What information does the Sophos client transmit to the Sophos Management Console?

Q: What information does the Sophos client transmit to the Sophos Management Console?

> **Starting July of 2021, IS&T has migrated to a new version of Sophos called Sophos Central.** MIT users have until the summer of 2022 before the old version will stop receiving updates. This page references the legacy version of Sophos. You can see documentation for the new Sophos Central here and download the newest version of Sophos here.

Answer

MIT's Sophos antivirus clients transmit information back to the Sophos Management Console. Most of the information pertains to the status and health of the Sophos client installed on a given machine. IS&T has listed all of the information transmitted from the Sophos client to the Sophos Management Console below.

> **Note**: ***red, bolded*** items reference Sophos modules that are not enabled, thus no information is transmitted to the Management Console and these fields are blank.

- Sophos Anti-Virus version
- HIPS rules
- HIPS configuration
- Detection data
- On-access scanning
- Anti-virus and HIPS policy
- Last scheduled scan completed
- Last message received from computer
- Up to date
- Updating policy
- Time installed package became available
- Time next package became available
- Primary update server
- Secondary update server
- Client firewall
- ***Sophos NAC policy***
- ***Compliance Agent (NAC) version***
- ***Sophos NAC compliance assessment***
- ***Application control policy***
- ***Application control on-access scanning***
- ***Data control scanning status***
- ***Device control scanning status***
- ***Data control policy compliance***
- ***Device control policy compliance***
- ***Tamper protection status***
- ***Tamper protection policy compliance***
- Patch assessment *(WIN domain only)*
- Patch policy *(WIN domain only)*
- Patch agent version *(WIN domain only)*
- ***Web control status***
- ***Web control policy***
- Group
- Items detected
- Sophos AutoUpdate status

The non-Sophos information collected by the Sophos Management Console is listed below:

Information Type	Description

Computer name	The name given to the computer by the user or domain
Computer description	The description given to the computer by the user or domain
Operating system	e.g. Windows 7, OS X 10.8
Service pack	e.g. Service Pack 1, OS X 10.8.4
Domain/workgroup	e.g. WIN, Workgroup
IP address	The last IP address the client had when it connected to the Console
Last logged on user	The last local or domain username logged in at the time of the last Console check-in

Why is this non-Sophos information important?

The non-Sophos information collected is important in the event that a software update by an operating system vendor (Microsoft, Apple, etc.) adversely affects the functionality of Sophos. By collecting this information, IS&T can accurately determine the impact of such an event on our community and act accordingly.

The Sophos Management Console also acts as a license server. By tracking the number of machines with Sophos installed, IS&T can accurately account for and license the product.

What does IS&T plan to do with this information?

The information gathered, specifically ***Items detected***, will be used to examine broad trends within the Sophos-using community. The ability to enumerate the number of endpoints infected with a specific piece of malware will provide IS&T with the ability to act (if warranted) to help better protect the community.

IS&T respects the privacy of its users and guards electronic data accordingly. For more information, please reference MIT's Polices and Procedures document: http://web.mit.edu/policies/13/13.2.html

See Also

- Sophos Landing Page

I still have concerns...

Please send additional questions/comments to servicedesk@mit.edu.