

SOPHOS

Security made simple.

Security Heartbeat Test guide for Beta users

For customers with Sophos Cloud
and Sophos Firewall

Product version: Beta

Document date: August 2015



About Security Heartbeat

Security Heartbeat:

- Lets you see the health of endpoint computers in the Sophos Firewall (“Copernicus”) and Sophos Cloud consoles.
- Lets you control network traffic based on the health of an endpoint computer.
- Enables ATP alerts to show more details about malicious traffic coming from an endpoint computer (for example, who the logged-in user is and which process sent the traffic).

1 Get started

1.1 Create a Sophos Cloud account

1. Go to <https://cloud.sophos.com>
2. Complete registration as prompted.
3. The first time you log in to the Sophos Cloud console, you are prompted to add users and protect computers. You’ll need a protected computer or computers for the Beta testing.

1.2 Install and start using the Sophos Firewall

Full instructions for setting up the Sophos Firewall (the “Copernicus” beta product) can be found on our bulletin board.

Go to <https://www.astaro.org/beta-versions/project-copernicus-public-beta/58559-project-copernicus-public-beta-starts.html>

In the Attachments, find **Installation and getting started guide.pdf.zip**.

Please note that:

- You are required to register to access this bulletin board.
- This process will not work if any upstream proxy is used.

1.3 Register the Sophos Firewall with Sophos Cloud

1. Login to your Firewall console.
2. Go to **System > System Services > Security Heartbeat**.

3. Enter your Sophos Cloud credentials and select **Register**.

A pop up message is displayed on your Firewall console to confirm your device is registered.

The Sophos Cloud console also shows details of the Firewall device you just registered. To check them, go to the Network tab.

1.4 Register your cloud account for beta

In the Sophos Cloud console, go to **Account > Beta Programs** and check the sign up check box.

A pop up message confirms that you have successfully joined the beta program.

1.5 Enable an endpoint to join the beta

1. In the Sophos Cloud console, go to **Users & Devices > Devices**.
2. Select the endpoint computer and click **Add to Beta**.

1.6 Check that the endpoint has the beta software

The endpoint software is updated to version 11.2 or later.

To check this:

1. At the endpoint computer, double-click the Sophos tray icon to open the Sophos Endpoint Security and Control GUI.
2. In the **Status** pane, look for the **Product version**.

2 Check Security Heartbeat is working

2.1 Check that the Firewall to endpoint heartbeat is active and reported

In the **Sophos Cloud** console, check as follows:

1. Go to **Users & Devices > Devices** page.
2. Click on the endpoint computer to display its details page. The “Heartbeat Status” should be shown as active.

In the **Sophos Firewall** console, check as follows:

The Security Heartbeat count should reflect the number of endpoints that have enabled active heartbeat.

2.2 Check that endpoint health status is reported

Now check that the endpoint's health status is reported in the Firewall and Sophos Cloud consoles.

The endpoint status should currently be healthy. In other words, all Sophos services are running and no malware or advanced threats are detected.

In the Sophos Cloud console, you should see:

- On the **Users and Devices > Devices** page, each healthy endpoint has a Green icon next to it.
- When you click on a healthy endpoint, its details page displays a large Green health icon to show that the endpoint has no warnings.
- When you click on the security status and computer status, the "Computer Software/Policy Status" should be Green.

In the Sophos Firewall dashboard you should see:

- The "Security Heartbeat" icon shows Green for the number of healthy endpoints.

3 Set up policies based on endpoint health

Now you set up test policies and download the Sophos Threat Detection test tool.

3.1 Set up policies to block network access when endpoint health is compromised

1. Go to the Sophos Firewall console.
2. Select or create a policy. In the policy, do as follows:
 - (a) Set the **Minimum Heartbeat permitted** to **Green**.
 - (b) Set the **Web Filter** under "Policy for User Applications" to **Allow All**.
 - (c) Specify an individual website to block.
 - (d) Save the configuration.

This policy should block access to this one website when an endpoint's health is Yellow or Red.

3. Create another policy and configure it as follows:
 - (a) Set the **Minimum Heartbeat permitted** to **Yellow**.
 - (b) Set the **Web Filter** under “Policy for User Applications” to **Allow All**.
 - (c) Specify blocking for all websites.
 - (d) Save the configuration.

This policy should block access to all external websites when the endpoint health status is Red.

Note: You’ll use this policy in conjunction with Advanced Threat Protection later.

For full instructions on configuring a policy, use the **Help** button at the **Policies** screen.

3.2 Download the Sophos Threat Detection test tool

To download a threat detection test tool:

1. On the endpoint, go to the root of the C: drive and create a directory called "BetaTestTool".
2. Download **SophosThreatTest.exe** to this directory from <https://www.sophos.com/Pages/DownloadRedirect.aspx?downloadKey=AAC5813D-44C6-4C87-AC8B-2709ED11C970>

4 Test your first policy

Now test your first policy, which should block a specified website.

4.1 Put the endpoint in a suspicious state (Yellow) and check that the policy controls network access

1. Check that the user can access the network (browse the internet).
2. Use the Sophos test tool to trigger an event and put the endpoint in a suspicious (Yellow) by entering this at the command prompt:

```
C:\BetaTestTool\SophosThreatTest.exe pua
```

This generates a PUA (Potentially Unwanted Application) alert.

3. In the Sophos Cloud console, check that:
 - At the **Users & Devices > Devices** page, each compromised endpoint has a Yellow icon next to it.

- When you click on an endpoint, its details page displays a large Yellow health icon to show that the endpoint has security warnings.
 - When you click on the security status tab, the "Computer Security Status" is Yellow and the "Computer Software/Policy Status" is Green.
4. At the Sophos Firewall console dashboard, check that:
 - The "Security Heartbeat" icon shows Yellow for the number of endpoints compromised.
 5. Check that the user can't browse to the external site specified in the policy and sees a Sophos block page, but can browse to all other external sites.

4.2 Check that health returns to Green when endpoint is cleaned up

1. In the Sophos Cloud console dashboard, select the PUA alert.
2. Click the action **Clean up PUA(s)**. The PUA will be removed from the endpoint.
3. In the Sophos Cloud and Sophos Firewall consoles, confirm that the endpoint's health status is once again Green.
4. Check that the user can now access the internal server again.

5 Test your second policy with Advanced Threat Protection

5.1 Configure the Firewall to provide Advanced Threat Protection (ATP)

In the Sophos Firewall console, go to **System > System Services > Advanced Threat Protection** and enable the ATP functionality with a "Log and Drop" policy.

5.2 Check that the Firewall detects ATP traffic and controls network access

1. Use the Sophos test tool to trigger an ATP event and put the endpoint in a compromised (Red) state by entering this at the command prompt:

```
C:\BetaTestTool\SophosThreatTest.exe callhome
```

2. Check that the Sophos Cloud and Firewall consoles show the endpoint in a Red state.
3. On the Firewall console, open the ATP widget which will show the details of the alert.
4. Check the details of the Endpoint, User and Endpoint process that triggered the ATP detection.
5. Check that the user can't browse to any external website and sees a Sophos block page.

5.3 Check that health returns to Green when the endpoint returns to good health

1. At the endpoint, double-click the Sophos tray icon to open the Sophos Endpoint Security and Control GUI.
2. In the **Anti-Virus and HIPS** panel, click **Manage Quarantine items**.
3. Select the detections in the quarantine list and click **Clear from list**.
4. In the Sophos Cloud and Sophos Firewall consoles, confirm that the endpoint health status is now shown as Green.
5. Check that the user can now access the internet and the internal server.

6 Test a policy that requires endpoints to send Heartbeats

You can configure the Firewall to require endpoints to send Security Heartbeats.

1. Modify the Sophos Firewall policies setup in section 3 to enable the option **Require Security Heartbeat**.
2. Check the health status of endpoints. You should now find that:
 - An endpoint connected to Security Heartbeat, with Green health, can access the internet and the internal server.
 - An endpoint not connected to Security Heartbeat (a computer not in the Beta) cannot access the internet or the internal server because it is not sending Heartbeats.

Legal notices

Copyright © 2015 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.