SOPHOS

Security made simple.

Sophos Central

Alerts and diagnostics

Product Version 1.15

Contents

1 Alerts

There are the following types of wireless alerts:

High

- **Access point has bad health**

  The load on the AP is too high. This is caused by too many connected clients. Check your installation (Are the access points well placed? Are there too few?).

Medium

- **Access point is offline**

  The AP has either no connection to the Internet, no power or there is an error with the software. If it is the software, a reboot may help. Otherwise, you should connect to the SOS SSID.

- **Access point is not broadcasting any network**

  There is currently no configuration on the AP. Configure the AP under **Wireless** > **Access Points**.

- **Access point has high data packet retries**

  802.11 retries alert is triggered when the data frame retries on the AP go beyond 20%. It helps you to understand if retries are the reason for a bad network service. WLAN frames are retried by the AP when the acknowledgement frames are not received from the intended recipient. If the retries go beyond the threshold, the overall performance of the network is shown.

- **Access point command done**

  The reboot is done.

- **Access point has a DNS timeout**

  DNS requests to the Internet are not answered. This is either caused by the Internet connection or by your network installation.

- **Access point has high DNS latency**

  The feature triggers alert for high 802.11 retries & DNS delay. This is either caused by the Internet connection or by your network installation.

  — DNS latency alert is triggered if the DNS roundtrip time is above 250 ms.

  — 802.11 retries alert is triggered if the retry percentage is above 20% (conservative).

There are some alerts where rebooting the access point may solve the problem:

- **Access point configuration failed**
- **Access point(s) failed to update to the new firmware**

In those cases, as first step, reboot the access point. If this does not help, call Sophos Support. They will need remote access to investigate the issue (**Wireless** > **Settings** > **Remote Login to Access Points for Sophos Support**).

Low

- **Access point will be updated with new firmware**

  Wireless is off for approximately 5 minutes.

- **All access points will be updated with new firmware**

  Wireless is off for approximately 5 minutes.

- **Access point has been successfully updated with new firmware**
- **All access points have been successfully updated**

2 Diagnostic and analysis settings

You can make some diagnostic and analysis settings under **Wireless** > **Settings**:

Forward access points logs

Your access point logs will be forwarded to Sophos technical support.

Remote login

In case of issues you can allow Sophos technical support to have remote access for a given time. The remaining time is displayed as soon as you activate the function. Deactivate to disable remote access immediately.

Traffic categorization

If the traffic categorization is enabled, the traffic generated by users will be categorized and listed on the **Usage Insight** page. This option is enabled by default.

3 Grant remote access

Before you begin

Before you grant remote access, reboot your APs and check if your problem still exists.

About this task

It could be, that you must grant remote access to Sophos Support. This may be the case when APs failed to update to the new firmware.

Procedure

1. Go to **Wireless** > **Settings**.
2. Enable **Remote login to access points for Sophos Support**.

3. Select the time frame for the remote login.
4. Save your settings.
5. Contact Sophos Support and provide additional information they may need.

Results

Sophos Support has remote login within the selected time frame.

What to do next

Deactivate the remote login at any time when you don't need it anymore.