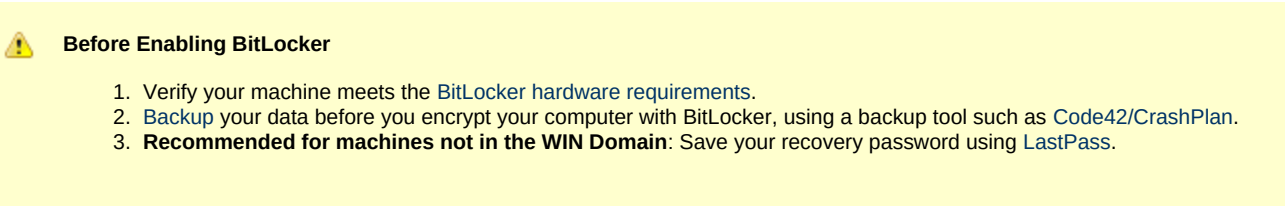
BitLocker

BitLocker

On this page:

Overview

Windows BitLocker Drive Encryption is a security feature that provides data protection for your computer by encrypting all data stored on the Windows operating system hard disk drive.



Before Enabling BitLocker

1. Verify your machine meets the BitLocker hardware requirements.
2. Backup your data before you encrypt your computer with BitLocker, using a backup tool such as Code42/CrashPlan.
3. **Recommended for machines not in the WIN Domain**: Save your recovery password using LastPass.

How to Enable

Windows computer in the WIN Domain

This information applies only to computers on the WIN domain and that may have the SCCM client installed.

- Enabling BitLocker on managed computers.

Windows computer not in the WIN Domain

This information applies only to computers that are self-managed and administered, including those that are not on the WIN domain.

- Enabling BitLocker on unmanaged computers.

How to Use

- Key recovery using BitLocker Helpdesk
- [Key recovery using BitLocker Self-Service]
- Key recovery using Active Directory Users and Computers
- Key recovery for unamanged (non-domain) computers
- How to decrypt a drive
- How to enable BitLocker encryption on a portable drive

See Also

- BitLocker Overview and Requirements
- Encryption services at MIT
- Encryption Landing Page

Help

- Frequently asked questions about BitLocker
- [What is the difference between a TPM owner password, recovery password, recovery key, PIN, enhanced PIN, and startup key?]
- Troubleshooting issues with BitLocker
- Users in need of further assistance can contact the Service Desk at 617.253.1101, servicedesk@mit.edu, or by submitting a request online (http://ist.mit.edu/help).