



The Mail Server for  
IT Professionals

# Axigen Mail Server Security Features

---

The AXIGEN messaging solution ensures an efficient and secure worldwide communication environment and business growth for both service providers and companies of all sizes and manages email traffic for more than 11.000 registered servers and approximately 8 million end-users.

Axigen has an extremely flexible configuration system. So far, the system has been able to accomplish every task we have handed it. The product appears to be evolving at an amazing pace. I can't wait to see what future versions contain.

We have been very impressed with the level of detail provided in the filtering and auto-responder features. In numerous cases we've found the environment gives you the power of a detailed script without having to do any of the scripting yourself.

**James Gill - RT Logic, USA**

## Incoming security options



### .01 Encryption



### .02 Multi-layer access control (firewall-like rules)



### .03 Flow control (anti-bombing)



### .04 SPF & DomainKeys compliant (check message sender & integrity)



### .05 Blacklist & Whitelist



### .06 Country Filtering



### .07 DNSBL



### .08 DNS Checks



### .09 AntiVirus Filtering (multiple applications)



### .10 Identity Confirmation



### .11 AntiSpam



### .12 Message Acceptance Policies



## Authentication / Encryption

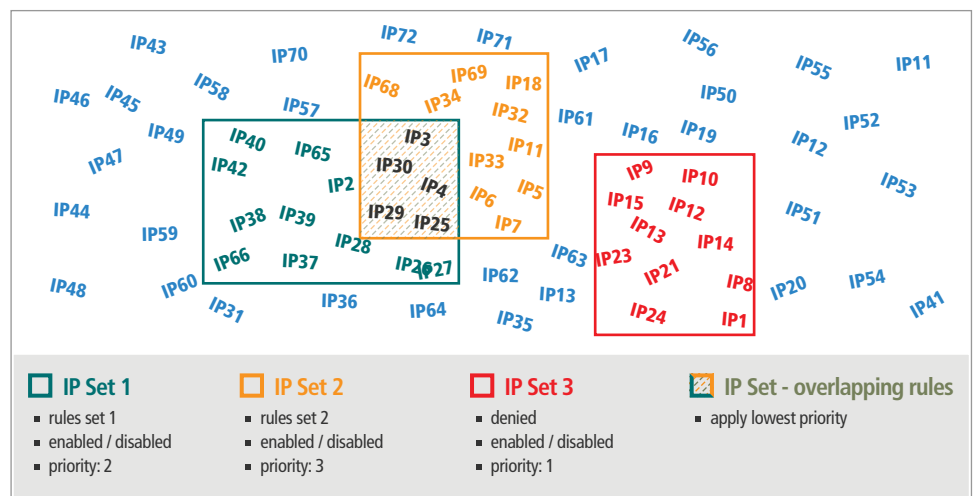
The Axigen server supports authentication, meaning it can be instructed to accept only connections/messages from authenticated entities. The CRAM-MD5, LOGIN, PLAIN, DIGEST-MD5 and GSSAPI methods (in this order) are available for client authentication, reducing the risk of unauthorized connections.

SSL/TLS: All Axigen communication protocols can benefit from SSL/TLS technology which allows sending encrypted messages across networks and preventing plain text messages to be intercepted on the way from sender to recipient. This encryption method guarantees secure data transmission over networks.

## Multi-layer access control (firewall-like rules)

Stopping spammers and preventing DOS attacks is one of the most important tasks of a mail server and the sooner the problem is identified in the mail stream, the better. This is why Axigen has a built in Firewall at the application (TCP listener) level that allows the administrator(s) to control connectivity parameters.

Furthermore, Administrators may define IP sets that have specific sets of such rules, applied with different priorities or IP sets whose connections are denied.



## Flow control

Flow control restrictions can be defined in addition to access control rules, in order to prevent the server and storage overload, as well as protect the server from DDoS attacks.

### Restrict maximum simultaneous connections

Restrict the total number of simultaneous connections that a service may accept, the maximum number of simultaneous connection accepted from the same IP address in order to avoid attacks from a single IP. Additionally, privileged IP address groups (trusted servers) may have different connection limits policies.

### Restrict maximum incoming connections rate

Restrict the total number of connection per time unit that a service may accept, the maximum number of connection per time unit accepted from the same IP address in order to avoid attacks from a single IP. Additionally, privileged IP address groups (trusted servers) may have different connection rate limits policies.

### Selectively restrict maximum messages size

The server can be configured to accept different maximum messages sizes based on sender/sender domain, recipient/recipient domain, remote IP address, connection security, authentication level and other message or connection related parameters, ensuring a flexible protection for the queue and the storage (privileged users may have extended rights).

## Sender validation (SPF compliant)

Axigen implements a standard-based SPF verification module for sender validation (if the remote domain is properly configured with SPF information).

# Outgoing security options



- .01 Encryption**
- .02 Anti-Impersonation**
- .03 Message Sending Policies** (incl. rules to block outgoing spam)
- .04 AntiVirus Filtering** (multiple applications)
- .05 SPF & DomainKeys compliant** (message signing)
- .06 Routing Policies**

## Message integrity validation (DomainKeys compliant)

The messages' integrity may be checked if the originating server used DomainKeys to sign them; locally-originated messages may be signed by Axigen to allow validation by DomainKeys-compliant remote servers (Yahoo associates a higher spam score to unsigned messages).

## Blacklisting / Whitelisting

Permanently reject emails coming from untrusted senders - can be defined globally by the administrator (server level) and further refined by the users according to their personal needs (WebMail interface).

Administrators can also define Whitelists in order to permanently accept emails coming from trusted sources (such as business partners or remote offices).

## Country Filtering

Based on an IP-to-country database, administrators can block all emails coming from untrusted countries; alternatively they can accept emails coming exclusively from selected countries.

## DNSBL (DNS Blacklists)

Administrators validate sender IPs against a selected list of DNSBLs (DNS Blacklists) in order to block emails; at the same time, they can also choose to skip this validation for custom defined IP Ranges.

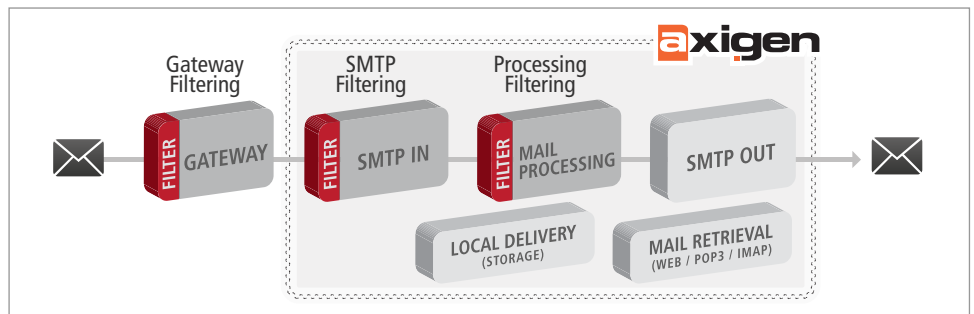
## DNS Checks

Additional validations that can be run to reject spam are by checking the originating domain for MX entries and the originating IP for a reverse DNS entry.

## Multiple AntiVirus Filtering

Axigen currently integrates with 15 of the most powerful AntiVirus applications (e.g. Kaspersky, BitDefender, McAfee, or Trend Micro). The Advanced Filtering System allows sysadmins to define a set of filters and priorities at server, domain or user level, offering unparalleled flexibility to setup company security policies:

- **Domain 1:** filter with 2 AV and 1 ASPAM applications
- **Domain 2:** filter with only 1 AV
- **General Manager:** filter with 3 AntiVirus and 1 AntiSpam applications



## Axigen Identity Confirmation ©

Basically the implementation of a Challenge/Response-based antispam method, Identity Confirmation enables users to block unwanted messages from reaching their inbox by intercepting incoming emails and requiring unknown senders to confirm their identity, while allowing legitimate communications to come through.

## AntiSpam

After applying the above mentioned antispam methods, the remaining traffic is further taken through a content filtering process (score based) & Bayesian filtering (through the included SpamAssassin). Administrators can set the thresholds over which the corresponding reject actions will be applied.

**Commtouch Real Time AntiSpam Protection** - prevents spam outbreaks the minute they occur, available for purchase as a separate add-on.

## Message Acceptance / Sending Policies

Based on an IP-to-country database, administrators can block all emails coming from untrusted countries; alternatively they can accept emails coming exclusively from selected countries.

### Reject:

- emails from impersonated users (authentication matching)
- emails from unauthenticated users
- emails suspicious to be spam (e.g. looping emails, emails with too large attachments and others)

### Require validation for emails coming from unknown sources

### Accept:

- emails coming from trusted sources (Whitelisting)
- secure connections only

## Routing Policies

### Virtual routing

Assign different outbound IP addresses to each domain; blacklisted IPs will only affect the associated domain, and not other domains operating on the same server.

Example:

- relay emails from domain 1 to route 1, using IP1
- relay emails from all other domains to route 2, using IP2
- specify a username/password authentication before routing emails

### Built in DNS Cache

DNS query responses are cached; subsequent queries are resolved locally instead of being re-sent over the network.

## Anti-Impersonation

Enforce user authentication on message submission and verify that the sender header matches the authentication credentials preventing impersonation attempts from local accounts.

Message and connection parameters for security policies (message size, anti-impersonation, SPF, access control, email address blacklisting / whitelisting, DNS checks, open relay blocking, etc):

- Originating host's IP, ports, greeting
- Originator's email address, domain or username
- Recipient email address, routing information
- Message size, headers, number of recipients
- Connection security level (SSL / non-SSL)
- Authentication information
- Session statistics (total mails sent, total size)
- SPF interrogation result; etc

## Secure passwords enforcement

Define password strength policies (minimum password length, required sets of characters and so on), restricting the users from setting simple passwords.

## Contact info

### GECAD TECHNOLOGIES

10A DIMITRIE POMPEI BLVD.,  
020337 BUCHAREST, ROMANIA

Tel: **+40 21-303 20 80**

Fax: **+40 21-303 20 81**

Email: **sales@axigen.com**

**www.axigen.com**

