

Dell Encryption

System Requirements v10.0



Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2012-2018 Dell Inc. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. Registered trademarks and trademarks used in the Dell Encryption, Endpoint Security Suite Enterprise, and Data Guardian suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Cylance®, CylancePROTECT, and the Cylance logo are registered trademarks of Cylance, Inc. in the U.S. and other countries. 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®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, 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™, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, App StoreSM, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®, and iPod nano®, Macintosh®, and Safari® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. 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. 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. 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. Bing® is a registered trademark of Microsoft Inc. Ask® is a registered trademark of IAC Publishing, LLC. Other names may be trademarks of their respective owners.

System Requirements v10.0

2018 - 08

Rev. A01

Contents

1 Introduction.....	4
Contact Dell ProSupport.....	4
2 Requirements.....	5
All Clients.....	5
All Clients - Prerequisites.....	5
All Clients - Hardware.....	5
All Clients - Localization.....	6
Encryption Client.....	6
Encryption Client Prerequisites.....	7
Encryption Client Hardware.....	7
Encryption Client Operating Systems.....	7
Encryption External Media Operating Systems.....	7
Server Encryption Client.....	8
Server Encryption Client Hardware.....	9
Server Encryption Client Operating Systems.....	9
Encryption External Media Operating Systems.....	10

Introduction

This document lists Dell Encryption requirements.

To access all Dell Encryption documentation, see www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals.

Contact Dell ProSupport

Call 877-459-7304, extension 4310039 for 24x7 phone support for your Dell product.

Additionally, online support for Dell products is available at dell.com/support. Online support includes drivers, manuals, technical advisories, FAQs, and emerging issues.

Be sure to help us quickly connect you to the right technical expert by having your Service Tag or Express Service Code available when you call.

For phone numbers outside of the United States, see [Dell ProSupport International Phone Numbers](#).

Requirements

All Clients

These requirements apply to all clients. Requirements listed in other sections apply to specific clients.

- IT best practices should be followed during deployment. This includes, but is not limited to, controlled test environments for initial tests, and staggered deployments to users.
- The user account performing the installation/upgrade/uninstallation must be a local or domain administrator user, which can be temporarily assigned by a deployment tool such as Microsoft SMS or Dell KACE. A non-administrator user that has elevated privileges is not supported.
- Back up all important data before beginning installation/uninstallation.
- Do not make changes to the computer, including inserting or removing external (USB) drives during installation.
- Ensure that outbound port 443 is available to communicate with the Security Management Server/Security Management Server Virtual if your master installer clients will be entitled using Dell Digital Delivery (DDD). The entitlement functionality will not work if port 443 is blocked (for any reason). DDD is not used if installing using the child installers.
- Be sure to periodically check www.dell.com/support for the most current documentation and Technical Advisories.

All Clients - Prerequisites

- Microsoft .Net Framework 4.5.2 (or later) is required for the master installer and child installer clients. The installer *does not* install the Microsoft .Net Framework component.

All computers shipped from the Dell factory are pre-installed with the full version of Microsoft .Net Framework 4.5.2 (or later). However, if you are not installing on Dell hardware or are upgrading the client on older Dell hardware, you should verify which version of Microsoft .Net is installed and update the version **prior to installing the client** to prevent installation/upgrade failures. To verify the version of Microsoft .Net installed, follow these instructions on the computer targeted for installation: [http://msdn.microsoft.com/en-us/library/hh925568\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx). To install Microsoft .Net Framework 4.5.2, go to <https://www.microsoft.com/en-us/download/details.aspx?id=42643>.

- Drivers and firmware for ControlVault, fingerprint readers and smart cards (as shown below) are not included in the master installer or child installer executable files. The drivers and firmware must be kept up-to-date, and can be downloaded from <http://www.dell.com/support> and selecting your computer model. Download the appropriate drivers and firmware based on your authentication hardware.
 - ControlVault
 - NEXT Biometrics Fingerprint Driver
 - Validity Fingerprint Reader 495 Driver
 - O2Micro Smart Card Driver

All Clients - Hardware

- The following table details supported computer hardware.

Hardware

- Intel Pentium or AMD Processor
- 110 MB of available disk space

Hardware

- 512MB RAM

NOTE: Additional free disk space is required to encrypt the files on the endpoint. This size varies based on policies and size of drive.

All Clients - Localization

- The Encryption and BitLocker Manager clients are Multilingual User Interface (MUI) compliant and are localized in the following languages.

Language Support

- | | |
|----------------|--|
| – EN - English | – JA - Japanese |
| – ES - Spanish | – KO - Korean |
| – FR - French | – PT-BR - Portuguese, Brazilian |
| – IT - Italian | – PT-PT - Portuguese, Portugal (Iberian) |
| – DE - German | |

Encryption Client

- The client computer must have network connectivity to activate.
- To reduce initial encryption time, run the Windows Disk Cleanup Wizard to remove temporary files and any other unnecessary data.
- Turn off sleep mode during the initial encryption sweep to prevent an unattended computer from going to sleep. Encryption cannot occur on a sleeping computer (nor can decryption).
- The Encryption client does not support dual boot configurations since it is possible to encrypt system files of the other operating system, which would interfere with its operation.
- The master installer does not support upgrades from pre-v8.0 components. Extract the child installers from the master installer and upgrade the component individually.
- The Encryption client now supports Audit Mode. Audit Mode allows administrators to deploy the Encryption client as part of the corporate image, rather than using a third-party SCCM or similar solutions to deploy the Encryption client. For instructions about how to install the Encryption client in a corporate image, see <http://www.dell.com/support/article/us/en/19/SLN304039>.
- The Encryption client has been tested and is compatible with McAfee, the Symantec client, Kaspersky, and MalwareBytes. Hard-coded exclusions are in place in for these anti-virus providers to prevent incompatibilities between anti-virus scanning and encryption. The Encryption client has also been tested with the Microsoft Enhanced Mitigation Experience Toolkit.

If your organization uses an anti-virus provider that is not listed, see <http://www.dell.com/support/article/us/en/19/SLN288353> or [Contact Dell ProSupport](#) for help.

- The TPM is used for sealing the GPK. Therefore, if running the Encryption client, clear the TPM in the BIOS before installing a new operating system on the client computer.
- In-place operating system upgrade is not supported with the Encryption client installed. Uninstall and decrypt the Encryption client, upgrade to the new operating system, and then re-install the Encryption client.

Additionally, operating system re-install is not supported. To re-install the operating system, perform a backup of the target computer, wipe the computer, install the operating system, then recover the encrypted data following established recovery procedures.

Encryption Client Prerequisites

- The master installer installs Microsoft Visual C++ 2012 Update 4 if not already installed on the computer. **When using the child installer**, you must install this component before installing the Encryption client.

Prerequisite

- Visual C++ 2012 Update 4 or later Redistributable Package (x86 and x64)
- Visual C++ 2015 Update 3 or later Redistributable Package (x86 and x64)

Encryption Client Hardware

- The following table details supported hardware.

Optional Embedded Hardware

- TPM 1.2 or 2.0

Encryption Client Operating Systems

- The following table details supported operating systems.

Windows Operating Systems (32- and 64-bit)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 with Application Compatibility template (hardware encryption is not supported)
- Windows 8: Enterprise, Pro
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (hardware encryption is not supported)
- Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) through Version 1803 (April 2018 Update/Redstone 4)
- VMware Workstation 12.5 and higher



NOTE:

UEFI is mode is not supported on Windows 7, Windows Embedded Standard 7, or Windows Embedded 8.1 Industry Enterprise.

Encryption External Media Operating Systems

- The following table details the operating systems supported when accessing media protected by Encryption External Media.



NOTE:

External media must have approximately 55 MB available plus open space on the media that is equal to the largest file to be encrypted to host Encryption External Media.

Windows Operating Systems Supported to Access Encryption External Media-Protected Media (32- and 64-bit)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro, Consumer

Windows Operating Systems Supported to Access Encryption External Media-Protected Media (32- and 64-bit)

- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) through Version 1803 (April 2018 Update/Redstone 4)

Mac Operating Systems Supported to Access Encryption External Media-Protected Media (64-bit kernels)

- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.4 and 10.12.5
- macOS High Sierra 10.13.5 - 10.13.6

Server Encryption Client

Server Encryption is intended for use on computers running in server mode, particularly file servers.

- Server Encryption is compatible only with Encryption Enterprise and Endpoint Security Suite Enterprise.
- Server Encryption provides the following:
 - Software encryption
 - Removable media encryption
 - Port control

NOTE:

The server must support port controls.

Server Port Control System policies affect removable media on protected servers, for example, by controlling access and usage of the server's USB ports by USB devices. USB port policy applies to external USB ports. Internal USB port functionality is not affected by USB port policy. If USB port policy is disabled, the client USB keyboard and mouse do not function and the user cannot use the computer unless a Remote Desktop Connection is set up before the policy is applied.

Server Encryption is for use on:

- File servers with local drives
- Virtual Machine (VM) guests running a Server operating system or non-Server operating system as a simple file server
- Supported configurations:
 - Servers equipped with RAID 5 or 10 drives; RAID 0 (striping) and RAID 1 (mirroring) are supported independent of each other.
 - Servers equipped with Multi TB RAID drives
 - Servers equipped with drives that can be changed out without shutting down the computer
 - Server Encryption is validated against industry-leading antivirus providers.. Hard-coded exclusions are in place for these anti-virus providers to prevent incompatibilities between anti-virus scanning and encryption. If your organization uses an anti-virus provider that is not listed, see KB article [SLN298707](#) or [contact Dell ProSupport](#) for help.

Not Supported

Server Encryption is not for use on:

- Security Management Servers/Security Management Server Virtuals or servers running databases for Security Management Servers/Security Management Server Virtual.
- Server Encryption is not compatible with Encryption Personal.
- Server Encryption is not supported with SED Management or BitLocker Manager client.
- Server Encryption is not supported on servers that are part of distributed file systems (DFS).
- Migration to or from Server Encryption is not supported. Upgrades from Encryption External Media to Server Encryption require that the previous product or products be uninstalled completely before installing Server Encryption.

- VM hosts (A VM Host typically contains multiple VM guests.)
- Domain Controllers
- Exchange Servers
- Servers hosting databases (SQL, Sybase, SharePoint, Oracle, MySQL, Exchange, etc.)
- Servers using any of the following technologies:
 - Resilient file systems
 - Fluid file systems
 - Microsoft storage spaces
 - SAN/NAS network storage solutions
 - iSCSI connected devices
 - Deduplication software
 - Hardware deduplication
 - Split RAIDs (multiple volumes across a single RAID)
 - SED drives (RAIDs and NON-RAID)
 - Auto-logon (Windows 7, 8/8.1) for kiosks
 - Microsoft Storage Server 2012
- Server Encryption does not support dual boot configurations since it is possible to encrypt system files of the other operating system, which would interfere with its operation.
- In-place operating system re-installs are not supported. To re-install the operating system, perform a backup of the target computer, wipe the computer, install the operating system, then recover the encrypted data by following recovery procedures. For more information about recovering encrypted data, refer to the *Recovery Guide*.

Server Encryption Client Hardware

Minimum hardware requirements must meet the minimum specifications of the operating system.

Server Encryption Client Operating Systems

The following table details supported operating systems.

Operating Systems (32- and 64-bit)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.0: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) through Version 1803 (April 2018 Update/Redstone 4)

Supported Server Operating Systems

- Windows Server 2008 R2 SP1: Standard Edition, Datacenter Edition, Enterprise Edition, Webserver Edition
- Windows Server 2012: Standard Edition, Essentials Edition, Datacenter Edition (Server Core is not supported)
- Windows Server 2012 R2: Standard Edition, Essentials Edition, Datacenter Edition (Server Core is not supported)
- Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition (Server Core is not supported)

Operating Systems Supported with UEFI Mode

- Windows 8: Enterprise, Pro
- Windows 8.1 : Enterprise, Pro

Operating Systems Supported with UEFI Mode

- Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) through Version 1803 (April 2018 Update/Redstone 4)

NOTE:

On a supported UEFI computer, after selecting **Restart** from the main menu, the computer restarts and then displays one of two possible logon screens. The logon screen that displays is determined by differences in computer platform architecture.

Encryption External Media Operating Systems

The following table details the operating systems supported when accessing media protected by Encryption External Media.

NOTE:

External media must have approximately 55MB available plus open space on the media that is equal to the largest file to be encrypted to host Encryption External Media.

Windows Operating Systems Supported to Access Encryption External Media-Protected Media (32- and 64-bit)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 Enterprise, Pro
- Windows 10: Education, Enterprise, Pro Version 1607 (Anniversary Update/Redstone 1) through Version 1803 (April 2018 Update/Redstone 4)

Supported Server Operating Systems

- Windows Server 2012 R2

Mac Operating Systems Supported to Access Encryption External Media-Protected Media (64-bit kernels)

- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6