

DriveLock

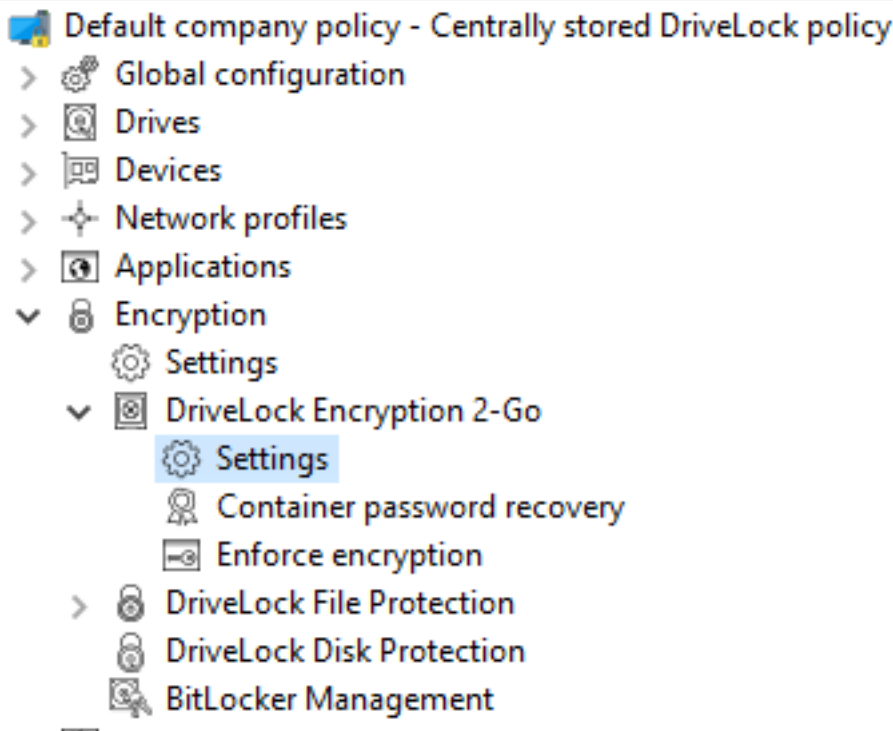
Automatic Encryption to USB Drives

In some scenarios it is important that any USB that is allowed in the organisation is encrypted.


Should there already be data on this device you can have the option to format first or automatically copy the data back onto the now encrypted device.

There are a number of settings that can be applied automatically or enforced. Encryption Strength, Password Strength, Method to delete Securely, Password recovery settings, Encryption user experience, End User restriction

These can be found within the Encryption area of your Policy:







Below is an example of the settings that can be commonly applied within some environments.



Encryption strength settings





These settings determine the encryption algorithms to be used.

-  [Enforcement of FIPS 140-2-validated cryptography](#) (On)
-  [Encryption algorithm to be used for encrypted drives](#) (AES (FIPS-mode))
-  [Password hash algorithm to be used for encrypted drives](#) (SHA-512 (FIPS-mode))
-  [Allow quick-format of encrypted containers](#) (Disabled)

DriveLock

Password strength settings

These settings determine required strength of user passwords.

-  [Minimum required password complexity for encrypted drives](#) (Strong)
-  [Password complexity policy](#) (Minimum 8 characters (with 1 lower case, 1 upper case, 1 numbers, 1 special))
-  [Container access lockout policy](#) (After 3 retries, lock container for 60 minutes)
-  [Encrypted container password saving options](#) (Not configured)



Method to securely delete files




Defines the algorithm to be used for secure deletion of files.

Random data



Password recovery settings

These settings configure the availability and user information for encrypted container password recovery.






-  [Encrypted volume password recovery methods](#) (Offline (Helpdesk), Online (Certificates on client))
-  [User contact information for offline container recovery](#) (Not configured)
-  [Enabled extend functions for "Change password"](#) (Allow removal of administrative password, Allow removal of user password, Allow setting user password if administrative password is present)

DriveLock



Encryption user experience






These settings determine the program options that are available to users.

-  [Context menus available in Windows Explorer](#) (Mount drive, Unmount drive, Change password, Unmount drive, Change password, Recover (enforced encryption), Mount (enforced encryption), Encrypt (enforced encryption), Securely delete, Securely delete, Record encrypted media)
-  [Start menu configuration](#) (Start | Programs | DriveLock Encryption 2-Go)
-  [Available Start menu items](#) (Manage encrypted volumes, Unmount encrypted drive, Change encrypted volume password, Create encrypted volume, Mount encrypted volume, Record encrypted media, Copy DriveLock Mobile Encryption, Recover encrypted volume, Help)
-  [Menu items available from the taskbar icon](#) (Manage encrypted volumes, Unmount encrypted drive, Change encrypted volume password, Create encrypted volume, Mount encrypted volume, Record encrypted media, Copy DriveLock Mobile Encryption, Recover encrypted volume, Help)
-  [Order of menu items in taskbar icon](#) (Manage encrypted volumes, Create encrypted volume, --- (Separator), Mount encrypted volume, Unmount encrypted drive, Change encrypted volume password, Record encrypted media, Recover encrypted volume, --- (Separator), Copy DriveLock Mobile Encryption, Help)
-  [Bring all dialogs to top-most position](#) (Enabled)



Encrypted drives settings

These settings determine how encrypted drives are created and made available to users.






-  [Encrypted drive file system](#) (FAT)
-  [Encrypted drive cluster size](#) (Default)
-  [Available drive letters for mounting encrypted drives](#) (Not configured)
-  [Enforce drive letter when mounting encrypted drives](#) (Not configured)
-  [Restrict size of user created drives](#) (Not configured (200 MB))

DriveLock



End user restrictions

These settings determine what functionality is available for users.

-  [No history for mounted volumes](#) (Not configured (Disabled))
-  [Do not allow creation of Mobile Encryption Disks](#) (Not configured (Disabled))
-  [Only allow encrypted containers created with current DriveLock license](#) (Not configured (Disabled))
-  [Do not allow opening encrypted containers with Mobile Encryption Application](#) (Not configured (Disabled))
-  [Do not automatically upgrade Mobile Encryption Application to newer version during enforced encryption](#) (Not configured (Disabled))

To discuss these options in details please feel free to contact us.

Unique solution ID: #1031

Author: Adam Gurrie

Last update: 2019-10-24 08:08