



McAfee Data Protection Encrypted USB

USB-x

Quickstart Scope Definition Guidelines

McAfee's Encrypted USB enables organizations to take advantage of the convenience and portability of USB storage devices guarded by the security of McAfee encryption. McAfee's Encrypted USB protects an organization's confidential and private data in the case these highly portable devices get lost or happen to fall into the wrong hands. Organizations data remains 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*

A McAfee Subject Matter Expert ("SME") will remotely configure encrypted USB based on McAfee's Best Practices.

- Review server and software requirements
- Install and Configure the McAfee Encrypted USB:
 - Connect McAfee Encrypted USB into a ePO managed system
 - Create McAfee Encrypted USB policies based on your environment (up to 5)*
- Test the encrypted USB policies to verify they are working properly.

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

McAfee's SME will perform the following tasks:

- Review server and software requirements
- Upgrade and Configure McAfee Encrypted USB:
 - Connect new McAfee Encrypted USB into a ePO managed system
 - Copy data from old USB to the new McAfee Encrypted USB
 - Confirm quality of data copied
 - Delete data from old USB device, and properly dispose
 - Import and Modify McAfee Encrypted USB policies (up to 5)*
- Test policies to verify proper operation.

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

McAfee's SME will perform the following tasks:

- Verify the McAfee Encrypted USB software functions as expected.
- McAfee Encrypted USB Features:
 - Access control
 - Zero-client footprint on systems connected
 - Two factor authentication
 - Built in anti-mailware

- McAfee Encrypted USB Framework:
 - Strong Encryption
 - Centralized management using ePO McAfee
- Encrypted USB Categories:
 - USB Sticks
 - USB Hard Disks
- Review current McAfee Encrypted USB policies for compliance with McAfee Best Practices (up to 5)*
- Validate Policy Assignment functionality.
- Confirm availability of queries and dashboards.

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

McAfee's 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-mailware
- Explain McAfee Encrypted USB Framework:
 - Strong Encryption
 - Centralized management using ePO
- Explain McAfee Encrypted USB Categories:
 - USB Sticks
 - USB Hard Disks
- Explain policy creation and assignment based on the previous uses mentioned (up to 5)*.
- Review the available McAfee Encrypted USB queries and dashboards (up to 5)*.

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

- Validate that all endpoints, databases and servers meet McAfee's hardware and software requirements (See Product Guide)
- Validate that all applicable McAfee software licenses have been installed via Client's valid grant number
- Perform necessary backups
- Client is 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 4.0 hours**