



Am Römerkastell 4
66121 Saarbrücken
Tel.: 06 81-9 67 51-0
Fax.: 06 81-9 67 51-66
Web.: www.iku-ag.de

SPONTS - Appliance

SPONTS is delivered as an **appliance** including the hardware of your choice: A handy Mini ITX or a 19" case (1U, rack-mount). The **SPONTS** appliance is **optimized for stability and reliability** according to its field of application. The hardware comprises **only failsafe components** and is therefore nearly **maintenance-free**. A standard installation of **SPONTS/UCÉ** can handle more than 550,000 mails per day which makes it also perfectly suitable for larger enterprises.

SPONTS - Modular architecture

SPONTS is based on a slim Linux system and the server software is written in Java which provides for highly robust operation. Java was chosen as the programming language because it is immune against so-called buffer overflows - with about 80 percent the most common cause of security holes. Among other spam detection techniques **SPONTS** utilizes the award winning Spamassassin software which excels in all current comparative tests with its **very high detection rate and very low failure rate**. All relevant data for mail processing - e.g. user data or black/whitelist information - is stored in a very fast SQL database. This ensures that **SPONTS** performs brisk even under high load and can be easily customized to meet individual customer requirements. The basic system consists of an SMTP proxy that feeds the mail parts to several server modules and forwards accepted mail to the actual mailserver (backend) per SMTP. The different **SPONTS** modules are plugged into the basic system:

SPONTS/UCÉ: Sustainable spam protection

Besides well known methods like RBL and custom black/whitelists **SPONTS/UCÉ** uses latest technologies for reliable spam detection including the **Spamassassin** software and **detection methods especially developed by iKu**. Typical spam mails are classified using a customizable score system. As a remarkable matter of principle **no mail is ever filtered out** or even deleted. Every mail is either accepted (and forwarded to the backend) or rejected by **SPONTS/UCÉ** at SMTP level returning the error message '550 user unknown'. (The error message is not sent as an email to the - potentially fake - sender address.). This way a spammer cannot distinguish a non-existent mail address from a mail address protected by **SPONTS/UCÉ**. (In some cases the immediate rejection is impossible. Then a two-step procedure is applied to achieve the same effect: A temporary rejection is followed by a definite rejection when the spammer retries to send the mail.) Since the average lifetime of an email address is 3 years (and just 2 years in the US), professional spammers remove invalid addresses from their databases. **SPONTS/UCÉ** systematically uses this fact to significantly **reduce the flood of incoming spam** soon after installation and accomplishes **spam reduction of over 99%**. Such success rates can be reached even if your spam detection settings are quite cautious, which leads to a very low **false positives rate of less than one per mille**. If a false positive ever occurs with **SPONTS/UCÉ** - which is not 100% avoidable especially when dealing with newsletters - the sender will get an error message notifying that the mail was rejected. This eliminates the risk of important mails left unnoticed in a spam folder while the sender assumes that his mail reached its destination successfully.

SPONTS/UMS: Uninterruptible mail supply

SMTP servers typically keep their mail queue inaccessible. While such a server is down important mail is 'locked' in its queue. In contrast, **SPONTS/UMS** provides **POP3 access to its mail queue**. If the backend (mailserver) is ever unreachable - e.g. due to failure, virus effects or faulty operation - incoming mail is kept safely and accessibly in the **SPONTS** mail queue until the backend is online again. Important mails can be fetched from the queue, crucial attachments can be saved, urgent mails can be printed out, etc. All mails in the queue are accessible via a single POP3 account which is usually operated by an administrator. The POP3 option 'Leave messages on server' should be enabled to make sure that the fetched mails are not deleted from the queue. Of course, the administrator is still free to selectively delete single mails. This results in **flexible access to all incoming mails**, safeguarding all mail based workflow and effectively **reducing the costs of a backend failure**.

SPONTS/REPLAY- Resend lost mail

Administrators know the scenario: The backend (mailserver) had a complete failure, only the backup of last night is available. During the recovery of the backend **SPONTS/UMS** gives access to all incoming mails. But the mail that arrived between the last backup and the backend failure is usually lost.

SPONTS/REPLAY actively prevents such loss of mail data: **SPONTS/REPLAY** saves a copy of all incoming mail in a ringbuffer, i.e. when new mail arrives the oldest entry is deleted and a copy of the new mail is stored in the buffer. The default capacity of 200 MB can be easily increased to a custom size through hardware extensions, so that the buffer can retain the mail of several weeks or months depending on the volume of your mail traffic.

If mail ever gets lost on the backend or on the client side - e.g. if an employee deletes an important mail by mistake - **SPONTS/REPLAY** can take the copy in the ringbuffer and send it again to the backend. The administrator can choose which mail to „replay“ based on sender, recipient and time range - for example resend all mails from between 2:15 and 6:30 of last night. The procedure can be repeated as often as necessary. The messages are sent exactly the same way as when they first arrived so that no extra customization of the backend is required. **Lost mail can be reproduced in a few seconds with just a few clicks - faster than any backup.**

SPONTS/JOURNAL - Keep a record of everything

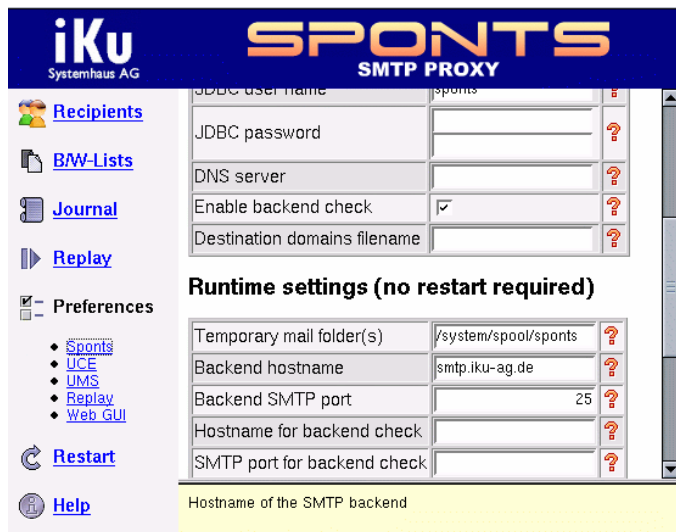
The **SPONTS/JOURNAL** provides a rich means of control for administration of daily mail traffic. **A record is kept for every single mail** no matter if it has been rejected or accepted. In contrast to other products not only the **sender, all recipients and time of arrival** are journalized but also the **mail subject as well as name and size of all attachments**. Using the journal the administrator can quickly find specific mails or monitor how accurately the spam detection works.

All journal data is stored in a MySQL database that the administrator can access. With a basic understanding of SQL **custom queries and reports can be easily realized**, for example how many bytes or how many spam mails arrived per day for a certain department, how the overall spam rate is, etc ...

Configuration

SPONTS can be easily configured through its **web interface**. The **first setup** takes less than **10 minutes** and makes **SPONTS** immediately **ready for operation**. It only requires the input of IP and DNS settings for the **SPONTS** server and the backend and a list of valid recipient (to prevent an open relay).

The web interface provides **convenient access to advanced configuration settings**, black/whitelists, the replay buffer, the queue and the journal data. **SPONTS is easy to configure and allows a quick start-up.**



The screenshot shows the web interface for SPONTS SMTP PROXY. The interface is divided into several sections:

- Recipients**: A table with columns for JDBC user name (sponts), JDBC password, DNS server, Enable backend check (checked), and Destination domains filename.
- Runtime settings (no restart required)**: A table with columns for Temporary mail folder(s) (/system/spool/sponts), Backend hostname (smtp.iku-ag.de), Backend SMTP port (25), Hostname for backend check, and SMTP port for backend check.
- Preferences**: A list of links for Sponts, UCE, UMS, Replay, and Web GUI.
- Restart**: A button to restart the service.
- Help**: A button for help.

At the bottom, there is a yellow box labeled "Hostname of the SMTP backend".