



McAfee Network Security Manager Appliance (“NSM”)

NSM-7.1.x

Quickstart Scope Definition Guidelines

As organizational infrastructures grow, so does the need for security device placement throughout the network environment. McAfee’s Network Security Manager allows an organization to manage all Intrusion Prevention System Sensors and Network Access Control Appliances from a single screen. Get the appropriate service type below to ensure it is implemented and configured fast, cost-effectively and securely.

New Installation: 2 X MD-QS-SMB-4HR*

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

Session 1

- Initial Configuration and Baseline
 - Add NSM to the network
 - Perform the initial setup wizard to configure base settings
 - Perform required update(s) to NSM if available

Session 2

- Advanced Configuration and Policy Tuning
 - Configure Multiple Domains (if required)
 - Test and tune all policies
 - Outline how to switch the appliance into production

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

McAfee’s SME will perform the following tasks:

- Upgrade 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)

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

McAfee’s SME will perform the following tasks:

- Configure device discovery
 - Intrusion Prevention Systems
 - Network Access Control Appliances
- Configure devices to be managed through the NSM
- Review current NSM policies to ensure compliance with McAfee Best Practices (up to 5)*
- Configure associated dashboards

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

McAfee’s SME will perform the following tasks:

- Explain device discovery
 - Intrusion Prevention Systems
 - Network Access Control Appliances
- Explain device configuration through the NSM
- Explain current NSM policies to ensure compliance with McAfee Best Practices (up to 5)*
- Explain associated dashboard

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**