The cipher command in Windows

The cipher command displays or changes the encryption of folders and files on NTFS volumes. If used without parameters, the cipher command displays the encryption status of the current directory and any files that contain it.

The **cipher** command displays or changes the encryption of folders and files on NTFS volumes. If used without parameters, the **cipher** command displays the encryption status of the current directory and any files that contain it.

For an example of how to use this command, please see the **Example** below.

Cipher command syntax

```
cipher [/e | /d | /c] [/s:] [/b] [/h] [PathName [.]] cipher /k cipher /r: [/smar
```

Parameters

Parameter Description / b Remove if an error occurs. By default, the **cipher** command continues to run even if an error occurs. / c Displays information on the encrypted file. / d Decrypt the specified file or directory. / e Encrypt the specified file or directory. The directory is marked so that the added files are then encrypted. / h Displays files with hidden properties or system. By default, these files are not encrypted or decrypted. / k Create new certificates and keys for use with the Encrypting File System (EFS) files. If the **/ k** parameter is specified, all other parameters will be ignored. / r: [/ smartcard] Create a key and EFS recovery agent certificate, then write them to a **.pfx** file (containing certificates and private keys) and a **.cer** file (containing only certificates). If **/ smartcard** is specified, it will write the recovery key and certificate to the smartcard and no **.pfx** file will be created. / s: Perform the specified operation on all subdirectories in the specified directory. / u [/ n] Find all encrypted files on the local drive (s). If used with the **/ n** parameter **,** no updates are made. If used without **/ n, / u** compare the user's file encryption key or recovery agent key with the current key and update them if they have changed. This parameter only works with **/ n.** / w: Remove data from unused space across the entire drive. If you use the **/ w** parameter **,** all other parameters will be ignored. The specified directory can be placed anywhere on a local drive. If it is a mount point or points to a folder in another drive, the data on that drive will be deleted. / x [: efsfile] [] Back up the EFS keys and certificates to the specified file name. If used with **: efsfile, / xbacks** will back up the user's certificate (s) used to encrypt the file. Otherwise, the EFS certificate and the user's current key will be backed up. / y Displays your current EFS certificate thumbnail on the local computer. / adduser [/ certhash: / certfile:] / rekey Update the encrypted file (s), specify to use the currently configured EFS key. / removeuser / certhash: Delete the user from the specified file (s). *The* provided *hash* **/ certhash** must be the SHA1 hash function of the certificate. /? Show help at the command prompt.

Note

1. If the root directory is not encrypted, an encrypted file can be decrypted when it is modified. Therefore, when you encrypt a file, you should also encrypt the root directory.
2. The administrator can add the contents of the **.cer** file to the EFS recovery policy to create recovery agents for users and then import the **.pfx** file to restore individual files.
3. You can use multiple directory names and wildcards.
4. You must set a space between multiple parameters.

For example

To display the encryption status of each file and subdirectory in the current directory, enter:

```
cipher
```

Encrypted files and folders are marked with **E.** Unencrypted files and folders are marked with **U.** For example, the following output indicates that the current directory and all its content are not currently encrypted:

```
Listing C:UsersMainUserDocuments New files added to this directory will not be en
```

To enable encryption on the **Private** folder used in the previous example, enter:

```
cipher /e private
```

The following output is displayed:

```
Encrypting files in C:UsersMainUserDocuments Private [OK] 1 file(s) [or director
```

The **cipher** command displays the following results:

```
Listing C:UsersMainUserDocuments New files added to this directory will not be en
```

Note that the Private folder is marked as encrypted.

See more:

1. Choice command in Windows
2. Cmstp command in Windows
3. Cmdkey command in Windows

You finished reading the article "**The cipher command in Windows**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.