



## McAfee Email & Web Security Virtual Appliance (“EWV”)

EWV-5.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\***

A McAfee Subject Matter Expert (“SME”) will remotely assist you in the initial configuration and policy baseline for the EWV appliance based on McAfee’s Best Practices.

##### **Session 1**

- Initial Configuration and Baseline
  - Add EWV to the network
  - Perform the initial setup wizard to configure base network settings
  - Perform required update(s) to EWV if available
  - Configure EWV to ePO Server if relevant to network
  - Introduction to Interface Settings

##### **Session 2**

- Intermediate Configuration & Policy Tuning
  - Configure FTP, ICAP, POP3, & SMTP Content policies
  - Configure HTTP scanning policies
  - Configure FTP, ICAP, HTTP, POP3 & SMTP action policies
  - Configure user/group mappings with LDAP, and Reporting

##### **Session 3**

- Advanced Configuration & Policy Tuning
  - Configure Multiple Domains (if required)
  - Test and tune all policies
  - Provide guidance to switch the EWV appliance into production (Domains, MX Records, Smart Hosts, Firewall rules, etc)

#### **Upgrading 5.0 to 5.X: 1 X MD-QS-SMB-4HR\***

McAfee’s SME will perform the following tasks:

- Review server and software requirements
- Upgrade and Configure EWV to 5.X
  - Backup EWV configuration
  - Flash the internal memory on the device with the upgraded image
  - Restore configurations on EWV 5.X
  - View migration results and configuration report
  - Perform the initial setup wizard to configure base network settings
  - Perform required update(s) to appliance if available
  - Validate appliance connection to ePO Server if relevant
  - Validate all migrated (new) policies and settings
- Test the EWV to confirm mail is passing thru appliance

#### **Optimization: 1 X MD-QS-SMB-4HR\***

McAfee’s SME will perform the following tasks:

- EWV environment and scanning
  - Review topologies and clustering present
  - Determine Ports and Protocols to allow or disallow
  - Define the scan order for re: emails
  - Regulate Scanner Options for Web content
- EWV Configuration tuning
  - Disable reverse lookup
  - Enable Kernel Mode Blocking
  - Configure policies how the appliance must respond to a threat
  - Align EWV with ePO, Monitoring & Reporting
  - Create rules for message processing, Greylisting
  - Process user-submitted blacklist and whitelist
  - Determine Alert Settings and Notifications

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

McAfee’s SME will perform the following tasks:

- Explain EWV environment and scanning
  - Topologies and clustering
  - Ports and Protocols to allow or disallow
  - Scan order for re: emails
  - Scanner Options for Web content
- Explain EWV Configuration tuning
  - Reverse lookup
  - Kernel Mode Blocking
  - Policies and how the appliance will respond to a threat
  - EWS and ePO Monitoring & Reporting
  - Create rules for message processing, Greylisting
  - User-submitted blacklist and whitelist
  - Determine Alert Settings and Notifications

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

- Validated that server(s) meet McAfee’s hardware requirements (See Product Guide)
- Download ePO extension if ePO is used to manage EWS
- Establish and verify virtual environment and ensure connectivity to virtual appliance
- Validated that the latest applicable ISO and required software have been downloaded via Client’s valid grant number
- Network Settings (Domains, MX Records, etc)
- 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**