



McAfee eMail Gateway Appliance (“MEG”)

MEG-6.7.x

Quickstart Scope Definition Guidelines

Email is arguably today’s most indispensable communication medium and one of the most mission-critical services in any business environment. Its ability to whisk a wide range of information payloads instantly across organizational, geographic, and political boundaries makes it both an essential tool and an extraordinarily security challenge—one that has grown increasingly urgent and complex over time. With today’s ever-increasing email security risks, it is imperative that organizations information is protected against inbound and outbound threats. Get the appropriate service type below to ensure it is implemented and configured fast, cost-effectively and securely.

New Installation: 3 X MD-QS-SMB-4HR

McAfee Subject matter Experts (“SME”) will assist you in creating an initial configuration and baseline of policies for the MEG based on McAfee’s Best Practices.

Session 1

- Initial Configuration and Baseline
 - Add MEG to the network
 - Perform the initial setup wizard to configure base settings
 - Perform required update(s) to MEG if available
 - Configure email domain(s) for routing to internal server(s)

Session 2

- Intermediate Configuration and Initial Policy Tuning
 - Configure Anti-Spam, Intrusion Defender & Anti-Virus policies
 - Configure Advanced Encryption (if licensed)
 - Configure user/group mappings with LDAP

Session 3

- Advanced Configuration and Policy Tuning
 - Configure Envelope Analysis
 - Configure Multiple Domains (if required)
 - Test and tune all policies
 - Outline how to switch the appliance into production (Domains, MX Records, Smart Hosts, Firewall rules, etc)

Upgrading: 2 X MD-QS-SMB-4HR*

McAfee’s SME will perform the following tasks:

Session 1

- Initial Configuration and Baseline
 - Backup current configuration
 - Flash the internal memory on the device with the upgraded image
 - Restore the recently saved configuration
 - Perform the initial setup wizard to configure base settings
 - Verify configuration for email domain(s) for routing to internal server(s)

Session 2

- Advanced Configuration, Policy Tuning & Deployment
 - Migrate Anti-Spam, Intrusion Defender & Anti-Virus policies
 - Configure Advanced Encryption (if licensed)

- Configure user/group mappings with LDAP
- Migrate Envelope Analysis rules (up to 5)*, Content Analysis rules (up to 5)*, Dictionaries (up to 5)*, and Whitelist entries (up to 5)*
- Configure Multiple Domains (if required)
- Switch the appliance into production (Domains, MX Records, Smart Hosts, Firewall rules, etc)

Optimization: 1 X MD-QS-SMB-4HR

McAfee’s SME will perform the following tasks:

- MEG Compliance Rules
 - Create Envelope and Content Analysis Rules
 - Review Dictionaries, Whitelisting and DLP Analysis
- MEG Anti-Spam Features
 - Configure Enterprise Spam Profiler
 - Determine Trusted Sources
 - Define End User Quarantine
 - DSN Bounce Verifications
 - Define Header Analysis
 - Establish Connection Control and Spam Reporting
- MEG Anti-Virus and Intrusion Defender Functionalities
- MEG Encryption, Reporting, Queue Management

Knowledge Transfer: 1 X MD-QS-SMB-4HR

McAfee’s SME will perform the following tasks:

- Explain Compliance Rules
 - Envelope and Content Analysis Rules
 - Dictionaries, Whitelisting and DLP Analysis
- Explain Anti-Spam Features
 - Enterprise Spam Profiler
 - Trusted Source
 - End User Quarantine
 - DSN Bounce Verifications
 - Header Analysis
 - Connection Control and Spam Reporting
- Explain Anti-Virus and Intrusion Defender Functionalities
- Explain Encryption, Reporting, Queue Management

Session Requirements - before getting started: Client’s responsibility...

- Validated that server(s) meet McAfee’s minimum hardware requirements (See Product Guide)
- Rack-mounted all systems with power and Network connectivity
- Configured the Appliance (IP, host name, DNS server, etc...) and out of band access to all systems for console access
- Validated that the latest applicable ISO and required software have been downloaded via Client’s valid grant number
- Perform necessary backups
- Indicate if there are any outstanding Service Requests/Trouble Tickets opened with McAfee Technical Support

* Configurations and deployments exceeding these numbers will require additional sessions. Each remote session lasts up to 4.0 hours