

# Feature Brief



## Managing Email using SMTP and POP3

### **Clavister SSP™ Security Services Platform**

firewall • VPN termination • intrusion prevention • anti-virus  
anti-spam • content filtering • traffic shaping • authentication

# **CLAVISTER®**

**Protecting Values**

## Introduction

Clavister Security Services Platform (SSP™) is our proven, feature-rich, service-oriented framework for providing best-in-class security solutions. Clavister SSP™ consists of **Clavister Network Security Elements**, **Clavister Lifecycle Systems**, and **Clavister Lifecycle Services**. Clavister SSP™ combines precise control, fine-granular administration, and seamless scalability making it easy to provision the perfect solution for any customer; be it a small organization, a large Internet Service Provider, a Managed Security Service Provider, or a multimedia-ready telecommunication operator.

### Clavister Network Security Elements

These are the physical building blocks that you install in your network. Clavister SSP™ currently offers two network security elements; Clavister Security Gateway Series and Clavister Secure Access Gateway. The Clavister Security Gateway is available both as a pre-packaged turnkey appliance solution for fast and easy deployment or as a distributed software-only solution for your preferred hardware platform. The Clavister Secure Access Gateway Series is available as a pre-package turnkey appliance solution only and offers SSL VPN, Single Sign-On (SSO) and multi-factor authentication (MFA).

### Clavister Lifecycle Systems

The Clavister Lifecycle Systems is a set of software components enabling true network security management throughout the entire lifecycle, including deployment, monitoring and reporting, configuration and integration, as well as analysis, optimization and troubleshooting. Clavister FineTune™ and the Web-based administration user interface enable you to manage a large set of Clavister Network Security Elements. Clavister InSight™ is our premium Security Event and Information Management (SEIM) system, which does not only support Clavister security network elements, but also a majority of other network devices. By correlating data from all network elements, you get a complete log of all activities in your network. Clavister PinPoint™ completes the Clavister Lifecycle Systems suite with accurate and precise real-time information packaged in a convenient dashboard-style application.

### Clavister Lifecycle Services

The Clavister Lifecycle Services empowers you and your products with tools, services, and resources that help maximize benefits and eliminate problems, including planning, deployment, optimization, operations and maintenance. The Clavister Lifecycle Services include the Clavister Service Provisioning Network (CSPN) for automated signature updates, the Clavister xPansion Lines™ license upgrade framework and Clavister's award-winning Technical Support.

The Clavister SSP™ service-oriented framework provides you with a secure environment for your business; either as a service provided to you by a Managed Security Service Provider (MSSP) or as systems and services integrated in your own network.

For more information about Clavister products and services, please visit us at: [www.clavister.com](http://www.clavister.com).

## Overview

Today email is ubiquitously. Email is used by everybody; from the busy corporate executive to grandmothers. People rely on email in almost all types of communication; be it corporate information, soccer practice schedules, birthday cards or any type of information. We expect that emails are free from viruses and that they do not contain spam or unsolicited information.

Unfortunately, we are all faced with an avalanche of unsolicited spam emails, virus and other malicious content. Wall Street Journal (WSJ) quoted in August 2003 analysis group Radicati Group, Palo Alto, CA which stated that "Spam accounts for 45% of all emails, or 15 billion messages every day, and costs business world-wide a total of \$20 billion a year in lost productivity and technology expenses. The firm predicts the number of daily spams will rise to more than 50 billion by 2007, and costs will reach almost \$200 billion per year." Kaspersky Lab continues to report on rising threats and malware.

Clavister Security Gateway supports both Simple Mail Transfer Protocol (SMTP) and Post Office Protocol, version 3 (POP3), and protocol have support for anti-virus scanning. In addition, the SMTP protocol also supports anti-spam filtering using DNS Blacklisting (DNSBL).

For more information on anti-spam, see **Feature Brief: Clavister Anti-Spam**. For more information on anti-virus, see **Feature Brief: Clavister Anti-Virus**.

## SMTP Application Layer Gateway

Simple Mail Transfer Protocol (SMTP) is a text-based protocol used for transferring email between mail servers over the internet. Typically the local SMTP server will be located on a Demilitarized Zone (DMZ) so that email sent by remote SMTP servers will traverse the Clavister Security Gateway to reach the local server. Local users will then use email client software to retrieve their email from the local SMTP server.

Clavister Security Gateway supports SMTP with a number of key features, including anti-virus scanning. The following text will highlight some of these features and give some detailed explanations on how to use them.

### SMTP ALG Options

The SMTP ALG comes with several options allowing you to configure it for both security, as well as easy maintenance. Table 1 below outlines the main set of options for the SMTP ALG.

PARAMETER	DESCRIPTION
Rate Limiting	This option specifies the maximum number of allowed email messages received per minute from a unique SMTP server. The default value is 0 (or empty), which means that there is no rate limiting. Maximum value is 65 535. Exceeding the maximum number will cause a: 451 Requested action aborted. Maximum email per host per minute is reached message and the email will not be delivered.
Verify Sender Email	This option specifies that the source address in the SMTP protocol header and the SMTP data load header must be the same. Spamming programs can cause the headers to be different.
Email Address Blacklisting	Specifying a blacklist of email addresses will block mail from these addresses. You can specify whether the address is a recipient address or a sender address. It is also possible to use wildcard characters in the email address, for example *@company.*, which will block mails from the domain company regardless if it is from a .com domain or a .eu domain.
Email Address Whitelisting	Specifying a whitelist of email addresses will allow mail from these addresses. You can specify whether the address is a recipient address or a sender address. It is also possible to use wildcard characters in the email address, for example *@company.*, which will allow mails from the domain company regardless if it is from a .com domain or a .eu domain.

Table 1: SMTP ALG Options

## POP3 Application Layer Gateway

In computing, local email clients use the Post Office Protocol version 3 (POP3), an application-layer Internet standard protocol, to retrieve email from a remote server over a TCP/IP connection. Many subscribers to individual Internet service provider email accounts access their email with client software that uses POP3.

POP3 is a mail transfer protocol that differs from SMTP in that the transfer of mail is directly from a server to a user's client software. Clavister Security Gateway supports POP3 with a number of key features, including anti-virus scanning. The following text will highlight some of these features and give some detailed explanations on how to use them.

## POP3 ALG Options

The POP3 ALG comes with several options allowing you to configure it for both security, as well as easy maintenance. Table 2 below outlines the main set of options for the POP3 ALG.

PARAMETER	DESCRIPTION
Allow Unknown Commands	Non-standard POP3 commands not recognized by the ALG can be allowed or disallowed.
Block USER and PASS Commands	Block connections between client and server that send the username/password combination as clear text. Note that some servers may only support this method.
Hide Username	This option prevents the POP3 server from revealing that a username does not exist. This prevents users from trying different usernames until they find a valid one.

Table 2: POP3 ALG Options

## Common Options

There are a number of parameters that pertain both to the SMTP ALG and the POP3 ALG. The following section details these parameters.

### File Integrity Options

Table 3 below outlines the file integrity options for the SMTP ALG and the POP3 ALG.

PARAMETER	DESCRIPTION
Fail Mode	This option specifies how the SMTP ALG and POP3 ALG should react when file integrity or content scanning fails. Available options are to either <b>Deny</b> the scanned file or <b>Allow</b> the scanned file.
Verify MIME Type	Email attachment file content can be checked against its file type. This prevents someone to rename the file extension to something else which does not correspond to the file content. For example, if Word-documents (.doc) are blocked and ZIP archives (.zip) are allowed. If someone would rename a file called <code>safe.doc</code> to <code>safe.zip</code> to allow it through, the verification would detect that it is in fact a Word-document and block it.
Allow/Block File Type	This option allows you to select which file types you want to allow or block. Clavister Security Gateway supports a large list of file types and it is even possible to add your own file type. For information on supported file types, see Clavister CorePlus™ Administration Guide.

Table 3: File Integrity Options

### Anti-Virus Options

Table 4 below outlines the anti-virus options for the SMTP ALG and POP3 ALG.

PARAMETER	DESCRIPTION
Anti-Virus Scanning	The anti-virus module can scan email attachments searching for malicious code. The available options are <b>Disabled</b> which disable the anti-virus scanning, <b>Audit</b> which allows attachments but logs it and <b>Enabled</b> which enables anti-virus scanning.
Scan Exclusion Control	This option allows you to exclude certain file types from scanning. Clavister Security Gateway supports a large list of file types and it is even possible to add your own file type. For information on supported file types, see Clavister CorePlus™ Administration Guide.

PARAMETER	DESCRIPTION
Compression Ration	This option allows you to specify the ration between a file in its compressed state and its uncompressed state. If the file reaches the specified number in its uncompressed state, the action in Compression Action will take place.
Compression Action	This option specifies which action to take if the Compression Ratio is exceeded. Available options are <b>Allow</b> which allows the file to go through without virus scanning, <b>Scan</b> which scans the file for virus and <b>Drop</b> which drops the file without scanning. In either case, the event is logged.

Table 4: Anti-Virus Options

## Conclusion

This Feature Brief describes how to use SMTP Application Layer Gateway (ALG) and POP3 Application Layer Gateway (ALG) to manage your email and how to use it with your Clavister SSP™ installation. Below are some key customer benefits:

### Clavister SSP™ Key Benefits

- **Robust Security**  
The purpose-built security offering from Clavister provides a complete set of security features, including Stateful Packet Inspection (SPI) firewall with DoS and DDoS protection, VPN with strong encryption, and User Authentication.
- **Rapid Deployment**  
The Clavister Security Gateway provides effortless and rapid deployment. A trained technician can easily deploy and configure new network security elements within minutes, even across continents.
- **Flexible Traffic Control**  
The highly sophisticated bandwidth management capabilities in the Clavister Security Gateway make it possible to not only guarantee bandwidth for business critical applications or server, but also to optimize the entire traffic flow in your network and avoid inefficient bandwidth usage.
- **Lowered Costs for Administration**  
The powerful administration system that comes with Clavister Security Gateway enables organizations to lower the costs for administration through centralized management. The administration system makes it possible to deploy and configure all devices across the network, no matter if they are located next door or across the globe.
- **High Performance**  
Scalable performance with unsurpassed maximum bandwidth, concurrent connections and simultaneous VPN tunnels makes the Clavister Security Gateway the ideal choice even in the most demanding environments like Internet Service Provider Networks, Data Centers, and telecom operators.
- **Low Total Cost of Ownership (TCO)**  
Clavister's goal is to provide complete security solutions more cost efficiently than any competitor. Clavister SSP™ with its unique combination of integrated features, world-class service and support, and powerful administration system provide the lowest TCO and the best price/performance ratio possible.

### SMTP Key Benefits

- The Rate Limiting feature offers a level of defense against email flooding from a single SMTP server
- The Verify Sender Email feature helps protect against spam attacks
- The Email Blacklisting feature allows you to blacklist known offenders whereas the Email Whitelisting feature enables you to specify trusted sources for email
- The Verify MIME Types feature protects against malicious attachments being masquerade as something else
- The support for anti-spam filtering protects against spam using DNS Blacklisting, which lets you select among both free and commercial spam list servers
- The built in anti-virus scanning stops viruses from reaching your network

## POP3 Key Benefits

- The Block USER and PASS commands feature protects you from inadvertently sending username and password in clear text
- The Hide Username feature prevents the POP3 server from reveal that a username do not exist, which could be used to elicit an existing username
- The Verify MIME Types option protects against malicious attachments being masquerade as something else
- The built in anti-virus scanning stops viruses from reaching your network

## Feedback

Clavister Product Marketing is always interested in feedback from our readers. Please direct suggestions, comments or questions regarding this document to [product-marketing@clavister.com](mailto:product-marketing@clavister.com). Please include the title of the document in your email.

---

### About Clavister

Clavister - a Swedish privately owned company developing IT security products, including its award-winning Clavister Security Services Platform (SSP™). This service-oriented framework enables organizations to monitor network traffic, protecting critical business assets and blocking undesirable surfing. It will also protect you against intrusion, viruses, worms, Trojans, and overload attacks. It requires minimal servicing, with central administration, and has exceptionally flexible configuration possibilities. Its seamless scalability makes it easy to provision the perfect solution for any customer; be it small organizations, large Internet Service Providers, Managed Security Service Providers, or multimedia-ready telecom operators.

Clavister was founded 1997 in Sweden, with R&D and headquarters based in Örnköldsvik and Sales and Marketing based in Stockholm. Its solutions are marketed and sold through International sales offices, distributors, and resellers throughout EMEA and Asia. Clavister also offers its technology to OEM manufacturers.

For more information, please visit us at [www.clavister.com](http://www.clavister.com).

---

### Limitation of Responsibilities

The information in this document represents the current view of Clavister AB on the issues discussed as of the date of publication. Because Clavister must respond to changing conditions, it should not be considered to be a commitment for Clavister, and Clavister cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only. CLAVISTER MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the written permission of Clavister. Clavister may have trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Clavister, the furnishing of this document does not give you any license to these trademarks, copyrights, or other intellectual property.

Part Number: `clavister-fbr-manageing_email_using_smtp_and_pop3` (0801)