

Dell Data Protection | Encryption

**Enterprise Edition
Administrator Guide**

DDP|E Encryption Client, SED, Advanced Authentication,
BitLocker Manager, and Cloud Edition



© 2014 Dell Inc.

Registered trademarks and trademarks used in the DDP|E, DDP|ST, and DDP|CE suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen Tec® and Eikon® are registered trademarks of Authen Tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloudSM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecurID® are registered trademarks of EMC Corporation. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc.

This product uses parts of the 7-Zip program. The source code can be found at www.7-zip.org. Licensing is under the GNU LGPL license + unRAR restrictions (www.7-zip.org/license.txt).

2014-08

Protected by one or more U.S. Patents, including: Number 7665125; Number 7437752; and Number 7665118.

Information in this document is subject to change without notice.

Contents

- Introduction 11

- Requirements 13
 - Encryption Client 13

 - SED Client 17

 - Advanced Authentication Client 19

 - BitLocker Manager Client 21

 - Cloud Edition Client 22

 - Interoperability 25

- Pre-Installation Configuration to Enable DDP|HCA 27
 - Upgrade Legacy HCA Computers 27
 - Requirements 27
 - Upgrade Legacy HCA Computers 27

 - DDP|HCA Pre-Installation BIOS Configuration 29

 - Reset System Password 30

- Pre-Installation Configuration to Set Up a BitLocker PBA Partition 31

- Set GPO on Domain Controller to Enable Entitlements 33

Extract the Child Installers from the Master Installer	37
Commonly Used Scenarios	39
DDP E Client and Advanced Authentication	40
SED Client (including Advanced Authentication) and External Media Edition	41
SED Client (including Advanced Authentication), External Media Edition, and Cloud Edition	42
DDP E Client and Cloud Edition	44
BitLocker Manager and External Media Edition	45
BitLocker Manager, External Media Edition, and Cloud Edition	45
SED Client (including Advanced Authentication), DDP E Client, and Cloud Edition	46
DDP E Client and Advanced Authentication for Computers with HCA	48
Section I. Dell Data Protection Installer (Master Installer).	51
Dell Data Protection Master Installer	53
Install DDP E Interactively	54
Install DDP E Using the Command Line	59
Uninstallation Process	60

Section II.	Drivers	61
	Drivers Installation Tasks	63
	Install Drivers	63
	Command Line Installation	63
Section III.	DDP E Encryption Client	65
	Encryption Client Installation Tasks	67
	Best Practices.	67
	Install Encryption Client.	67
	Command Line Installation	68
	Install External Media Edition (EME)	69
	Convert External Media Edition to Enterprise Edition	70
	Create a Custom Transform File	70
	Encryption Client Uninstallation and Decryption Tasks	73
	Best Practices.	73
	Prerequisites	73
	Uninstall Encryption Client.	74
	Command Line Uninstallation	74
	Uninstall External Media Edition.	76
	How to Create an Encryption Removal Agent Log File (Optional).	77
	Check Encryption Removal Agent Status.	77
	Encryption Client Data Recovery.	79
	Prerequisites	79
	Retrieve the Recovery Bundle.	79
	Recover Data	79

Troubleshooting HCA Recovery	83
Check the Recovery Log File	83
When Escrow Cannot Be Completed during the WinPE Recovery (HCA)	83
Reset TPM Security (HCA)	83
Recover User Access to a Computer Equipped with HCA	84
Self-Recovery	84
Recover Access using Challenge/Response Codes.	86
Assisted Recovery.	86
Configure Dell Key Server	87
Windows Service Instructions	87
Key Server Config File Instructions	87
Sample Configuration File	88
Windows Service Instructions	88
Remote Management Console Instructions	89
Use WSScan	91
Section IV. SED Management and Advanced Authentication	93
SED Management and Advanced Authentication Installation Tasks	95
Best Practices.	95
Install SED Management and Advanced Authentication.	95
Command Line Installation	96
SED and Advanced Authentication Deactivation and Uninstallation Tasks	99
Prerequisites	99
Deactivate the PBA	99

Uninstall SED Client	100
Command Line Uninstallation	100
SED and OS Recovery	103
Self-Recovery, OS Logon	103
Self-Recovery, PBA	106
Assisted Recovery, PBA	108
Prerequisites	108
Retrieve the Recovery Bundle	108
How to Turn Off Manager SSL Trust Validation	109
How to Use the Initial Access Code Policy	111
How to Create a PBA Log File for Troubleshooting	112
Section V. User Experience - Credential Management and Authentication Applications	113
Configure Credentials in the Security Console	115
Use the Authentication Applications.	123
Credentials.	124
Enrollment Status	124
Backup and Restore	126
Back up Data	127
Restore Data	129
Password Manager	131
Website and Application Logon Training	131
Add Logon	132
Icon Context Menu	134
Web Domain Support	135

	Logging on to Trained Logon Screens	135
	Filling in with Windows Credentials	136
	Use Old Password	137
	Password Change	138
	Password Manager Page.	139
	Settings Page.	141
Section VI.	BitLocker Manager	143
	BitLocker Manager Installation Tasks.	145
	Best Practices.	145
	Install BitLocker Manager	145
	Command Line Installation	145
	BitLocker Manager Uninstallation Tasks.	147
	Prerequisites	147
	Uninstall BitLocker Manager	147
	Command Line Uninstallation	147
	BitLocker Manager Recovery	149
	Recover Data	149
	How to Turn Off Manager SSL Trust Validation	151
Section VII.	Cloud Edition	153
	Cloud Edition Installation Tasks.	155
	DDP Server Tasks	155
	Configure DDP Enterprise Server - VE for Cloud Edition	155
	Configure Dell Enterprise Server for Cloud Edition	155
	Allow/Deny Users on Whitelist /Blacklist.	156

Use Dropbox for Business	158
Run Reports.	160
Provide Temporary Folder Management Rights	160
Update Cloud Edition Policy	160
Client Tasks	161
Before Installing	161
Best Practices	161
Install Cloud Edition	161
Notify End Users	162
Activate Cloud Edition and Install a Cloud Sync Client	162
Cloud Edition Uninstallation Tasks	163
Prerequisites	163
Remove Protected Files.	163
Dropbox	163
Box.	164
OneDrive	164
Uninstall Cloud Edition	164
Command Line Uninstallation	164
Section VIII. User Experience - Cloud Edition	167
Cloud Edition Activation and User Experience	169
Activate Cloud Edition.	169
Install a Cloud Sync Client	169
Authenticate Dropbox for Business	170
Sync Folders.	170
Dropbox for Business	170
Box.	171
OneDrive	171
Work with Folders and Files	171
Cloud Storage Provider Help.	171

Pre-existing Folders with Unencrypted Files	171
Access a Cloud Storage Provider	172
Dropbox for Business	173
Connect Cloud Edition and Dropbox.	173
Use Dropbox for Business Context Menu	173
Use Business and Personal Dropbox Accounts.	173
Understand the Cloud Edition System Tray Menu Items	174
Details Screen	174
Cloud Edition Manage Folders Menu	175
Using Cloud Edition with iOS or Android	176
Prerequisite.	176
Cloud Edition on an iOS device.	176
Cloud Edition on an Android device.	176
Share Files With External Users	177
Administrator Tasks	177
External User Tasks	177
Cloud Edition Frequently Asked Questions (FAQs)	178
Administrator FAQs	178
Folder Management FAQs	179
Dropbox FAQs	180
Box Sync Client FAQs	180
Miscellaneous FAQs.	181
Appendix A Change Secure Boot/UEFI to Legacy Boot Mode in BIOS	183
Glossary	185