SecurityGateway

SecurityGateway 8.5 - New Features

SecurityGateway for Email Servers protects businesses from inbound and outbound threats, while also helping them adhere to the latest data security and compliance regulations. This feature brief highlights various key new features. A comprehensive list of all new features and enhancements can be found in the [SecurityGateway Release Notes](#).

Note: *32-bit builds and support for 32-bit operating systems has been discontinued. Starting with SecurityGateway 8.5.0 only 64-bit builds will be distributed. This allows for us to streamline development and testing and utilize libraries that are only available as 64-bit. If you are currently running a 32-bit build on a supported 64-bit operating system, you can simply download the 64-bit build and install on top of the existing installation.*

Secure Messaging Web Portal

With the new Secure Messaging portal, administrators can create content filter rules, data leak prevention rules, and sieve scripts to scan email messages for sensitive content. These messages are stored on the SecurityGateway server, and can be viewed by the recipient over an encrypted connection via the new Secure Messaging web portal. Secure message recipients may also optionally compose new secure messages to a pre-defined list of local users.

[Figure 1-1]

Microsoft (Office) 365 Integration App

SecurityGateway's new Office 365 app allows users to mark email messages as spam or non-spam from within Office 365.

[Figure 1-2]

Advanced Malware Detection Engine

Threat actors use a variety of packing and obfuscation techniques to make it easier for malicious files to evade detection and bypass network defenses to infect an organization. To help protect businesses from these threats, SecurityGateway now includes Cyren's Advanced Malware Detection Engine.

Cyren's Advanced Malware Detection Engine can quickly break a large file down into its smallest components and scan them individually for malicious components. This allows you to proactively detect new malware as well as other threats such as scripts inside a PDF, macros inside Microsoft Office documents, and files within a Zip attachment.
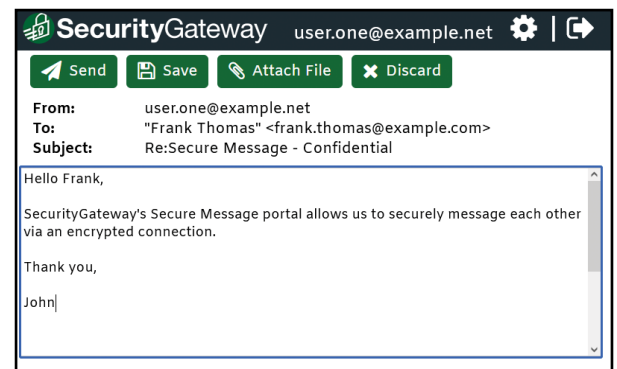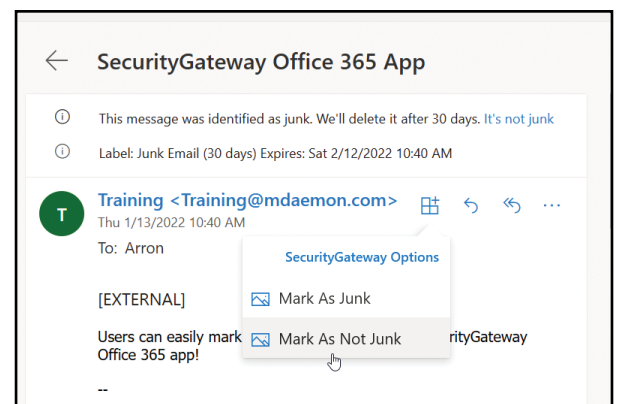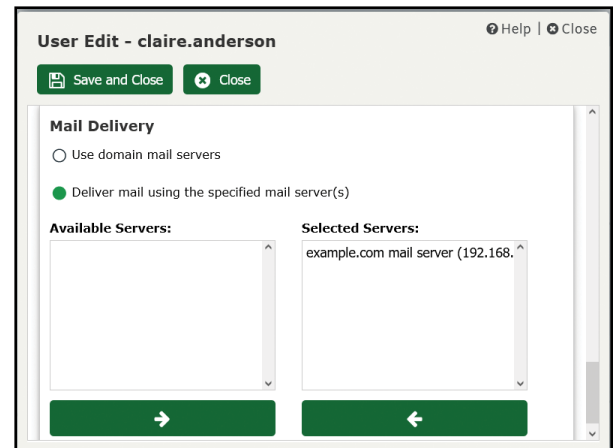

Figure 1-1

Figure 1-2

Hybrid Network User Mail Routing

User-based mail routing allows Securitygateway to be deployed in a hybrid environment where email can be routed to specific mail servers or cloud mail services on a per-user basis. This is useful for environments in which email for some of a domain's users is hosted on cloud services while email for other users is hosted on on-premise mail servers.
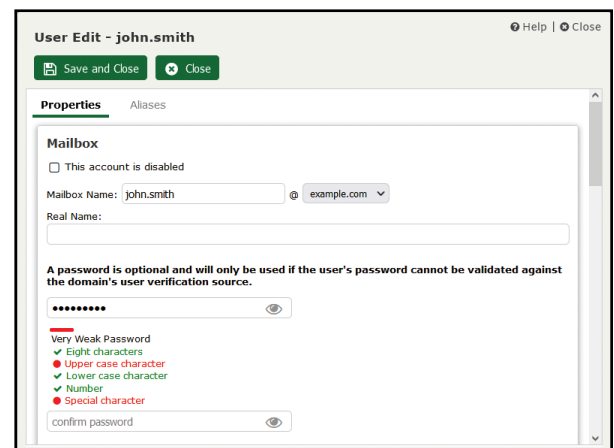
[Figure 2-1]

Password Policy Strength Meter

A password strength meter has been added to help encourage use of stronger passwords when adding or modifying user accounts.

[Figure 2-2]

Performance Counters

Performance counters have been added to make it easier for administrators to monitor SecurityGateway using third-party tools.

Other Improvements for SecurityGateway 8.5

- Recipient whitelists have been added for attachment filtering. A list of recipient addresses may be defined to bypass filtering for both attachment blocking and quarantining.

- An option to require strong passwords has been added to the Setup/ Users | Accounts | User Options configuration screen. This feature can be disabled per user.

For a complete list of new features & updates, please see the SecurityGateway Release Notes.

2-1

2-2