AntiVirus and AntiSpam email scanning
The Axigen-Kaspersky solution

The present document offers a comprehensive analysis of the ways to secure corporate email systems. It provides an expert opinion on the available approaches, architectures and deployment options for implementing security applications in the email infrastructure, while keeping a special focus on the benefits of using the integrated Axigen-Kaspersky solution.

1. Today's challenge

In today's fast-paced and competitive business environment, email communication is mission-critical. Companies of all sizes and Service Providers altogether need robust and secure messaging solutions that they can count on 24x7. Protecting the email infrastructure is not only a challenge, but also an imperative for business productivity and continuity.

2. Possible solutions

To defend business email systems, it is necessary and recommended to implement scanning at one or more points within the email delivery process. While several approaches can be taken, each having its own set of unique strengths and weaknesses, email security deployment options mainly fall under three categories: scanning at mail gateway / mail relay / firewall (application proxy), using security solutions on end-users' work-stations (usually desktop computers), and implementing security solutions at the mail server level.

2.1 Security on mail gateway, mail relay, firewall

By enabling the interception and scanning of messages before they even reach company mail servers, this specific architecture entails numerous benefits. The mail gateway and other platforms sit in front of the existing messaging solution, providing immediate protection against inbound and outbound threats. They also:

- Reduce the amount of scanning to be performed by mail servers (thus reducing their workload).
- Act as a first point of contact (proxy) with the Internet, decreasing threats to the mail server.
- Can be installed on separate servers, bypassing the need to integrate them with the email system, while also making it possible to achieve a higher security by combining different security solutions within the same network.

The main disadvantages of this approach include the fact that it may:

- Necessitate the modification of the mail server configuration to allow the scanning of outgoing email messages.
- Lead to a lower performance of the mail gateway / relay / firewall, because of the constant scanning of the SMTP flow of messages.
- Provide low end-user protection once malware has reached the organization's internal network.
- Not be able to handle the loads of larger organizations (requiring large investments in servers).

2.2 Scanning on end-users' workstations

Client-side scanning, or using security applications directly on users' desktop computers or mobile devices are regarded as an important part of a sound security strategy. In this approach, email messages are scanned when users attempt to open / send them, which:

Brings benefits such as:

- The scanning process is distributed, thus having minimal effect on the performance of each user's machine.
- Malware infecting a client machine is stopped before spreading to the mail server / other users.
- It usually does not require modifications to the mail server (this saves time with administration).
- It protects against inbound and outbound email threats, but also against other attack vectors such as web pages etc.

Presents disadvantages such as:

- It can be troublesome to centrally manage, maintain and update such applications, especially when dealing with mobile devices, laptops; or with larger environments, with multiple, distributed locations.
- End-users have access to the security scanner and may disable (accidentally or on purpose) a part or all of its functionalities.

2.3 Security on the mail server

A wide range of security applications can be used at the mail server level, for scanning messages against viruses, spam or other types of email-borne threats. In this architecture:

Benefits include the fact that security applications:

- Also inspect email messages sent between internal users, which usually do not pass through the mail gateway, mail relay or the firewall.
- Provide an extra layer of protection against malware and help stop internal malware outbreaks.
- Can be integrated with most email servers, by using application programming interfaces (APIs).
- Additionally, this approach enables centralized security management and updates, and compliance with company security policies.

Disadvantages revolve around the following facts:

- The requirement to scan all email messages may have a negative impact on the performance of the messaging solution.
- Deploying security applications at this level may require significant modification of the existing mail server configuration.

In a nutshell, in comparison with the other email security deployment options, implementing scanning at the mail server level represents a sustainable approach through major, valuable benefits such as:

- Gateway security is able to stop threats at the perimeter, but mail server security is essential in inspecting inbound and outbound communications, stored email and internal communications.
- Server-level scanning allows for centralized, and thus easier and more secure, administration and updates, complemented by logging for monitoring application activity and security status.

Notes:
There are some other aspects to consider when looking to secure the email infrastructure.

* In addition to scanning for malware scanning, corporate email systems need to be also protected by means of content filtering – a mechanism employed to look for emails containing (in message body or attachment) undesirable content other than malware. This can and should be performed on both the incoming and outgoing flow of messages, and at the same level as malware scanning (above-mentioned).
** The above-described framework refers to implementing premise-based email security solutions (software running on mail servers and desktop computers, typically installed, configured and maintained by the company's IT department), and not perimeter-based solutions (which ensure the protection outside of the corporate network, typically via one / more geographically-dispersed data centers.

Conclusions:
To reduce the time and inherent costs associated with the installation, deployment, administration, maintenance and support of security solutions, malware scanning, content filtering or any other security mechanisms should be incorporated into a single security product, used at the mail server level.

3. The Axigen-Kaspersky solution

As with other popular mail servers, various security applications can be used with the Axigen mail server in order to ensure a higher security level for the email communication.

3.1 Integrating Axigen with security applications

This can be achieved through:

- The Milter protocol (Kasperky, AVG, ClamAV, Symantec) – filtering takes place at the SMTP level.
- External filters (developed as external components of Axigen) – they communicate with the server through dedicated protocols, generally described as AFSL (Axigen Filter Scripting Language); these apply once the Spam and malicious messages have already been thinned-out by the previous SMTP level filters e.g. Amavis, AVG, SpamAssassin.
- And, in a particular case (the integration with the Commtouch AntiSpam technology) – via the HTTP protocol.

How it works:
Security scanners receive instructions from the server through these filters and once the scan is complete, they provide the relevant results back to the server. Using the results, Axigen decides the fate of the email messages, including dropping or accepting them. These actions can be fully customized to fit the requirements of any email traffic regulations.

When comparing the two main types of filtering (Milter-based and through external filters), the following facts need to be outlined:

Benefits:
While external filters usually provide a higher performance, through the close communication with third-party scanners, Milter-based filtering presents a distinct advantage – that of enabling the scanning of the incoming SMTP connections.

The ability to scan a message before receiving it opens a new perspective:

- In regards to unwanted traffic, it enables the server to refuse a message if content filters strongly indicate that the scanned email is unwanted.
- By not accepting the message, no further resources are allocated to this mail (for processing, storage, backup, double-checks etc).

Disadvantages:

- While ensuring a broader compatibility with third-party scanners, Milter-based filters generally have lower performance results, due to the typically larger protocol overhead.
- Applying for both types of filtering, there is the inability to configure and update the AntiVirus / AntiSpam engines by using Axigen's administration services (WebAdmin and CLI).
- And also, a potential lower reliability, since they both employ components developed by another party (security vendors).

3.2 The integration of Axigen with Kaspersky

The latest and most innovative implementation, however, is represented by the integration of Kaspersky Lab's award-winning malware detection engine into the Axigen mail server. The Axigen-Kaspersky partnership brings together the reliable Axigen messaging solutions with the proactive Kaspersky AntiVirus and AntiSpam, message content and attachment filtering technologies to secure the mail traffic of both companies and Service Providers.

3.2.1 Embedded Kaspersky AntiVirus & AntiSpam

How it works, at a glance:

The Axigen mail server communicates, through a dedicated protocol, with two internal, custom-built services (Kaspersky AntiVirus Server and Kaspersky AntiSpam Server) created specifically for the Axigen platform, based on Kaspersky Lab's AntiVirus and AntiSpam SDKs (Software Development Kits).

Key differentiators:

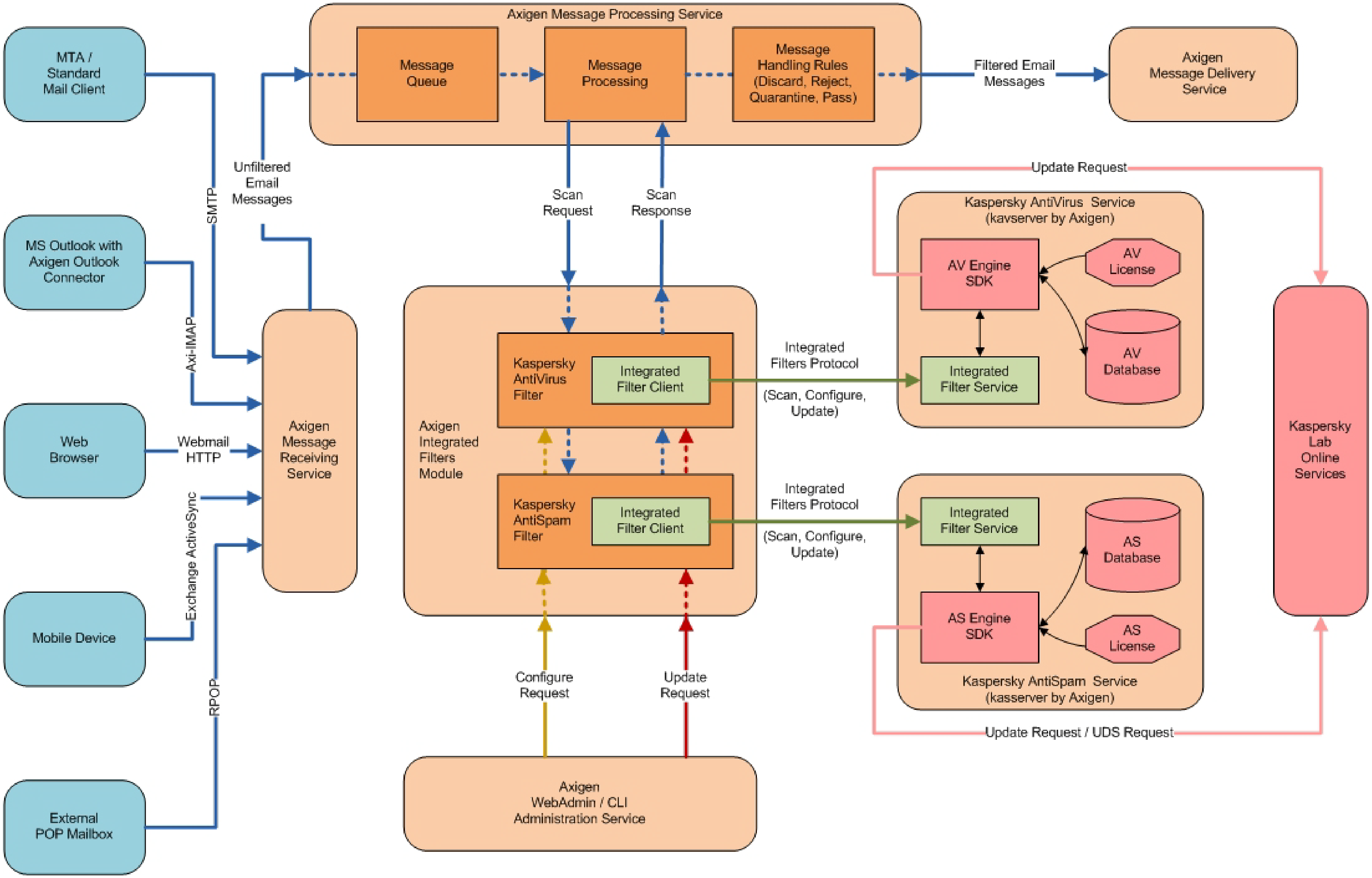
Compared with the other filtering mechanisms used by Axigen (described above), this implementation offers significant benefits such as:

- **Increased reliability –** The Axigen team has designed and implemented all the components of this functionality – the communication protocol (Integrated Filters Protocol), the filters on the Axigen server, as well as the Kaspersky technology-based filtering services.
- **Centralized configuration and updates –** via Axigen's managing services (the protocol has been specifically developed to provide these functionalities).
- **Increased mail scanning and delivery speed** – thanks to the lower protocol overhead and to the fact that emails are scanned directly from Axigen's message queue.

In terms of speed, the integrated Axigen-Kaspersky solution offers for:

- **AntiVirus scanning:** an average speed of 160 messages scanned per second (for regular emails, with sizes between 4-8KB), reaching a maximum speed of over 210 messages per second (for messages smaller than 3KB).
- **AntiSpam scanning:** from an average speed of about 40 messages per second (for emails varying between 4-8KB in size) up to a maximum 80 emails scanned per second (depending on the chosen scanning options and the volume of spam messages).

Integration architecture



MTA / Standard Mail Client
MS Outlook with Axigen Outlook Connector
Web Browser
Mobile Device
External POP Mailbox
SMTP
Axi-IMAP
Webmail HTTP
Exchange ActiveSync
RPOP
Unfiltered Email Messages
Axigen Message Receiving Service
Axigen Message Processing Service
Message Queue
Message Processing
Message Handling Rules (Discard, Reject, Quarantine, Pass)
Filtered Email Messages
Axigen Message Delivery Service
Scan Request
Scan Response
Axigen Integrated Filters Module
Kaspersky AntiVirus Filter
Integrated Filter Client
Kaspersky AntiSpam Filter
Integrated Filter Client
Integrated Filters Protocol
(Scan, Configure, Update)
Integrated Filters Protocol
(Scan, Configure, Update)
Update Request
Kaspersky AntiVirus Service (kavserver by Axigen)
AV Engine SDK
AV License
AV Database
Integrated Filter Service
Integrated Filter Service
AS Database
AS Engine SDK
AS License
Kaspersky AntiSpam Service (kasserver by Axigen)
Update Request / UDS Request
Kaspersky Lab Online Services
Configure Request
Update Request
Axigen WebAdmin / CLI Administration Service

How it works, in detail:

Email messages can be received by an Axigen server through the following interfaces and protocols:

- Messages sent (relayed) through other MTAs using (E)SMTP protocol;
- Messages sent directly by other general mail clients (MUAs) also using (E)SMTP protocol;
- Messages sent from MS Outlook with Axigen Outlook Connector installed through Axigen's extension of IMAP protocol (Axi-IMAP);
- Messages sent from Axigen's Webmail interfaces (Standard, Ajax, Mobile) using PC or Mobile web browsers;
- Messages sent from mobile devices with built-in or installed Exchange ActiveSync clients;
- Messages retrieved by Axigen server through RPOP protocol from other external mailboxes with POP accessibility enabled.

➢ The Axigen Message Receiving Service is responsible for receiving messages on all these incoming flows and for passing all the messages to the Axigen Message Processing Service in order for them to be filtered. The Processing Service stores the messages in the Message Queue, and then passes them along with a processing (scan / filter) request to different instances of filters (processing elements) or chains or filters.

After a message has been processed by a filter, a processing response is returned indicating if the message in question represents a threat (virus, spam, phishing) or not. Using this response, the message handling rules corresponding to the filter instance or belonging to the same filtering chain are applied for that message (discard, reject – send a NDR message in response, move to Quarantine, pass). If the decision is to let the message pass forward, then it will be delivered to its destination by the Axigen Message Delivery Service.

➢ The integration with Kaspersky Lab's technology has been implemented by creating two new types of filters (processing elements), Kaspersky AntiVirus Filter and Kasperky AntiSpam Filter, both using a new technique of processing messages. For emails to be processed by these filters, scan requests are sent to two new external filtering services: Kaspersky AntiVirus Service and Kaspersky AntiSpam Service; these services are executable components separated from the Axigen mail server, developed by the Axigen Team and based on the SDKs provided by Kaspersky Lab, encapsulating their AntiVirus / AntiSpam technologies.

Upon receiving a request from the Axigen Kaspersky AntiVirus / Kaspersky AntiSpam filters, the KAV / KAS Filtering services scan the email messages which reside in the Axigen Message Queue with the filtering AntiVirus / AntiSpam engine from Kaspersky and respond with a result that is interpreted by the KAV / KAS Filters to make a decision on how emails will be further handled. Scanning requests and responses are exchanged between the KAV / KAS Filters and KAV / KAS Filtering Services through a newly-created protocol, named Integrated Filters Protocol, which will be used from now on by the Axigen Team for integrating new filtering technologies.

➢ In addition to the support for scan requests, the Integrated Filters Protocol also supports, as brand new capabilities, configure and update requests. A configure request allows the passing of a set of filter-specific parameters from a filter defined in Axigen to the external filtering service. An administrator can specify through Axigen's Administration Services (WebAdmin and CLI) a configuration for a certain filter and that configuration will be applied to the engine of the corresponding filtering service through a configure request on the Integrated Filters Protocol.

In a similar way, a system administrator can ask for an update of the filtering engine functionality, if that engine has such a capability, and in this case an update request is sent through the Integrated Filters Protocol from the filter to be updated to its corresponding filtering service. In the case of KAV / KAS Filters and Filtering Services, both configure and update requests are supported and have proper implementations that allow the setting of different configurations for the KAV / KAS filtering engines and the updating of these engines by using the online services from Kaspersky Lab.

3.2.2 Solution capabilities, technologies, benefits

The integrated Axigen-Kaspersky solution minimizes complexity and lowers costs with centralized management, flexible configuration options, broad platform support and friendly licensing model, with technical support included.

It lowers security risks with proactive threat intelligence that blocks threats before they even reach the corporate network:

- Combines all the technologies required for comprehensive email security into a single, integrated solution, scanning the mail traffic with industry-leading precision, low system footprint and high speed.
- Delivers low TCO with easy, flexible deployment and administration, consolidated and centralized security functions and extensive database updates.

Effective AntiVirus protection

Integrated as an additional module into the existing Axigen mail system, Kaspersky AntiVirus ensures effective detection and removal of viruses, creating a reliable barrier to their penetration onto the corporate network:

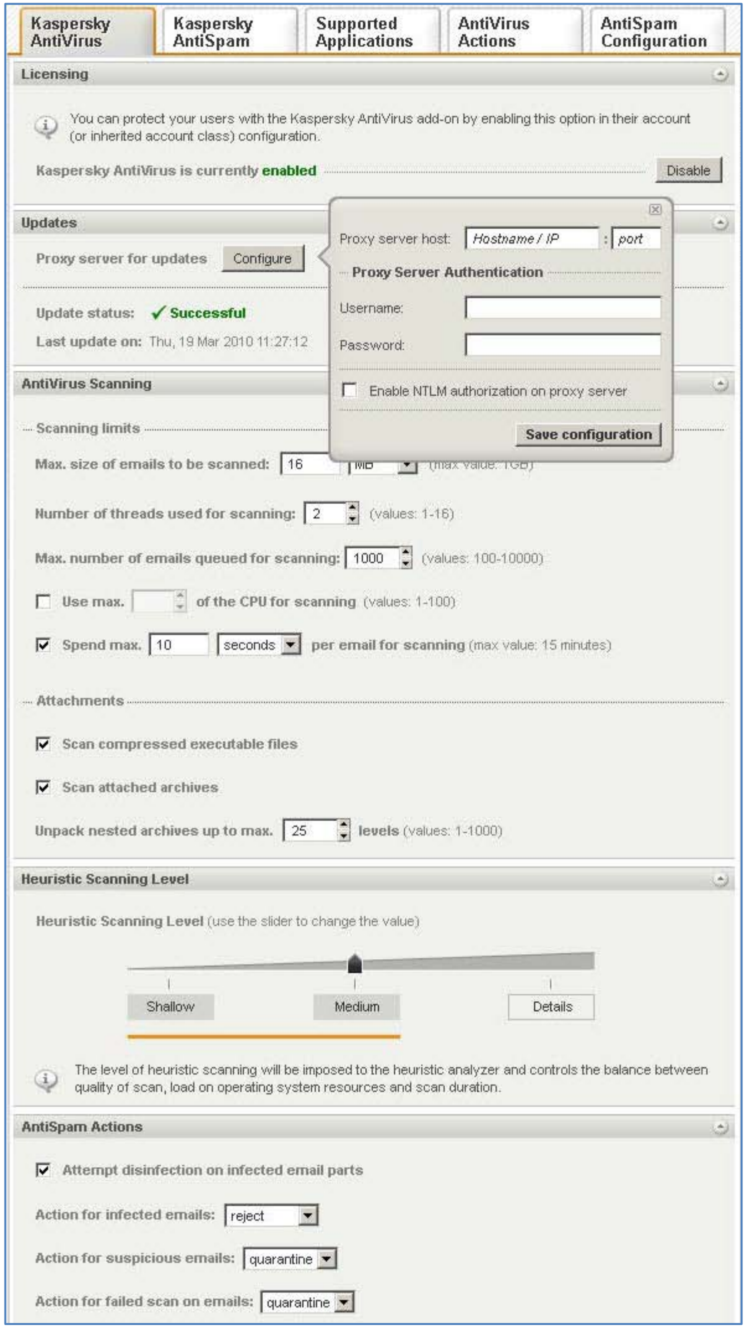
- **Real-time scanning** – The program scans for all types of viruses, malicious and potentially hostile programs in all the elements of incoming / outgoing messages, including attachments in any format.
- **Superior protection –** Defends against existing and emerging threats, via updates to AntiVirus databases and by using the heuristic analyzer (detects threats that have not yet been recorded in signature databases).
- **Quarantine –** Infected, suspicious and damaged objects detected during scans can be delivered, discarded, rejected or moved to the quarantine folder, according to the settings made by the system administrator.

Effective AntiSpam protection

Kaspersky protects both company and Internet Providers mail systems from unsolicited email. It provides a multi-layered defense against spam, scanning mail traffic with using multiple, intelligent technologies such as:

- **Analysis of formal attributes** – The application recognizes spam by such typical characteristics, such as sender email address, size and format of email messages, attachment type etc.
- **Content filtration** – Analyzes the message content, including the "Subject" header and document attachments, by using artificial intelligence.
- **Image recognition** – This technology blocks email messages that contain spam images by using graphic spam analysis.
- **In-the-cloud UDS** (Urgent Detection System) – Emails that could not be assigned a definitive status (spam / not spam) can be also scanned by using the UDS system, which is updated with information about spam messages seconds after they first appear on the Internet.
- **Linguistic heuristics** – The application scans emails (contents and attachments) for words and phrases that are typical of spam messages.

Axigen WebAdmin console
– Kaspersky AntiSpam configuration tab (screenshot)



Licensing

You can protect your users with the Kaspersky AntiVirus add-on by enabling this option in their account (or inherited account class) configuration.

Kaspersky AntiVirus is currently **enabled**

Updates

Proxy server for updates

Update status: ✓ Successful

Last update on: Thu, 19 Mar 2010 11:27:12

Proxy server host: Hostname / IP : port

Proxy Server Authentication

Username:

Password:

□ Enable NTLM authorization on proxy server

AntiVirus Scanning

Scanning limits

Max. size of emails to be scanned: 16 MB (max value: 1GB)

Number of threads used for scanning: 2 (values: 1-16)

Max. number of emails queued for scanning: 1000 (values: 100-10000)

□ Use max. of the CPU for scanning (values: 1-100)

☑ Spend max. 10 seconds per email for scanning (max value: 15 minutes)

Attachments

☑ Scan compressed executable files

☑ Scan attached archives

Unpack nested archives up to max. 25 levels (values: 1-1000)

Heuristic Scanning Level

Heuristic Scanning Level (use the slider to change the value)

The level of heuristic scanning will be imposed to the heuristic analyzer and controls the balance between quality of scan, load on operating system resources and scan duration.

AntiSpam Actions

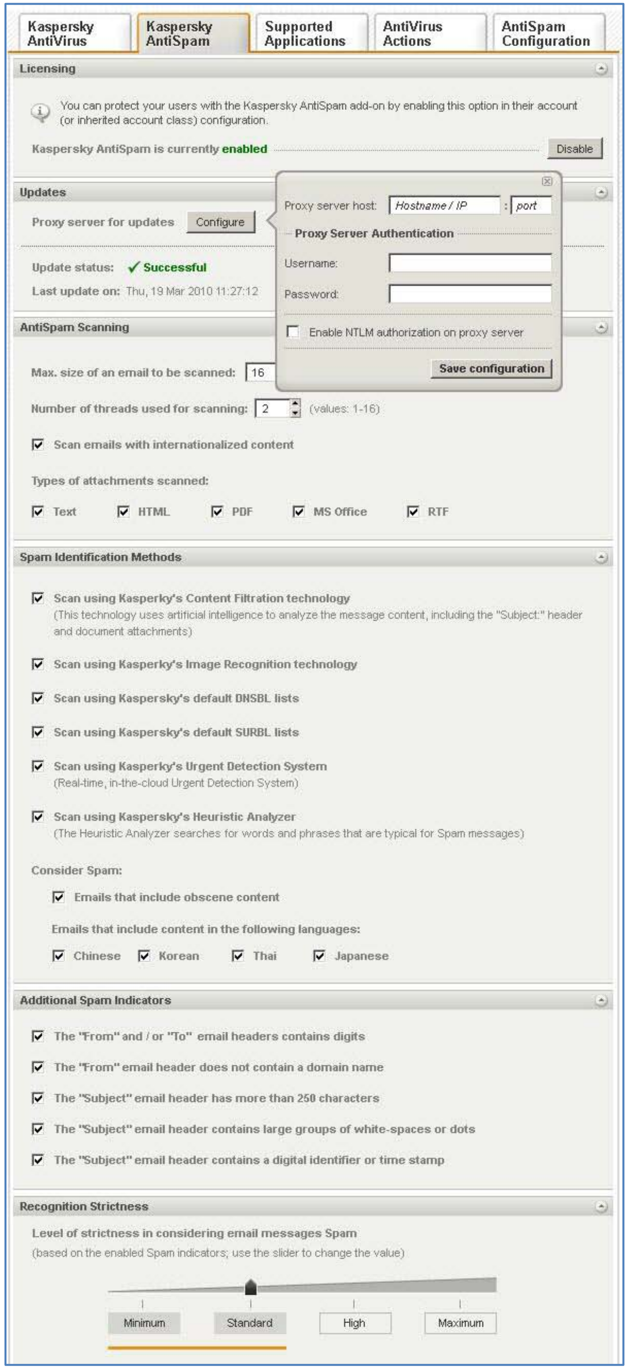
☑ Attempt disinfection on infected email parts

Action for infected emails: reject

Action for suspicious emails: quarantine

Action for failed scan on emails: quarantine

Axigen WebAdmin console
– Kaspersky AntiSpam configuration tab (screenshot)



Licensing

You can protect your users with the Kaspersky AntiSpam add-on by enabling this option in their account (or inherited account class) configuration.

Kaspersky AntiSpam is currently **enabled**

Updates

Proxy server for updates

Update status: ✓ Successful

Last update on: Thu, 19 Mar 2010 11:27:12

Proxy server host: Hostname / IP : port

Proxy Server Authentication

Username:

Password:

□ Enable NTLM authorization on proxy server

AntiSpam Scanning

Max. size of an email to be scanned: 16

Number of threads used for scanning: 2 (values: 1-16)

☑ Scan emails with internationalized content

Types of attachments scanned:

☑ Text ☑ HTML ☑ PDF ☑ MS Office ☑ RTF

Spam Identification Methods

☑ Scan using Kasperky's Content Filtration technology
(This technology uses artificial intelligence to analyze the message content, including the "Subject:" header and document attachments)

☑ Scan using Kasperky's Image Recognition technology

☑ Scan using Kaspersky's default DNSBL lists

☑ Scan using Kaspersky's default SURBL lists

☑ Scan using Kasperky's Urgent Detection System
(Real-time, in-the-cloud Urgent Detection System)

☑ Scan using Kaspersky's Heuristic Analyzer
(The Heuristic Analyzer searches for words and phrases that are typical for Spam messages)

Consider Spam:

☑ Emails that include obscene content

Emails that include content in the following languages:

☑ Chinese ☑ Korean ☑ Thai ☑ Japanese

Additional Spam Indicators

☑ The "From" and / or "To" email headers contains digits

☑ The "From" email header does not contain a domain name

☑ The "Subject" email header has more than 250 characters

☑ The "Subject" email header contains large groups of white-spaces or dots

☑ The "Subject" email header contains a digital identifier or time stamp

Recognition Strictness

Level of strictness in considering email messages Spam
(based on the enabled Spam indicators; use the slider to change the value)

Effective system administration

The integrated Kaspersky protection saves companies time and money, with consolidated protection and streamlined management and configuration:

- **Centralized administration and updates** – The program can be configured and administered both locally and remotely, by using Axigen's Web Administration (WebAdmin) console or the Command Line Interface.
- **Flexible configurations –** System administrators can define the maximum size of messages and types of attachments to be scanned, set the detail level for the heuristic scanning and strictness in considering email messages as Spam, or configure the solution to block obscene messages or with contents in East Asian languages etc.
- **Performance optimization** – Administrators can also set the scanning process based on traffic volume and server hardware characteristics; e.g. define the maximum number of threads and amount of CPU to be used for scanning, the maximum number of emails queued for scanning.
- **Advanced scalability and multi-platform support** – The solution protects both Windows and Linux messaging environments, being suitable for deployment at companies of all sizes, from SMBs to large-scale Service Providers.

4. Conclusions

The Axigen-Kaspersky solution offers the essential protection businesses require in today's connected world. It combines all of the critical technologies required for comprehensive email security into a single, integrated product, delivering real-time defense against viruses, spam and malicious blended attacks, reducing the cost of protecting the messaging solution and facilitating system administration.

Axigen cannot be held responsible for any special, collateral or accidental damages, related in any way to the use of this document. Axigen does not guarantee either implicitly or explicitly the suitability of this material for your specific needs. This material is provided on an 'as-is' basis.