



Data Encryption

CA ARCserve® D2D is a new disk-based backup product designed to provide the perfect combination of fast, simple and reliable protection and recovery for all of your business information. You can be confident meeting your SLAs for recovery time with the only product that has Bare Metal Restore to dissimilar hardware and Block-Level infinite incremental snapshots, based on CA'S I2 Technology™, in one package. In addition, CA ARCserve D2D also lets you copy and restore backed-up data from your specified cloud storage location. This set it and forget it solution makes protecting and recovering your data a snap.

CA ARCserve D2D provides encryption protection to the recovery points created by CA ARCserve D2D. This makes data safe from unauthorized access, making it ideal for laptop and workstation protection to external USB devices as well as copying a recovery point into cloud storage. CA ARCserve D2D Encryption password management provides a memory feature so that you do not need to remember encryption passwords when attempting to restore encrypted data. For every encrypted backup, the encryption password will be saved in a password list file.

OVERVIEW

CA ARCserve D2D lets you quickly and easily protect critical business information across your company. Provides the capability to restore files/folders, volumes, applications, and perform bare metal recovery from a single backup.

CA ARCserve D2D data protection uses secure, AES (Advanced Encryption Standard) encryption algorithms to achieve maximum security and privacy of your specified data. CA ARCserve D2D lets you choose one of different encryption options (No Encryption, AES-128, AES-192, and AES-256).

CA ARCserve D2D enables moving backups of any machine to a different machine, and restore data from there, it supports Data Interoperability both ways between CAPI and CNG, data encrypted on Windows XP/2003/Vista/2008 can be decrypted on Windows 7/2008 R2.

BENEFITS

- Provides encryption password management so that you do not need to remember encryption passwords.
- Prevents unauthorized access to your data; users having access to passwords would only be able to access the backup data.
- Supports encryption for both uncompressed backup and compressed backup data.
- Uses secure Advanced Encryption Standard (AES-128, AES-192, and AES-256) encryption algorithms to achieve maximum security and privacy of your specified data.

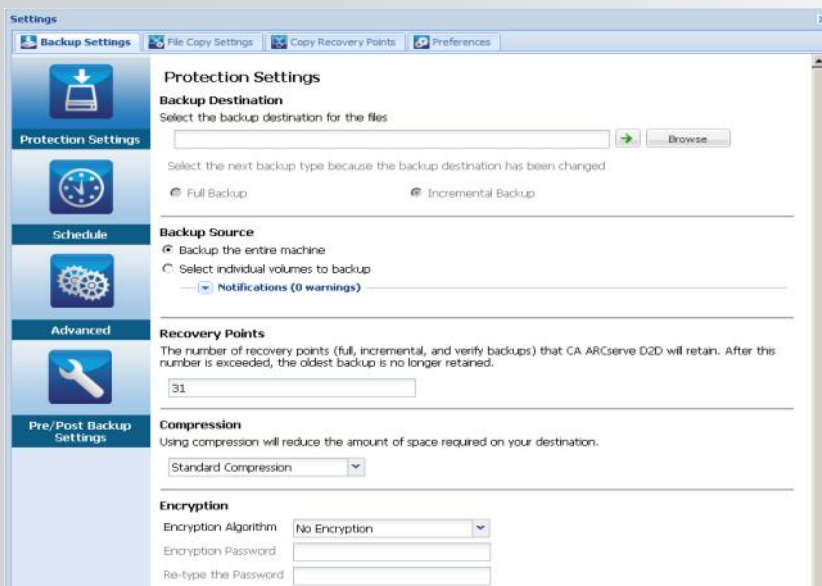
Install / Configure

The CA ARCserve D2D installation is straight forward and wizard-driven. Installation and configuration of CA ARCserve D2D involves the following tasks: Install the Prerequisite Components (if required), Accept the terms of the Licensing Agreement, and follow the prompts and complete all required information on the subsequent dialogs. A reboot of the computer is required before CA ARCserve D2D can be used effectively.

You must configure CA ARCserve D2D backup settings prior to performing your first backup. You can configure CA ARCserve D2D using the web UI Manager. Specify the destination for your backup, desired backup schedule, the number of recovery points, compression level, Encryption level and other settings for your backup jobs. CA ARCserve D2D lets you modify the backup settings at any time from the CA ARCserve D2D home page. Also, CA ARCserve D2D lets you change the Encryption settings at any time, including after several backups of the same data.

How CA ARCserve D2D Encryption Works

CA ARCserve D2D not only lets you perform backup and recovery of your data, but also helps you protect the data from unauthorized access using different encryption levels, you can choose to use the different Encryption options depending on your site requirements. CA ARCserve D2D supports the following encryption options: No Encryption, AES-128, AES-192, and AES-256. If you choose not to encrypt data you can choose the No Encryption option.



CA ARCserve D2D provides encryption password management so that you do not need to remember encryption passwords. CA ARCserve D2D also encrypts the Password and stores it so that you do not have to key in the password if you restore to the same machine. However, if you are restoring onto a different machine you need to provide the password.

CA ARCserve D2D does not require you to enter password if you are attempting to export a recovery point that contains encrypted data and the recovery point belongs to backups performed on the current machine. However, password is always required if you are attempting to

recover encrypted data from an exported recovery point.

CA ARCserve D2D requires you to enter the encryption password to perform Bare Metal Recovery of your machines.

CA ARCserve D2D updates the activity log when encryption is enabled. A message is recorded in the activity log about the encryption algorithm selected for every backup. Also, the activity log is updated to include information about why an incremental or verify backup was converted to a full backup (password change or algorithm change).

Frequently Asked Questions

- Q:** If I change the encryption type or the encryption password and the maximum number of recovery points are then reached, what happens?
- A:** The image consolidation during backups will continue as usual for images with the older password. When the remaining oldest image is the last Full Backup with the old password, that Full Backup will be deleted.
- Q:** If I enter a new encryption password, will the old encryption password be asked for first?
- A:** No. CA ARCserve D2D will immediately apply the new password and no longer requests for the old password.
- Q:** What happens to data which is already encrypted either using Windows Encrypting File System (EFS) or a third-party encryption system?
- A:** For Windows EFS encryption, CA ARCserve D2D will write in encrypted format used in the EFS and BitLocker format. For third-party-encryption, it depends on the technology. If volume encryption is enabled or locked, CA ARCserve D2D will not be able to read it and will generate an error.

Summary

CA ARCserve D2D provides robust data protection that helps secure your business information against a wide range of threats, to help ensure that your data is available, and more importantly, accessible. CA ARCserve D2D provides protection against unauthorized retrieval of data in stored recovery points using the new Encryption feature. CA ARCserve D2D Encryption feature lets you protect recovery points with enhanced AES Standards-based encryption, supports AES 128, AES 192, and AES 256 encryption algorithms.

For more information about the CA ARCserve Family of products, please visit arcserve.com/products or test drive our products at arcserve.com/software-trials.