McAfee Data Protection Encrypted USB
McAfee Security Quickstart Scope Definition Guidelines

McAfee® Encrypted USB enables organizations to take advantage of the convenience and portability of USB storage devices guarded by McAfee encryption. McAfee Encrypted USB protects an organization's confidential and private data in the event these portable devices get lost or fall into the wrong hands. Your organization’s data stays secure with the use of strong encryption and advanced management. Get the appropriate service type below to ensure it is implemented and configured fast, cost effectively, and securely.

New Installation: 1 X MD-QS-SMB-4HR*

The McAfee SME will perform the following tasks:
• Review server and software requirements
• Install and configure the McAfee Encrypted USB:
  - Connect McAfee Encrypted USB into a McAfee ePolicy Orchestrator® (McAfee ePO™) managed system
  - Create McAfee Encrypted USB policies based on your environment (up to five)*
• Test the encrypted USB policies to verify that they are working properly

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

The McAfee SME will perform the following tasks:
• Review server and software requirements
• Upgrade and configure McAfee Encrypted USB:
  - Connect new McAfee Encrypted USB into a McAfee ePO managed system
  - Copy data from the old USB to the new McAfee Encrypted USB
  - Confirm quality of data copied
  - Delete data from the old USB device, and properly dispose of it
• Import and modify McAfee Encrypted USB policies (up to five)*
• Test policies to verify proper operation

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

The McAfee SME will perform the following tasks:
• Verify that the McAfee Encrypted USB software functions as expected
• McAfee Encrypted USB features:
  - Access control
  - Zero-client footprint on connected systems
  - Two-factor authentication
  - Built-in anti-malware

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

The McAfee SME will perform the following tasks:
• Explain the McAfee Encrypted USB features:
  - Access control
  - Zero-client footprint on systems connected
  - Two factor authentication
  - Built in anti-malware
• Explain McAfee Encrypted USB framework:
  - Strong encryption
  - Centralized management using McAfee ePO
• Explain McAfee Encrypted USB categories:
  - USB sticks
  - USB hard disks
• Explain policy creation and assignment based on the previous uses mentioned (up to five)*
• Review the available McAfee Encrypted USB queries and dashboards (up to five)*

Session Prerequisites—Client Responsibilities

• Validate that all endpoints, databases, and servers meet McAfee hardware and software requirements (see the McAfee Product Guide)
• Validate that all applicable McAfee software licenses have been installed via client's valid grant number
• Perform necessary backups
• Clients are responsible for scheduling the session with their appropriate change control authorities
• 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 four hours.

For more information about McAfee® Security Quickstart, email quickstart_support@mcafee.com, or visit www.mcafeequickstart.com.