Migrating from GFI MailEssentials to Security Gateway

This guide provides instructions for migrating to SecurityG ateway from GFI MailEssentials.

Deployment Considerations

Before migrating from any on-premise email gateway product to Security Gateway, determine whether Security Gateway will be installed on the current email gateway server or on a new/separate server. When installing on a separate server, DNS records will need to be updated to reflect the host name and IP address of the new server. Please allow up to 24 hours for DNS records to propagate. During this time, email will continue to flow to GFI MailEssentials.

When installing on the same server, no DNS record changes are needed, but GFI will need to be shut down before launching Security Gateway to avoid port conflicts. Downtime should not exceed five minutes.

Migration Overview

The following steps are based on the assumption that Security Gateway has already been installed. Please refer to the Security Gateway installation Guide for initial setup of Security Gateway.

Migrating from GFI MailEssentials to Security Gateway involves the following tasks.

1. Exporting whitelist & blacklist data from GFI into an XML file
2. Converting data from the exported XML file to CSV format
3. Importing the CSV file containing blacklist & whitelist data into Security Gateway
4. DNS record updates (when installed on a separate server)

Note: Security Gateway can be configured to add users and domains automatically by querying Active Directory, MDaemon, or any other LDAP data source or mail server (using SMTP verification). Therefore, it is not necessary to export users and domains from GFI & import them into Security Gateway.

Note: Be sure to check for any quarantined messages in GFI MailEssentials and moderate them accordingly to remove them before migration.

Step 1: Export Whitelist & Blacklist Data from GFI MailEssentials

Follow these steps to export spam filter whitelist & blacklist entries from GFI MailEssentials.

1. Navigate to **Anti-Spam | Whitelist**
2. Click on the **Whitelist** tab
3. Click on the **Export** button to generate the XML file containing your whitelist entries
4. Enter a name for the file, and then click the **SAVE** button

To export blacklist entries, navigate to **Anti-Spam | Anti-Spam Filters | Email Blocklist**, and then follow steps 3 and 4 (above).

Step 2: Convert Exported Whitelists and Blacklists to CSV Format

Before importing whitelist and blacklist entries into Security Gateway, they will need to be converted to CSV format. Many tools for converting XML files to CSV are available online. All blacklist and whitelist entries for email addresses, domains, and IP addresses can be combined into a single CSV file. When imported into Security Gateway, they will appear on the appropriate screen based on the data type and associated content for each entry.

The following example can be used as a guide for proper formatting. Be sure to include quotation marks for all column labels.

“Domain”	"User"	"IP"	"Value"	"Type"	"Comments"
			exampt@example.com	WhiteListAddressGlobal	Whitelist address (global)
			spammer@abc.biz	BlackListAddressGlobal	Blacklisted address (global)
			host.example.com	WhiteListHostGlobal	Whitelist host (global)
		5.5.5.5		WhiteListIPGlobal	Whitelist IP address (global)
		1.1.1.1		BlackListIPGlobal	Blacklist IP (global)
example.com			bob@example.com	WhiteListAddressDomain	Whitelist address for domain example.com
example.com			spammer@abc.gov	BlackListAddressDomain	Blacklisted address for domain example.com
example.net			test3@example.com	WhiteListAddressDomain	Whitelist address for domain example.net
example.net			spammer@xyz.com	BlackListAddressDomain	Blacklisted address for domain example.net
	frank.thomas@example.com		john@example.org	WhiteListUser	Frank's colleague - whitelist.
	frank.thomas@example.com		spammer@example.com	BlackListUser	Frank's blacklisted email address
example.net			*@example.biz	WhiteListAddressDomain	Whitelist domain (using wildcard) for domain example.net

Step 3: Import Whitelist & Blacklist data into Security Gateway

Note: The following steps are performed after Security Gateway has been installed. For more information on installing Security Gateway, please refer to the Security Gateway Installation Guide.

To import a CSV file containing whitelist & blacklist entries into SecurityGateway:

1. Navigate to **Security | Whitelists | Addresses** [Figure 3-1]
2. Click on the **Import** button at the top (The Import button can also be found under the **Whitelists & Blacklists | Hosts & IP screens**). [Figure 3-1]
3. Click on **Browse,** navigate to the CSV file containing your whitelist and blacklist entries, and then click on **Open**
4. Click on **Import Lists**

A confirmation window indicating the number of items successfully imported will be displayed.

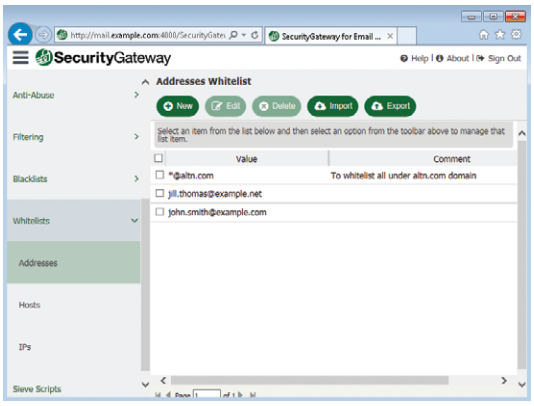

Figure 3-1

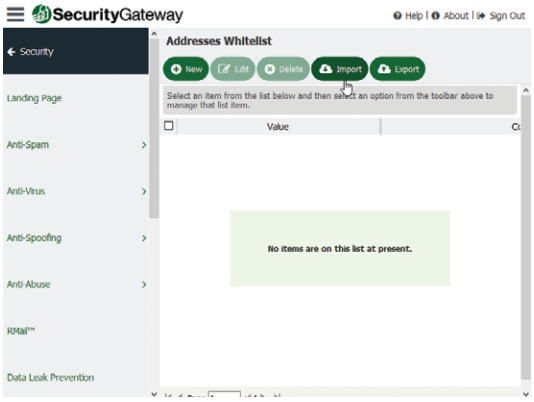

Figure 3-2

Note: When the CSV file is properly formatted, all entry types are imported into the appropriate whitelist/blacklist screen regardless of which screen is used to access the **Import** button.

Step 4 - Update DNS Records (when installed on a separate server)

After Security Gateway has been installed and all mail servers protected by Security Gateway have been specified (per steps outlined in the Security Gateway Installation Guide), the appropriate DNS records (A, MX, PTR, CNAME, DMARC, and others) will need to be updated to reflect any changes.

Note: *DNS record changes can take up to 24 hours to propagate. During this time, email will continue to pass through GFI until these updates have completed.*

Note: *Make sure the proper firewall ports are open between SecurityGateway and the mail server. A list of ports used by SecurityGateway can be found by navigating to* **Setup/Users | Mail Configuration | Email Protocol** *and* **Setup | System | HTTP Server**.

MDaemon® technologies