Enabling BitLocker - Managed Computers

Enabling BitLocker - Managed Computers

> ⚠ This article pertains only to computers on the WIN domain. It also applies to computers that have the SCCM client installed.

Bitlocker will be deployed by IT administrators in two main ways

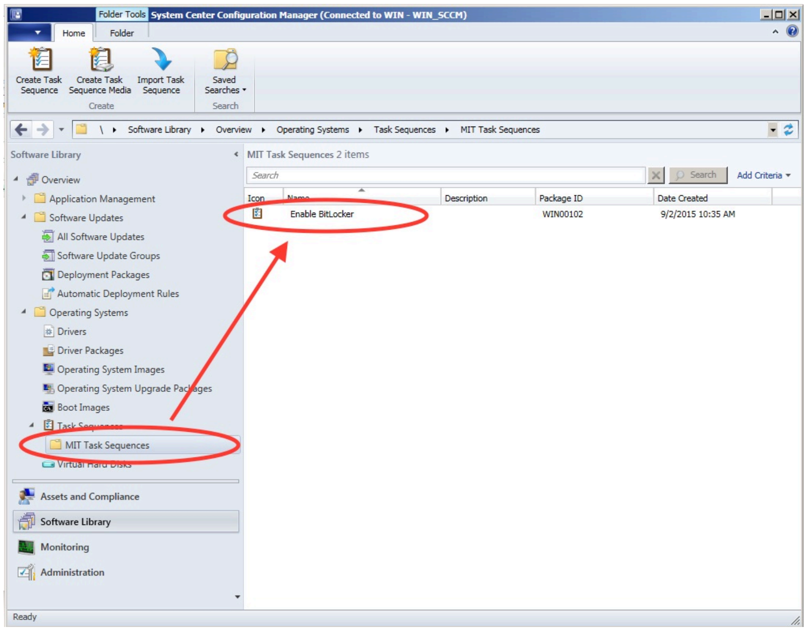
- Via MECM for existing computers
- Via Lite Touch imaging for new computers being joined to the WIN domain

EUC Lite Touch

All computers imaging using EUC Lite Touch and joined to the WIN domain (under the Endpoints OU) during imaging will be automatically enabled with BitLocker encryption. TPM will be enabled (Lenovo and Dell computers only), the MBAM client will be installed, and the BitLocker encryption keys will be stored in the MBAM database. If you are putting a computer into Endpoints and would like to NOT encrypt, please select to Opt-Out of BitLocker from the bottom of the applications list. End-users and IT administrators will be able to recover BitLocker Recover Keys via the MBAM self-service web portal.

MECM

IT Administrators can deploy a task sequence to their computer via MECM. The task sequence can be found in the software library under Operating Systems -> Task Sequences -> MIT Task Sequences -> Enable BitLocker.



Icon	Name	Description	Package ID	Date Created
	Enable BitLocker		WIN00102	9/2/2015 10:35 AM

Deploy the task sequences in the same manner as any other application.

Notes:

- If the MECM task sequence is applied to a computer that already has BitLocker enabled, a new key will NOT be created.
- If the disk was encrypted before joining the computer to the domain, the recovery key will NOT be automatically escrowed in AD, you must manually upload it. The existing key will simply be escrowed in the MBAM database.

See Also

- Encryption Landing Page