Buyer's Guide:

MAILMARSHAL™
SERVICE PROVIDER EDITION

Contents

This document serves as a guide for administrators and IT professionals representing service providers interested in MailMarshal Service Provider Edition (SPE). The intention of this document is to provide the reader with background information on MailMarshal SPE, explore the kinds of services and opportunities that MailMarshal provides and outline how the solution works. After reviewing this document, the reader should have an appreciation of the technical architecture of MailMarshal SPE and how it can deliver a platform for a service provider to provide their own quality hosted email security service to customers.

MARSHAL™
Secure. Protect. Comply.

Introduction to MailMarshal Service Provider Edition

MailMarshal Service Provider Edition (MailMarshal SPE) is a business enablement solution for managed service providers and ISPs to offer their own hosted email content security services to customers. It is a software solution designed to be deployed by a service provider within their environment and forms a platform for hosting email security services. Any customer with their own email domain is capable of subscribing to the service via a simple MX record change.

MailMarshal SPE offers a range of potentially different hosted services including email content filtering, anti-spam, anti-virus, policy compliance, email archiving and reporting. MailMarshal SPE possesses a centrally managed and highly scalable architecture capable of supporting thousands of customers and hundreds of thousands of email accounts.

MailMarshal SPE enables service providers to easily offer email hosting services to businesses as well as SOHO customers with a customizable user interface and tiered service levels.

Why Offer Hosted Email Security Services?

Email is the most prevalent form of business communication today. For many companies it is a mission critical business tool, essential to support their daily operations. However, as much as email has become the life-blood of business, spam, viruses, hackers and other undesirables have tarnished email's usefulness and effectiveness. These threats have de-valued email to the point where many see it as a curse rather than a blessing.

Every year companies spend billions of dollars on email security, anti-spam, anti-virus and other preventative technologies. Many of these technologies and security measures are out of reach for some businesses as they are either cost-prohibitive or too complex to manage with their in-house resources. Additionally, many organizations are looking to shed themselves of the burden of in-house email security and are turning to the expertise and benefits of outsourcing and managed service providers.

Respected industry analyst firm Frost & Sullivan predicts that managed email services will be worth US$825 million by 2012 and constitute more than 31% of the global email filtering market.

MailMarshal SPE is a business enablement solution that allows a Service Provider to host and offer their own email filtering services. With MailMarshal SPE you can offer your customers access to high quality, professional email security services that they would not normally wish to, or be able to, support themselves. These services can be as simple and straight-forward as "cleansing" customers' email of viruses and spam. Or, they can be more comprehensive and cover business requirements such as email compliance, archiving and confidentiality protection.

What is the Revenue Opportunity?

Hosting your own email security service with MailMarshal SPE presents many opportunities. Marshal will help evaluate your specific business opportunity as part of a consultative approach by reviewing your customer segment, business model, pricing, implementation and any special requirements you may have.

A sample scenario could be as follows:

A service provider has 50 customers, each with 100 employees totaling 5,000 email users. Marshal offers the service provider a flat fee of US$1.00 per user per month. The service provider introduces an email "cleansing" service at US$2.00 per user per

[1] *Please note that this price is used as an example only.*

month, thus making a $1.00 margin per user per month. 100% of the service provider's customers opt for this cleansing service which includes anti-virus, anti-spam and DOS protection.

The service provider also offers a more advanced email service encompassing blocking of offensive content, profanity, restricted file types and email activity reporting. This service is offered at an additional $3.00 per user per month. 50% of the service provider's customers opt for this additional service.

Thus the service provider has 5,000 users on the cleansing service at $2.00 each per month, plus a further 2,500 users on the advanced service at $3.00 each per month. The service provider is receiving $17,500 per month in service revenue and has $5,000 in fees to Marshal per month. This provides the service provider with $12,500 net profit per month, or $150,000 per year.

The above scenario is merely an indicative example of what the revenue opportunity might be for a service provider. Pricing arrangements can be flexible to help meet the requirements of your business model. Also, this example only covers two of the many possible service options. You can host multiple additional services with MailMarshal SPE such as archiving or pornographic image filtering. MailMarshal SPE provides you with the means to generate an incremental and a healthy recurring revenue stream with excellent margins.

The Benefits of Outsourcing Email Security to Customers

There is a strong business case for Service Providers to offer hosted email services to customers. But why would customers turn to outsourcing their email security? What are the benefits to them? What is the return on their investment?

Major industry analysts such as Gartner, IDC and Frost & Sullivan forecast that the managed email security market is set to explode in the near future. This is primarily because of spam and the immediate benefits that can be found in a "mail scrubbing" service which removes spam and viruses before those messages reach the customer's email network. Here are some of the reasons and benefits why customers are turning to managed security and how they can realize a return on their investment:

- Blocking spam at the service provider level means that the customer is receiving a "clean" email stream free from spam, viruses, phishing and spyware. This means that the customer can be more confident that their email is free of risks and enjoy the benefits of using email without many of the disadvantages.
- Blocking spam upstream means that the customer may see anything from a 60 percent to 90 percent reduction in their overall incoming email. Most customers today will be seeing about 80% of their incoming email as spam. By eliminating up to 99.9% of these messages with MailMarshal SPE the customer will be receiving far less email volumes and making a substantial saving on their bandwidth and storage/archive costs.
- Outsourcing means that the customer incurs no upfront hardware costs. This assists with the budgeting process and means that the customer doesn't have associated costs such as actually operating additional hardware, maintaining it, servicing it and powering it. The customer doesn't have to set it up, unpack it or find room for it in their office. They just subscribe to the service and that's it.
- The customer benefits from your expertise and resources in email security management. This means they do not have to employ specialist technical staff to manage their own in-house email security resources. They also benefit from the knowledge and resources that you have available as the service provider to ensure their email's protection.

MARSHAL™
Secure. Protect. Comply.

- Rather than finding the headcount budget to employ email security administration staff, customers can use the funds to employ IT staff for their own proactive and positive projects such as roll-outs, new developments and projects that will actually add to their bottom line.

What Hosted Email Services Can I Offer With MailMarshal SPE?

MailMarshal SPE can support a wide range of hosted services that you can tailor to your desired service model or to the specific requirements of your customers. These services can include (but are not restricted to) the following:

- Email Filtering & Security – typically the object of this service is to cleanse or "scrub" the customer's incoming email of threats before they reach the customer's network. The make up of this type of hosted service would normally cover:
    - Anti-spam and anti-phishing
    - Anti-virus and anti-spyware
    - Screening out Denial of Service Attacks
- Policy Enforcement & Compliance – the general objective of this type of service is to manage the overall content of incoming and outgoing emails in line with the customer's policy needs. This might cover:
    - Blocking profanity in incoming and/or outgoing email
    - Blocking racist, sexist or other politically insensitive remarks, particularly in outgoing email
    - Blocking sexually explicit images attached to email messages
    - Blocking specific types of attachments for some users, such as MP3 audio files, AVI video files and executables. Customers may also wish to restrict some outgoing file formats such as CAD files or database files to protect the distribution of commercially sensitive information.
    - Restricting the size of incoming or outgoing emails
    - Blocking outgoing messages containing sensitive or confidential information from unauthorized email accounts
    - Adding customer specific disclaimers to all outgoing messages
    - Any message can be managed based on the sender, the recipient, message size, IP address, domain, attached files, recursively packed files, or text in the message header, body or subject line
- Email Archiving & Retrieval – the purpose of this service is to retain copies of all incoming and outgoing messages (minus spam) for the customer, so that they can retrieve specific messages on demand from a central location. Retention periods can be flexible depending on the needs of the individual customer, and you can charge customers different fees based on the length of time they wish email to be archived for. With MailMarshal SPE, the customer can search for messages themselves and forward copies of messages to themselves. Search facilities are comprehensive, but very intuitive. Customers can search based on sender, recipient, date, subject, message size and other criteria.
- Email Reporting – there are several reasons to offer customers reporting services:

- It allows the customer to measure the effectiveness of the hosted service. For example, if the customer is using the filtering service to block spam, they will have no idea how effective the service is without reporting. Reports will highlight exactly how much spam is being blocked and demonstrate the benefits of the service. This in-turn reinforces the value of the service to the customer and ensures the customers continued business.
- Reporting is flexible. It can be linked to the services that the customer is subscribing to. For example, you can offer anti-spam and anti-virus reporting to customers as part of the Filtering service but charge them separately for more advanced reports such as bandwidth usage and attachment detail reports.
- A more advance service offering could be based on Policy & Compliance where reporting is instrumental in allowing the customer to see a summary of which policies are being breached and by whom. Reports can tell the customer who is sending and receiving the most email, who is consistently using profanity in email and which users have been attempting to transmit sensitive documents.

- Secure Email – the purpose of this service is to provide the customer with a secure channel for email when they need it. Via TLS encryption you can host a secure platform for customers who need greater levels of security on their email.
  - With TLS you can establish secure links between the end customer and your environment. This can also be extended to organizations that your customer wants to communicate with if they support TLS. The result is a hosted, encrypted communication channel between the customer and their partners.

What Level of Service Commitment does MailMarshal SPE Provide?

Email is a mission critical resource for customers and hosting email security services means that email must be fast, reliable and safe. For service providers it is important to be able to provide high levels of service and dependability to customers. MailMarshal SPE is capable of supporting even the most stringent service levels:

- Uptime – if you are hosting email services, customers need to know that their email will be delivered in a reliable and timely fashion. Thus, service uptime is of paramount importance. Depending on the hardware provided, MailMarshal's array architecture can allow you to achieve scheduled uptimes of 99.999%.

MARSHAL™
Secure. Protect. Comply.

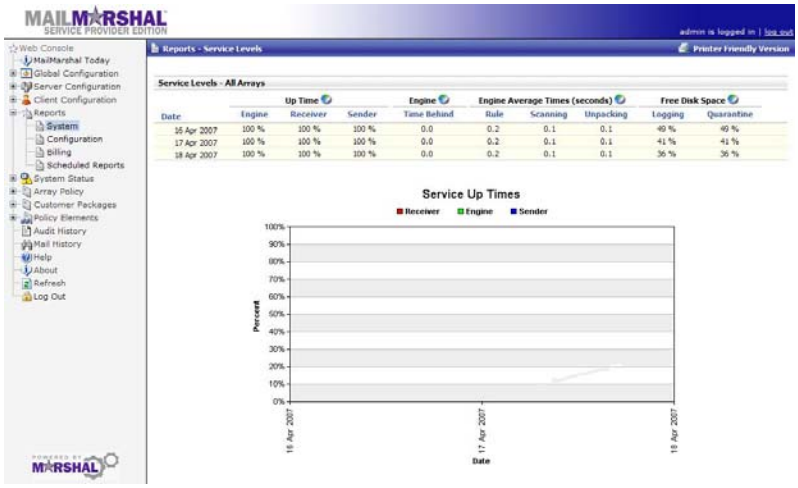


Figure 1: MailMarshal SPE service uptime report

- Performance – Spam clogs email and slows down the speed of delivery. Ideally, any truly effective anti-spam solution should not only reduce spam, it should also improve email performance. Often deployment of email filtering and security products can result in a performance bottleneck; delaying email as it is processed and checked. MailMarshal is extremely fast and utilizes a multi-threaded architecture. In fact, MailMarshal is at least twice as fast as other email filtering solutions. With MailMarshal, you can assure customers that after receiving an email, it will be no longer than 60 seconds on average to begin delivery of the message to the customer.

- Spam Filtering – Today spam accounts for anywhere from 70%-90% of global email depending on whom you talk to. This means that for every 10 emails a user receives, between 7 and 9 messages will be unsolicited, commercial emails. This has a huge effect on productivity, bandwidth and storage resources. The common standard spam blocking rate for an effective anti-spam solution varies between 95% to 99%. MailMarshal SPE achieves consistent spam blocking rates of 99.5% or better. This exceptional blocking rate is balanced against a false positive rate of 0.001% or 1 in 100,000 messages. Your customers can define their own spam white lists of domains and email addresses that they regularly communicate with and never receive spam from to further reduce false positives.

- Virus Blocking – MailMarshal SPE supports a range of leading anti-virus and spyware scanners, even allowing the operation of multiple scanners together simultaneously for added protection. You can assure customers that 100% of known viruses will be blocked and additional anti-virus measures can quickly be implemented for all users during an unknown virus outbreak.

MARSHAL™
Secure. Protect. Comply.

10 Reasons to Choose MailMarshal Service Provider Edition

1. Unique Service Provider Architecture

MailMarshal SPE is one of the world's few true email security solutions for large, distributed, multi-server environments. MailMarshal's unique Array Manager architecture allows centralized administration and control of policy and email handling across hundreds of email processing nodes.

This is a critical factor for service providers who want to offer high volume, high quality and high availability email security services. The ability for MailMarshal SPE to support thousands of customers across multiple servers located in geographically distributed environments makes it second to none.

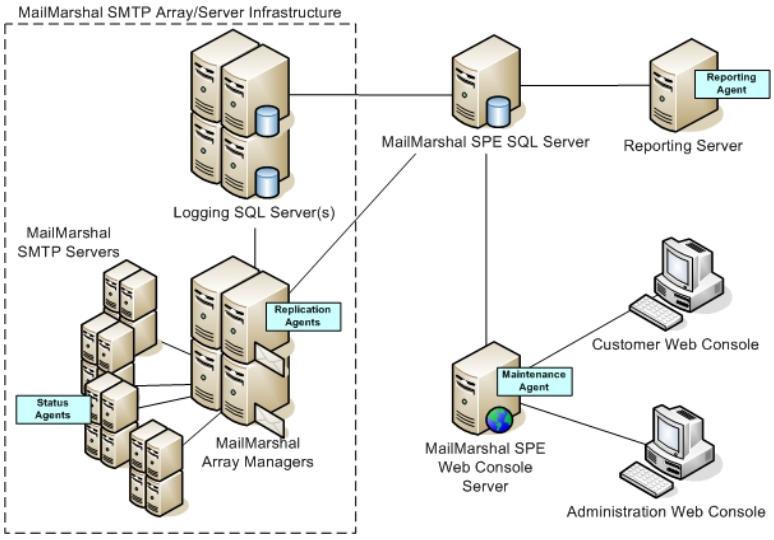
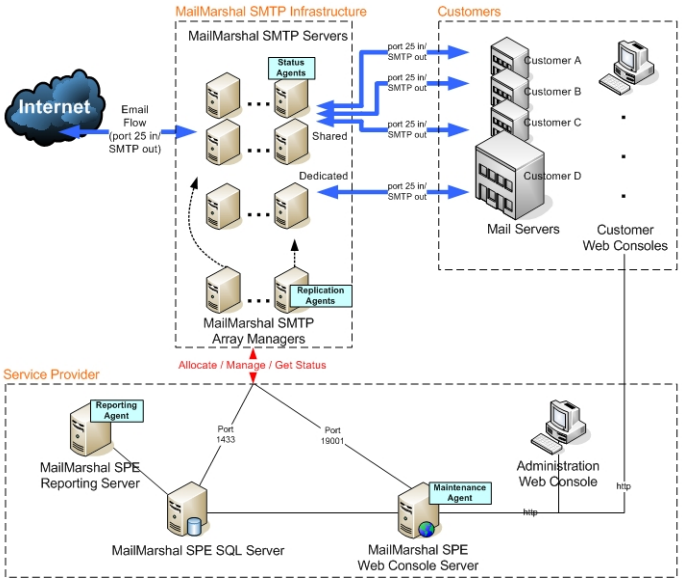


Figure 2

Figure 4 shows how the overall MailMarshal SPE solution can be hosted on multiple servers, separated to perform specific function. Separate mail processing nodes (shown as MailMarshal SMTP Servers) function as the mail processing and filtering servers. The MailMarshal Array Managers operate as the controllers and monitoring stations for the MailMarshal SPE environment with separate SQL logging servers for increased performance and redundancy.

MARSHAL™
Secure. Protect. Comply.



2. Performance, Scalability and Redundancy

Because of MailMarshal's unique array architecture, it is possibly the most scalable and capable enterprise security solution in the world. MailMarshal is deployed in very large user environments supporting over 150,000 users. Its ability to link multiple email servers together in clustered and load-balanced arrays provides an opportunity for service providers to centrally and reliably manage hundreds of thousands of email accounts.

MailMarshal's Array Manager architecture is not only very scalable and high performing; it is also a strong redundant platform. Email processing nodes can continue to run for extended periods while disconnected from the Array Manager or SQL logging servers. Nodes can be connected in load-balanced, redundant arrays ensuring "always on" availability and allowing flexibility for maintenance and support.

3. Comprehensive Policy Management

MailMarshal is one of the most comprehensive email security solutions on the market; able to implement even the most complicated or specific email processing rules. It can identify and strip attachments. Lexically analyze the headers, body and attachments and contextually find keywords and phrases of importance. It can process spam in a multitude of ways including subject line marking, DNS blacklisting, end-user message release or simple deletion. It can allow customers to reject oversized messages or delay delivery of large messages.

Almost any conceivable rule or policy that you wish to offer your customers, or your customers wish you to implement, can be delivered by MailMarshal. MailMarshal gives you the flexibility to offer different levels of advanced services and create revenue accordingly.

4. Flexible Customer Administration

MailMarshal SPE allows you to offer customer different levels of administrative access. This can include the ability to schedule reports or alter rules and release quarantined messages. Customer administrators can be granted rights to set up their own internal sub-administrators and privileges, such as giving managers rights to schedule and create their own reports but not the ability to alter rules.

To set-up and maintain customer email account information, the MailMarshal SPE Connector Agent allows easy synchronization of customer user account information

MARSHAL™
Secure. Protect. Comply.

from their site over secure HTTP. This means that your administrative overheads are lower and your staff can focus on other, more productive tasks. The connector agent will update MailMarshal SPE with the customer's latest LDAP and Active Directory account information.

5. Easy Service Provider Administration

Your own staff will find it easy to manage multiple users and servers with a centralized management console. The administration web console makes it easy to manage policies, user accounts and messages spread across multiple email processing nodes.

Comprehensive logging assists with diagnostics and troubleshooting, while administrative change auditing allows you to track who has made changes, when and what was changed.

Billing and accounting systems can easily be integrated through reporting and logging outputs.

6. Best-in-Class Content Security

MailMarshal is often used as the benchmark for email content security by businesses and competitors alike. MailMarshal's email filtering engine recursively unpacks archive files, detecting viruses and inappropriate content. It identifies file types by their characteristic signatures rather than using less reliable methods like file extensions. Lexical analysis combines Boolean logic operators, regular expressions, wildcards, special character matching, weighted scoring and increasing/decreasing multipliers for absolute flexibility and thoroughness.

MailMarshal's email filtering engine is not only one of the most thorough, it is also the fastest. Multi-threaded architecture and message processing allows MailMarshal to achieve throughput rates that are at least twice as fast as our nearest competitors.

7. Leading Anti-Spam Performance

MailMarshal uses a layered, multi-faceted approach to spam detection called *SpamCensor*. SpamCensor is not reliant on any one technology but instead combines multiple anti-spam methods together into a heuristic solution.

MailMarshal routinely achieves spam detection rates of 99.5% or better with a fractional number of false positives in the range of 1 in 100,000 messages. Completely customizable, MailMarshal SPE cannot only handle spam differently for different customers; it can also be tuned with exception lists by customer domain and individual user account.

8. Flexible and Comprehensive Reporting

MailMarshal SPE provides extensive reporting capabilities for both customers and service administrators. Dedicated system reports for service providers cover billing, rules, service uptimes and total numbers of accounts and messages.

You and your customers can schedule automatic generation of reports or run reports on demand. You can have reports automatically emailed to defined email addresses. Reports can cover a range of criteria including bandwidth, cost apportioning, rules triggered, reports by domain, user, customer, and customer group or department.

9. Chosen by Enterprises and Service Providers the World Over

MailMarshal is used by 18,000 corporate customers around the world, protecting over 7 million users. Our customers include 40% of the Global Fortune 500 companies.

MailMarshal has been in use with multiple service providers for many years and Service Provider Edition has been developed incorporating their close input and feedback.

MARSHAL™
Secure. Protect. Comply.

10. Proven World Leader in Email Security

Marshal is a proven technology leader in the email and Internet content security space. With 10 years of industry experience, over 18,000 customers, consistent growth and profitability, and a track record of product excellence and quality customer service, Marshal is a strong technology partner for any service provider.

Frost & Sullivan highlights our history in developing "state-of-the-art technologies". In a recent Marshal customer survey over 96% said that they would recommend Marshal solutions to others.

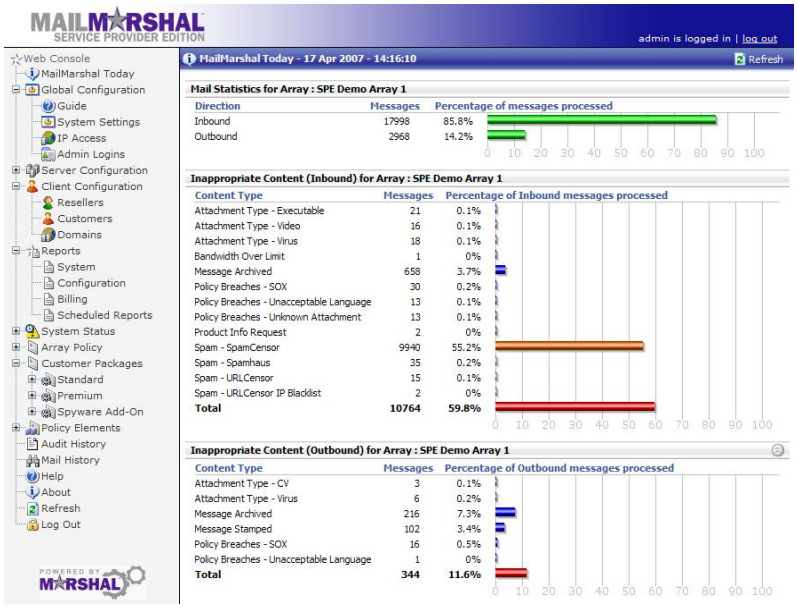
MARSHAL™
Secure. Protect. Comply.

Branding and Customization

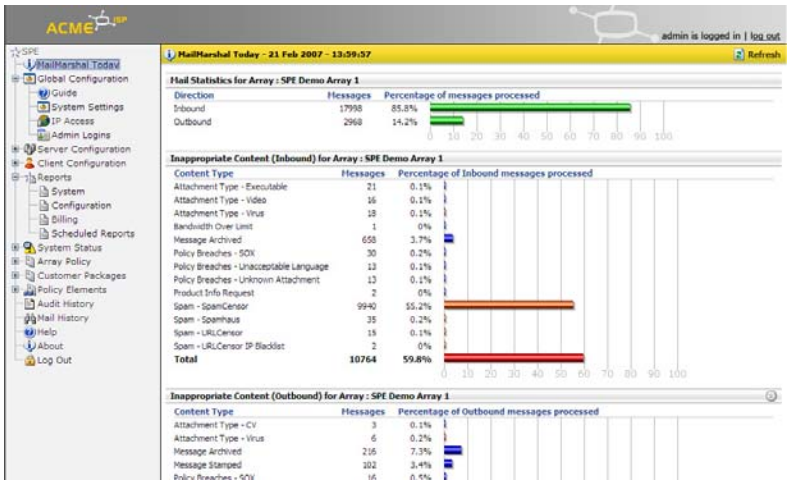
Another important aspect of MailMarshal SPE is the ability to customize and re-brand the service to your specific requirements. It is simple to change the product screen color scheme, insert your company logo and rename the service to meet your own branding guidelines.

Below you can see a screenshot of the default MailMarshal SPE user interface complete with blue colour scheme and MailMarshal logo. Underneath is a screenshot showing an example of a re-branded screen by a service provider named ACME ISP. The color scheme and logos have changed to adhere to ACME branding guidelines.

MailMarshal SPE Default Branding



Example ACME ISP Customized Branding



MARSHAL™
Secure. Protect. Comply.

Technical Overview of MailMarshal SPE

What does MailMarshal SPE provide?

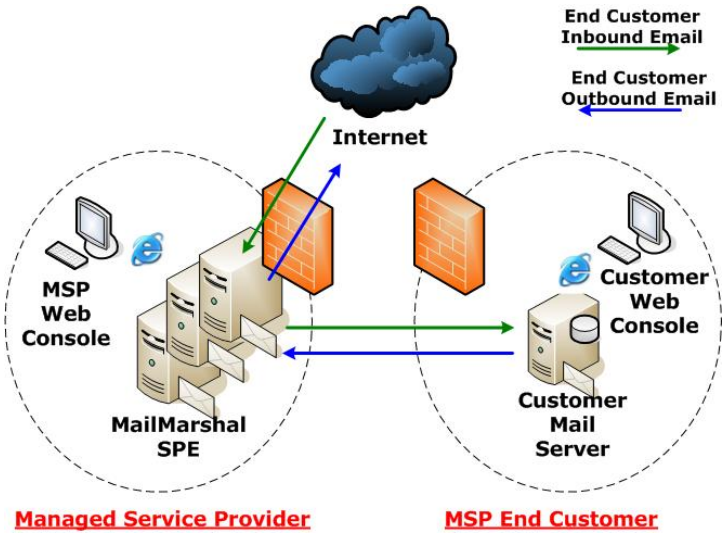
MailMarshal SPE provides a framework that allows a Service Provider to deliver managed email content security services for other organizations. Email processing tasks are performed by a number of MailMarshal servers located within the Service Provider's network.

With MailMarshal SPE, the Service Provider can dynamically allocate MailMarshal servers to a particular customer organization as an email content security service. All policy elements, including enforcing Acceptable Use Policy and protecting against spam, viruses and other undesirable content, can be managed remotely by the Service Provider and the customer using a Web-based console. The web based interfaces to meet the needs of administrators and email recipients are:

- Service Provider Administration Web Console - Allows the Service Provider Administrator(s) to monitor and manage customers, review MailMarshal server information, and establish preset policies for customers.
- Customer Web Console - Allows the Customer to monitor and control email activity for their respective organization. Customers who have advanced subscriptions can establish their own email policies. Customers can also have different levels of administrative rights within the web console with some administrators able to perform more advanced tasks.

MailMarshal SPE provides total administrative control of all underlying MailMarshal servers. The product provides Service Provider administrators with granular control of policies, and the ability to delegate email monitoring and control to other email administrators. Further customizations can be achieved by allowing customer administrators to configure email policies.

MailMarshal SPE provides the ability to manage arrays of MailMarshal servers. This function delivers a Service Provider architecture that is scalable to large numbers of customers. MailMarshal SPE is designed to deliver email content security services for very large user numbers and very large volumes of email.



How MailMarshal SPE Works

The underlying technology for MailMarshal SPE is based on the award-winning MailMarshal SMTP platform. MailMarshal SMTP is a server-based Simple Mail Transfer Protocol (SMTP) email content scanning product. MailMarshal SPE uses one or more MailMarshal SMTP Servers as email gateways to enforce email content security policies for customer organizations. All configuration of the gateway for delivery and scanning rules is provided through MailMarshal SPE.

Understanding What MailMarshal SMTP Does

The MailMarshal SMTP server functions as an email gateway. All inbound and outbound email passes through MailMarshal SMTP. Each MailMarshal Server runs several component services, including the Receiver, Engine, and Sender services. Email enters the MailMarshal Server at the Receiver, where MailMarshal SMTP applies any enabled Receiver rules.

Receiver rules offer powerful protection because they can refuse incoming email based on criteria such as email not addressed to a recipient in your customer's organization. Receiver rules that block email this way conserve resources for other legitimate email.

Next, the MailMarshal Engine unpacks each email by splitting it into header, and message, and expanding any attached archive or compressed files. The Engine then checks each component against the email policy (rules) you have enabled, including SpamCensor scripts, URLCensor, TextCensor scripts, and any other rules you have enabled. You can alter the effects of MailMarshal SMTP rules by changing the rule order and by changing specific characteristics of the rule.

MailMarshal SMTP also scans email for viruses by running antivirus scanning software against messages during the engine unpacking phase. MailMarshal SMTP directly supports many commercially available scanners. The product is versatile enough to support most antivirus scanners that provide a scanning response in the correct format (most antivirus scanners do). Furthermore, MailMarshal can simultaneously employ two or more virus scanners for additional protection and security.

After the MailMarshal Engine evaluates each email component against the rules, it determines whether to accept, modify, or quarantine the email.

- Accepted email is passed to the MailMarshal SMTP Sender, which then delivers it to the appropriate recipients.
- Modified email may be delivered to recipients with attachments removed.
- Virus-laden email is typically quarantined and interested parties are notified if desired.

MailMarshal SMTP can also notify administrators of specific actions or notify end-users of quarantined email. You can associate the appropriate rule action when you create or modify rules.

What does SPE add to MailMarshal SMTP?

MailMarshal SPE builds on top of MailMarshal SMTP and provides web based administration interfaces that are organized around being able to associate a number of domains to a particular customer and then manage policy around that customer. It removes any complexity caused by this requirement in MailMarshal SMTP, which is designed to manage by Domain.

MailMarshal SPE also offers a 'Self Provisioning' customer console which an end customer can use to define their own policy options, run reports and any other day to day administration function that they would quite often have to rely on the service provider to perform.

MARSHAL™
Secure. Protect. Comply.

SPE also adds a number of advanced management tools to MailMarshal SMTP that have been designed to further simplify the administration task, these are defined in full later in this document but include:-

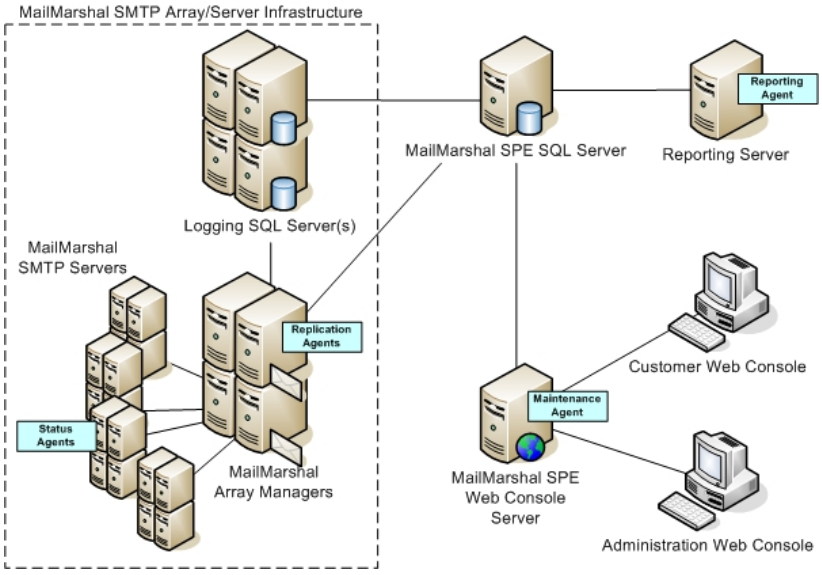
- Availability & status monitoring
- Email based alerting
- Administration auditing
- Reporting

Technical Architecture

Understanding MailMarshal SPE Components

MailMarshal SPE consists of several software components, which you can install on different computers in your network. These components can be installed in a variety of configurations to suit various deployment requirements of the Service Provider. The MailMarshal SPE components are shown on separate computers in the following figure.

As a minimum, you can install the components on a single computer, with the SPE SQL Server run on a separate machine.



MailMarshal SPE Components

As you can see from the diagram above there are a number of components in MailMarshal SPE, these are explained below:-

Customer Web Console

Web-based console that allows customer administrators to define organization users and email policy (rules), and to configure additional email gateway settings.

Administration Web Console

Web-based console that allows Service Provider administrators to manage and monitor customer information, configure system wide policies, and control global MailMarshal SMTP settings.

Web Console Server

Provides website services for the Customer Web Console and Administration Web Console. The Web Console must be installed on a server with Microsoft IIS (including the Active Server Pages component) installed.

Reporting Server

Used to prepare pre-existing scheduled reports and emails selected reports to Administrators and end users.

SPE SQL Server

Stores data and configuration information for MailMarshal SPE. For more information, see "MailMarshal SPE Architecture".

MailMarshal SPE Agent Services are essential run-time components used to carry out management tasks as configured by Service Provider and customer administrators. To operate properly, MailMarshal SPE requires MailMarshal SMTP Array/Server infrastructure. The Replication Agent and Status Agent must be installed on each Array Manager and SMTP Server respectively.

Maintenance Agent

Provides performance optimization and manages temporary data retention for the Web Console server and the database. This agent must always be running and is installed on the same server as the web console

Replication Agent

A Replication Agent is installed on every MailMarshal Array Manager that is managed by MailMarshal SPE. The Agent provides integration between MailMarshal SPE and the Array Managers, including policy updates.

Status Agent

A Status Agent is installed on each MailMarshal SMTP Server that is managed by MailMarshal SPE. The Agent supplies real-time notifications about the server's conditions to MailMarshal SPE.

Reporting Agent

Performs regular data mining and reporting functions from the SPE SQL Server.

MARSHAL™
Secure. Protect. Comply.

Other Software and Services

Logging SQL Server

MailMarshal SPE retrieves data about each MailMarshal SMTP Array from the respective Logging databases. This typically includes message logging and configuration of each Array.

Array Manager

The Array Manager controls an array of MailMarshal SMTP email processing servers. The Array Manager connects to the email processing servers and to the Logging database, hosted using Microsoft SQL Server.

MailMarshal SMTP Email Processing Server

Accepts email, applies policy in the form of rules, and forwards email to the appropriate internal or external recipient.

Understanding Email Flow in MailMarshal SPE

MailMarshal SPE provides a single access point that allows a service provider to configure, control and report email flows for multiple organizations. Email flow in MailMarshal SPE is largely identical to the flow in MailMarshal SMTP. However with MailMarshal SPE, the processing and logging of email for several organizations is carried out on a shared array of email processing servers.

MailMarshal SPE allows each subscribing organization to assess and enforce its own company email Acceptable Use Policy, manage client use of bandwidth, prevent confidential information from leaving the company, and increase employee productivity.

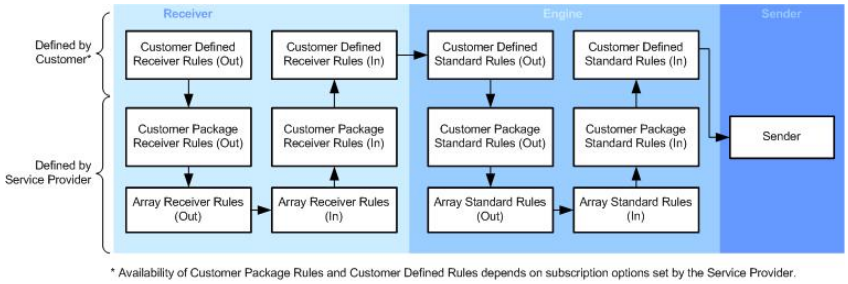
Working transparently to all users, MailMarshal SPE works at the Service Provider gateway, filtering and removing dangerous and undesirable objects before they can enter the organization's network.

MailMarshal SPE allows email processing rules to be managed at three levels.

1. The Service Provider can apply global rules to all arrays in the infrastructure.
2. The Service Provider can individually set rules for each array.
3. Each customer organization can configure rules. Customer-defined Rules allow each customer the flexibility to match and enforce its own Acceptable Use Policy. For example, the rules can check for inappropriate content, confidential material, specific keywords, and other criteria important to the organization Customer defined rules can be offered as a value-added option on a subscription plan.

To better explain how MailMarshal SPE manages email for multiple organizations and to help plan your MailMarshal SPE installation, the following sections describe how MailMarshal SPE controls inbound and outbound email flows.

MARSHAL™
Secure. Protect. Comply.



* Availability of Customer Package Rules and Customer Defined Rules depends on subscription options set by the Service Provider.

Inbound Email Flow

Each organization's inbound email at the internet gateway is immediately directed to a pre-assigned array of MailMarshal SMTP email processing servers.

Once email has been received, the processing flow is identical for all customer organizations. First, connections and messages are validated against MailMarshal SMTP Receiver rules. Receiver rules can reject email based on various criteria. For example, the Denial of Service (DoS) receiver rules handle a deluge of SMTP requests that can result in system overload to protect the system from this type of attack. Receiver rules help cull much undesirable email before it enters your network. None of this traffic enters the network, so MailMarshal SPE does not log this activity.

If an email is not blocked by a Receiver rule, the MailMarshal SMTP server copies the email to a working folder. The MailMarshal Engine component splits the email into header, message, and attachment components. If necessary, the Engine recursively uncompresses any attachments to analyze the original files.

MailMarshal can apply a number of filtering mechanisms to identify viruses, spam (SpamCensor), undesirable URLs embedded in the email (URLCensor), specific text (TextCensor), country of origin (CountryCensor), and other content to exclude, flag, or log. Rules can block email based on attachment size, unapproved relaying, sender or recipient, inclusion on unapproved lists, such as DNS, Phishing, or URL blacklists, and many more characteristics.

The rules can direct MailMarshal to take specified actions based the rule results. For example, if an email contains a virus, MailMarshal quarantines it. If the message is acceptable but the attachment is not, MailMarshal can strip the attachment but deliver the message, and notify the recipient of its actions.

If the email is virus-free and not flagged by any other rules, MailMarshal SMTP deletes the copy of the email from the working folder and delivers the original message to the MailMarshal Sender. Optionally, the service provider can enforce Global and Array level rules just before the final delivery to the Sender. For example, messages can be stamped with the Service Provider's name and support number. Upon final acceptance, the Sender delivers the message to the customer organization's email server for delivery.

If the message does trigger a rule, MailMarshal SMTP can quarantine the message, notify the recipient, and log the event. MailMarshal SMTP can also take additional actions such as to notify an administrator, strip attachments, classify the message for reporting, or conditionally deliver messages based on group membership. For example, a customer administrator can configure rules to deliver email with image file attachments to the Marketing group but not to the Help desk group.

MARSHAL™
Secure. Protect. Comply.

Outbound Email Flow

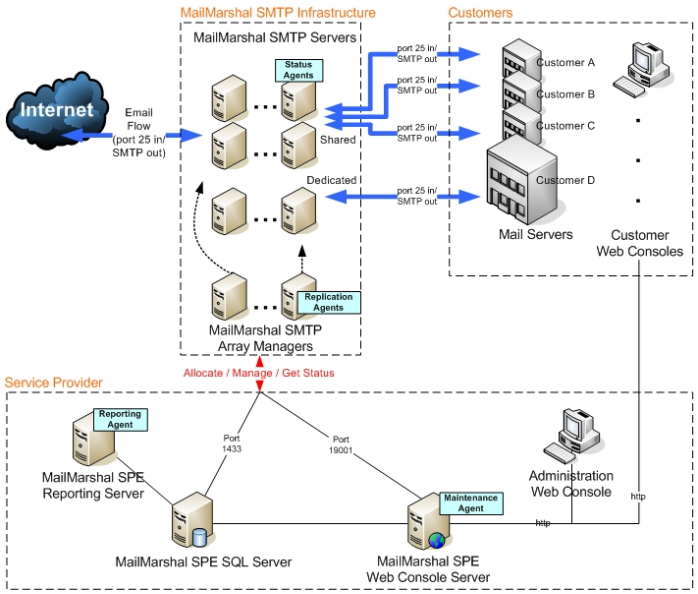
MailMarshal SPE handles outbound email flow in a similar way to inbound email flow. An organization's internal email server sends email to the service provider's email infrastructure. Messages are routed to a designated array of MailMarshal SMTP Servers for processing. The MailMarshal Receiver inspects each message, and then places a copy of the email in a working folder. The MailMarshal Engine splits the email into the header, message body, and any attachments to analyze using the outbound rules. If the email components pass all rules (including those from the Service Provider at Global and Array levels), the MailMarshal Sender queues or forwards the message for delivery. If the email triggers a rule, MailMarshal SPE processes the email as specified by the rule action.

MailMarshal SPE Architecture

The architecture of MailMarshal SPE is summarized in the figure below. MailMarshal SMTP Servers can be installed on a number of computers to create one or more arrays of email processing servers in a Demilitarized Zone (DMZ). The MailMarshal SMTP servers will receive inbound email on port 25, process it, and forward it for delivery to the customer mail servers. Similarly for outbound SMTP traffic, MailMarshal SMTP servers will process all outgoing emails from the customers.

An array of MailMarshal SMTP email processing servers can be used to process email for several small to medium-sized organizations. The assignment of arrays to customers is performed from Administration Web Console. You can add more email processing power for large enterprises by dedicating a whole array of email processing servers to a single customer.

To cater for larger and increasing email volumes, the underlying MailMarshal SMTP Array/Server infrastructure provides a broad range of enterprise configurations that can include redundancy and failover support over. For more information about MailMarshal arrays, please refer to "Array Installation" in the *MailMarshal User Guide*.



Note: For any infrastructure configuration, it is essential to install Replication Agent and Status Agent on each Array Manager and SMTP Server respectively.

To cater for increased numbers of customers, MailMarshal SPE is designed to scale up and out, by supporting both multi-processor and multi machine configurations. MailMarshal SPE is also designed to work with geographically separated servers.

MARSHAL™
Secure. Protect. Comply.

The Service Provider aspects to consider for scalability are:

- MailMarshal SPE Web Console Server
- MailMarshal SPE SQL Server
- MailMarshal SPE Reporting Server

The **MailMarshal SPE Web Console Server** hosts the Administration Web Console and the Customer Web Console thin clients using Microsoft IIS Web server(s). To handle increasing HTTP requests, you can install load balancing software to manage peak traffic to the website.

The **MailMarshal SPE SQL Server** stores data and configuration information for MailMarshal SPE This SQL Server supports use of a number of cluster techniques offered by Microsoft SQL Server: High Availability, Load-balancing, and High performance clusters.

The **MailMarshal SPE Reporting Server** gathers data from MailMarshal SPE SQL Server, and performs data processing. The install location of the Reporting Server does not affect email processing performance, but it can affect the performance of the MailMarshal SPE SQL Server. For best results, install Report Servers in one of the following locations, depending on your preference:

- To consolidate CPU processing resource, install Reporting Server on the same server as the MailMarshal SPE Web Console Server. Since Reporting Server performs scheduled reports and emailing operations in bursts, installing the Reporting Server on the computer that hosts Microsoft IIS results in saving of unused processing resources.
- To allow efficient interaction between the database and reporting, install Reporting Server on the same server as the SQL database server for direct communication. Ensure this server has the capacity to run these two services.
- For portability, install Reporting Server on another computer in the network close to the computer hosting the database. Ensure that these servers have a high-speed network connection.

Recommended Software Configuration

The following table indicates which components can share servers in production environments:-

Server Role	Shared Server	Dedicated Server
SQL Server	✗	✓
Web Console (IIS Server)	✓	✓
Reporting Server	✓	✓
Array Manager	✓	✓
SMTP Email Processing Server	✓	✓

MailMarshal SPE with one server

It is possible to install all of the components of MailMarshal SPE on a single server. This scenario is not recommended for a production environment, but it can be done to test or demonstrate an installation.

MailMarshal SPE with two servers

The table below shows the recommended installation using two servers:

Server Role	Server 1	Server 2
SQL Server	✓	

Server Role	Server 1	Server 2
Web Console (IIS Server)		✓
Reporting Server	✓	
Array Manager		✓
SMTP Email Processing Server		✓

MailMarshal SPE with three servers

The table below shows the recommended installation using three servers:

Server Role	Server 1	Server 2	Server 3
SQL Server	✓		
Web Console (IIS Server)		✓	
Reporting Server		✓	
Array Manager			✓
SMTP Email Processing Server			✓

MailMarshal SPE with four servers

The table below shows the recommended installation using four servers:

Server Role	Server 1	Server 2	Server 3	Server 4
SQL Server	✓			
Web Console (IIS Server)		✓		
Reporting Server		✓		
Array Manager			✓	
SMTP Email Processing Server				✓

MARSHAL™
Secure. Protect. Comply.

Advanced Administration Features

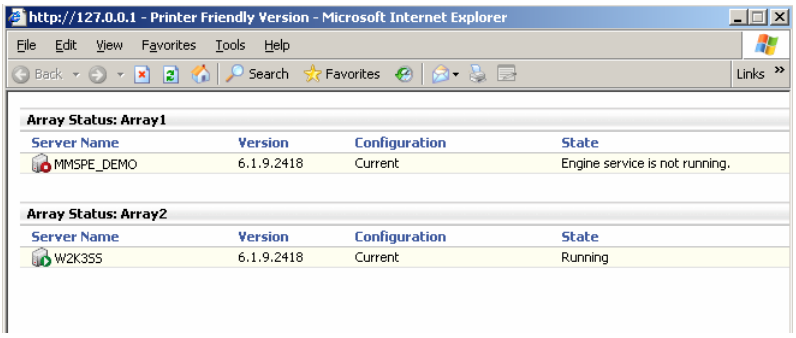
The MailMarshal SPE Console provides a number of features that allow Service Provider and Customer administrators to easily monitor, review and report on MailMarshal activity.

Availability & Monitoring

For monitoring, MailMarshal SPE allows an MSP administrator to view the current status by Array, Server and individual agent on those servers.

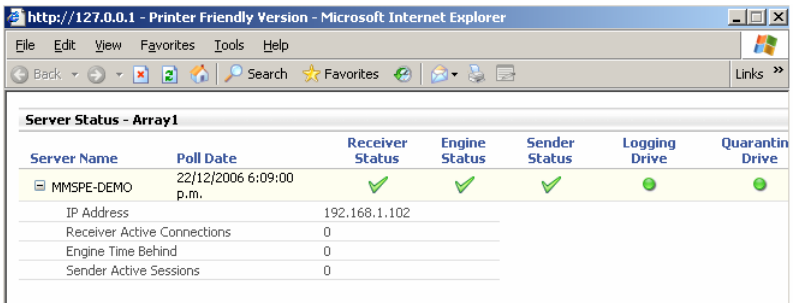
Examples of these status views:-

Array Status



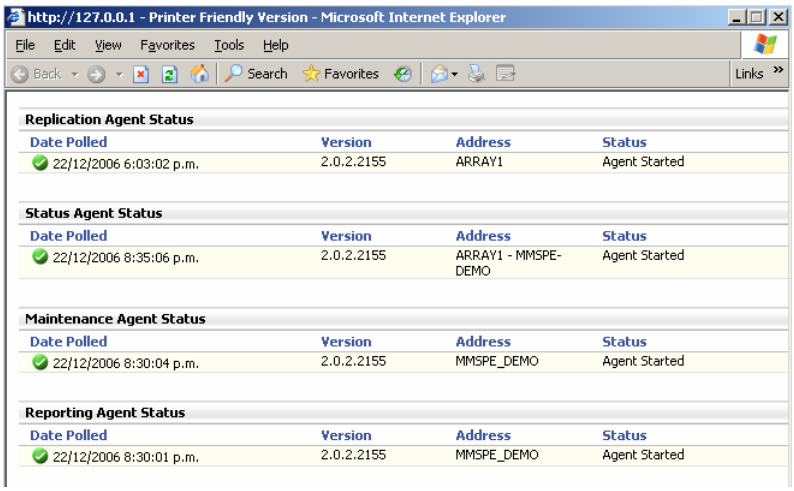
Here we can see the presence of two arrays in our example configuration, and the status screen is advising that the 'engine' service is not running on one of the servers in Array 1, Array 2 is functioning correctly.

Server Status



Here we can see the individual service status on one MailMarshal SMTP server and also the current status of the logging drive space and the quarantine drive space.

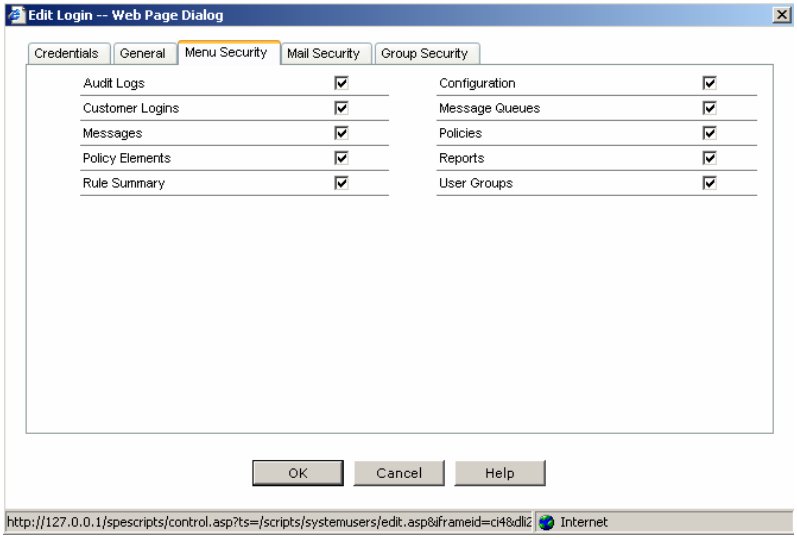
Agent Status



In the Agent Status screen we can see the current state of each agent that makes up MailMarshal SPE, the Status agent polls each of the other agents periodically and is polled itself for status.

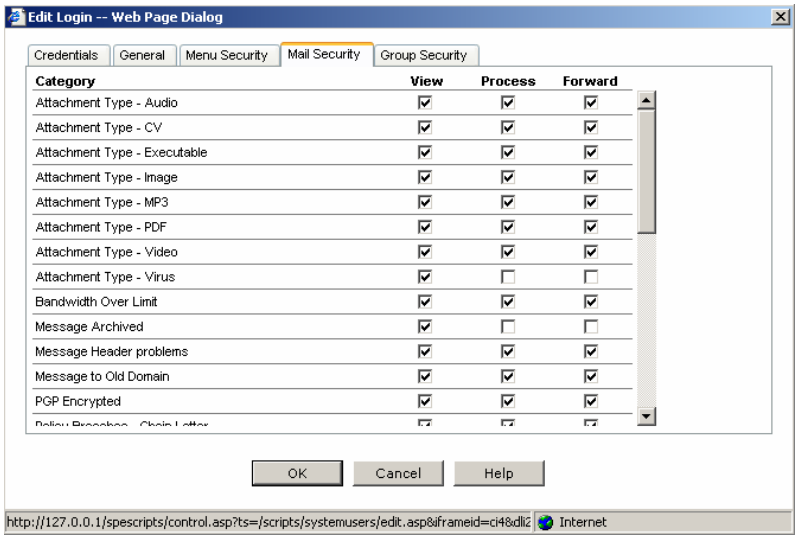
Administration Delegation

The administrator can also delegate access for other users to specific Console functions or specific quarantine folders in either the MSP console or the customer console shown in the example below:-



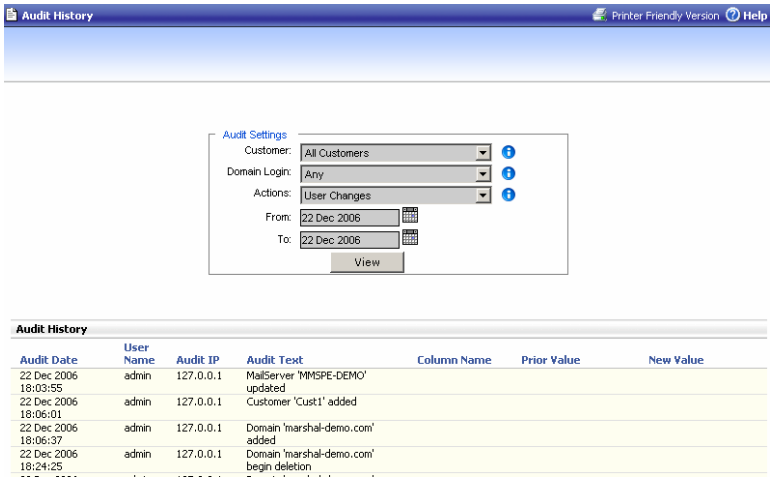
This allows a MSP to define multiple administrators for the MSP console and support slightly different roles and tasks with those logins, any user can be setup as read only or full rights access in addition to the more detailed options as shown above.

Within the customer web console, an administrator can also define what types of quarantined email another user may or may not access based on how that email was categorized as shown below:-



Auditing

Auditing is a vital part of any complex installation; MailMarshal SPE offers full auditing through both the MSP and customer web consoles. Any action undertaken in either of the tools is saved to the audit log, which can then be queried and displayed as per the example below:-



Reporting

For reporting, the reports available to service administrators are more extensive than the reports available for customers. Depending on the type of login used, you will see reports appropriate to that login within the web console. There are several report types available for either role (customer or service administrator), any of which can be scheduled for automatic generation, and or forwarded to an email account.

MailMarshal SPE is pre-configured with 9 different report types. For reports on individual users, you have the ability to drill down right to the actual message logs.

MARSHAL™
Secure. Protect. Comply.

Report options

You can customize the reports by changing a number of relevant options for each report, the full list of these options is:-

Direction

Choose Inbound or Outbound. Note you need to have configured your mail server to send outbound mail through MailMarshal before you can report on outbound mail.

Period

Choose a predefined period or custom period from the drop down box. If you select Custom Period, choose the From and To periods.

Format

Certain reports are available in both text and graphic. Choose the report type from the drop down box.

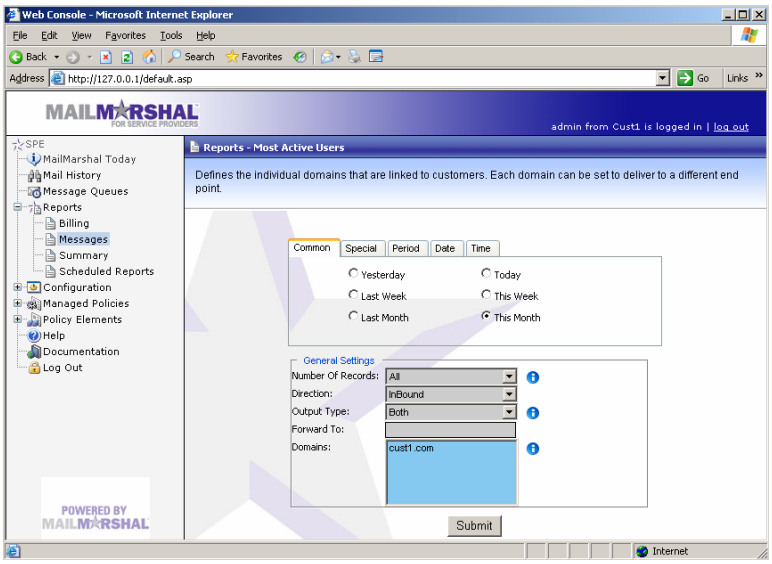
Number of Records

Certain reports may return a large number of records. To limit the load on the server, the default number of records that a report on users will return is 50. To increase this amount, select the maximum number of users you wish to return from the drop down box.

Forward To

If you wish to receive a copy of the report via email, or send a copy to someone else, you can fill in the recipient's email address in this field.

The screen where these options are set will be similar to the example below, this example is from the Customer web console and the 'Most Active Users' report:-



MARSHAL™
Secure. Protect. Comply.

MSP reports

The MSP is able to run reports across the entire infrastructure or drill down to a particular server or customer depending on the report.

The full list of reports available to the MSP is:-

- System
  - Arrays reload History
  - Configuration Checker
  - Customer Configuration Checker
  - Customers due to expire
  - Domain Status
  - Expired Customers
  - Growth reports
  - Service Levels
- Configuration
  - Customer Checker
  - Suspect Rules
- Billing
  - Billing by Message
  - Billing Configured

Customer Reports

A customer access their reports through the standard customer console, they can generate reports that only show their data and statistics even though they maybe sharing infrastructure with other customers at the MSP.

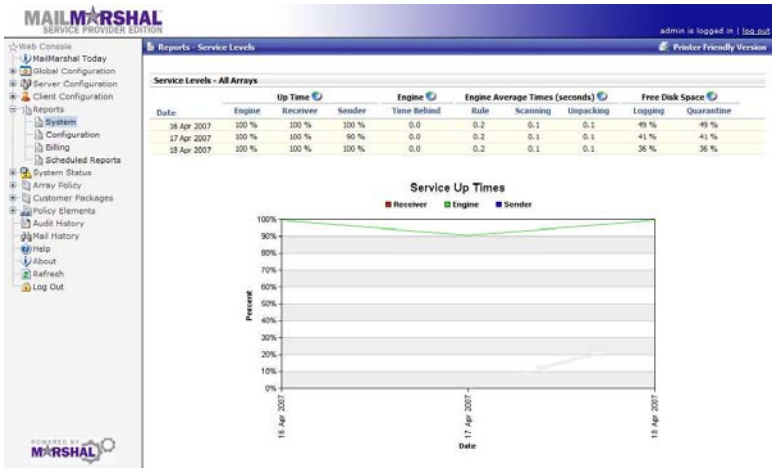
The full list of reports available to the customer is:-

- Billing
  - Billing
  - Estimated Bandwidth Savings
- Messages
  - Domain Sending Top Category Items to Organization
  - Messages Blocked by Category per User
  - Messages Blocked by Category Trend
  - Messages from Domain
  - Messages per Category Per user
  - Most active users
- Summary
  - Overall message Summary
  - Total Messages Received

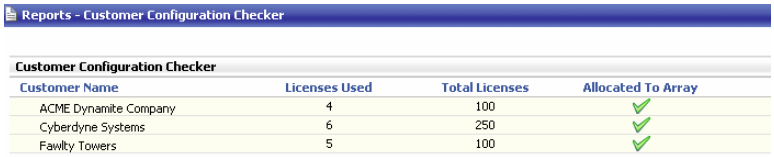
MARSHAL™
Secure. Protect. Comply.

Sample MSP Reports

Service Levels Report

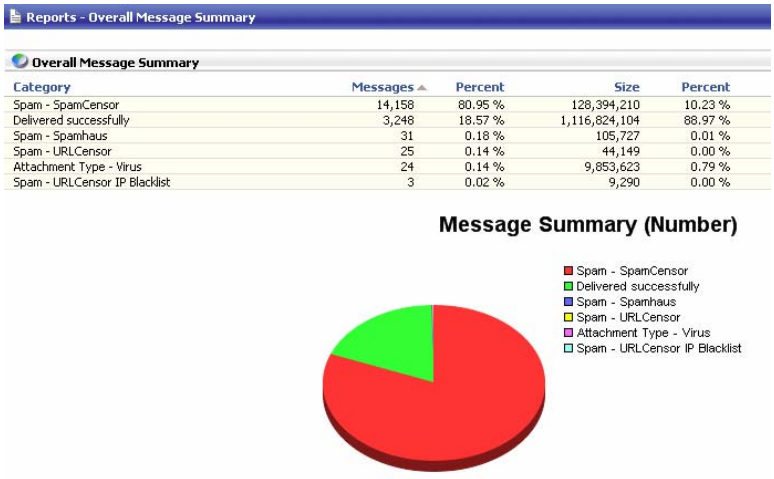


Customer Configuration Check



Sample Customer Reports

Overall Message Summary



MARSHAL™
Secure. Protect. Comply.

Marshal's Worldwide and EMEA HQ
Marshal Limited,
Renaissance 2200,
Basing View,
Basingstoke,
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Email:emea.sales@marshal.com

Americas
Marshal Inc.
5909 Peachtree Dunwoody Road NE,
Suite 770,
Atlanta,
GA 30328
USA

Phone: +1 404 564-5800
Fax +1 404 564-5801

Email: americas.sales@marshal.com

Asia-Pacific
Marshal Software (NZ) Ltd
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Greenlane, Auckland
New Zealand

Phone: +64 9 984 5700
Fax: +64 9 984 5720

Email: apac.sales@marshal.com

info@marshal.com | www.marshal.com