SecurityGateway 12 - New Features

SecurityGateway for Email 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: Beginning with SecurityGateway 12.0, Windows 7, Windows 8, Windows 8.1, and Windows Server 2008 R2 are no longer supported. The minimum supported operating systems are now Windows 10 and Windows Server 2012.

Display Name Protection to protect against BEC & Impersonation

SecurityGateway's new Display Name Protection feature helps protect against display name impersonation attacks where threat actors use display names similar to trusted users (such as executives, vendors, or colleagues) to trick recipients into taking actions like transferring money or revealing sensitive information. This feature provides comprehensive protection through multiple layers of defense. Key features include:

- Advanced name similarity detection
- Protected user management
- Stricter policies for free email providers
- Flexible response actions (reject, quarantine, add warning header, tag message subject, move to Spam folder)
- Integration with SecurityGateway's Sieve scripts for advanced processing
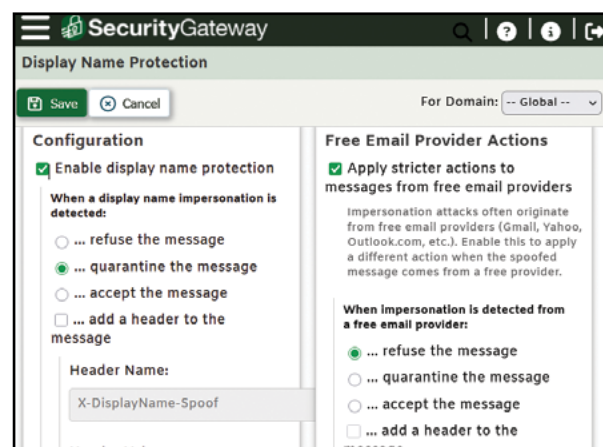 [Figure 1-1]

Figure 1-1

Database Connection Pooling for Improved Performance & Reliability under High Load

Database connection pooling helps improve performance by reusing existing database connections instead of creating new ones for each operation. It also automatically retries transient failures using increasing wait times as needed, and provides circuit breaker protection to prevent cascade failures during database outages. Global administrators can monitor database connection pool health in real-time from the dashboard. Statistics include current pool size, maximum pool size, active connections, idle connections, circuit breaker status, and consecutive failure count. Database connection pool metrics are exposed as Windows Performance Monitor counters for integration with external monitoring tools and alerting systems.
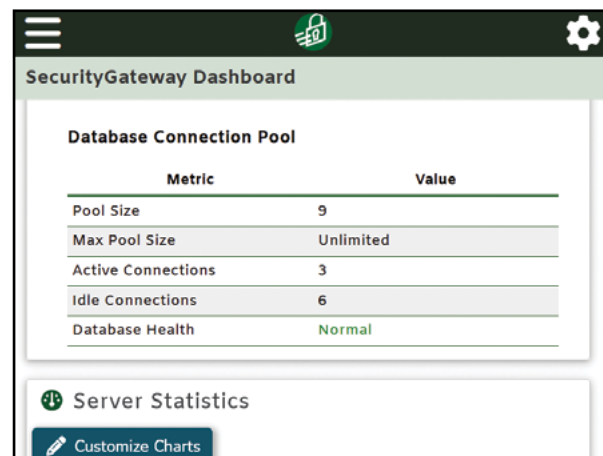
[Figure 1-2]

Figure 1-2

On-demand Quarantine Reports

Quarantine reports can now be sent on-demand. Users who have been granted quarantine access permissions can request on-demand quaranitne reports, and administrators can send on-demand quarantine reports to individual users. This allows immediate delivery of quarantine report emails without waiting for the scheduled report interval.

[Figure 2-1]

Administrator IP Access Restrictions

Administrator login access can now be restricted to specific IP addresses or IP ranges, providing an additional layer of security for administrative accounts. This feature helps prevent unauthorized access by limiting where administrators can authenticate from.

[Figure 2-2]

Figure 2-1

Email alerts for failed scheduled database backups

Administrators can now configure SecurityGateway to send email notifications to all global administrators when scheduled database backups fail. This helps ensure critical backup failures are promptly addressed.

Archive improvements

On-demand Archiving of Retained Messages

SecurityGateway's archiving feature now includes on-demand archiving of messages that are still retained in the database but not yet archived. This is useful when first enabling archiving to backfill historical messages, or to recover messages that are missing from the archive but still exist in the database.

Figure 2-2

Archive Failure Queue

Messages that cannot be archived due to errors (disk full, archive store unavailable, etc.) are now saved to a dedicated archive failure queue.

Other Improvements for SecurityGateway 12

- The user settings page has been reorganized into logical sections for improved usability.
- To help protect against service interruptions, the SecurityGateway system service is now configured with recovery options to automatically restart the service in the event that the service terminates unexpectedly.
- Archive search now includes the Sender/Recipient in default search criteria.
- We've added an option to exclude external administrators from receiving administrative quarantine summary emails.

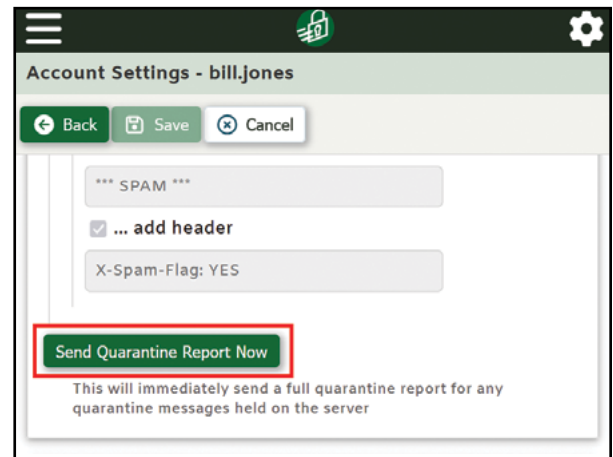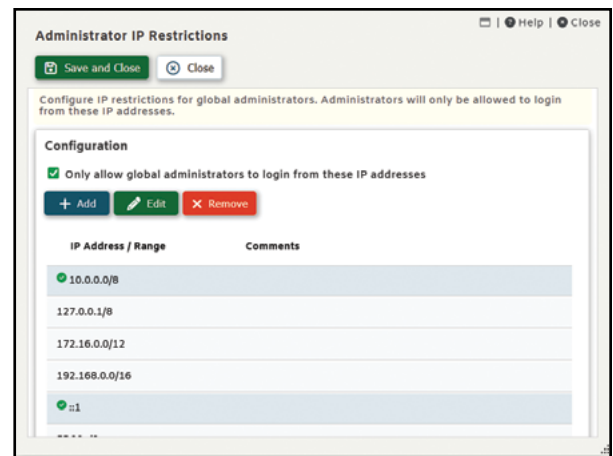**For a complete list of new features & updates, please see the SecurityGateway Release Notes.**