



Simple, comprehensive, enterprise-level management and audit capabilities for Microsoft® BitLocker.

Management for BitLocker

Included in Microsoft® Windows™ 7 Ultimate and Enterprise, BitLocker Drive Encryption is a feature that can protect information on a drive. Many find BitLocker appealing because purchasing a separate encryption solution is not required. However IT needs enterprise-level management with centralized reporting and audit capabilities to effectively leverage BitLocker to help address security and regulatory compliance concerns.

BitLocker Manager, part of a comprehensive data protection portfolio called Dell Data Protection | Encryption, solves these issues and enables IT to enforce encryption across your organization. Designed for simple management, comprehensive protection and flexibility, BitLocker Manager features include:

Simplified deployment and management

- **Highly scalable and easy to deploy** - Enables large-scale deployment through live, operational rapid deployment capabilities, while helping reduce total cost of ownership.
- **Seamless integration** - Administrators manage all users and devices, including BitLocker users, through a centralized Dell Data Protection | Encryption Management Console, which supports a comprehensive offering of encryption solutions.
- **Comprehensive key management** - Centralized escrow of the critical recovery keys helps ensure that

users can access information on encrypted systems whenever needed, with minimal work from IT and helpdesk teams, without storing them in Active Directory®.

- **Policy enforcement** - Define and enforce policies from a single, centralized console. Take advantage of group policies to manage BitLocker without altering Active Directory. The management console provides all the flexibility and control you need for your enterprise.
- **Automated TPM management** - Enabling BitLocker TPM capabilities can require significant setup activities. BitLocker Manager automates TPM initialization and stores the TPM password for recovery, helping reduce work and the risk that systems are left unprotected.

Comprehensive protection and compliance reporting

- **FIPS compliance** - Secure, centralized recovery key escrow ensures that your encryption deployment remains FIPS compliant.
- **Compliance reporting** - BitLocker Manager helps provide extensive auditing and reporting capabilities to easily demonstrate that systems are encrypted. It helps provide compliance and audit managers all the information they need, when they need it, with less work. It provides audit trail, compliance and system metric reports, helping to define and facilitate regulatory requirements.



Beyond BitLocker Manager

BitLocker Manager is one part of a complete and flexible security solution—Dell Data Protection | Encryption. Together with Dell Data Protection | Encryption Enterprise Edition, which includes software based Data Centric Encryption and hardware-based Full Volume Encryption, as well as External Media Encryption and BitLocker Manager, can quickly and easily secure critical business data on desktops, laptops, USB thumb drives, external storage devices and optical media.¹ Encryption across your organization and infrastructure can help overcome security challenges.

Each offering is accessible from a single console—enabling IT and end users to get more done, while giving them the assurance that their data is protected.

Improve your data security today

BitLocker Manager can help simplify protection for your valuable data. It's just one more way to give you the power to do more. For more information, visit Dell.com/Encryption.

Technical Specifications

BitLocker Manager requires Dell Data Protection | Encryption Management Console

Operating systems supported:

Microsoft Windows 7

- Enterprise
- Ultimate

Microsoft Windows Server® 2008 R2

- Standard Edition
- Enterprise Edition

¹ Full Volume Encryption expected availability later this year