Business Brief

Management of Native Encryption

For Apple FileVault and Microsoft BitLocker

TM

The proliferation of data and devices in today's enterprises has increased the complexity of protecting confidential data and meeting compliance mandates. Given that a large amount of data can now be stored on PCs, tablets, and other devices, it's never been more important to ensure that sensitive data is secured.

Businesses need to control access to sensitive data to achieve regulatory compliance and reduce liability. Through the use of best practices, encryption can be a simple and effective way to protect your enterprise data. Encryption is essential, as it hides the underlying data and prevents any unauthorized access to the information. This means that even if a device containing confidential information is lost or stolen, the information will remain secure. In most cases, the actual data on the lost or stolen device is much more valuable than the device itself, thus reinforcing the need to invest time and effort in a data protection solution for your business.

Comprehensive Data Protection

Organizations have a variety of encryption options available in protection suites from McAfee, a part of Intel Security, that include:

- **Drive encryption:** Provides comprehensive enterprise-grade encryption for system drives on Microsoft Windows based desktop PCs, laptops, and tablets.
- **File and removable media protection:** Encrypts data on network files and folders, removable media, USB portable storage devices, and cloud storage services.
- **Management of native encryption:** Manages the native encryption function offered by Apple FileVault on Mac OS X, and Microsoft BitLocker on Windows, directly from the McAfee® ePolicy Orchestrator® (McAfee ePO™) management console.

What Is Native Encryption?

One option enterprises can choose to adopt is encryption of data on the system drive (full disk encryption) through the native encryption supplied with the operating system by the OS vendor. Native encryption is offered by Apple as FileVault on Macintosh systems and by Microsoft as BitLocker on Windows platforms. BitLocker and FileVault are native security features available in modern versions of Windows and OS X operating systems. These native encryption functions provide whole drive encryption by encrypting data on the drive that Windows or OS X is installed on.

Benefits Common to Both FileVault and BitLocker Management

- Ability to upgrade from one major OS X version to next without having to decrypt and re-encrypt the drive.
- Zero-day compatibility with OS X and Windows patches, upgrades, and firmware updates from Apple and Microsoft.
- Zero-day support for new hardware from Apple and tablet hardware from Microsoft.
- Self-service portal, which allows users to recover their own machines.
- Support for a BYOD model, where the device is not managed—only the state of compliance is reported in McAfee ePO software (suitable for contractors).
- Simple administration and management.

intel Security

Similar to other forms of encryption, native encryption uses encryption keys for the encryption process, which are required to decrypt the data on the system drive. The encryption keys can be unmanaged (stand-alone) or in the case of enterprise IT, managed (escrowed) by a management console. In the case of Intel Security solutions, that is handled by the McAfee ePO console.

Management of Native Encryption

With the adoption of native encryption and other encryption layers across your organization, centralized management ensures that you have consistent policy and compliance enforcement across your encryption technology stack. Management of native encryption allows you to manage native encryption directly from the McAfee ePO management console. This capability enables you to easily:

- Manage Apple FileVault and Microsoft BitLocker.
- Report encryption and compliance status.
- Escrow, import, store, and retrieve recovery keys.

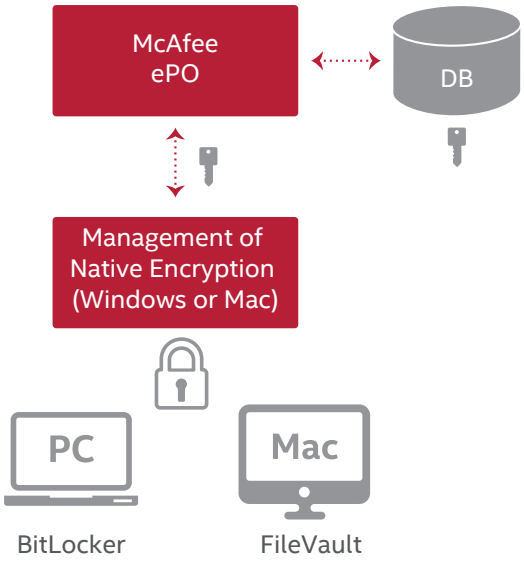

Figure 1. Management of native encryption can manage the native encryption of Windows PC and laptops and Apple Macs.

Deployment and Provisioning

Management of native encryption lets you manage native encryption functionality directly from McAfee ePO software, providing ease of deployment coupled with a flexible, mix-and-match licensing model that lets you choose the perfect fit for your organization.

McAfee ePO software is the most advanced, extensible, and scalable centralized security management software in the industry. Unifying security management through an open platform, McAfee ePO software enables you to connect your security solutions to your enterprise infrastructure to increase visibility, gain efficiencies, and strengthen protection.

Key Features for Mac Environments

- Ability to SSO from the FileVault pre-boot environment directly into OS X.
- Manage FileVault on any Mac hardware that can run OS X Mountain Lion, Mavericks, or Yosemite directly from McAfee ePO software.
- Enforce a standard password complexity policy on local OS X users
- Report compliance in various reports and dashboards in McAfee ePO software.
- Provide the FileVault Recovery Key, when required, in recovery use cases to use Apple-provided recovery tools and workflows.
- Allow administrators to manually import FileVault Recovery Keys where users have already manually enabled FileVault.
- Proof-of-compliance report in the event of a lost or stolen laptop
- IT-enforceable password policies for OS X.
- Full compatibility in pre-boot for all languages supported by Apple.

Management of native encryption is deployed in the same method as all Intel Security software. First, the agent is deployed to the Mac or Windows endpoint through McAfee ePO software (if the endpoint does not already have the agent). Next, management of native encryption is deployed to the endpoint and enabled through the McAfee ePO management console. There is no need to decrypt and re-encrypt endpoints when deploying management of native encryption. Once management of native encryption is deployed and enabled, it can be configured for "Reporting" mode or "Full Management" mode. "Reporting Only" mode implies that the system is under the user's control. In this mode, McAfee ePO software still has continuous reporting oversight. "Full Management" mode implies the system is under McAfee ePO software administrative control and enforcement. Keys are escrowed in McAfee ePO software for administrative access and recovery.

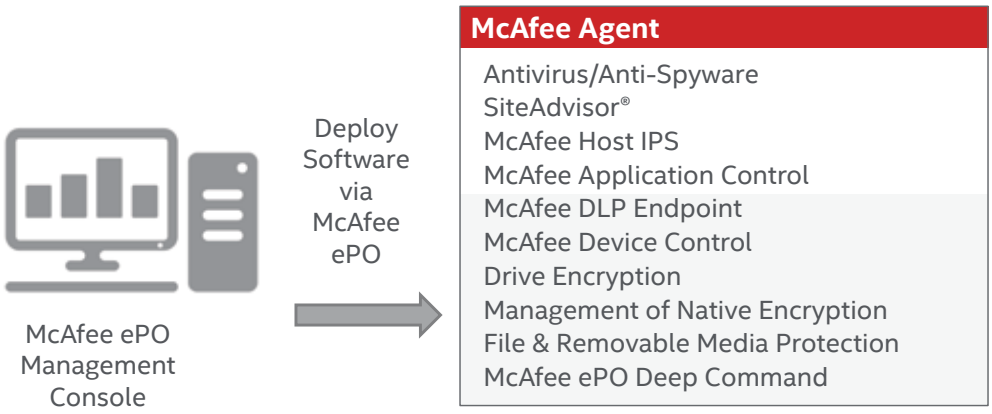

Figure 2. Management of native encryption is deployed the same as other Intel Security software.

Some of the key features of management of native encryption deployment through McAfee ePO software include:

Simplified deployment:

- Identifies PCs and Macs that are not protected and then deploys the McAfee ePO software agent to protect PCs and Macs according to policies.
- Enables lower administrative overhead with single-console and common management agent for data protection and endpoint security products.
- Enables remote, no-touch Microsoft Windows XP to Microsoft Windows 7 migration, including keeping the user's data and machine encrypted during the entire process.

Mix-and-match provisioning:

- McAfee encryption solutions are sold on a per-node basis, giving you complete flexibility to choose the perfect mix-and-match combination for how you'd like to provision your licenses across your encryption solutions. For example, each license can provision a Windows PC with either drive encryption or management of native encryption for BitLocker. The choice is yours.
- Customers can mix and match drives. For deployments that have common drives, deployments can be templated in McAfee ePO software to reduce provisioning time.

Key Features for Windows Environments

- Supports certified Windows To Go devices.
- Manage BitLocker on Windows 7 or 8 hardware directly from McAfee ePO software.
- Utilizes the Trusted Platform Module (TPM) 1.2 and 2.0 hardware to provide a transparent user experience.
- Supports FIPS 140-2 requirements.
- Supports Microsoft eDrive.
- Includes a consistent user interface for both FileVault and BitLocker management.
- Provides the BitLocker Recovery Key, when required, in recovery use cases.
- Reports compliance in various reports and dashboards in McAfee ePO software.
- Manage BitLocker from McAfee ePO software, without the need for a separate Microsoft BitLocker Management and Monitoring (MBAM) server.

Daily Management

Daily management of native encryption with McAfee ePO software couldn't be easier. You get centralized management, consistent policy enforcement and compliance, and single-pane-of-glass visibility that ensure you have consistent protection. Only McAfee ePO software offers you these capabilities:

Simplified security operations

- Helps organizations of every size streamline administrative tasks, ease audit fatigue, and reduce security management-related hardware costs.

Flexible, shared infrastructure

- Supports mixed encryption environments, enabling organizations to maintain a single policy and management infrastructure for the entire environment, regardless of whether it is software- or hardware-based encryption.
- Allows you to share tasks, policies, and management infrastructure, regardless of your encryption mix.

Customizable, granular policies

- Offers customization by user (individual, shared by groups, or the entire company), PC/Mac, or server.
- Enables you to specify a new encryption policy at any level of the organization to handle specific use cases.

Holistic, single-pane-of-glass visibility

- Stores all audit and logging information inside the McAfee ePO console.
- Generates standard or custom reports on the entire McAfee ePO software-managed network.

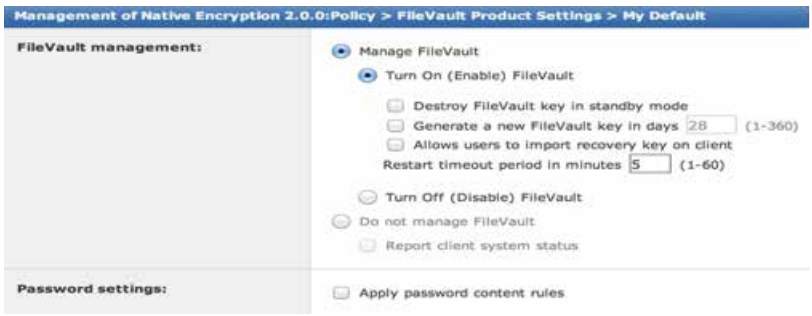

Figure 3. Manage BitLocker and FileVault with the same look and feel from the McAfee ePO management console.

Microsoft BitLocker Administration and Monitoring (MBAM) Server Migration

Adopting management of native encryption for BitLocker means you no longer need to license, manage, or maintain Microsoft BitLocker Administration and Monitoring (MBAM) and its associated servers. This lets you consolidate servers and eliminate the related Microsoft licenses, which provides significant cost savings and reduced management overhead.

Management of native encryption lets you manage native encryption functionality directly from the McAfee ePO management console, along with all your other Intel Security software. Migration from MBAM to McAfee ePO software is a seamless, two-step process. The first step involves deploying and configuring the management of native encryption client on each endpoint, followed by enabling the management mode in the second step.

When management of native encryption is first installed on a system where BitLocker is running, any existing recovery keys are backed up to McAfee ePO software by simply pulling them from the client using the BitLocker API. Management of native encryption recovery keys are added as well and are also safely stored in McAfee ePO software. This occurs automatically with the first policy enforcement as management of native encryption pulls BitLocker into compliance with the management of native encryption policy.

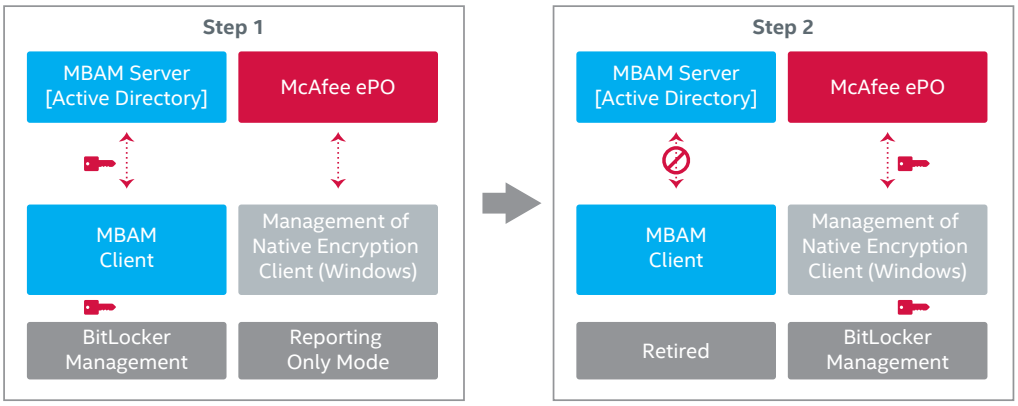

Figure 4. MBAM to management of native encryption migration process.

Detailed Reports

Management of native encryption provides comprehensive reports that put all the information at your fingertips to give you 360-degree visibility of your organization's encryption status—with dashboards and standard and customizable reports that provide detailed views of your encryption enforcement across your organization.

Report queries can also be used as a dashboard monitor that is automatically updated every five minutes, making it easy to stay informed on any high priority items. Likewise, reports can easily be exported in several formats:

- **CSV:** Use the data in a spreadsheet application (for example, Microsoft Excel).
- **XML:** Transform the data for other purposes.
- **HTML:** View the exported results as a web page.
- **PDF:** Print the results.

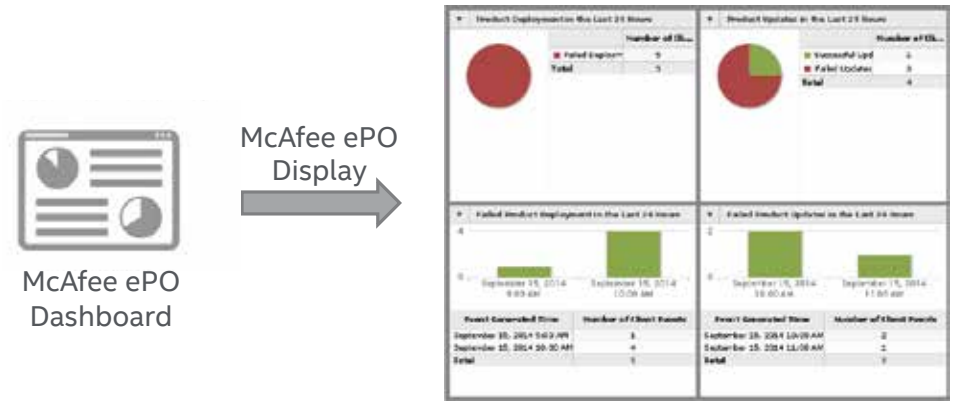

Figure 5. McAfee ePO software dashboard.

Management of Native Encryption Availability

Management of native encryption is available as part of four endpoint protection suite offerings. Intel Security data protection solutions safeguard your critical data and provide multilayered protection for your data, regardless of where it resides—on the network, in the cloud, or at the endpoint.

Management of native encryption is available as a key component in the following Intel Security suites:

For enterprises with 2,000 nodes or more:

- **McAfee Complete Data Protection**
- **McAfee Complete Data Protection—Advanced**
- **McAfee Complete Data Protection—Essential**

For commercial businesses with up to 2,000 nodes:

- **McAfee Complete Endpoint Protection—Business**

For additional resources on management of native encryption please read the **Management of Native Encryption Product Guide** and visit the **Management of Native Encryption Expert Center**.

Conclusion

Management of native encryption empowers you to take full advantage of Apple FileVault and Microsoft BitLocker native encryption with centralized management through McAfee ePO software, which ensures that you have consistent policy and compliance enforcement across your encryption technology stack.

For more information about Intel Security endpoint encryption and management solutions, or to download a free, 90-day trial of management of native encryption, please visit **www.mcafee.com/dataprotection**, or call us at 888 847 8766, 24 hours a day, seven days a week.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com