

**McAfee Endpoint Encryption for Files and Folders (“EEFF”)****EEFF-6.1.x****Quickstart Scope Definition Guidelines**

McAfee Endpoint Encryption for Files and Folders (“EEFF”) delivers powerful encryption integrated with centralized management that helps prevent unauthorized access and loss or theft of sensitive data. McAfee offers multiple layers of encryption solutions for your PC, network files and folders. It uses industry-leading encryption algorithms and offer multiple layers of protection that address specific risk areas. Endpoint Encryption allows you to transparently secure a broader scope of confidential information including customer data, intellectual property, legal and financial records, and employee communications with no system performance degradation. 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\***

A McAfee Subject Matter Expert (“SME”) will remotely configure your ePO server to manage and deploy EEFF using McAfee Best Practices and will have your ePO server ready to protect your endpoints.

**Session 1**

- Review server and software requirements
  - Ensure ePO version is compatible with EEFF’s current version
- Install and Configure EEFF from the ePO Server:
  - Install the EEFF Extension
  - Install License
  - Setup Key Groups and Create Keys
  - Add the EEFF deployment package to the ePO Repository

**Session 2**

- Advanced Configuration, Policy Tuning & Deployment
  - Deploy and enable the EEFF Agent to endpoints (up to 3)\*
  - Create EEFF policies based on your environment (up to 3)\*
- Test the EEFF policies to verify they are working properly.
  - Begin encrypting drives on 3 deployed systems

**Upgrading 6.0.x to 6.1: 1 X MD-QS-SMB-4HR\***

McAfee’s SME will perform the following tasks:

- Review server and software requirements
- Upgrade and Configure EEFF from the ePO Server:
  - Export current EEFF policies
  - Install the latest EEFF extension
  - Update the EEFF license
  - Verify Key Groups and Keys
  - Add the latest EEFF deployment package to the ePO Repository
  - Install and enable the new EEFF on endpoints (up to 5)\*
  - Import and Modify EEFF policies (up to 5)\*
- Test the EEFF policies to verify proper operation.

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

McAfee’s SME will perform the following tasks:

- Verify the EEFF software functions as expected.

## ○ EEFF Features:

- Encrypts all data stored
- Enforces strong access control with pre-boot authentication
- Enables automatic/transparent encryption in the background

## ○ EEFF Framework:

- Military-strength certified encryption algorithms
- Enhanced performance through Intel AES-IN technology

## ○ EEFF Categories:

- Software-based encryption
- Hardware-based encryption
- Solid-state drives
- Self-encrypting drives

- Review current EEFF policies for compliance with McAfee Best Practices (up to 5)\*

- Validate EEFF Policy Assignment functionality.

- Confirm availability of EEFF queries and dashboards.

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

McAfee’s SME will perform the following tasks:

## ○ Explain EEFF Features:

- Encrypts all data stored
- Enforces strong access control with pre-boot authentication
- Enables automatic/transparent encryption in the background

## ○ Explain EEFF Framework:

- Military-strength certified encryption algorithms
- Enhanced performance through Intel AES-IN technology

## ○ Explain EEFF Categories:

- Software-based encryption
- Hardware-based encryption
- Solid-state drives
- Self-encrypting drives

- Explain current EEFF policies for compliance with McAfee Best Practices (up to 5)\*

- Explain EEFF Policy Assignment functionality.

- Explain EEFF queries and dashboards.

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

- ePO should be running and be properly configured within the environment with the appropriate version
- 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
- Performed any 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**