

SpamActive FAQ

What's SpamActive?

SpamActive is Clearswift's newest initiative in the fight to combat spam. It is a Managed Anti-Spam Filter freely available to Clearswift Support & Maintenance customers, and the latest addition to our ThreatLab™ Active service.

Why has Clearswift introduced SpamActive?

To help Clearswift customers lessen the pressures on their IT staff as they battle against the rising tide of spam. Whilst Clearswift products already offer a comprehensive range of tools and techniques to eradicate spam, many customers need additional help in keeping these defences up to the minute.

How much does it cost?

SpamActive is a free managed Anti-Spam Filter service for Clearswift support customers.

Who is entitled to use SpamActive?

Clearswift customers with a current Support and Maintenance contract receive this service free by registering under the ThreatLab™ Active service on the Clearswift website (www.clearswift.com)

What's new about SpamActive?

SpamActive assists customers by essentially having Clearswift manage part of the their anti-spam defences. Customers still own and operate their Clearswift products, but they can now incorporate the new SpamActive filter, which is automatically managed by Clearswift via the Internet.

How does it work exactly?

SpamActive comprises a product plug-in filter, a database of spam detection rules for the filter and a service to automatically update that database. The filter product component can be downloaded from the Clearswift web site and plugged into MAILsweeper™ for SMTP. The database used by the filter to detect spam is automatically downloaded from the Clearswift web site on a periodic basis.

How does Clearswift build this database?

Clearswift has established a spam-trapping network that continuously collects samples of spam. These samples are combined and then converted into detection rules that become part of the database used by the SpamActive filter. As the database creation process is automated, Clearswift performs daily updates to the database to ensure the latest spam can be detected.

How and where do I get updates to the database?

You can download the database, either manually or automatically, directly from the Clearswift support website via special URLs. A special batch file can be used to fully automate the process if desired.

Can I add spam examples to the database?

Not directly. You can supply spam examples to Clearswift, who will incorporate them into the central database. Otherwise, you can continue to use the other techniques provided by the Clearswift products to control any residual spam.

What can I do with the spam once it's detected?

This depends on the policy you set. In addition to the ability to quarantine or block spam messages, SpamActive provides the option to “tag” messages as spam but allow them through. The tagging option allows individual email users to set local rules to deal with email classified as spam according to their own preferences e.g. they may set automatic rules to delete or perhaps to place in a special folder.

What about regional differences in spam?

Spam varies across the world, as a result Clearswift have established three separate regional spam-trapping networks. From these networks a separate spam database is build for Europe, the Americas and Asia-Pacific. Customers can choose which of these databases to use with SpamActive.

NOTE: Only Europe and US databases are populated; there are no accounts from Asia as yet.

What do I need to use SpamActive?

SpamActive is currently available for MAILsweeper for SMTP version 4.2 or 4.3. A version for the ENTERPRISEsuite will follow.

Do I need to fight spam in any other way?

Yes. Clearswift advocates a “layered” defence against today’s spam problem. SpamActive is intended to help organisations deal primarily with the detection of spam “in the wild”. Customers will therefore benefit from augmenting SpamActive with techniques that identify “generic” types of spam, for example using the textual analysis techniques offered by the Clearswift products. In addition, the use of Real-time Block Lists (RBLs) can assist in preventing the more common spam offenders from even getting close to an organisations messaging system.