

Dell Data Protection | Encryption

**Managed Migration Utility**

**Quick Start Guide**

**and**

**User Guide**



---

© 2015 Dell Inc.

Registered trademarks and trademarks used in the DDP|E, DDP|ESS, 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. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. 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. Dropbox<sup>SM</sup> 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 Store<sup>SM</sup>, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud<sup>SM</sup>, 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](http://www.7-zip.org). Licensing is under the GNU LGPL license + unRAR restrictions ([www.7-zip.org/license.txt](http://www.7-zip.org/license.txt)).

2015-03

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

- DDP | Managed Migration Utility Interactive Mode ..... 5
  - Requirements** ..... 5
  - Interactive Mode** ..... 5
  
- Post-Migration ..... 9
  
- Set Forensic Administrator Privileges ..... 11
  
- Glossary ..... 13



# DDP | Managed Migration Utility Interactive Mode

The Managed Migration Utility converts [Dell Data Protection | Personal Edition](#) to [Dell Data Protection | Enterprise Edition](#), a comprehensive, centrally managed encryption solution that provides security based on users, groups, and devices.

## Requirements

- The administrator performing the migration must be a domain administrator with Forensic Administrator rights on the Dell Enterprise Server and Administrator rights on the local computer. For more information about setting Forensic Administrator rights, see [Set Forensic Administrator Privileges](#).
- The Managed Migration Utility can be run only on the local computer to be migrated. The computer must have network connectivity and access to a Dell Enterprise Server v8.5 or later.
- Dell Data Protection | Personal Edition v8.3 or later must be installed on the computer to be migrated.

**NOTE:** Dell Data Protection | Personal Edition v8.4.1 or later is required if either of these conditions exist:

- The user is not a member of a domain.
- Hardware Crypto Accelerator (HCA) is present on the computer.

- Before beginning migration, for non-domain users, the following registry key must be set on the client computer:  
[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]  
AllowNonDomainActivations=REG\_DWORD:1
- Before beginning migration, if Security Tools is installed on the client computer, and a self-signed certificate is used on DDP Enterprise Server - VE, SSL trust validation must be disabled on the client computer. On the VE Server, SSL trust validation is disabled by default.  
On the client computer, add the following registry entry:  
[HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]  
DisableSSLCertTrust=REG\_DWORD (32-bit):1

## Interactive Mode

To convert Personal Edition to Enterprise Edition using the interactive mode, follow the steps below.

- 1 Copy **Dell.Assimilation.exe** and its supporting files listed below to the computer to be migrated to Enterprise Edition. The Managed Migration Utility requires that the following files are stored in the same folder on the local computer:

Dell.Assimilation.exe  
CmgAssimilationDll.dll  
CmgCryptoLib.dll  
CmgCryptoLib.mac

- 2 Double-click **Dell.Assimilation.exe** to launch the Managed Migration Utility.

**DDP | Personal Edition**

Encryption Administrator Password:

Backup File:

**DDP | Enterprise Management**

Server Administrator Username:

Server Administrator Password:

Dell Enterprise Server Name:

Dell Security Server URL:

Dell Migration Server URL:

START CANCEL

Dell Data Protection | Managed Migration Utility v2.0

- 3 Enter the following information about **Dell Data Protection | Personal Edition**:  
**Encryption Administrator Password** - Encryption Administrator Password for the [LSARecover backup file](#).  
**Backup file** (will auto-populate if available) - Path to LSARecover backup file.
- 4 Enter the following information about **Dell Data Protection | Enterprise Management**:  
**Server Administrator Username** - Username of the Admin user authorized to run the Managed Migration Utility. Must have Forensic Administrator privileges on the Dell Enterprise Server.  
**Server Administrator Password** - Domain password of the Admin user running the Managed Migration Utility.  
**Dell Enterprise Server Name** - The fully qualified domain name of the Dell Enterprise Server. For example: server.domain.com.  
**Dell Security Server URL** - Specify the URL of the Dell Security Server that the endpoint will activate against upon reboot. For example: <https://server.domain.com:8443/xapi/>  
**Dell Migration Server URL** - The Migration Server is a component of the Dell Security Server. Specify the URL of the Dell Migration Server/Dell Security Server. For example: <https://server.domain.com:8443/assimilation/xmlrpc/>

- 5 Click **Start**.
- 6 When prompted to reboot the computer, click **Restart**.





# Post-Migration

After the Dell Managed Migration Utility has completed its tasks, the computer reboots.

Upon reboot, the endpoint attempts to activate each user as they log in. The sequence in which users log in is not important.

Upon successful login, the endpoint is managed by the Dell Enterprise Server, and the policies that were in effect with Personal Edition are overridden by Enterprise Edition policies.

Migration events are logged in C:\ProgramData\Dell\Dell Data Protection and in C:\ProgramData\Dell\Dell Data Protection\Encryption\CmgAssimilation.log.

Identical key material from Personal Edition is used for Enterprise Edition. The Dell Enterprise Server polls the endpoint as it normally would for policy and inventory. The [Dell Remote Management Console](#) displays more information about the endpoint after it receives an inventory, as with any activation.

If migration fails, you receive a notification of the failure, and the migration is rolled back to Personal Edition. At this point, you will need to manually upgrade to Enterprise Edition by decrypting and uninstalling Personal Edition, then completing a fresh installation of Enterprise Edition.

For uninstallation of Personal Edition, see the *Dell Data Protection / Personal Edition Installation Guide* for instructions.

For installation of Enterprise Edition, see the *Dell Data Protection / Enterprise Edition Administrator Guide* for instructions.

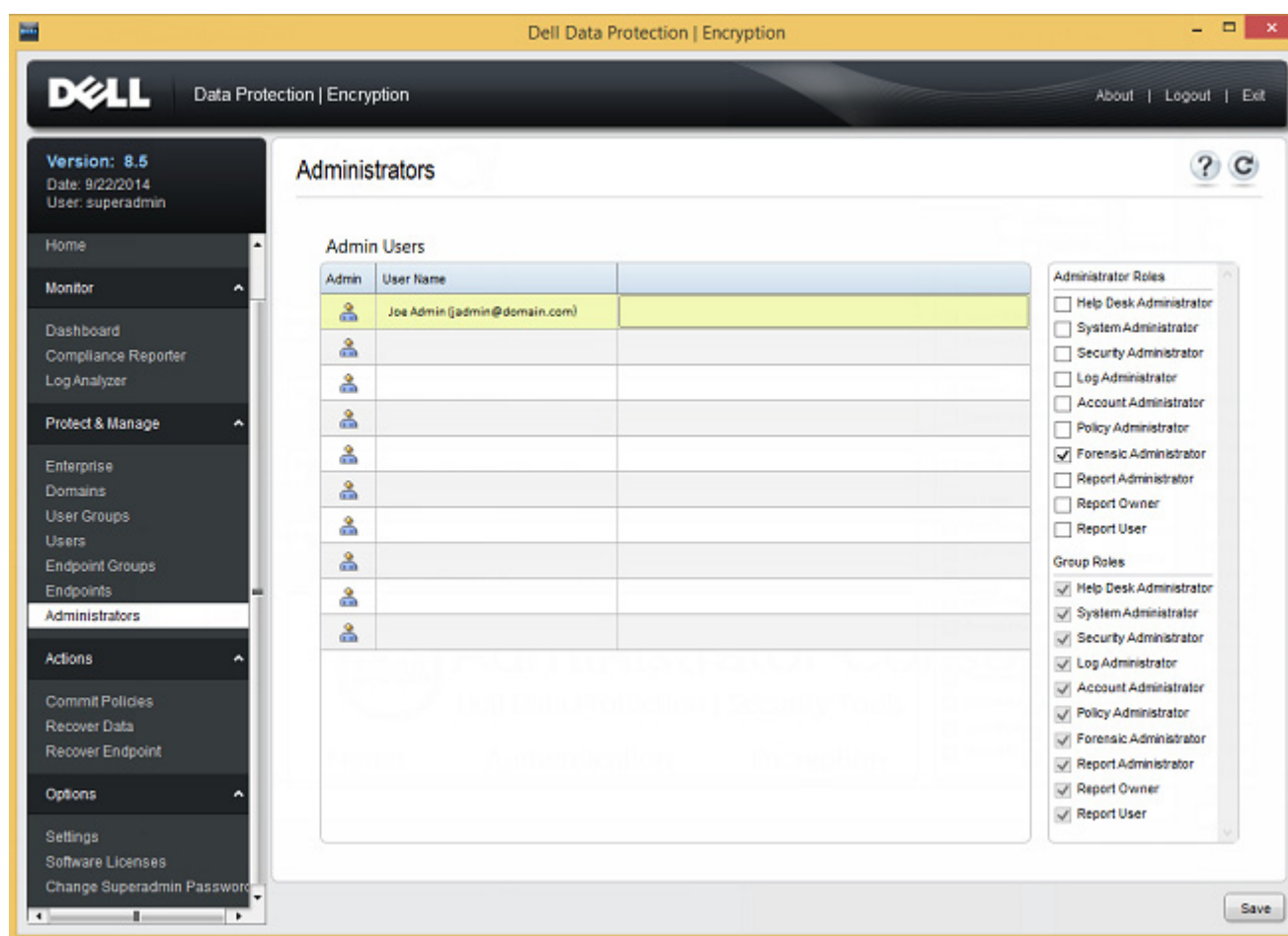


## Set Forensic Administrator Privileges










To set Forensic Administrator privileges on the Dell Enterprise Server, follow these steps:

- 1 Log on to the Dell Remote Management Console.
- 2 In the left pane, under Protect & Manage, select **Administrators**.
- 3 In the list of Admin Users, select the administrator to have Forensic Administrator privileges.

Selecting the administrator highlights the row.



The screenshot shows the Dell Data Protection | Encryption console interface. The left sidebar contains a navigation menu with categories like Home, Monitor, Dashboard, Compliance Reporter, Log Analyzer, Protect & Manage, Enterprise, Domains, User Groups, Users, Endpoint Groups, Endpoints, Administrators, Actions, Options, Settings, Software Licenses, and Change Superadmin Password. The main content area is titled 'Administrators' and features a table of 'Admin Users'. The first row is highlighted in yellow and contains the user 'Joe Admin (jadmin@domain.com)'. To the right of the table is a list of 'Administrator Roles' with checkboxes. The 'Forensic Administrator' role is checked, along with several other roles. A 'Save' button is located at the bottom right of the console.

Admin	User Name
	Joe Admin (jadmin@domain.com)
	
	
	
	
	
	
	
	

**Administrator Roles**

- Help Desk Administrator
- System Administrator
- Security Administrator
- Log Administrator
- Account Administrator
- Policy Administrator
- Forensic Administrator
- Report Administrator
- Report Owner
- Report User

**Group Roles**

- Help Desk Administrator
- System Administrator
- Security Administrator
- Log Administrator
- Account Administrator
- Policy Administrator
- Forensic Administrator
- Report Administrator
- Report Owner
- Report User

- 4 In the right pane, under Administrator Roles, select **Forensic Administrator**.
- 5 Click **Save**.



# Glossary

Dell Data Protection | Enterprise Edition - The centrally managed Encryption Client that is deployed enterprise-wide.

Dell Data Protection | Personal Edition - The locally managed Encryption Client. Central management is not available.

Dell Migration Server - The Dell Migration Server is the component of the Dell Enterprise Server that is used to transform Dell Data Protection | Personal Edition clients to Dell Data Protection | Enterprise Edition clients.

Dell Remote Management Console - The administrative console for the entire enterprise deployment. The Dell Remote Management Console is one component of the Dell Enterprise Server.

Dell Security Server - The Dell Security Server is used for client activation.

Encryption Administrator Password (EAP) - The EAP is an administrative password that is unique to each computer. Most configuration changes require this password. This password is also the same password that is required if you have to use your LSARecovery\_[hostname].exe file to recover your data.

LSARecovery backup file - The backed up encryption keys are wrapped in an application named LSARecovery\_[hostname].exe.







0XXXXXA0X