTicks 12099475
10.131.52.4 SNMPv2-MIB sysContact 0 DisplayString demo@akips.com
10.131.52.4 SNMPv2-MIB sysName 0 DisplayString nokia-131-52-4
10.131.52.4 SNMPv2-MIB sysLocation 0 DisplayString Minneapolis MN
#,tt=1636431258,runtime=0,ip=10.131.52.4,status=success,reason=outside requested scope,object=SNMPv2-MIB.system,packets=3,retries=0,bytes=787,oids=11,maxrep=5,rtt=0 0 1,
```

| | |
|---|---|
| Group Filter | Group Filter |
| Group | All Groups |
| Device Filter | |
| Device | nokia-131-52-4<br>nortel-131-53-1<br>nortel-131-53-2<br>nutanix-131-54-1<br>nutanix-131-54-2<br>oneaccess-131-0-19<br>opengear-131-55-1<br>opengear-131-55-2<br>opengear-131-55-3<br>opengear-131-55-4<br>opengear-131-55-5<br>opengear-131-55-6<br>opengear-131-55-7 |
| IPv4 Address | ● 10.131.52.4 |
| IPv6 Address | ○ |
| MIB Selector | System |
| MIB.Object | SNMPv2-MIB.system |
| Version | 3   5 |
| Username | barney |
| Context | |
| Auth | sha   password |
| Priv | aes128   password |
| SNMP Errors | |

*Graphic 7: walking a device*

### 3.4.5 Ruling out other common reasons for missing devices

## To rule out other 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

Using AKIPS's grouping rules, you can:

- specify what to include in, or 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). 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)
```

### Case studies

A customer used `add` and `assign` to add a device to a device group based on certain interface characteristics. He did this by combining a more specific group (device and interface) with a less specific group (device):

```
add interface group InterfaceMPLS
assign * * * IF-MIB.ifType value /mpls/ = InterfaceMPLS

add device group DeviceWithInterfaceMPLS
assign * * * any group InterfaceMPLS = DeviceWithInterfaceMPLS
```

### 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**.

Enable the required empty groups by switching the relevant switches **Off**:

- **Prune Device Groups**
- **Prune Interface Groups**
- **Prune Super Groups**

Click **Save**.

## 4.2 Manual grouping

Use manual grouping to:

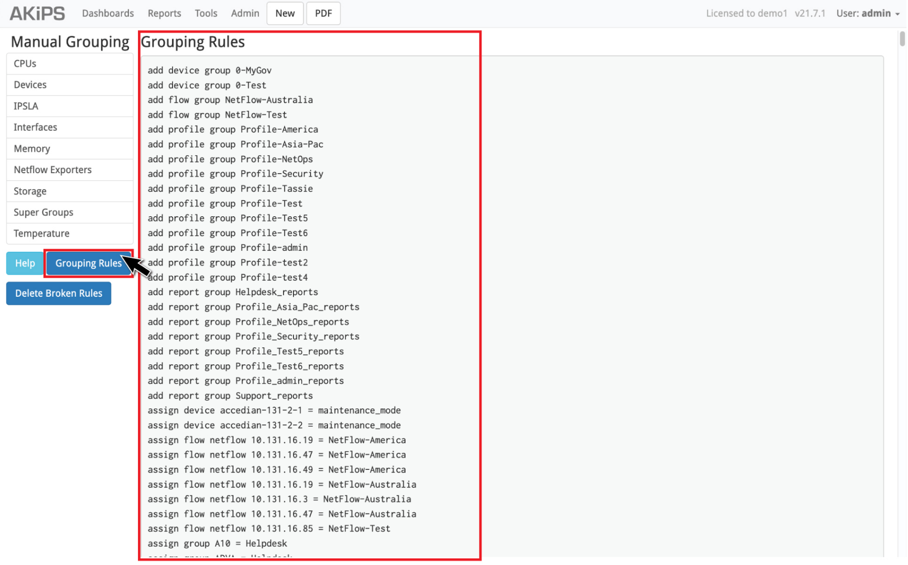
- view grouping rules and delete broken rules (see 4.2.1)
- add groups (see 4.2.2)
- rename groups (see 4.2.3)
- assign/remove devices to/from groups (see 4.2.4)
- delete groups (see 4.2.5).

### 4.2.1 Grouping rules

## To view grouping rules:

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

Click **Grouping Rules**.



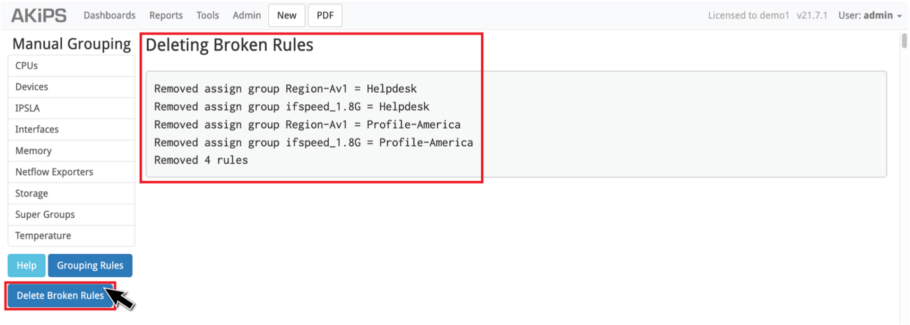
```
add device group 0-MyGov
add device group 0-Test
add flow group NetFlow-Australia
add flow group NetFlow-Test
add profile group Profile-America
add profile group Profile-Asia-Pac
add profile group Profile-NetOps
add profile group Profile-Security
add profile group Profile-Tassie
add profile group Profile-Test
add profile group Profile-Test5
add profile group Profile-Test6
add profile group Profile-admin
add profile group Profile-test2
add profile group Profile-test4
add report group Helpdesk_reports
add report group Profile_Asia_Pac_reports
add report group Profile_NetOps_reports
add report group Profile_Security_reports
add report group Profile_Test5_reports
add report group Profile_Test6_reports
add report group Profile_admin_reports
add report group Support_reports
assign device accedian-131-2-1 = maintenance_mode
assign device accedian-131-2-2 = maintenance_mode
assign flow netflow 10.131.16.19 = NetFlow-America
assign flow netflow 10.131.16.47 = NetFlow-America
assign flow netflow 10.131.16.49 = NetFlow-America
assign flow netflow 10.131.16.19 = NetFlow-Australia
assign flow netflow 10.131.16.3 = NetFlow-Australia
assign flow netflow 10.131.16.47 = NetFlow-Australia
assign flow netflow 10.131.16.85 = NetFlow-Test
assign group A10 = Helpdesk
```

*Graphic 8: viewing grouping rules*

## To delete broken grouping rules:

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

Click **Delete Broken Rules**.



Deleting Broken Rules

```
Removed assign group Region-Av1 = Helpdesk
Removed assign group ifspeed_1.8G = Helpdesk
Removed assign group Region-Av1 = Profile-America
Removed assign group ifspeed_1.8G = Profile-America
Removed 4 rules
```

*Graphic 9: deleting broken grouping rules*

### 4.2.2 Adding groups

#### To add a group:

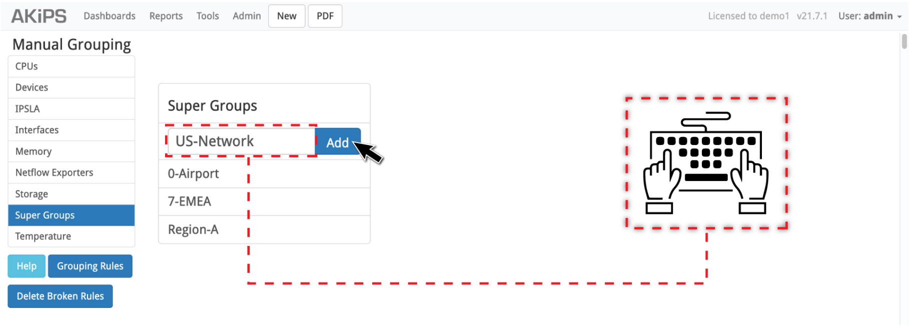
Go to **Admin > Grouping > Manual Grouping**.

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.



*Graphic 10: adding a group*

### 4.2.3 Renaming groups

#### To rename a group:

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

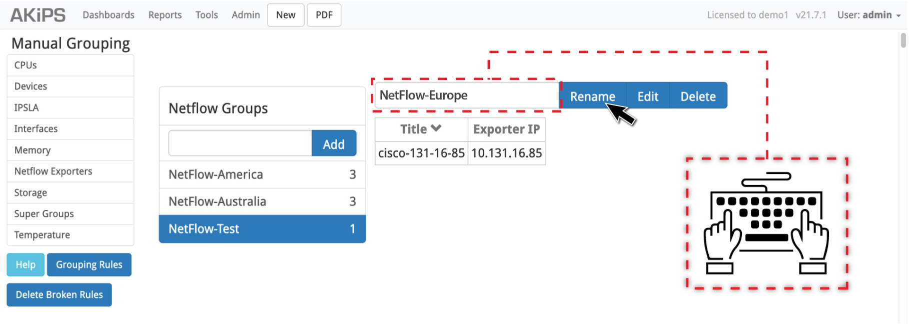
Select the group type.

Select the group name.

Overtype the new name.

Click **Rename**.

AKIPS will also update the group's associated rules.



| Title | Exporter IP |
|---|---|
| cisco-131-16-85 | 10.131.16.85 |

*Graphic 11: renaming a group*

### 4.2.4 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**.

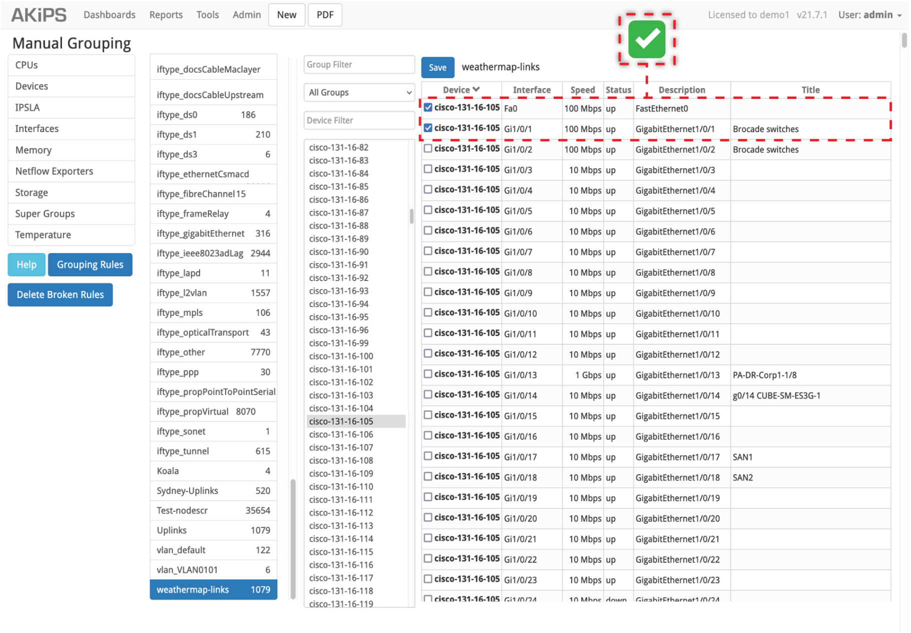
**To assign devices to the group:**

Select the checkbox next to a device.

**To remove devices from the group:**

Deselect the checkbox next to a device.

Click **Save**.



| | |
|---|---|
| iftype_docsCableMaclayer | |
| iftype_docsCableUpstream | |
| iftype_ds0 | 186 |
| iftype_ds1 | 210 |
| iftype_ds3 | 6 |
| iftype_ethernetCsmacd | |
| iftype_fibreChannel | 15 |
| iftype_frameRelay | 4 |
| iftype_gigabitEthernet | 316 |
| iftype_ieee8023adLag | 2944 |
| iftype_lapd | 11 |
| iftype_l2vlan | 1557 |
| iftype_mpls | 106 |
| iftype_opticalTransport | 43 |
| iftype_other | 7770 |
| iftype_ppp | 30 |
| iftype_propPointToPointSerial | |
| iftype_propVirtual | 8070 |
| iftype_sonet | 1 |
| iftype_tunnel | 615 |
| Koala | 4 |
| Sydney-Uplinks | 520 |
| Test-nodescr | 35654 |
| Uplinks | 1079 |
| vlan_default | 122 |
| vlan_VLAN0101 | 6 |
| weathermap-links | 1079 |

cisco-131-16-82
cisco-131-16-83
cisco-131-16-84
cisco-131-16-85
cisco-131-16-86
cisco-131-16-87
cisco-131-16-88
cisco-131-16-89
cisco-131-16-90
cisco-131-16-91
cisco-131-16-92
cisco-131-16-93
cisco-131-16-94
cisco-131-16-95
cisco-131-16-96
cisco-131-16-99
cisco-131-16-100
cisco-131-16-101
cisco-131-16-102
cisco-131-16-103
cisco-131-16-104
cisco-131-16-105
cisco-131-16-106
cisco-131-16-107
cisco-131-16-108
cisco-131-16-109
cisco-131-16-110
cisco-131-16-111
cisco-131-16-112
cisco-131-16-113
cisco-131-16-114
cisco-131-16-115
cisco-131-16-116
cisco-131-16-117
cisco-131-16-118
cisco-131-16-119

weathermap-links

| Device | Interface | Speed | Status | Description | Title |
|---|---|---|---|---|---|
| ☑ cisco-131-16-105 | Fa0 | 100 Mbps | up | FastEthernet0 | |
| ☑ cisco-131-16-105 | Gi1/0/1 | 100 Mbps | up | GigabitEthernet1/0/1 | Brocade switches |
| ☐ cisco-131-16-105 | Gi1/0/2 | 100 Mbps | up | GigabitEthernet1/0/2 | Brocade switches |
| ☐ cisco-131-16-105 | Gi1/0/3 | 10 Mbps | up | GigabitEthernet1/0/3 | |
| ☐ cisco-131-16-105 | Gi1/0/4 | 10 Mbps | up | GigabitEthernet1/0/4 | |
| ☐ cisco-131-16-105 | Gi1/0/5 | 10 Mbps | up | GigabitEthernet1/0/5 | |
| ☐ cisco-131-16-105 | Gi1/0/6 | 10 Mbps | up | GigabitEthernet1/0/6 | |
| ☐ cisco-131-16-105 | Gi1/0/7 | 10 Mbps | up | GigabitEthernet1/0/7 | |
| ☐ cisco-131-16-105 | Gi1/0/8 | 10 Mbps | up | GigabitEthernet1/0/8 | |
| ☐ cisco-131-16-105 | Gi1/0/9 | 10 Mbps | up | GigabitEthernet1/0/9 | |
| ☐ cisco-131-16-105 | Gi1/0/10 | 10 Mbps | up | GigabitEthernet1/0/10 | |
| ☐ cisco-131-16-105 | Gi1/0/11 | 10 Mbps | up | GigabitEthernet1/0/11 | |
| ☐ cisco-131-16-105 | Gi1/0/12 | 10 Mbps | up | GigabitEthernet1/0/12 | |
| ☐ cisco-131-16-105 | Gi1/0/13 | 1 Gbps | up | GigabitEthernet1/0/13 | PA-DR-Corp1-1/8 |
| ☐ cisco-131-16-105 | Gi1/0/14 | 10 Mbps | up | GigabitEthernet1/0/14 | g0/14 CUBE-SM-ES3G-1 |
| ☐ cisco-131-16-105 | Gi1/0/15 | 10 Mbps | up | GigabitEthernet1/0/15 | |
| ☐ cisco-131-16-105 | Gi1/0/16 | 10 Mbps | up | GigabitEthernet1/0/16 | |
| ☐ cisco-131-16-105 | Gi1/0/17 | 10 Mbps | up | GigabitEthernet1/0/17 | SAN1 |
| ☐ cisco-131-16-105 | Gi1/0/18 | 10 Mbps | up | GigabitEthernet1/0/18 | SAN2 |
| ☐ cisco-131-16-105 | Gi1/0/19 | 10 Mbps | up | GigabitEthernet1/0/19 | |
| ☐ cisco-131-16-105 | Gi1/0/20 | 10 Mbps | up | GigabitEthernet1/0/20 | |
| ☐ cisco-131-16-105 | Gi1/0/21 | 10 Mbps | up | GigabitEthernet1/0/21 | |
| ☐ cisco-131-16-105 | Gi1/0/22 | 10 Mbps | up | GigabitEthernet1/0/22 | |
| ☐ cisco-131-16-105 | Gi1/0/23 | 10 Mbps | up | GigabitEthernet1/0/23 | |
| ☐ cisco-131-16-105 | Gi1/0/24 | 10 Mbps | down | GigabitEthernet1/0/24 | |

*Graphic 12: assigning devices to a group*

### 4.2.5 Deleting groups

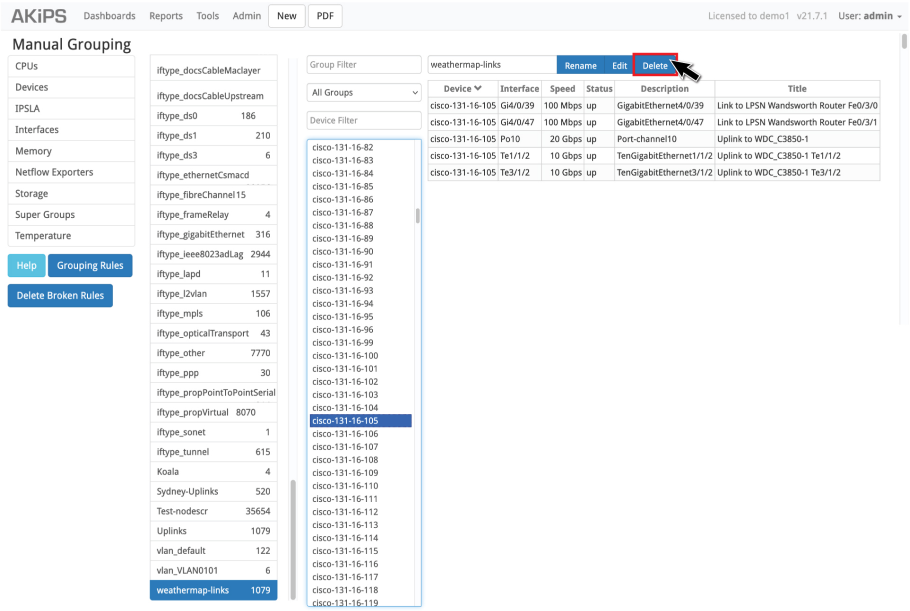
## To delete a group:

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

Select the group type.

Select the group name.

Click **Delete**.



| | |
|---|---|
| iftype_docsCableMaclayer | |
| iftype_docsCableUpstream | |
| iftype_ds0 | 186 |
| iftype_ds1 | 210 |
| iftype_ds3 | 6 |
| iftype_ethernetCsmacd | |
| iftype_fibreChannel | 15 |
| iftype_frameRelay | 4 |
| iftype_gigabitEthernet | 316 |
| iftype_ieee8023adLag | 2944 |
| iftype_lapd | 11 |
| iftype_l2vlan | 1557 |
| iftype_mpls | 106 |
| iftype_opticalTransport | 43 |
| iftype_other | 7770 |
| iftype_ppp | 30 |
| iftype_propPointToPointSerial | |
| iftype_propVirtual | 8070 |
| iftype_sonet | 1 |
| iftype_tunnel | 615 |
| Koala | 4 |
| Sydney-Uplinks | 520 |
| Test-nodescr | 35654 |
| Uplinks | 1079 |
| vlan_default | 122 |
| vlan_VLAN0101 | 6 |
| weathermap-links | 1079 |

cisco-131-16-82
cisco-131-16-83
cisco-131-16-84
cisco-131-16-85
cisco-131-16-86
cisco-131-16-87
cisco-131-16-88
cisco-131-16-89
cisco-131-16-90
cisco-131-16-91
cisco-131-16-92
cisco-131-16-93
cisco-131-16-94
cisco-131-16-95
cisco-131-16-96
cisco-131-16-99
cisco-131-16-100
cisco-131-16-101
cisco-131-16-102
cisco-131-16-103
cisco-131-16-104
cisco-131-16-105
cisco-131-16-106
cisco-131-16-107
cisco-131-16-108
cisco-131-16-109
cisco-131-16-110
cisco-131-16-111
cisco-131-16-112
cisco-131-16-113
cisco-131-16-114
cisco-131-16-115
cisco-131-16-116
cisco-131-16-117
cisco-131-16-118
cisco-131-16-119

weathermap-links

| Device | Interface | Speed | Status | Description | Title |
|---|---|---|---|---|---|
| cisco-131-16-105 | Gi4/0/39 | 100 Mbps | up | GigabitEthernet4/0/39 | Link to LPSN Wandsworth Router Fe0/3/0 |
| cisco-131-16-105 | Gi4/0/47 | 100 Mbps | up | GigabitEthernet4/0/47 | Link to LPSN Wandsworth Router Fe0/3/1 |
| cisco-131-16-105 | Po10 | 20 Gbps | up | Port-channel10 | Uplink to WDC_C3850-1 |
| cisco-131-16-105 | Te1/1/2 | 10 Gbps | up | TenGigabitEthernet1/1/2 | Uplink to WDC_C3850-1 Te1/1/2 |
| cisco-131-16-105 | Te3/1/2 | 10 Gbps | up | TenGigabitEthernet3/1/2 | Uplink to WDC_C3850-1 Te3/1/2 |

*Graphic 13: deleting a group*

# 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}`<br>`version 3 user {username} md5\|sha {auth password}`<br>`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 **SNMP Trap Settings** and **Discover** log 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.

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.

# 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).

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**.

## Case studies

A customer wrote the following rule to place a wait time of three minutes on Cisco IPSLA alerts:

```
wait 3m * * * CISCO-RTTMON-MIB.rttMonLatestRttOperSense
value /ok|timeout/ = call example-script
```

A customer wrote the following rule to specify a time and wait parameter in a status alert:

```
wait 15m time "not sun to sat 7:00 to 22:00" * *
ping4 PING.icmpState value down any group 4-Critical =
email xyz@xyz.xyz
```

## 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**.

## Case study

A customer wrote the following rule to trigger a threshold alert for a group of interfaces which experienced more than one ifInErrors during the past minute:

```
last1m avg above 1 counter * * IF-MIB.ifInErrors any group 2-Core
= flag critical
```

## 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:

- configure the device using either version 2 or 3 (AKIPS does not support SNMPv1 traps)
- 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**.

## 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

AKIPS creates unique IDs for integration alerts and events using
device_ child_attribute

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).

## 7.1 Opsgenie

### To integrate Opsgenie:

Sign into your Opsgenie account. (For assistance using Opsgenie, contact their support team.)

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_opsgeni
```

## 7.2 PagerDuty

### To integrate PagerDuty:

Sign into your PagerDuty account. (For assistance using PagerDuty, contact their support team.)

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 using 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 using 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 using 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.

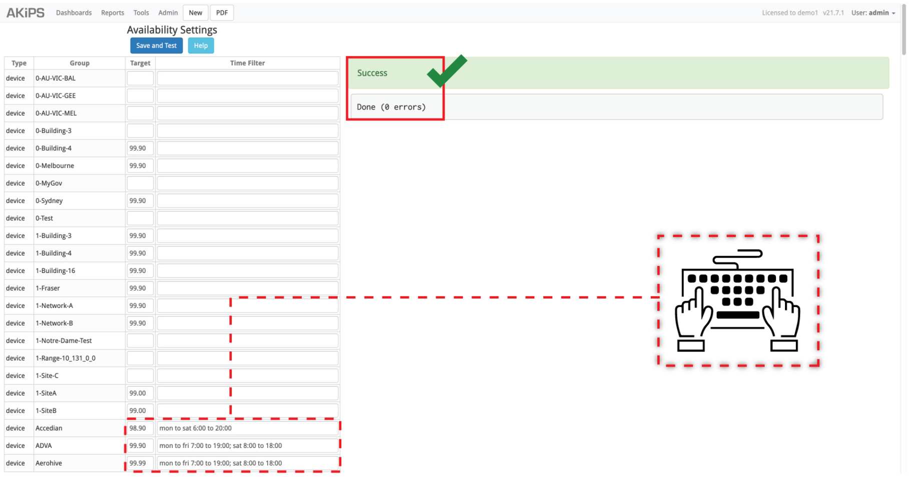
### To define availability settings:

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**.



Availability Settings

| Type | Group | Target | Time Filter |
|---|---|---|---|
| device | 0-AU-VIC-BAL | | |
| device | 0-AU-VIC-GEE | | |
| device | 0-AU-VIC-MEL | | |
| device | 0-Building-3 | | |
| device | 0-Building-4 | 99.90 | |
| device | 0-Melbourne | 99.90 | |
| device | 0-MyGov | | |
| device | 0-Sydney | 99.90 | |
| device | 0-Test | | |
| device | 1-Building-3 | 99.90 | |
| device | 1-Building-4 | 99.90 | |
| device | 1-Building-16 | 99.90 | |
| device | 1-Fraser | 99.90 | |
| device | 1-Network-A | 99.90 | |
| device | 1-Network-B | 99.90 | |
| device | 1-Notre-Dame-Test | | |
| device | 1-Range-10_131_0_0 | | |
| device | 1-Site-C | | |
| device | 1-SiteA | 99.00 | |
| device | 1-SiteB | 99.00 | |
| device | Accedian | 98.90 | mon to sat 6:00 to 20:00 |
| device | ADVA | 99.90 | mon to fri 7:00 to 19:00; sat 8:00 to 18:00 |
| device | Aerohive | 99.99 | mon to fri 7:00 to 19:00; sat 8:00 to 18:00 |

Success

```
Done (0 errors)
```

*Graphic 14: defining availability settings*

# Chapter 9

# Scheduling a report

To view the video *Scheduling a report in AKIPS*,
visit https://vimeo.com/manage/videos/568701873

### 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

Warning: for expert use only.

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

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

To view the video *AKIPS config crawler*,
visit https://vimeo.com/manage/videos/546259184

## 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.

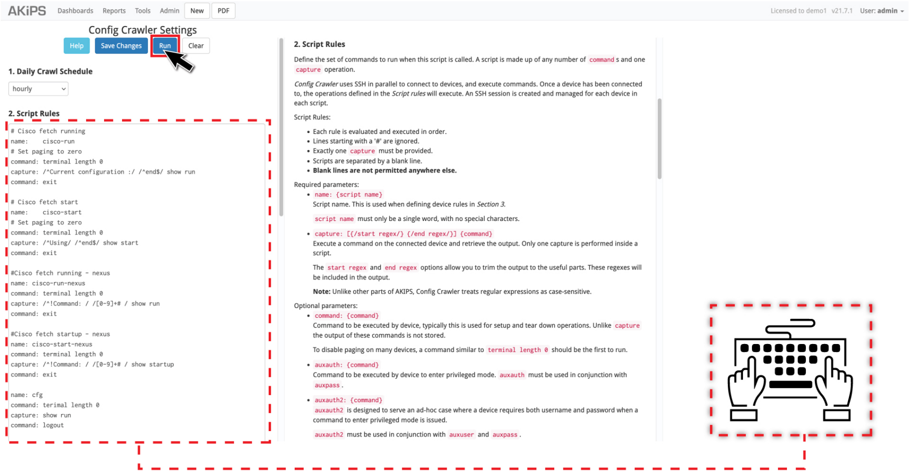
To generate the output which the AKIPS server will keep, each script rule must have:

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

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**.



1. Daily Crawl Schedule

hourly

2. Script Rules

```
# Cisco fetch running
name:    cisco-run
# Set paging to zero
command: terminal length 0
capture: /^Current configuration :/ /^end$/ show run
command: exit

# Cisco fetch start
name:    cisco-start
# Set paging to zero
command: terminal length 0
capture: /^Using/ /^end$/ show start
command: exit

#Cisco fetch running - nexus
name: cisco-run-nexus
command: terminal length 0
capture: /^!Command: / /[0-9]+# / show run
command: exit

#Cisco fetch startup - nexus
name: cisco-start-nexus
command: terminal length 0
capture: /^!Command: / /[0-9]+# / show startup
command: exit

name: cfg
command: terimal length 0
capture: show run
command: logout
```

2. Script Rules

Define the set of commands to run when this script is called. A script is made up of any number of `command`s and one `capture` operation.

*Config Crawler* uses SSH in parallel to connect to devices, and execute commands. Once a device has been connected to, the operations defined in the *Script rules* will execute. An SSH session is created and managed for each device in each script.

Script Rules:

- Each rule is evaluated and executed in order.
- Lines starting with a '#' are ignored.
- Exactly one `capture` must be provided.
- Scripts are separated by a blank line.
- **Blank lines are not permitted anywhere else.**

Required parameters:

- `name: {script name}`
  Script name. This is used when defining device rules in *Section 3*.

  `script name` must only be a single word, with no special characters.

- `capture: [{/start regex/} {/end regex/}] {command}`
  Execute a command on the connected device and retrieve the output. Only one capture is performed inside a script.

  The `start regex` and `end regex` options allow you to trim the output to the useful parts. These regexes will be included in the output.

  **Note:** Unlike other parts of AKIPS, Config Crawler treats regular expressions as case-sensitive.

Optional parameters:

- `command: {command}`
  Command to be executed by device, typically this is used for setup and tear down operations. Unlike `capture` the output of these commands is not stored.

  To disable paging on many devices, a command similar to `terminal length 0` should be the first to run.

- `auxauth: {command}`
  Command to be executed by device to enter privileged mode. `auxauth` must be used in conjunction with `auxpass`.

- `auxauth2: {command}`
  `auxauth2` is designed to serve an ad-hoc case where a device requires both username and password when a command to enter privileged mode is issued.

  `auxauth2` must be used in conjunction with `auxuser` and `auxpass`.

*Graphic 15: setting up config crawler*

## 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 view the last change:**

Click **Show Last Change**.

**To view the current revision:**

Click **View**.

**To compare revisions:**

Click **View**.

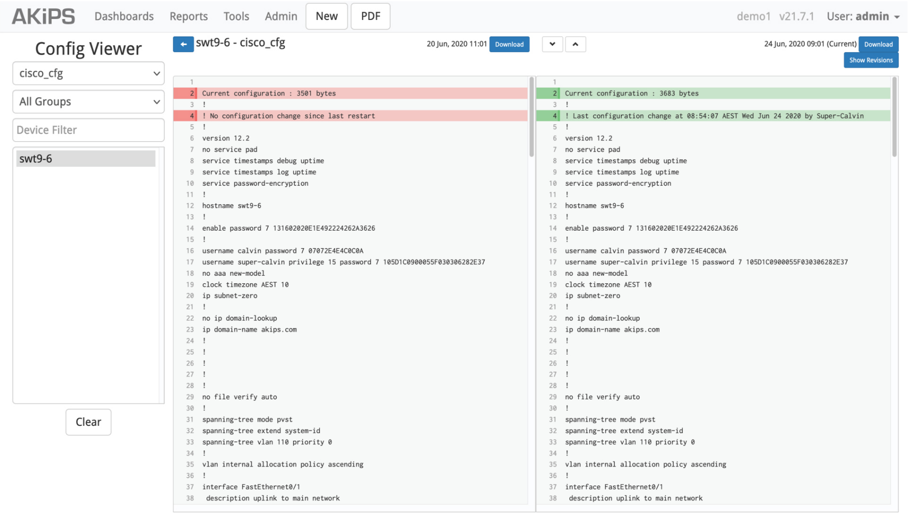
(Optional) Config Viewer shows when it has detected config changes.
If multiple changes occur in the same day, it shows the latest one.
Tick **All Revisions** to see all of the revisions that occurred on each day.

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**.



20 Jun, 2020 11:01

```

Current configuration : 3501 bytes
!
! No configuration change since last restart
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname swt9-6
!
enable password 7 131602020E1E492224262A3626
!
username calvin password 7 07072E4E4C0C0A
username super-calvin privilege 15 password 7 105D1C0900055F030306282E37
no aaa new-model
clock timezone AEST 10
ip subnet-zero
!
no ip domain-lookup
ip domain-name akips.com
!
!
!
!
!
no file verify auto
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 110 priority 0
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 description uplink to main network
```

24 Jun, 2020 09:01 (Current)

```

Current configuration : 3683 bytes
!
! Last configuration change at 08:54:07 AEST Wed Jun 24 2020 by Super-Calvin
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname swt9-6
!
enable password 7 131602020E1E492224262A3626
!
username calvin password 7 07072E4E4C0C0A
username super-calvin privilege 15 password 7 105D1C0900055F030306282E37
no aaa new-model
clock timezone AEST 10
ip subnet-zero
!
no ip domain-lookup
ip domain-name akips.com
!
!
!
!
!
no file verify auto
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 110 priority 0
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 description uplink to main network
```

*Graphic 16: comparing revisions in config viewer*

## 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.

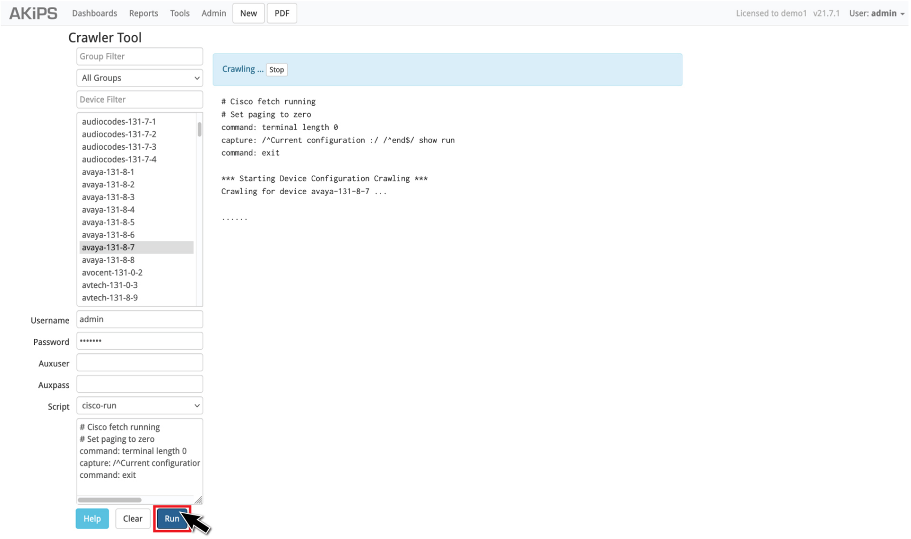
In the **Username** text field, enter your username.

In the **Password** text field, enter your password.

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**.



Username: admin

Password: •••••••

Auxuser:

Auxpass:

Script: cisco-run

```
# Cisco fetch running
# Set paging to zero
command: terminal length 0
capture: /^Current configuratior
command: exit
```

```
# Cisco fetch running
# Set paging to zero
command: terminal length 0
capture: /^Current configuration :/ /^end$/ show run
command: exit

*** Starting Device Configuration Crawling ***
Crawling for device avaya-131-8-7 ...

......
```

*Graphic 17: running the crawler tool*

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**.

## 10.4 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**.

### Case study

The config viewer (see 10.2) displays only scripts which have succeeded, so a customer checked the crawler log (**Admin** > **Config Crawler** > **Log Viewer** > **Crawler Log**) to learn why his script had failed.

# 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 (excluding index and AS numbers)
- J-Flow v5/9
- IPFIX Netstream.

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.

## To customise NetFlow protocol settings:

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

## Case study

A customer wanted to rename some NetFlow devices which he had not added to AKIPS. He did this by going to **Admin** > **General** > **NetFlow Exporters** and overtyping the default device names.

# 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.

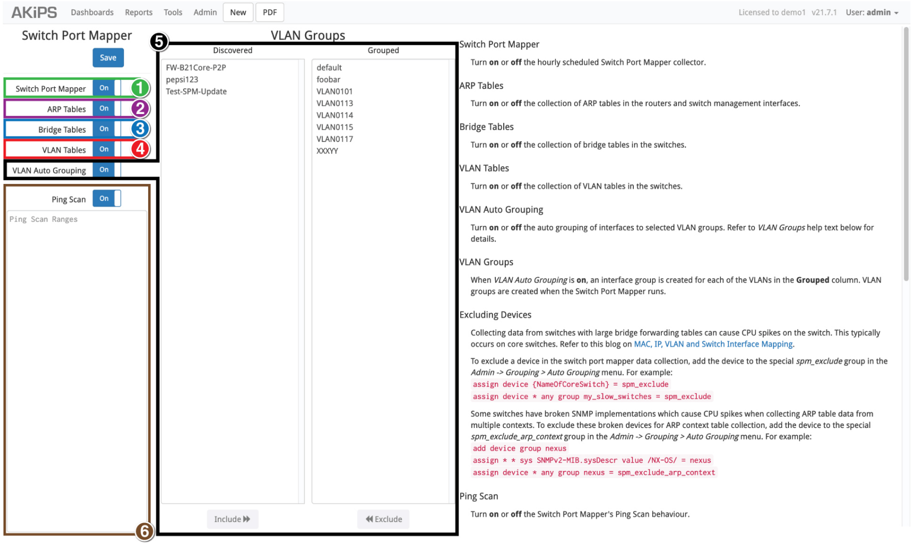
By default, all switch port mapper options are switched on.

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).

To view the video *AKIPS switch port mapper*,
visit https://vimeo.com/manage/videos/493899838



Switch Port Mapper

Switch Port Mapper On

ARP Tables On

Bridge Tables On

VLAN Tables On

VLAN Auto Grouping On

Ping Scan On

Ping Scan Ranges

VLAN Groups

| Discovered | Grouped |
|---|---|
| FW-B21Core-P2P | default |
| pepsi123 | foobar |
| Test-SPM-Update | VLAN0101 |
|  | VLAN0113 |
|  | VLAN0114 |
|  | VLAN0115 |
|  | VLAN0117 |
|  | XXXYY |

Switch Port Mapper

Turn **on** or **off** the hourly scheduled Switch Port Mapper collector.

ARP Tables

Turn **on** or **off** the collection of ARP tables in the routers and switch management interfaces.

Bridge Tables

Turn **on** or **off** the collection of bridge tables in the switches.

VLAN Tables

Turn **on** or **off** the collection of VLAN tables in the switches.

VLAN Auto Grouping

Turn **on** or **off** the auto grouping of interfaces to selected VLAN groups. Refer to *VLAN Groups* help text below for details.

VLAN Groups

When *VLAN Auto Grouping* is **on**, an interface group is created for each of the VLANs in the **Grouped** column. VLAN groups are created when the Switch Port Mapper runs.

Excluding Devices

Collecting data from switches with large bridge forwarding tables can cause CPU spikes on the switch. This typically occurs on core switches. Refer to this blog on MAC, IP, VLAN and Switch Interface Mapping.

To exclude a device in the switch port mapper data collection, add the device to the special *spm_exclude* group in the *Admin -> Grouping > Auto Grouping* menu. For example:

```
assign device {NameOfCoreSwitch} = spm_exclude
assign device * any group my_slow_switches = spm_exclude
```

Some switches have broken SNMP implementations which cause CPU spikes when collecting ARP table data from multiple contexts. To exclude these broken devices for ARP context table collection, add the device to the special *spm_exclude_arp_context* group in the *Admin -> Grouping > Auto Grouping* menu. For example:

```
add device group nexus
assign * * sys SNMPv2-MIB.sysDescr value /NX-OS/ = nexus
assign device * any group nexus = spm_exclude_arp_context
```

Ping Scan

Turn **on** or **off** the Switch Port Mapper's Ping Scan behaviour.

*Graphic 18: navigating the switch port mapper settings*

*1. switch port mapper collector (see 12.1); 2. ARP tables collector (see 12.2); 3. bridge tables collector (see 12.3); 4. VLAN tables collector (see 12.4); 5. VLAN auto grouping (see 12.5); 6. ping-scan settings (see 12.6).*

## 12.1 Switch port mapper collector

The switch port mapper collector (see 12) runs every hour.

### 12.1.1 Turning off the switch port mapper collector

#### To turn off the switch port mapper collector:

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

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

Click **Save**.

### 12.1.2 Excluding a device

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 (see 12) gathers data in routers and switch management interfaces.

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

### 12.2.1 Turning off the ARP tables collector

#### To turn off the ARP tables collector:

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

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

Click **Save**.

### 12.2.2 Excluding a device

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 (see 12) 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 (see 12) 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**.

## 12.5 VLAN auto grouping

This feature enables you to configure VLAN auto grouping (see 12).

### 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**.

## 12.6 Ping-scan settings

This feature enables you to configure the ping-scan settings (see 12).

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 the video *AKIPS settings history*,
visit https://vimeo.com/manage/videos/571087518

### 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 device name |
| **IPv4/IPv6** | the IPv4/6 address |
| **SNMP IP** | an IP address to receive SNMP requests.<br>This is usually the same as **IPv4/IPv6** |
| **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).

### Case study

A customer wrote the following script to access the content of **Tools > Device to IP Mapping** and view the device IPs:

```
sub custom_ip_to_name_mapping
{
     my $ip_to_name_ref = config_load_ip2name();
     for my $ip (sort keys %{$ip_to_name_ref}) {
          printf ("%s,%s\n", $ip_to_name_ref->{$ip}, $ip);
     }
     return;
}
```

## 13.5 Resetting a password

To view the video *Resetting AKIPS passwords*,
visit https://vimeo.com/manage/videos/524594756

### 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**.

Click **Reboot Server**.

Warning: you will have only a short amount of time to complete the next step.

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

Warning: for expert use only.

### To configure IP firewall rules:

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

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

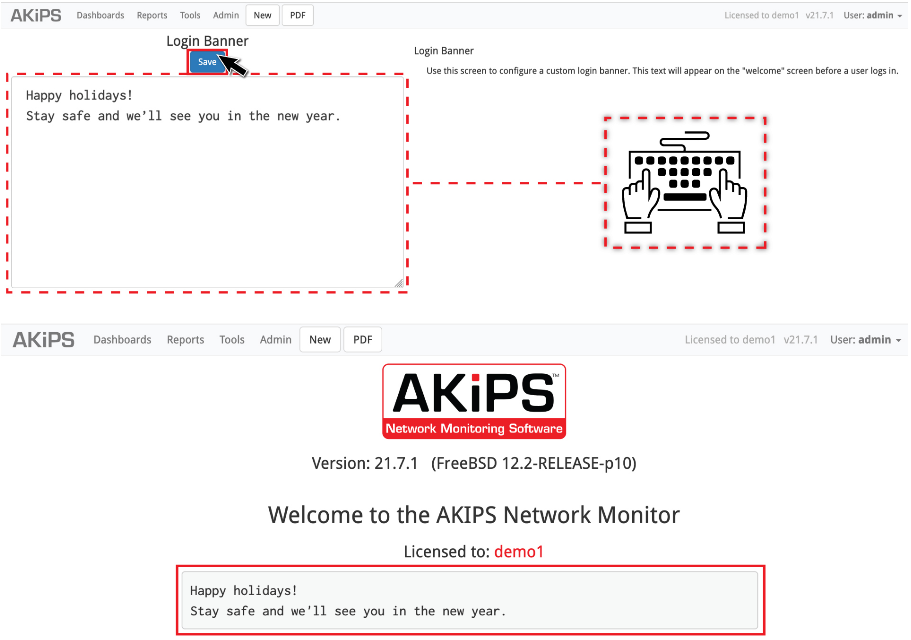
The login banner tool enables you to display a personalised message for users on your AKIPS login page.

### To add a personalised login banner:

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

Type your message into the text field.

Click **Save**.



Use this screen to configure a custom login banner. This text will appear on the "welcome" screen before a user logs in.

```
Happy holidays!
Stay safe and we'll see you in the new year.
```

AKiPS
Dashboards
Reports
Tools
Admin
New
PDF
Licensed to demo1 v21.7.1 User: admin
AKiPS™
Network Monitoring Software

Version: 21.7.1 (FreeBSD 12.2-RELEASE-p10)

Welcome to the AKIPS Network Monitor

Licensed to: demo1

```
Happy holidays!
Stay safe and we'll see you in the new year.
```

*Graphic 19: adding a personalised login banner to AKIPS*

# Chapter 14

# Access control

To view the video *AKIPS profile groups & user accounts*,
visit https://vimeo.com/manage/videos/539410999

## 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)<br>`{IP address}[:{port number}]`<br>E.g. `10.2.78.20` |
| **SSL/TLS** | from the list, select the appropriate protocol:<br>• none<br>• SSL<br>• STARTTLS |
| **Base DN** | type the DN for the section of the directory where AKIPS should start searching for users and groups<br>E.g. `dc=mydomain,dc=com` |
| **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<br>E.g. `cn=admin1,cn=users,dc=mydomain,dc=com` |

*(continued)*

| Text field | Details |
|---|---|
| **Bind Password** | (optional) type the password for the bind DN |
| **Scope** | select the appropriate search scope:<br>• subtree<br>• one-level |
| **Login Attribute** | select the appropriate attribute to authenticate the user<br>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)<br>`{IP address}[:{port number}]`<br>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)<br>`{IP address}[:{port number}]`<br>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/from selected groups:**

Click **Edit Groups**.

From the list, select the required group.

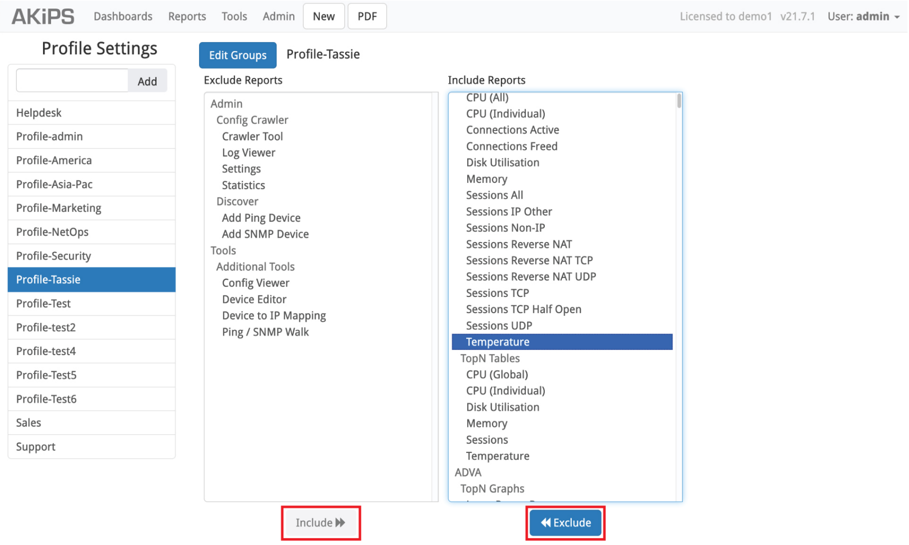
Click **Include/Exclude**.

**To allocate/remove access to/from selected reports:**

Click **Edit Reports**.

From the list, select the required report.

Click **Include/Exclude**.



Profile-Tassie

Helpdesk
Profile-admin
Profile-America
Profile-Asia-Pac
Profile-Marketing
Profile-NetOps
Profile-Security
Profile-Tassie
Profile-Test
Profile-test2
Profile-test4
Profile-Test5
Profile-Test6
Sales
Support

Exclude Reports

Admin
Config Crawler
Crawler Tool
Log Viewer
Settings
Statistics
Discover
Add Ping Device
Add SNMP Device
Tools
Additional Tools
Config Viewer
Device Editor
Device to IP Mapping
Ping / SNMP Walk

Include Reports

CPU (All)
CPU (Individual)
Connections Active
Connections Freed
Disk Utilisation
Memory
Sessions All
Sessions IP Other
Sessions Non-IP
Sessions Reverse NAT
Sessions Reverse NAT TCP
Sessions Reverse NAT UDP
Sessions TCP
Sessions TCP Half Open
Sessions UDP
Temperature
TopN Tables
CPU (Global)
CPU (Individual)
Disk Utilisation
Memory
Sessions
Temperature
ADVA
TopN Graphs

*Graphic 20: allocating/removing a profile group's access to/from selected reports*

## 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 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 edit a user account:

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

Select **Edit** beside the account.

Make the required changes in the relevant text fields.

Click **OK**.

### 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:

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.

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**.

## 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