Email Security Best Practices
Settings to Protect Your Mail Server

The following are best practice recommendations to protect your business email with SecurityGateway.

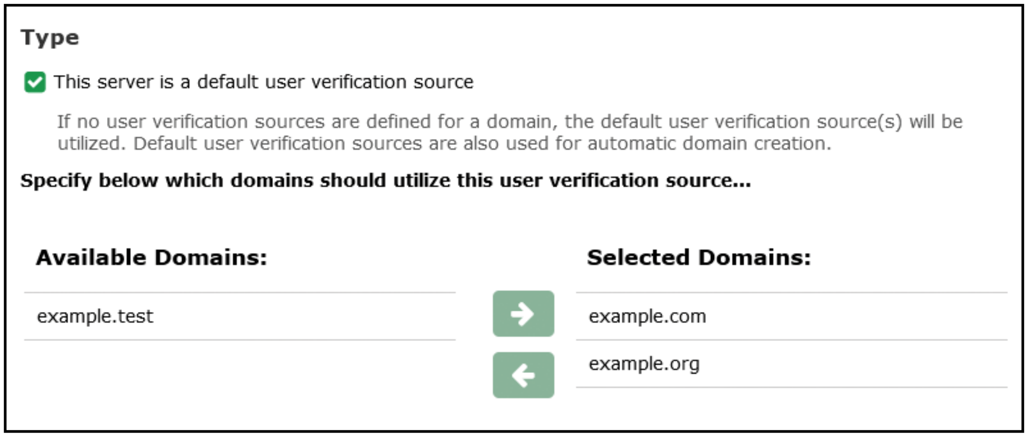
Verify That a User is Valid Before Creating an Account

Whenever an incoming message is addressed to an unknown local user, SecurityGateway will query the User Verification Sources configured for the user's domain to verify whether or not the unknown address is legitimate. If the address is valid then SecurityGateway will create a user account for that address and attempt to deliver the message to the domain's mail server. If the address is invalid then the message will be rejected.

We recommend using one of the five user verification sources in SecurityGateway (located under **Setup / Users | Accounts | User Verification Sources**) to verify the validity of a user before an account is created in SecurityGateway. Users can be verified via SMTP (call forward), Active Directory, Microsoft 365, MDaemon (using Minger), or LDAP. Instructions for setting up Microsoft 365 as a user verification source can be found here:
https://knowledge.mdaemon.com/securitygateway-setup-microsoft-365-user-verification-source

We also recommend having at least one default user verification source. If no user verification sources are defined for a domain, then the default user verification source will be used.

To designate a default user verification source, simply check the box **"This server is a default user verificaiton source"** on the **Edit User Verification Source** screen.



Type

☑ This server is a default user verification source

If no user verification sources are defined for a domain, the default user verification source(s) will be utilized. Default user verification sources are also used for automatic domain creation.

Specify below which domains should utilize this user verification source...

Available Domains:		Selected Domains:
example.test	→	example.com
	←	example.org

Use SMTP Authentication to Prevent Unauthorized Account Access

To help prevent unauthorized account access, we recommend requiring SMTP Authentication unless a message is transmitted from a domain mail server. This helps to ensure that the identity of users sending mail is valid.

In SecurityGateway, SMTP authentication can be configured by navigating to **Setup/Users | Mail Configuration | Domain Mail Servers**. Select your mail server, and then click **Edit**. Then, check the **"Requires SMTP authentication"** box and enter a valid username and password.

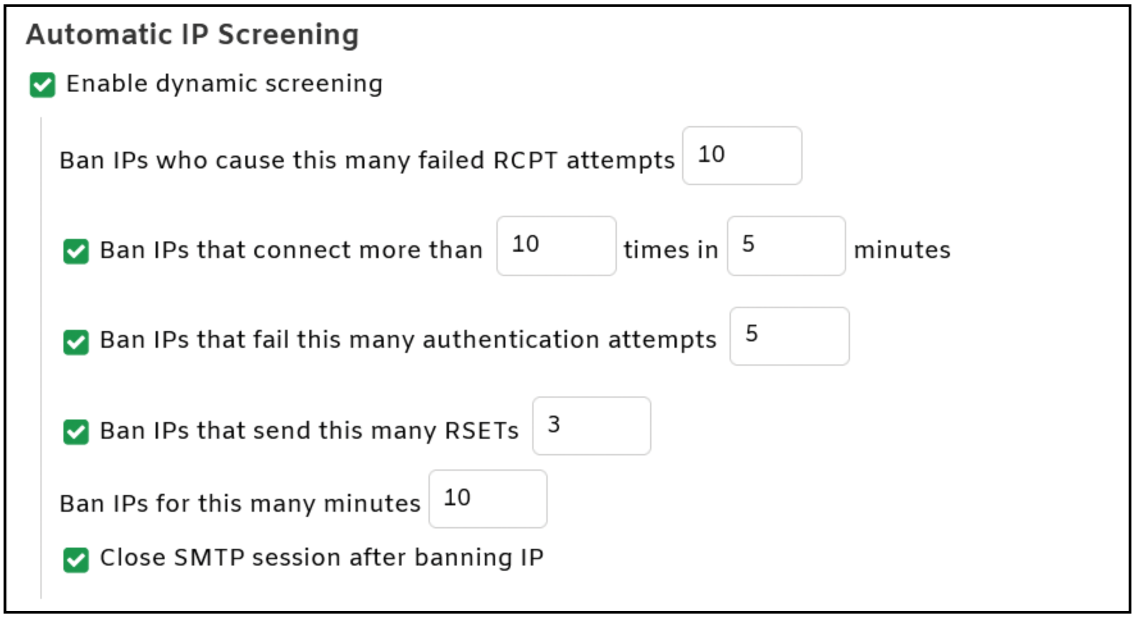
Use Strong Passwords

Spammers will often try to hijack an email account by guessing its password. Therefore, passwords that are easy to guess should always be avoided. If SecurityGateway is configured to create accounts automatically by querying a user verification source, then make sure your user verification source is configured to require strong passwords. Passwords can also be assigned to users manually via the Domains and Users menu.

Enable Dynamic Screening

Enable Dynamic Screening to block connections that exhibit suspicious activity, such as failing too many authentication attempts, connecting too many times in a given period of time, attempting to keep a connection open too long, or sending to too many invalid recipients. Dynamic Screening makes it more difficult for a malicious person to guess passwords by detecting the malicious activity and blocking the connection.

To configure Dynamic Screening settings in SecurityGateway, navigate to **Security | Anti-Abuse | Dynamic Screening**.



Automatic IP Screening

☑ Enable dynamic screening

Ban IPs who cause this many failed RCPT attempts 10

☑ Ban IPs that connect more than 10 times in 5 minutes

☑ Ban IPs that fail this many authentication attempts 5

☑ Ban IPs that send this many RSETs 3

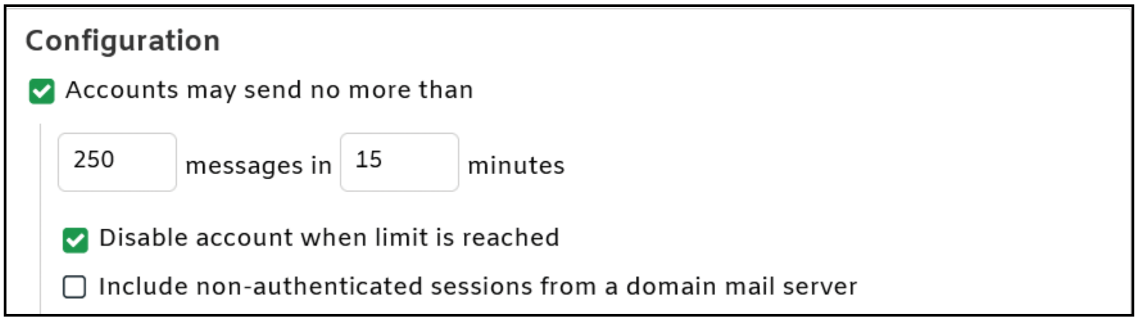
Ban IPs for this many minutes 10

☑ Close SMTP session after banning IP

Enable Account Hijack Detection

If a spammer guesses an account's password, he can then use that account to send out spam. To limit the spammer's ability to abuse a compromised account, enable Account Hijack Detection, and then enter the maximum number of messages that can be sent in a given time frame. Once the limit has been reached, the account is disabled and the administrator is notified.

To configure Account Hijack Detection settings in SecurityGateway, navigate to **Security | Anti-Abuse | Account Hijack Detection**.



Configuration

☑ Accounts may send no more than

250 messages in 15 minutes

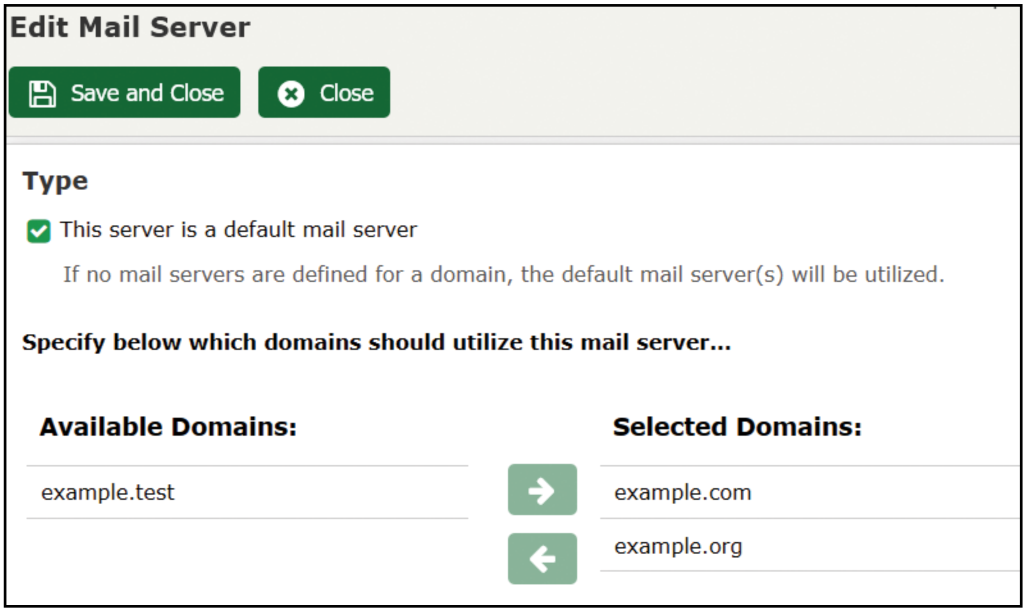
☑ Disable account when limit is reached

□ Include non-authenticated sessions from a domain mail server

Enable at Least One Default Mail Server

When email arrives for a domain that has not been assigned its own mail server, SecurityGateway needs to know where to send those messages. We recommend adding a default mail server for all SecurityGateway domains that have not had domain mail servers specifically associated with them.

To select a default mail server in SecurityGateway, navigate to **Setup / Users | Mail Configuration | Domain Mail Servers**. Select a mail server and click **Edit** (or double-click), and under the **Type** section, check the box **"This server is a default mail server."**



Edit Mail Server

Type

☑ This server is a default mail server

If no mail servers are defined for a domain, the default mail server(s) will be utilized.

Specify below which domains should utilize this mail server...

Available Domains:	Selected Domains:
example.test	example.com
	example.org

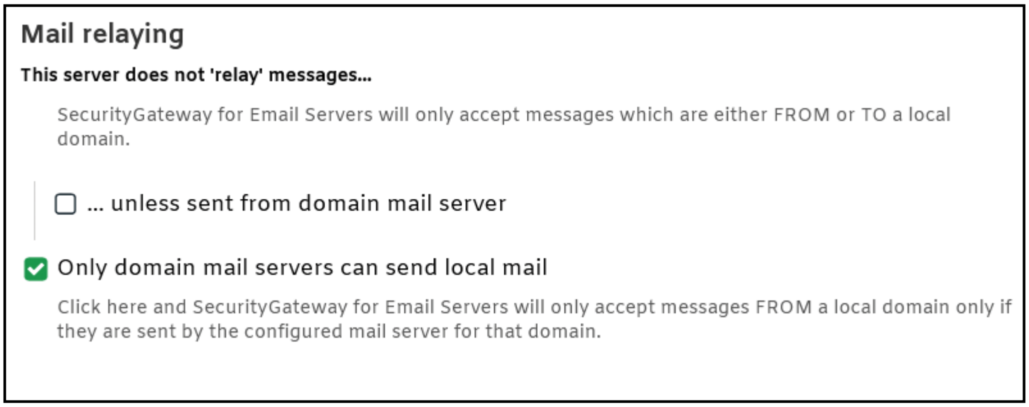
Prevent Unauthorized Mail Relaying

Relaying occurs when mail that is neither to nor from a local account is sent through your server. Servers that are not properly configured to prevent relaying can end up on a blocklist.

In SecurityGateway, relay control settings are located at **Security | Anti-Abuse | Relay Control**. By default, SecurityGateway does not allow mail relaying.

For optimal security, we recommend enabling only these settings:

- ✓ Only domain mail servers can send local mail (under the Mail Relaying section)
- ✓ SMTP MAIL address must exist if it uses a local domain (under the Account Verification section)



Mail relaying

This server does not 'relay' messages...

SecurityGateway for Email Servers will only accept messages which are either FROM or TO a local domain.

□ ... unless sent from domain mail server

☑ Only domain mail servers can send local mail

Click here and SecurityGateway for Email Servers will only accept messages FROM a local domain only if they are sent by the configured mail server for that domain.

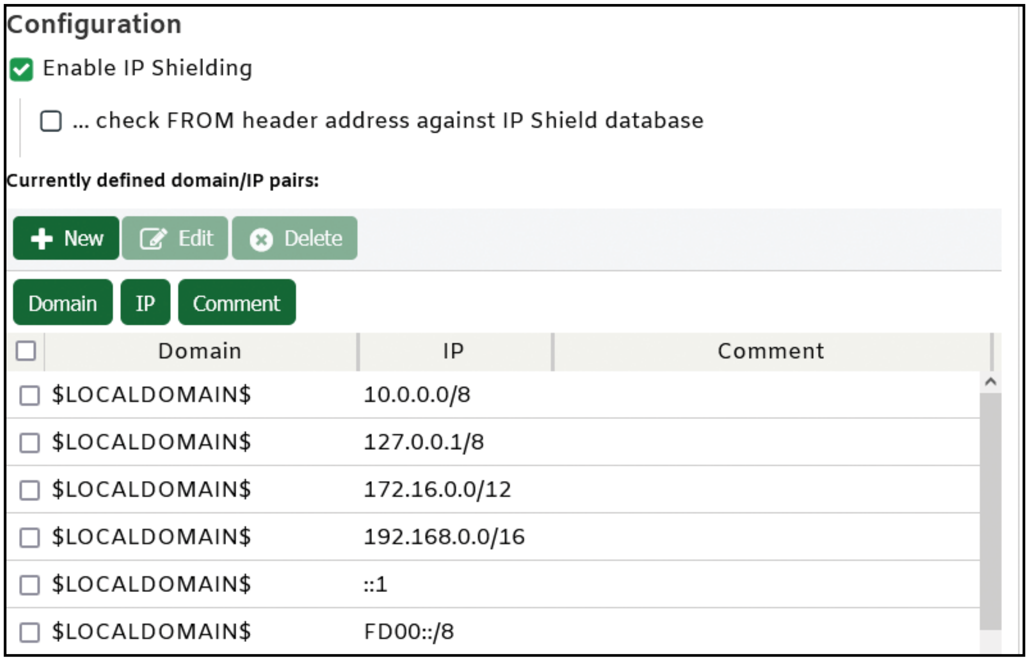
Note: *We do not recommend enabling any of the exceptions on this screen.*

Protect Your Domain with IP Shielding

IP Shielding is a security feature that only honors SMTP sessions claiming to be from someone at one of the listed domains if they are coming from an IP address associated with that domain.

The best way to secure outbound email is via SMTP authentication. However, for businesses that need to send email from a printer or other device that is not capable of authenticating, IP Shielding can be used to exclude certain IP's or ranges from having to authenticate. Messages from authenticated sessions can optionally be exempt from IP Shielding requirements.

IP Shield settings are located at **Security | Anti-Abuse | IP Shielding**



Configuration

☑ Enable IP Shielding

□ ... check FROM header address against IP Shield database

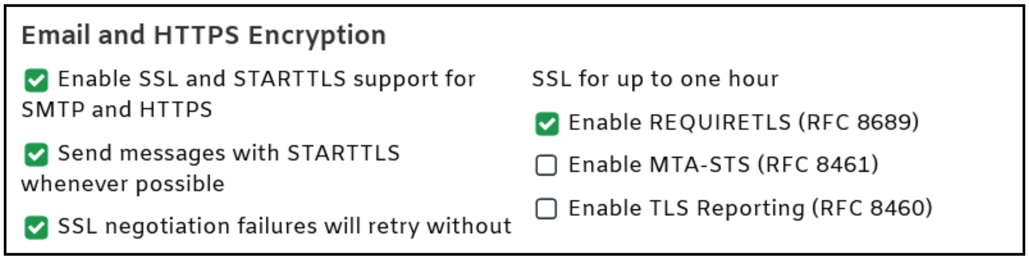
Currently defined domain/IP pairs:

□	Domain	IP	Comment
□	$LOCALDOMAIN$	10.0.0.0/8	
□	$LOCALDOMAIN$	127.0.0.1/8	
□	$LOCALDOMAIN$	172.16.0.0/12	
□	$LOCALDOMAIN$	192.168.0.0/16	
□	$LOCALDOMAIN$	::1	
□	$LOCALDOMAIN$	FD00::/8	

Enable TLS to Ensure Data Privacy

To protect the privacy of transmitted data, we recommend enabling the TLS encryption features for SMTP and HTTP.

SSL & TLS settings are located at **Setup / Users | System | Encryption**.



Email and HTTPS Encryption

☑ Enable SSL and STARTTLS support for SMTP and HTTPS

☑ Send messages with STARTTLS whenever possible

☑ SSL negotiation failures will retry without SSL for up to one hour

☑ Enable REQUIRETLS (RFC 8689)

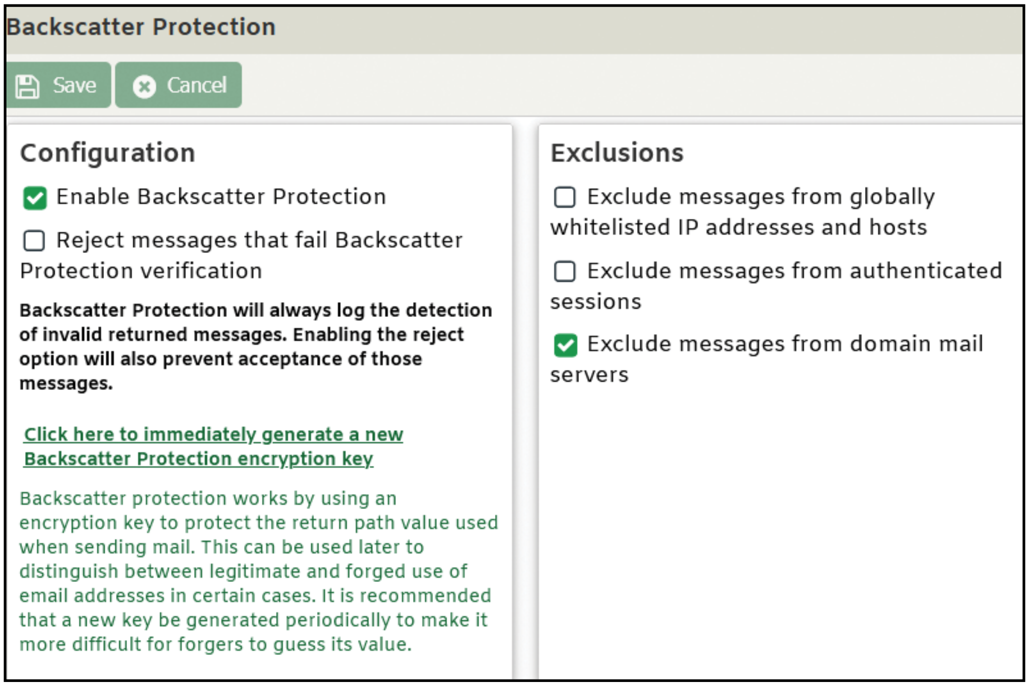
□ Enable MTA-STS (RFC 8461)

□ Enable TLS Reporting (RFC 8460)

Enable Backscatter Protection

Most spam messages contain a forged return path. This often leads to users receiving thousands of delivery status notices, autoresponders, and other messages in response to messages that the user never sent. This is known as backscatter. To combat backscatter, SecurityGateway's Backscatter Protection feature can help to ensure that only legitimate delivery status notifications and auto-responders get delivered to your domains.

Backscatter Protection settings are located under **Security | Anti-Spam | Backscatter Protection**.



Configuration

☑ Enable Backscatter Protection

□ Reject messages that fail Backscatter Protection verification

Backscatter Protection will always log the detection of invalid returned messages. Enabling the reject option will also prevent acceptance of those messages.

Click here to immediately generate a new Backscatter Protection encryption key

Backscatter protection works by using an encryption key to protect the return path value used when sending mail. This can be used later to distinguish between legitimate and forged use of email addresses in certain cases. It is recommended that a new key be generated periodically to make it more difficult for forgers to guess its value.

Exclusions

□ Exclude messages from globally whitelisted IP addresses and hosts

□ Exclude messages from authenticated sessions

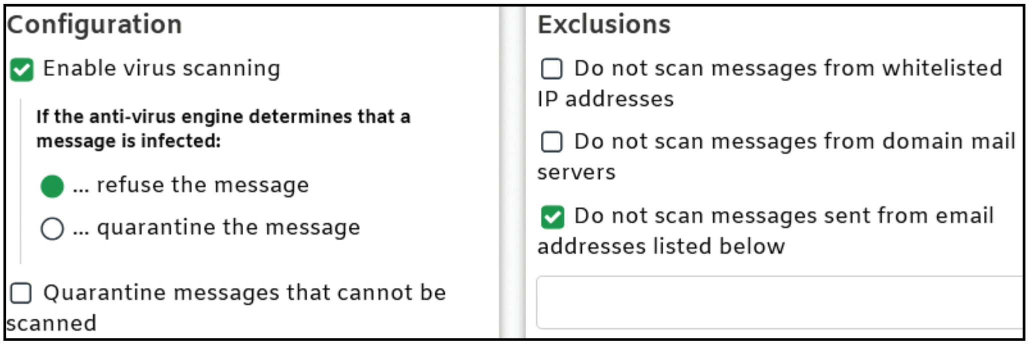
☑ Exclude messages from domain mail servers

Don't Whitelist Local Email Addresses

In many cases, local IP addresses or host names may need to be added to the "allowed senders" list. However, we do not recommend whitelisting local email addresses. If a local address is added to the whitelist, messages sent to this address could bypass many of your security settings and put your server at risk of being blacklisted.

Protect your Email Infrastructure from Malware

SecurityGateway scans all inbound and outbound mail using the Ikarus and ClamAV antivirus engines. We recommend enabling these features. These settings are located under **Security | Anti-Virus | Virus Scanning**.



Configuration

☑ Enable virus scanning

If the anti-virus engine determines that a message is infected:

● ... refuse the message

○ ... quarantine the message

□ Quarantine messages that cannot be scanned

Exclusions

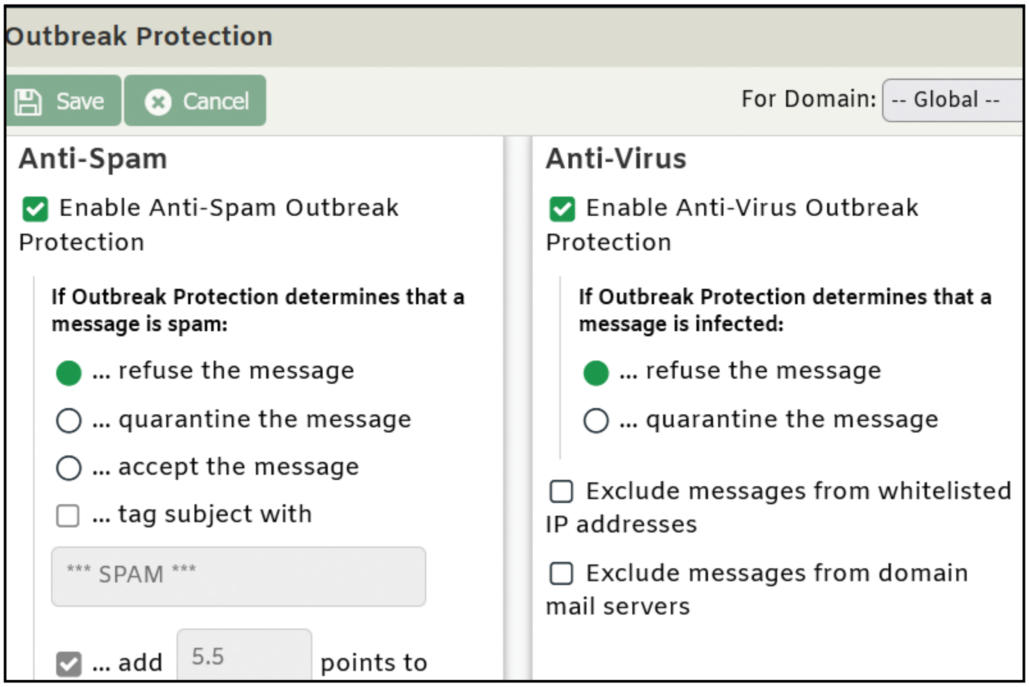
□ Do not scan messages from whitelisted IP addresses

□ Do not scan messages from domain mail servers

☑ Do not scan messages sent from email addresses listed below

Use Outbreak Protection to Detect Spam and Virus Outbreaks

We recommend enabling the Outbreak Protection features found under **Security | Anti-Spam | Outbreak Protection**. Outbreak Protection analyzes global structural and distribution email patterns to detect the latest emerging spam and virus outbreaks within minutes after they are first released.



Outbreak Protection

For Domain: -- Global --

Anti-Spam

☑ Enable Anti-Spam Outbreak Protection

If Outbreak Protection determines that a message is spam:

● ... refuse the message
○ ... quarantine the message
○ ... accept the message
□ ... tag subject with

*** SPAM ***

☑ ... add 5.5 points to

Anti-Virus

☑ Enable Anti-Virus Outbreak Protection

If Outbreak Protection determines that a message is infected:

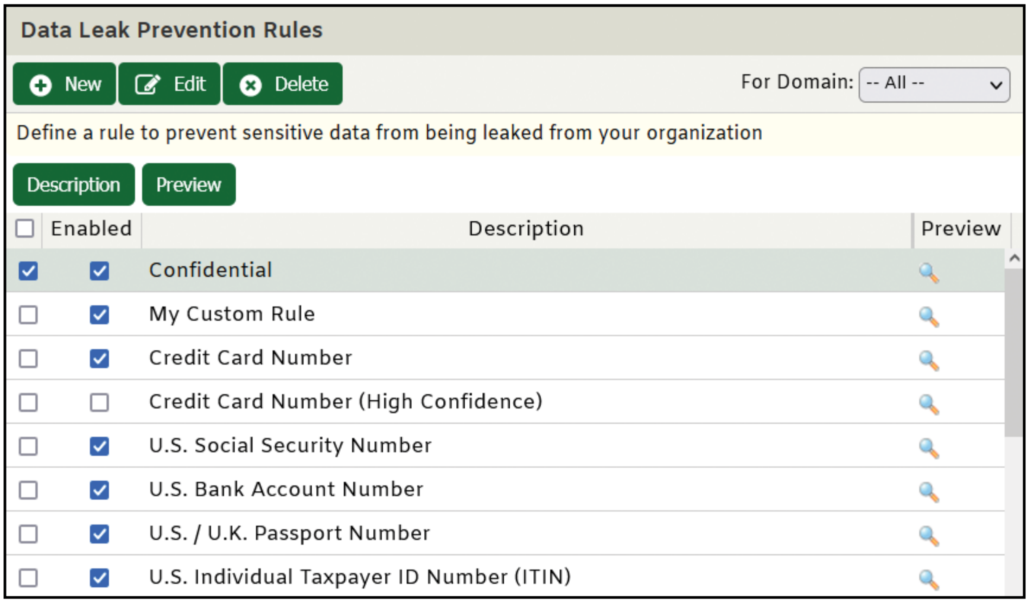
● ... refuse the message
○ ... quarantine the message

□ Exclude messages from whitelisted IP addresses

□ Exclude messages from domain mail servers

Prevent Data Leaks

SecurityGateway includes over 70 Data Leak Prevention rules to help prevent unauthorized transmission of sensitive information such as personal identification numbers, credit card numbers, and other types of confidential data. These rules can be configured to send messages containing sensitive content to the administrative quarantine for further review, redirect the message to a designated address, or encrypt the message. We recommend enabling the appropriate Data Leak Prevention rules to suit the needs of your specific business or industry.



Data Leak Prevention Rules

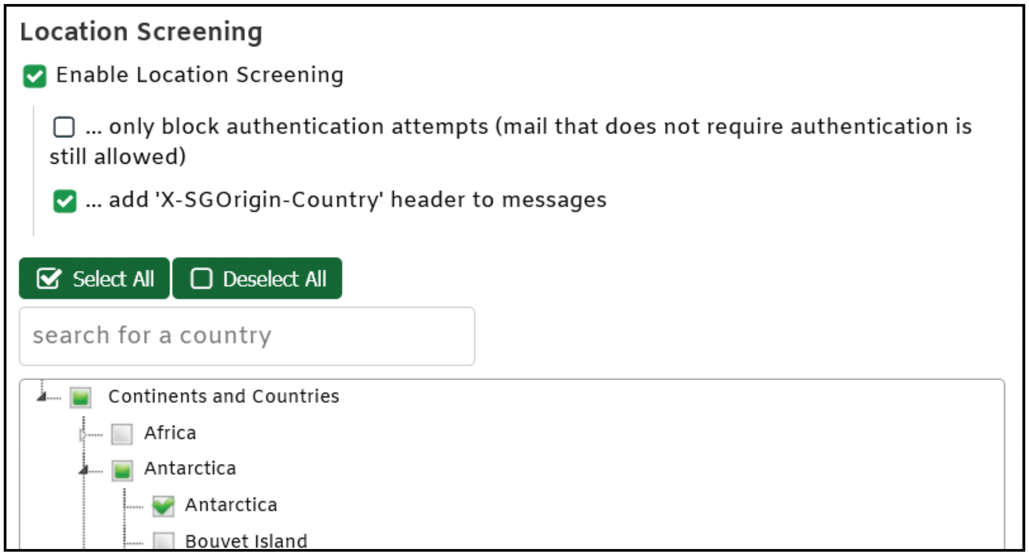
For Domain: -- All --

Define a rule to prevent sensitive data from being leaked from your organization

□	Enabled	Description	Preview
☑	☑	Confidential	🔍
□	☑	My Custom Rule	🔍
□	☑	Credit Card Number	🔍
□	□	Credit Card Number (High Confidence)	🔍
□	☑	U.S. Social Security Number	🔍
□	☑	U.S. Bank Account Number	🔍
□	☑	U.S. / U.K. Passport Number	🔍
□	☑	U.S. Individual Taxpayer ID Number (ITIN)	🔍

Enable Location Screening to Block Connections from Unauthorized Regions

Use Location Screening to block inbound SMTP and HTTP connections from unauthorized countries. If your company has no legitimate business need to communicate with a particular country, then refusing connections from that country can potentially block large amounts of spam. Alternatively, you can configure Location Screening to only prevent authentication from unauthorized countries. Location Screening settings are located under **Security | Anti-Abuse | Location Screening**.



Location Screening

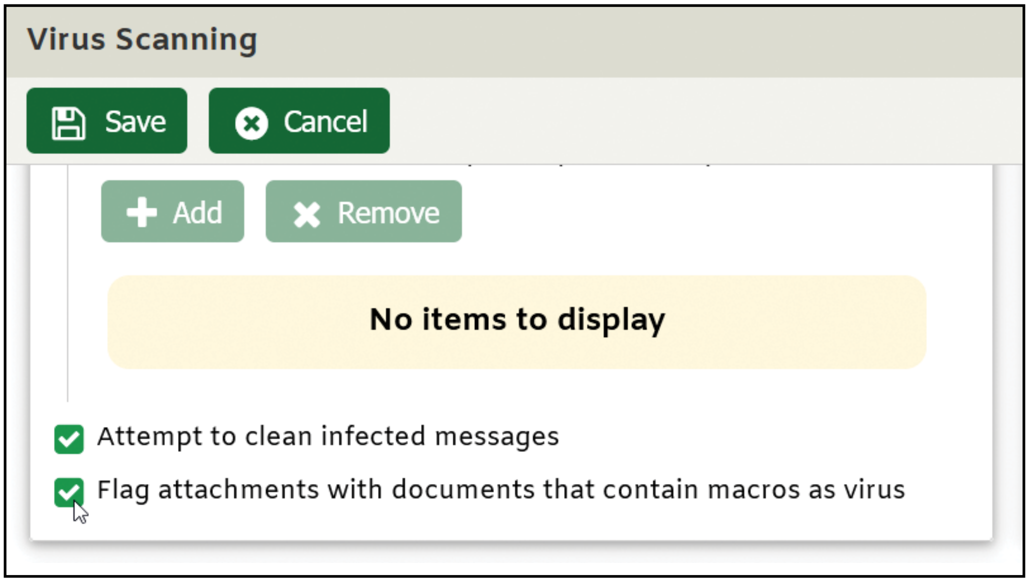
☑ Enable Location Screening

☐ ... only block authentication attempts (mail that does not require authentication is still allowed)

☑ ... add 'X-SGOrigin-Country' header to messages

Enable Macro Detection in Microsoft Office Documents

Cybercriminals often use macros in email attachments to spread malware. In SecurityGateway 6.5 and up, the Virus Scanning settings (located at **Security | Anti-Virus | Virus Scanning**) include an option to detect macros in Microsoft Office documents and flag them as infected. SecurityGateway can refuse these messages or quarantine them for administrative review.



Virus Scanning

No items to display

☑ Attempt to clean infected messages

☑ Flag attachments with documents that contain macros as virus

Summary

These best practices will help ensure that your email infrastructure is protected from spam, viruses, phishing attempts, unauthorized relaying, and other threats. Other helpful resources can be found under the Support tab at www.mdaemon.com.

6.23.2023