Dell Encryption

System Requirements v10.2

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.

2019 - 03

Rev. A01

Contents

1

Introduction

To access all Dell Encryption documentation, see dell.com/support.

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.

2

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. 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 Dell Server if your master installer clients will be entitled using Dell Digital Delivery. The entitlement feature does not function if port 443 is blocked (for any reason). Dell Digital Delivery is not used if installing using the child installers.
- Be sure to periodically check dell.com/support for the most current documentation and Technical Advisories.

Prerequisites

- Microsoft .Net Framework 4.5.2 (or later) is required for the master and child installers. 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.
- Drivers and firmware for ControlVault 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 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

Hardware

- The following table details supported computer hardware.

Hardware
– Intel Pentium or AMD Processor
– 110 MB of available disk space
– 512MB RAM

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

Localization

- Encryption and BitLocker Manager are multilingual user interface 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

- 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).
- 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.
- 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.
- Encryption now supports audit mode. Audit mode allows administrators to deploy Encryption as part of a corporate image, rather than using a third-party SCCM or similar solutions for deployment. For instructions about how to install Encryption in a corporate image, see KB article SLN304039.
- Encryption 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. Encryption has also been tested with the Microsoft Enhanced Mitigation Experience Toolkit.

  If your organization uses an anti-virus provider that is not listed, see KB article SLN288353 or Contact Dell ProSupport for help.
- The TPM is used for sealing the General Purpose Key. Therefore, if running Encryption, clear the TPM in the BIOS before installing a new operating system on the client computer.
- In-place operating system upgrade is not supported. To upgrade the operating system, uninstall and decrypt, upgrade to the new operating system, and then re-install Encryption.

  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.

Prerequisites

- The master installer installs Microsoft Visual C++ 2012 Update 4 if not already installed on the target computer. **When using the child installer**, you must install these components before installing clients.

Prerequisite
– Visual C++ 2012 Update 4 or later Redistributable Package (x86 and x64)

Prerequisite

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

Hardware

- The following table details supported hardware.

Optional Embedded Hardware

- TPM 1.2 or 2.0

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
- Windows 8.1: Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro v1607-v1809 (Anniversary Update/Redstone 1 - October 2018 Update/Redstone 5)
- VMware Workstation 12.5 and higher
- **Deferred Activation** includes support for all of the above

Encryption External Media

Operating Systems

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

Windows Operating Systems Supported to Access Encrypted Media (32- and 64-bit)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 with Application Compatibility template
- Windows 8.1: Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro v1607-v1809 (Anniversary Update/Redstone 1 - October 2018 Update/Redstone 5)

Mac Operating Systems Supported to Access Encrypted Media (64-bit kernels)

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14.0 - 10.14.3

Encryption on Server Operating Systems

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

- Encryption on server operating systems is compatible only with Encryption Enterprise and Endpoint Security Suite Enterprise.
- Encryption on server operating systems provides:
  - Software encryption
  - Removable media encryption
  - Port controls

> **NOTE:**
> The server must support port controls.
>
> 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.

Encryption of server operating systems is for use with:

- 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.

Encryption of server operating systems is not for use with:

- Security Management Servers/Security Management Server Virtuals or servers running databases for Security Management Servers/ Security Management Server Virtual.
- Encryption Personal.
- SED management, PBA advanced authentication or BitLocker Manager.
- Servers that are part of distributed file systems (DFS).
- Migration to or from Encryption on a server operating system. Upgrade from External Media Edition to Encryption of server operating systems requires that the previous product is uninstalled completely before installing Encryption on server operating systems.
- 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)
  - SEDs (RAIDs and NON-RAID)
  - Auto-logon (Windows 7, 8/8.1) for kiosks
  - Microsoft Storage Server 2012
- Encryption on a server operating system 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*.

Operating Systems

The following table details supported operating systems.

Operating Systems (32- and 64-bit)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro v1607-v1809 (Anniversary Update/Redstone 1 - October 2018 Update/Redstone 5)

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 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro v1607-v1809 (Anniversary Update/Redstone 1 - October 2018 Update/Redstone 5)

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

- 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.
- The following details the supported operating systems when accessing Dell-protected media:

Windows Operating Systems Supported to Access Encrypted Media (32- and 64-bit)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1 Enterprise, Pro

Windows Operating Systems Supported to Access Encrypted Media (32- and 64-bit)

- Windows 10: Education, Enterprise, Pro v1607-v1809 (Anniversary Update/Redstone 1 - October 2018 Update/Redstone 5)

Supported Server Operating Systems

- Windows Server 2012 R2

Mac Operating Systems Supported to Access Encrypted Media (64-bit kernels)

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14.0 - 10.14.3