حفاظت از اطلاعات کول دیسک ها و هارد دیسک های اکسترنال

یکی از سئوالاتی که این روزها در اکثر سایت ها و انجمن های آنلاین مطرح می شود روش های قرار دادن پسورد روی فولدر ها و یا درایو های مختلف برای محافظت از اطلاعات است که در بیشتر موارد با توجه به اینکه در ویندوز، روش مشخص و دوستانه ای برای انجام این کار وجود ندارد کاربران به نرم افزار های جانبی برای محافظت از اطلاعات روی می آورند که با توجه به اینکه اکثر این نرم افزارها فقط در همان سیستمی که نصب شده اند می توانند از اطلاعات محافظت کنند نمی توان به آنها اعتماد کرد.
در این مقاله سعی دارم یکی از متدهای پیشرفته محافظت از اطلاعات را که توسط مایکروسافت در ویندوزهای برپایه NT (ویندور 2000 و جدیدتر) ارائه شده معرفی کنم و روش استفاده از آن را روی هارددیسک های اکسترنال و کول دیسک ها آموزش بدهم.

Microsoft Encryption File System

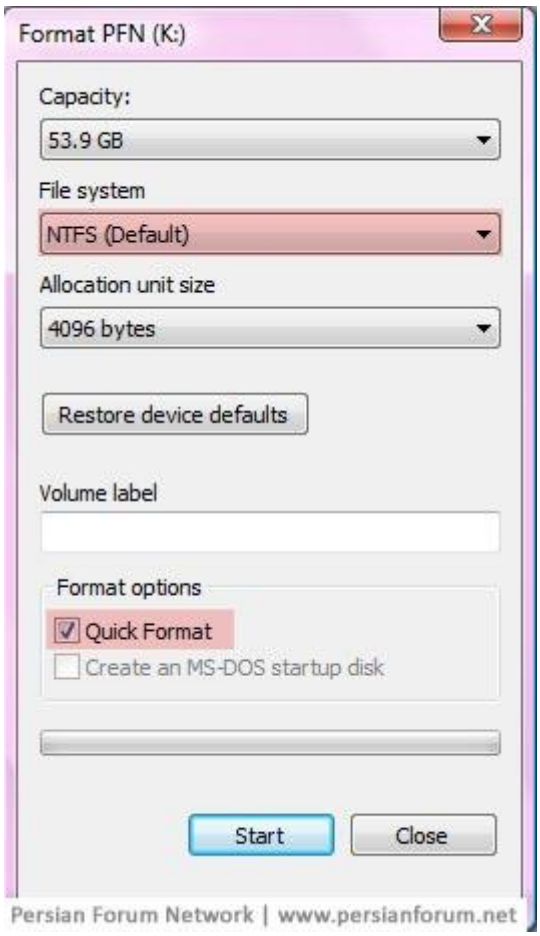
پروسه ی غیرقابل حل و رمز کردن اطلاعات برای جلوگیری از دسترسی های غیرقانونی Encryption نام دارد. برای دسترسی به این اطلاعات رمز شده و رمزگشایی آنها به Key یا کلید نیاز است. تکنولوژی Microsoft Encryption File System یا EFS رمز کردن فایل ها را در فایل سیستم NTFS فراهم می کند. زمانیکه یک فایل یا فولدر را Encrypt می کنید، EFS یک FEK یا File Encryption Key جدید تولید می کند که از اعدادی تصادفی تشکیل شده، سیستم از این عدد و الگوریتم DESX یا Data Extended Standard X (بعد از ویندوز XP SP1 از الگوریتم Advanced Encryption Standard استفاده می شود) برای تولید فایل رمز شده و کپی کردن آن روی هارد دیسک استفاده می کند. سپس FEK را با استفاده از Public Key یا کلید عمومی شما رمز و همراه با فایل رمز شده ذخیره می کند. زمانیکه قصد دارید از فایل رمز شده استفاده کنید سیستم از Private Key یا کلید خصوصی شما استفاده می کند و FEK را رمزگشایی می کند و در مرحله بعد با استفاده از FEK فایل مورد نظر را رمزگشایی می کند. در اولین استفاده از EFS سیستم بصورت خودکار یک گواهینامه همراه با دو کلید عمومی و خصوصی برای کاربر ایجاد می کند و از آنها برای Encryption و Decryption فایل ها استفاده می کند. از ویژگیهای سیستم EFS پنهان بودن مراحل رمز کردن و رمز گشایی فایل ها از دید کاربر است. در صورت نیاز به اطلاعات بیشتر در رابطه با EFS و روش کار آن سئوالات خود را در بخش انجمن های پرشین فروم نتورک (وب سایت منبع اصلی مقاله) مطرح کنید.

قبل از شروع آموزش روش استفاده از EFS و محافظت از اطلاعات، باید مطمئن شوید که فایل سیستم کول دیسک یا درایو مورد نظر شما NTFS است برای این کار در My Computer روی آیکون مربوط به کول دیسک یا درایو مورد نظر خود راست کلیک کنید و بر روی Properties کلیک کنید، در پنجره باز شده داخل

تب General بخش System File را چک کنید، در صورتیکه فایل سیستم NTFS بود نیازی بـه تغییـر نیست و می توانید از EFS استفاده کنید، در غیراینصورت یکی از دو راه زیر را انتخـاب و فایـل سیـستم درایـو مورد نظر خود را به NTFS تغییر دهید.

روش اول : درصورتیکه روی کول دیسک و یا درایو مورد نظر خود اطلاعاتی وجود ندارد و مـی توانیـد آن را فرمـت کنید از این روش استفاده کنید. توجه کنید که برای تبدیل فایل سیستم کول دیسک فقـط مـی توانیـد از ایـن روش استفاده کنید و تنها ویندوز ویستا قابلیت فرمت کردن کول دیـسک هـا را بـا فایـل سیـستم NTFS دارد.

1. روی آیکون درایو و یا کول دیسک مورد نظر خود راست کلیک کنید و بر روی گزینه Format کلیـک کنیـد، در پنجره باز شده (عکس شـماره 1) از بخـش File System گزینـه NTFS را انتخـاب کنیـد و از بخـش Format Options گزینه Quick Format را تیک بزنید و در آخر بر روی کلید Start کلید نمایید.

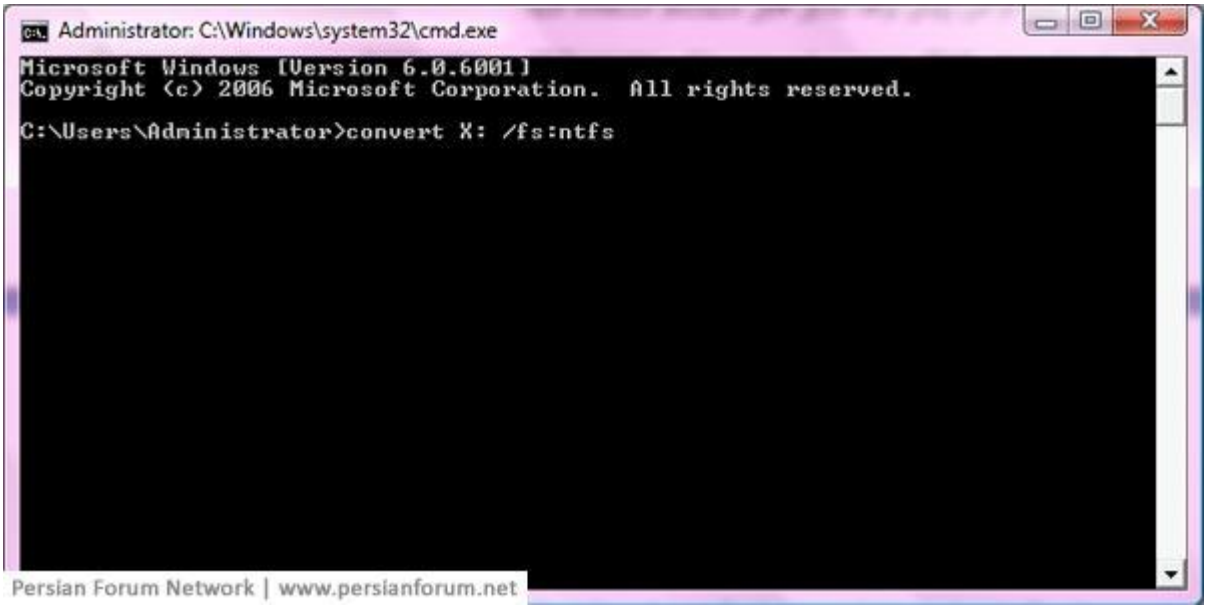


عکس شماره 1

روش دوم : درصورتیکه روی درایو مورد نظر خود فایل و اطلاعات ذخیره کرده اید و نمی توانید از روش اول استفاده کنید از این روش برای تبدیل فایل سیستم استفاده نمایید.

1. ابتدا از منوی Start به ترتیب وارد بخش های All Programs و Accessories شوید و برنامه Command Prompt را اجرا کنید.
2. در پنجره Command Prompt (عکس شماره 2) دستور زیر را تایپ کنید.

convert X: /fs:ntfs



عکس شماره 2

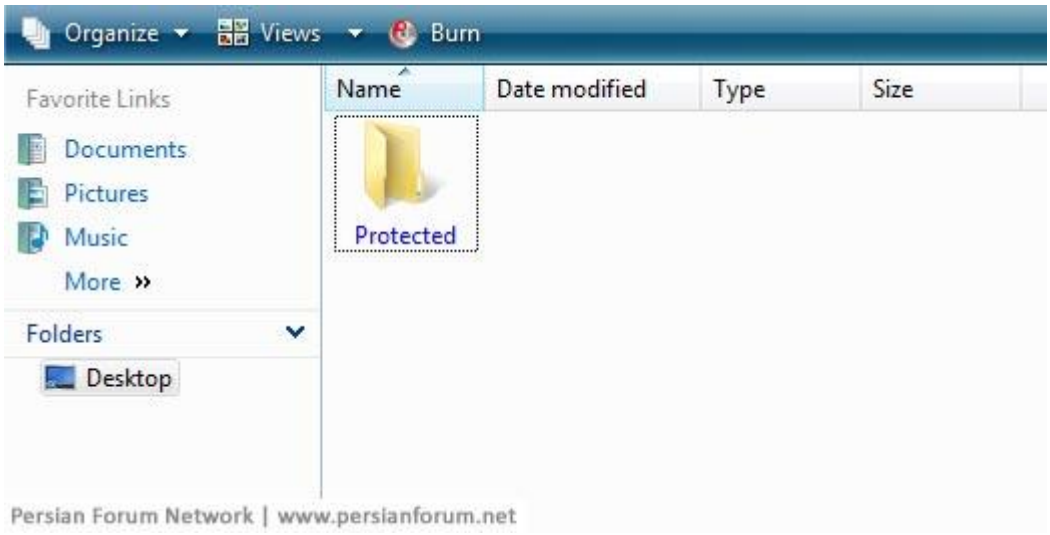
بجای :X نام درایو مورد نظر خود را وارد کنید، برای مثال ممکن است شما قصد تبدیل درایو D کامپیوتر خود را داشته باشید بنابراین باید : D را بجای :X وارد کنید. تمامی برنامه های باز و در حال اجرا را ببندید و این دستور را با زدن کلید Enter اجرا کنید، درصورتیکه در حال تبدیل درایو C هستید سیستم از شما می خواهد که برای ادامه مراحل تبدیل، کامپیوتر را ریست کنید.

بعد از اتمام مراحل تبدیل، درایو و یا کول دیسک را چک کنید و مطمئن شوید که فایل سیستم با موفقیت به NTFS تبدیل شده است.

رمز کردن فایل ها، فولدر ها و محافظت از اطلاعات (Encryption)

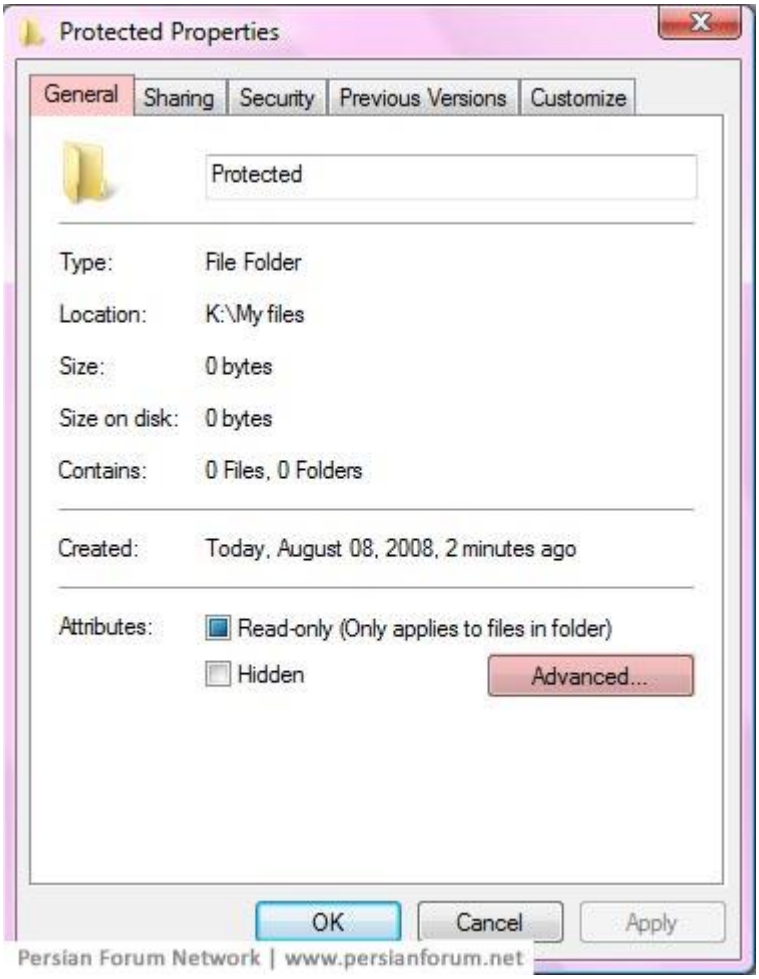
برای Encrypt کردن فایل یا فولدر مورد نظر خود با استفاده از تکنولوژی EFS مایکروسافت از روش زیر استفاده کنید

1. یک فولدر جدید برای قرار دادن فایل های Encrypt شده در درایو و یا کول دیسکی که به NTFS تبدیل شده بسازید. (عکس شماره 3)



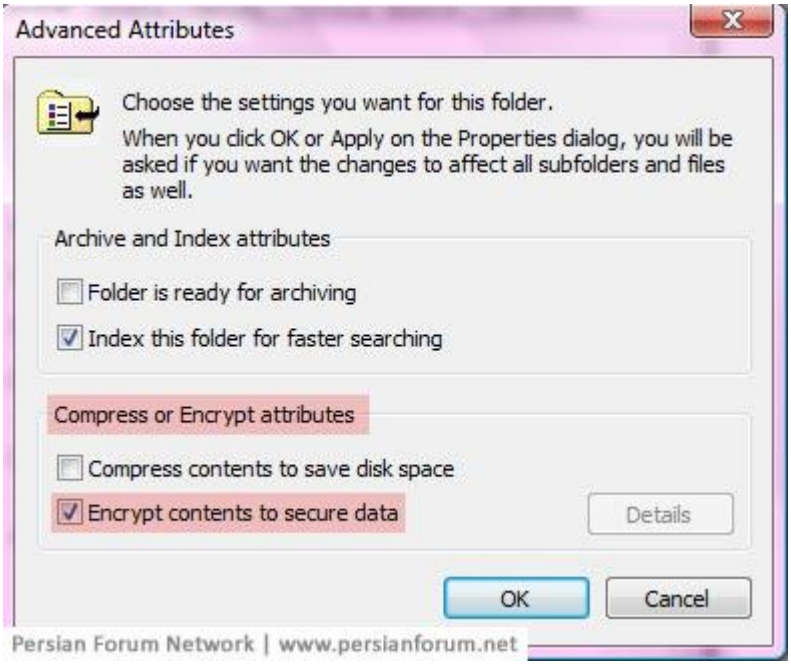
عکس شماره 3

2. روی فولدر راست کلیک کنید و از منوی باز شده روی گزینه Properties کلیک کنید، در پنجره باز شده داخل تب General روی کلید Advanced کلیک کنید. (عکس شماره 4)



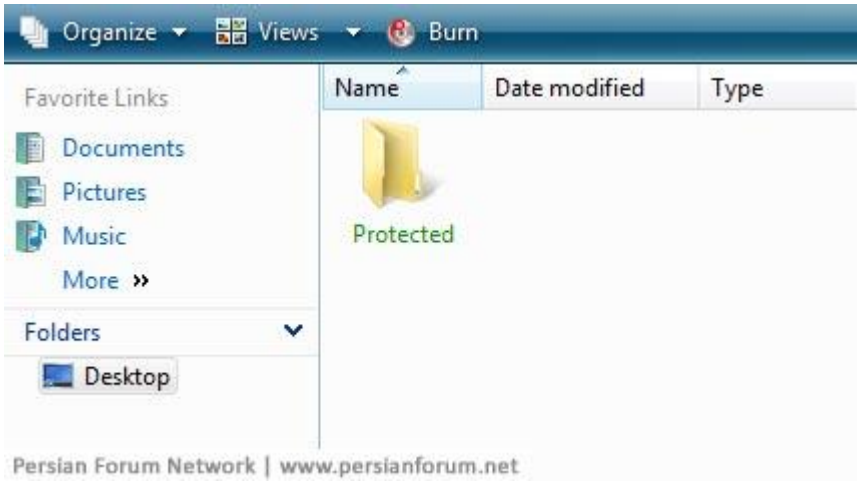
عکس شماره 4

3. در بخش Compress and Encrypt attribute گزینــه Encrypt contents to secure data را تیک بزنید و بر روی کلید OK کلیک کنید (عکس شماره 5) ، همچنین بر روی کلید OK در صــفحه Properties کلیک نمایید.



عکس شماره 5

درحال حاضر فولدر مورد نظر شما Encrypt شده است، ویندوز رنگ فونت نام فولدر را به سبز تغییر مـی دهـد و این نشان می دهد که این فولدر Encrypt شده اسـت (عکـس شـماره 6) (درصـورتیکه در بخـش Folder Option تعیین نشده باشد رنگ فونت تغییر نمی کند).



عکس شماره 6

برای Encrypt کردن فایل ها و فولدر های مورد نظر خود کافیست آنها را داخل این فولـدر کپـی کنیـد. بعـد از

Encrypt کردن فایل ها هیچکس جز شما اجازه دسترسی به این فایل ها را ندارد، می توانید با منتقل کردن فایل ها به کامپیوتری دیگر، آن را امتحان کنید.

رمزگشایی فایل ها و فولدر ها (Decryption)

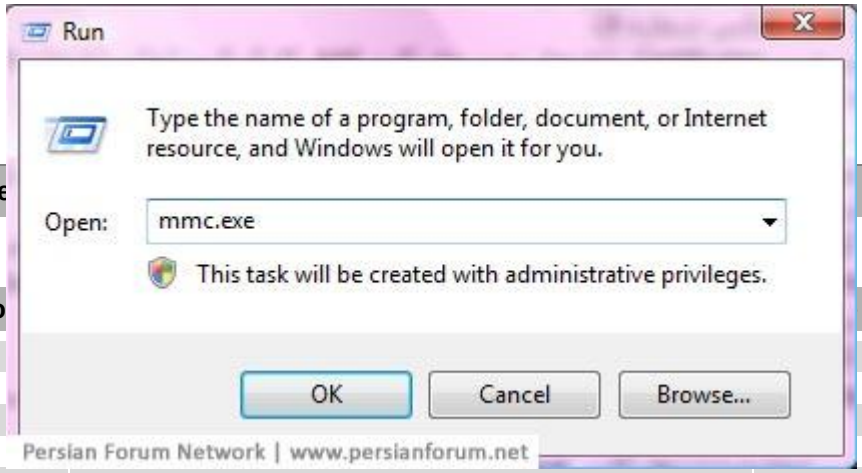
1. روی فولدر و یا فایل مورد نظر خود راست کلیک کنید و از منوی باز شده روی گزینه Properties کلیک کنید، در پنجره باز شده داخل تب General روی کلید Advanced کلیک کنید. (عکس شماره 4)
2. در پنجره باز شده، در بخش Compress and Encrypt attribute گزینه Encrypt contents to secure data را با برداشتن تیک آن غیرفعال کنید بر روی کلید OK کلیک کنید (عکس شماره 5) ، همچنین بر روی کلید OK در صفحه Properties کلیک نمایید.
3. در پنجره باز شده گزینه Apply changes to this folder, subfolders and files را انتخاب و بر روی کلید OK کلیک نمایید. (درصورتیکه فولدر خالی نباشد این پنجره ظاهر می شود) (عکس شماره 7)

عکس شماره 7

فایل یا فولدر هایی که Encrypt شده اند فقط توسط کلید خصوصی EFS ، مربوط به کاربری که آنها را Encrypt کرده است قابل دسترس، Decrypt و رمزگشایی کردن هستند. درصورتیکه ویروس و یا تغییر سیستم عامل، باعث از بین رفتن Certificate Encryption یا گواهینامه رمزگذاری و Private Key یا کلید خصوصی شود ، دسترسی به فایل های رمز شده غیرممکن می شود. برای جلوگیری از غیرقابل دسترس شدن فایل های Encrypt شده و همچنین دسترسی به فایل ها در اکانت ها یا کامپیوتر های دیگر با سیستم عامل های مایکروسافت (ویندوز 2000 و جدید تر از آن) نیاز است که یک کپی پشتیبان از Encryption Certificate یا گواهینامه رمزگذاری و کلید خصوصی داشته باشید برای دریافت نسخه پشتیان از کلید خصوصی خود، از روش زیر استفاده کنید.

دریافت نسخه پشتیبان از Encryption Certificate و Private Key

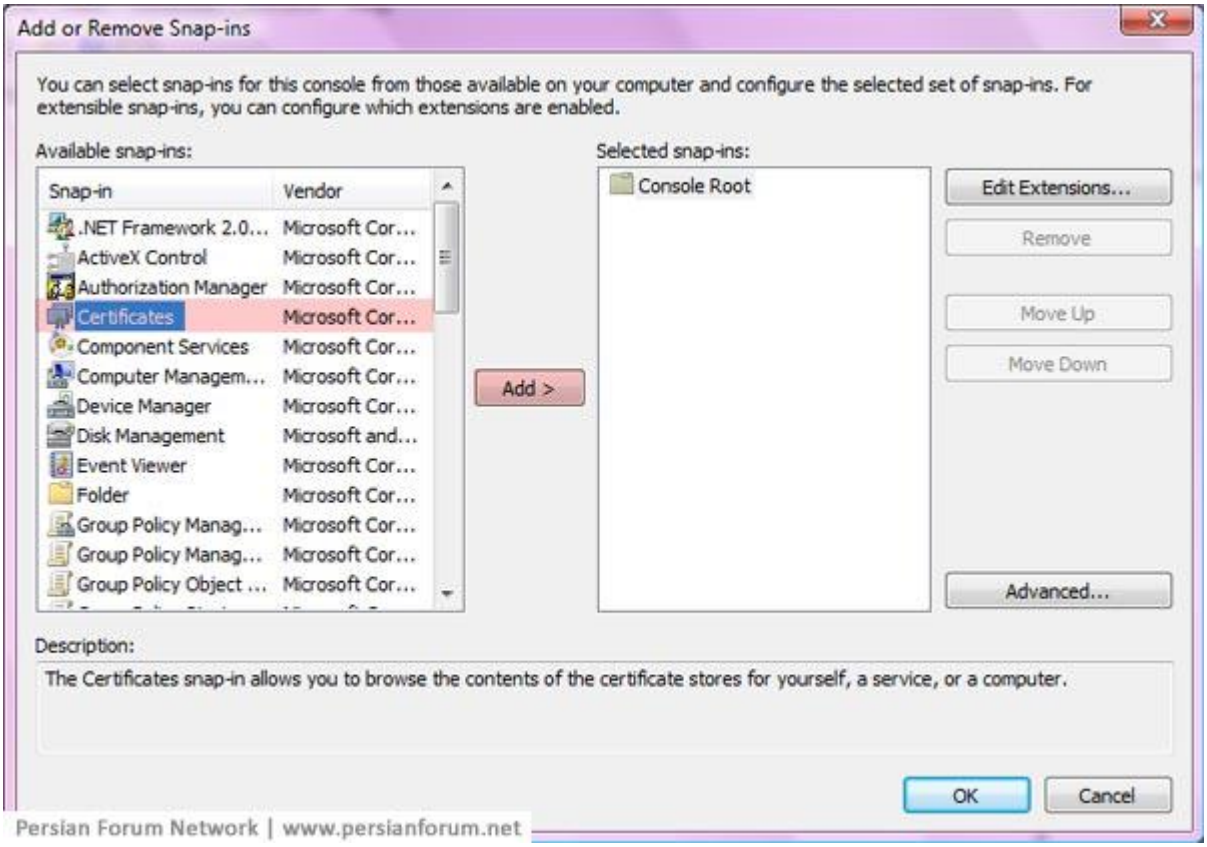
1. منوی Start را باز کنید و برنامه Run را اجرا کنید (درصورتیکه Run در Start منوی شما قرار ندارد روی Task Bar راست کلیک کنید و روی گزینه Properties کلیک کنید در صفحه باز شده تب Start Menu را باز کنید گزینه Start Menu را انتخاب و بر روی کلید Customize رو بروی آن کلیک کنید در صفحه باز شده از لیست، گزینه Run Command را انتخاب و تیک بزنید سپس بر روی کلید OK کلیک کنید) در پنجره باز شده mmc.exe را تایپ و بر روی کلید OK کلیک کنید. (عکس شماره 8)



عکس شماره 8

2. در صفحه باز شده منوی File را باز کنید و روی گزینه Add/Remove Snap-In کلیک کنید در این صفحه بر روی کلید Add کلیک کنید (در ویندوز XP) .

3. در این صفحه از سمت چپ Certificates را انتخاب و بر روی کلید Add کلیک کنید (عکس شماره 9) .

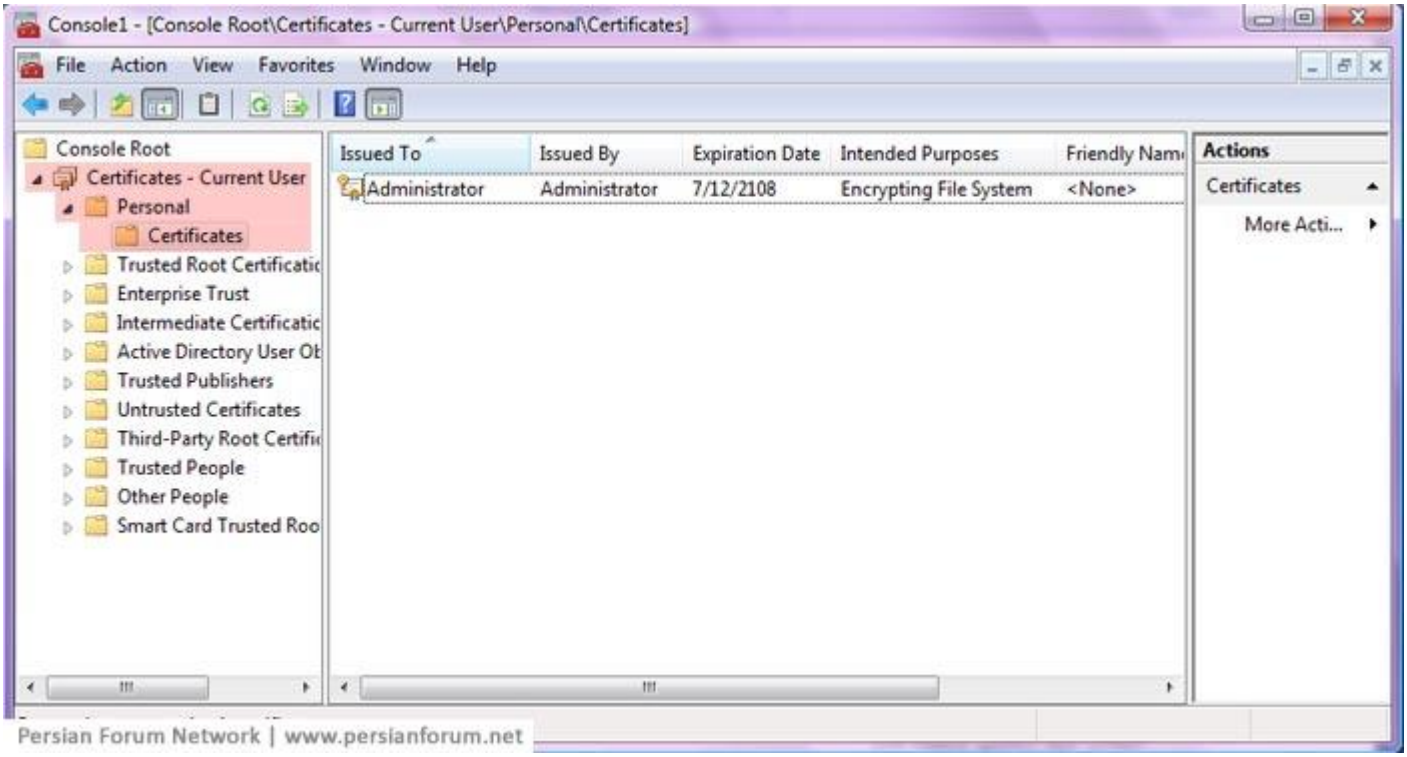


عکس شماره 9

4. در صفحه جدید گزینه My user account را انتخاب و بر روی کلید Finish کلیک کنید.

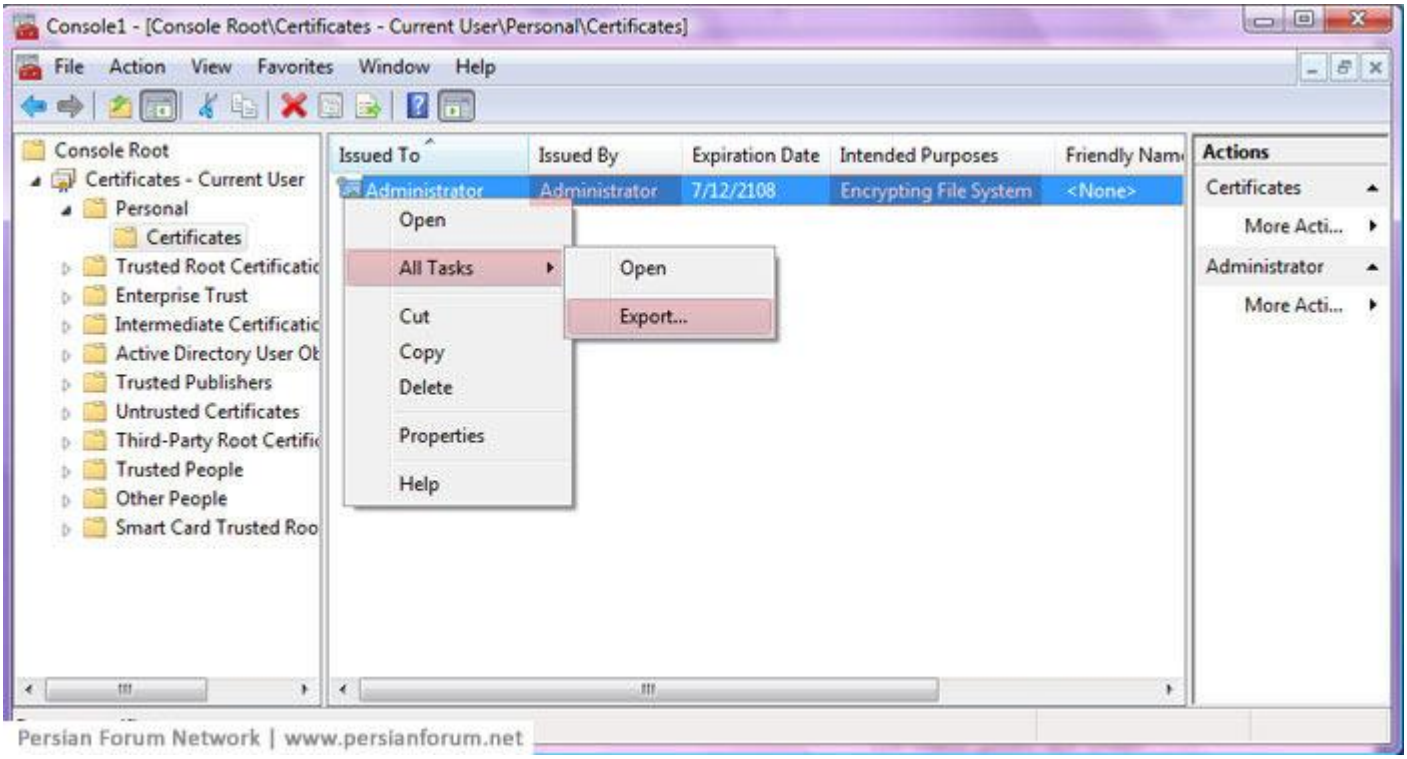
5. کلید Close (در ویندوز XP) و سپس کلید OK را کلیک کنید.

6. در پنجره باز شده سمت چپ Certificates – Current User را باز کنید سپس بخـش Personal را باز و بر روی Certificates کلیک کنید (عکس شماره 10)



عکس شماره 10

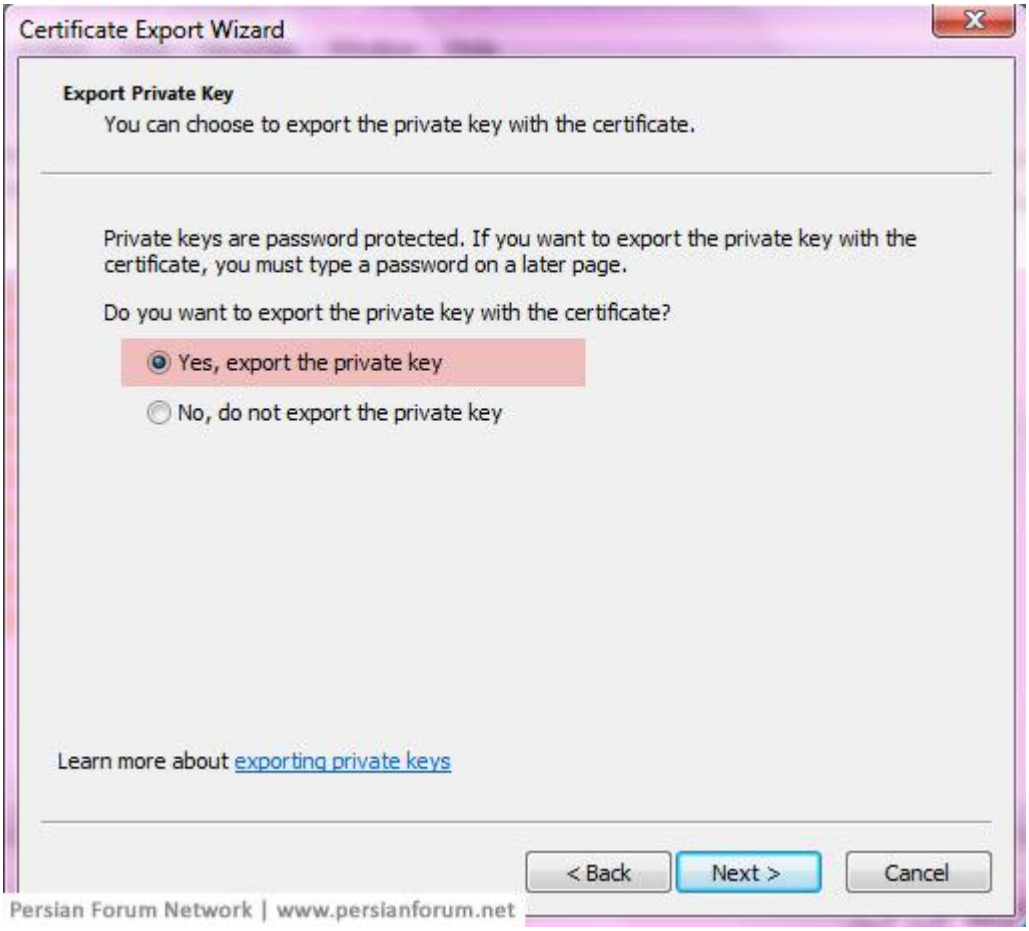
7. سمت راست پنجره، گواهینامه های مربوط به اکانت شما نمایش داده می شود بر روی گواهینامه ی مربوط به Encrypting File System و اکانت خود راست کلیک کنید و از منوی All Tasks گزینه ی Export را انتخاب کنید (عکس شماره 11)



عکس شماره 11

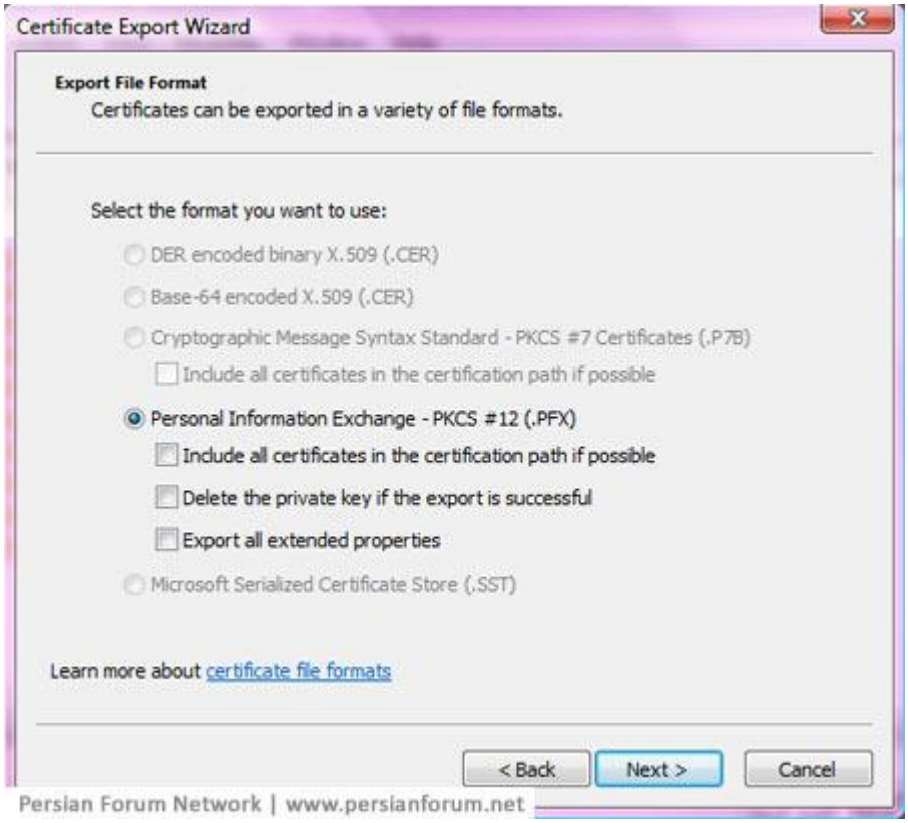
8. در این پنجره بر روی کلید Next کلید کنید.

9. در صفحه جدید، گزینه Yes, export the private key را انتخاب و روی کلید Next کلید کنید (عکس شماره 12)



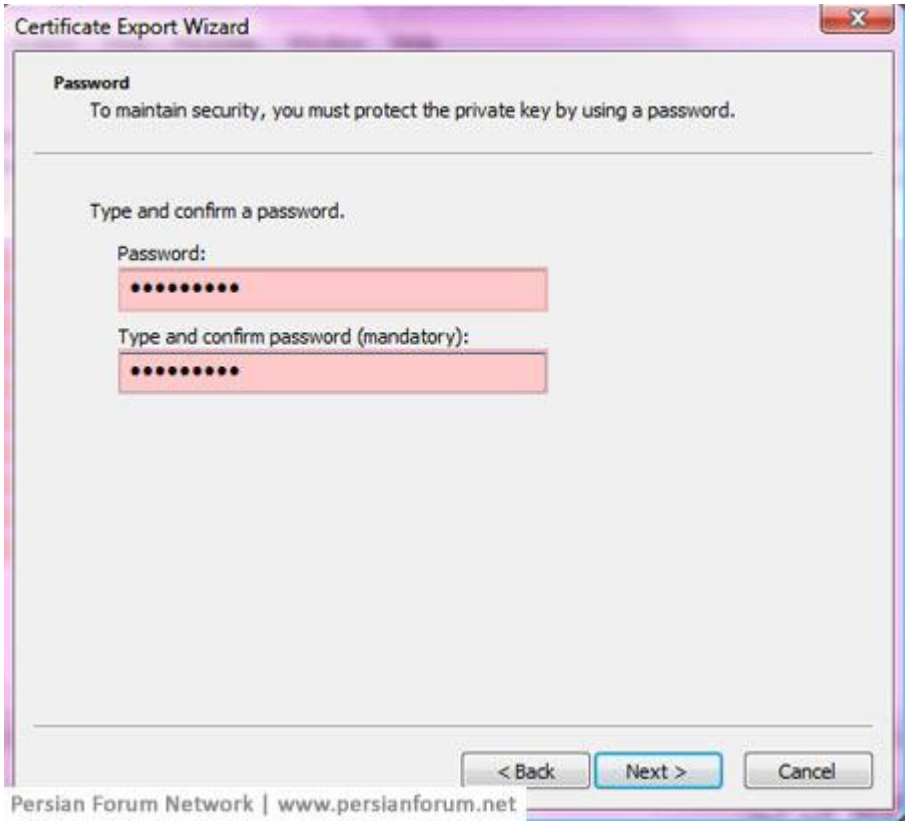
عکس شماره 12

10. در این صفحه بدون تغییر اطلاعات بر روی کلید Next کلید کنید (عکس شماره 13)



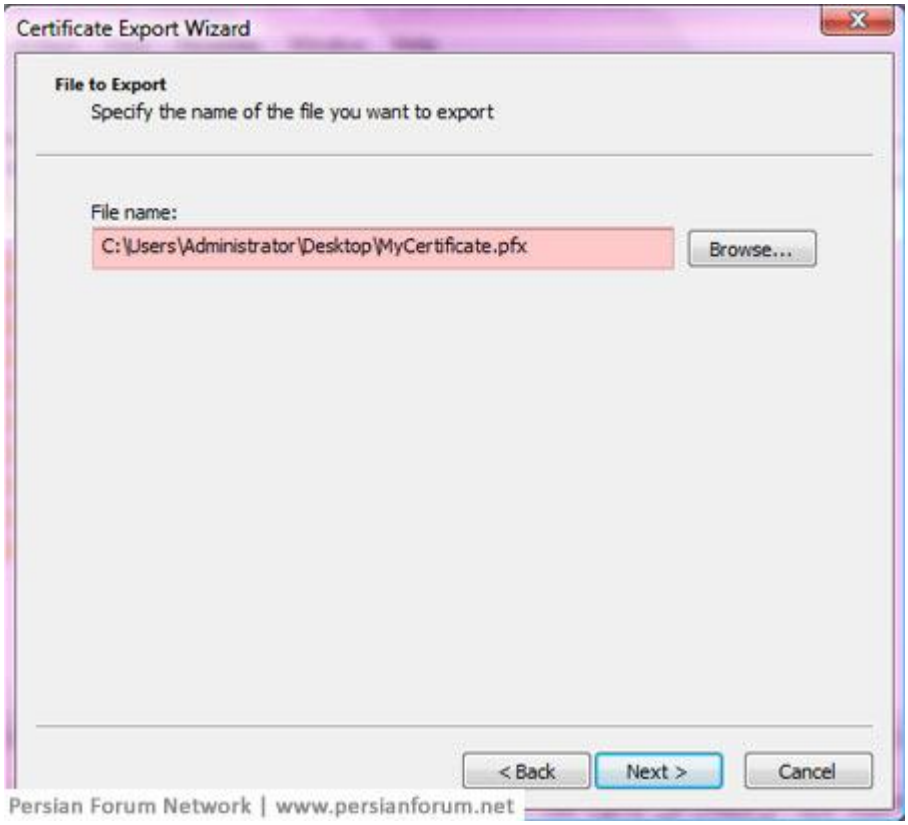
عکس شماره 13

11. **در صفحه باز شده، پسورد مربوط به نسخه پشتیبان گواهینامه رمزگذاری فایل های خود را انتخاب و تایپ کنید و بر روی کلید Next کلیک کنید، در انتخاب این پسورد دقت کنید این کلمه عبور وسیله محافظت از اطلاعات و فایل های شما است (عکس شماره 14)**



عکس شماره 14

12. در این صفحه نام فایل گواهینامه و محل ذخیره ی آن را انتخاب کنید و بر روی کلید Next کلیک کنید. (عکس شماره 15)



عکس شماره 15

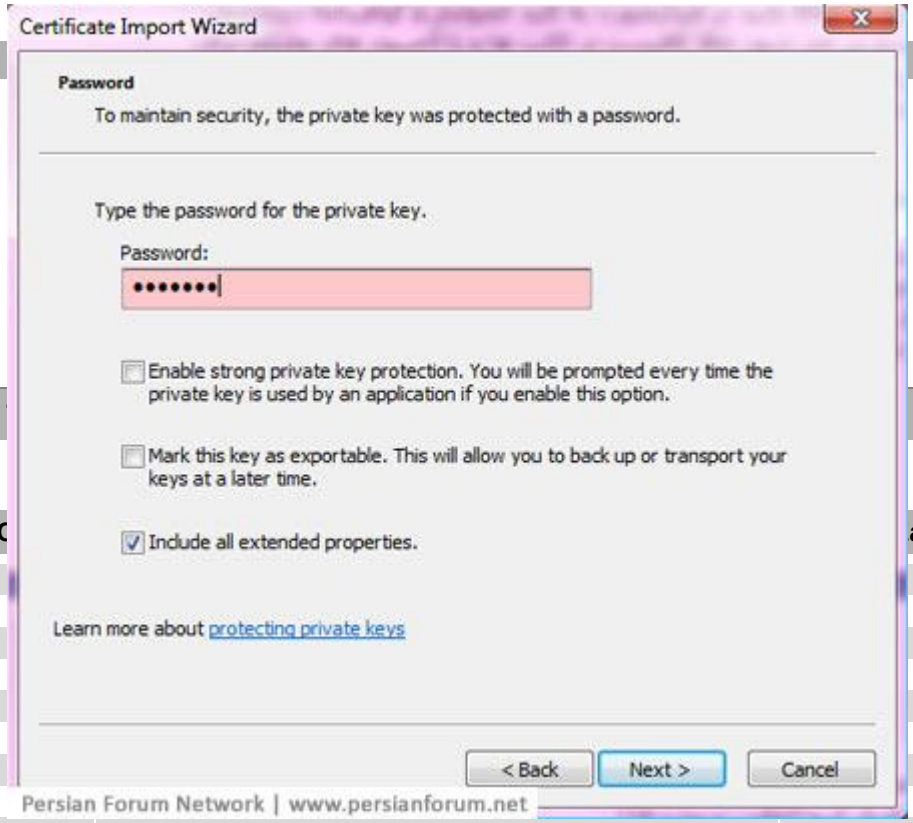
13. روی کلید Finish کلیک کنید.

این فایل را داخل درایو و یا کول دیسک در کنار فولدر Encrypt شده قرار دهید توجه کنید که فایل را به اشتباه داخل فولدر Encrypt شده قرار ندهید و آن را Encrypt نکنید در غیراینصورت به کلید خصوصی و گواهینامه دسترسی نخواهید داشت و اطلاعات غیر قابل دسترس می شود. حالا کافیست در اکانت ها و یا کامپیوتر های مختلف برای دسترسی به فایل های خود این فایل را اجرا کنید و اطلاعات کلید خصوصی را وارد کامپیوتر و یا اکانت مورد نظر خود کنید. برای Import کردن و یا وارد کردن کلید خصوصی در کامپیوترهای دیگر به روش زیر عمل کنید.

Import کردن گواهینامه ی رمزگذاری و کلید خصوصی

1. بر روی فایل گواهینامه کلیک و آن را اجرا کنید، در پنجره باز شده بر روی کلید Next کلیک کنید.
2. در این صفحه بدون تغییر اطلاعات بر روی کلید Next کلیک کنید.

3. در صفحه جدید پسورد مربوط به این گواهینامه را وارد کنید (پسوردی که زمان دریافت نسخه پشتیبان برای آن تعیین کردید) درصورتیکه گزینه های پایین صفحه فعال هستند با برداشتن تیک آنها، همه را غیرفعال کنید و بر روی کلید Next کلیک کنید. (عکس شماره 16)



عکس شماره 16

4. در این صفحه بدون تغییر اطلاعات بر روی کلید Next کلیک کنید.

5. بر روی کلید Finish کلیک کنید.

بعد از این مرحله سیستمی که گواهینامه رمزگذاری و کلید خصوصی را روی آن Import کرده اید می تواند براحتی به فایل های Encrypt شده دسترسی داشته باشد، توجه کنید در صورتیکه قصد دارید فایلی را از روی این سیستم در فولدر Encrypt شده در هارد دیسک و یا کول دیسک خود کپی کنید باید به کاربر خود (کاربری که در سیستم شخصی خود برای Encrypt کردن فایل ها از آن استفاده کرده اید) دسترسی جدید بدهید، این بدین دلیل است که زمانیکه شما فایلی را روی سیستمی دیگر به فولدر Encrypt شده خود اضافه می کنید سیستم با استفاده از اکانت روی آن سیستم فایل شما را Encrypt می کند و اگر شما به کاربر خود

دسترسی ندهید زمانیکه در سیستم شخصی خود قصد استفاده از فایل را داشته باشید سیستم اجازه استفاده از فایل را به شما نمی دهد، برای این کار و دسترسی دادن به کاربر خود از روش زیر استفاده کنید.

اضافه کردن کاربر جدید به لیست دسترسی کاربران در فایل Encrypt شده

در این مثال کاربر Administrator نام کاربری اکانت شما در کامپیوتر شخصی شما، کامپیوتری که فایل ها را داخل آن Encrypt کرده اید است، و نام کاربری Ali نام اکانت مربوط به کامپیوتر یکی از دوستانتان است ، یک فایل از روی این سیستم روی هارددیسک اکسترنال خودتان داخل فولدر Encrypt شده کپی می کنید و حالا قصد دارید به کاربر خود برای استفاده از این فایل دسترسی بدهید. توجه کنید که لیست دسترسی کاربران در فولدرها قابل دسترس نیست و برای تغییر لیست باید از طریق فایل ها اقدام کنید. قبل از اینکه بتوانید کاربر خود را به لیست دسترسی کاربران اضافه کنید باید گواهینامه خود را به بخش Trusted People اضافه یا Import کنید، برای این کار از روش زیر استفاده کنید.

1. بر روی فایل گواهینامه کلیک و آن را اجرا کنید، در پنجره باز شده بر روی کلید Next کلیک کنید.
2. در این صفحه بدون تغییر اطلاعات بر روی کلید Next کلیک کنید.
3. در صفحه جدید پسورد مربوط به این گواهینامه را وارد کنید (پسوردی که زمان دریافت نسخه پشتیبان برای آن تعیین کردید) درصورتیکه گزینه های پایین صفحه فعال هستند با برداشتن تیک آنها، همه را غیرفعال کنید و بر روی کلید Next کلیک کنید. (عکس شماره 16)

4. در این صفحه گزینه Place all certificates in the following store را انتخاب و بر روی کلید Browse کلیک کنید و از لیست باز شده Trusted People را انتخاب و بر روی کلید OK کلیک نمایید سپس بر روی کلید Next کلیک کنید.

5. بر روی کلید Finish کلیک کنید.

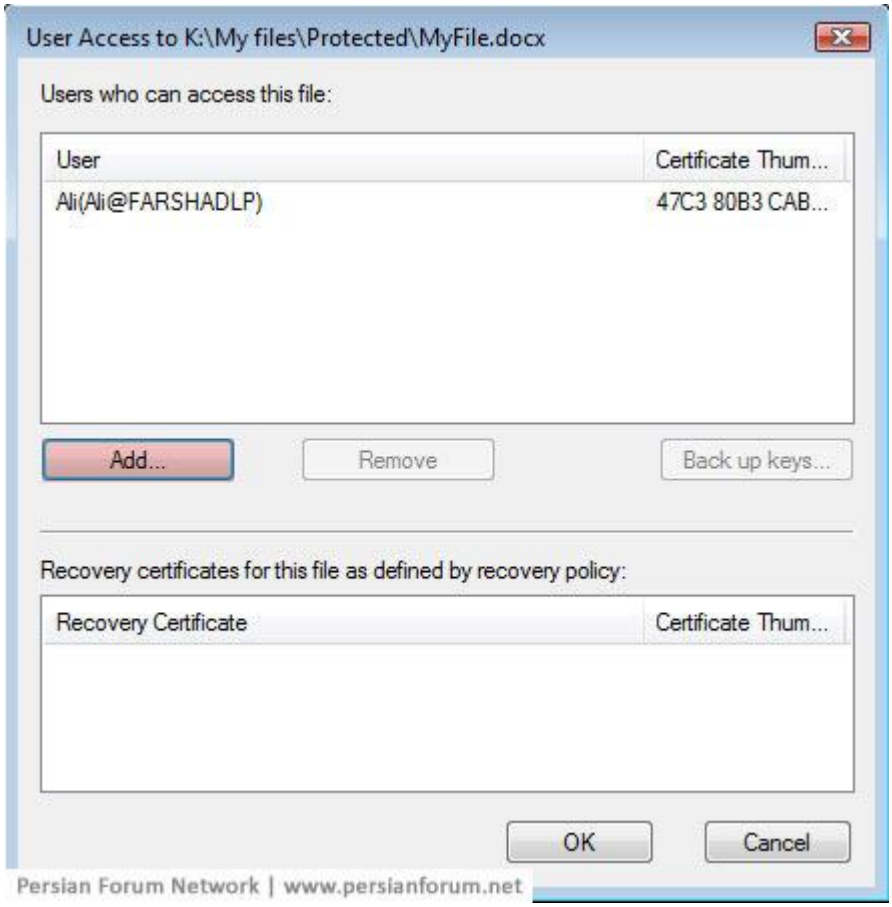
اضافه کردن کاربر به لیست دسترسی ها

1. روی فایل مورد نظر راست کلیک کنید و از منوی باز شده روی Properties کلیک کنید.
2. در تب General بر روی کلید Advanced کلیک کنید

3. در این پنجره، روبروی گزینه Encrypt contents to secure data بر روی کلید Details کلیک کنید (عکس شماره 17)

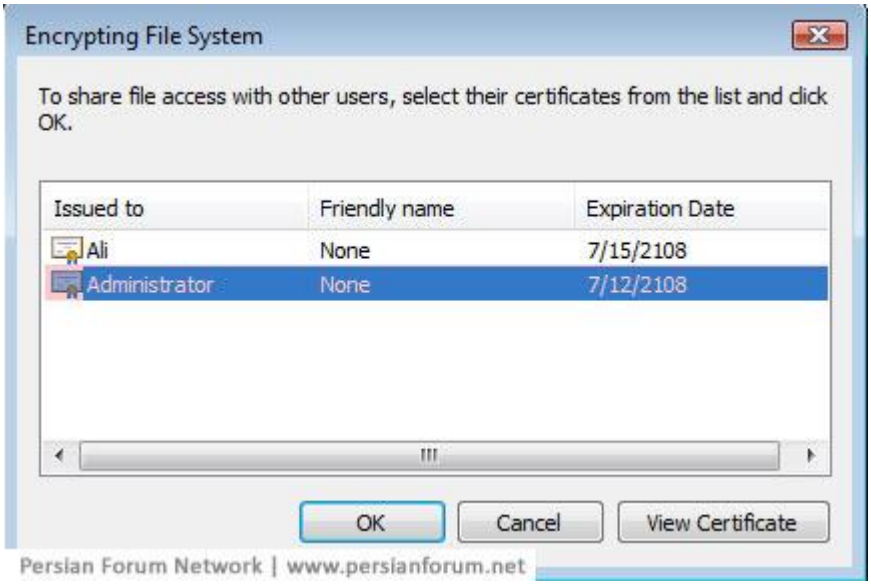
عکس شماره 17

4. در این صفحه بر روی کلید Add کلیک کنید (عکس شماره 18)



عکس شماره 18

5. از لیست گواهینامه ها، گواهینامه ی مربوط به نام کاربری خود را انتخاب کنید و بر روی کلید OK کلیک نمایید (در مثال ما نام کاربری Administrator است) (عکس شماره 19)



عکس شماره 19

6. در صفحه دسترسی ها بر روی کلید OK کلیک کنید

7. روی کلید OK کلیک کنید

8. مجددا بر روی کلید OK کلیک کنید و پنجره Properties مربوط به فایل را ببندید. بعد از این مرحله کاربر شما براحتی می تواند به فایل دسترسی داشته باشد. همینطور که قبلا توضیح دادم، برای دسترسی به فایل های کول دیسک و یا هارددیسک اکسترنال خود در کامپیوتر های دیگر نیاز است که اطلاعات گواهینامه و کلید خصوصی را روی کامپیوتر مورد نظر خود Import کنید توجه کنید اگر بعد از اتمام کار با فایل ها در کامپیوتر موردنظر خود گواهینامه خود را از کامپیوتر حذف نکنید کاربر آن سیستم می تواند در آینده، در صورتیکه فایل های Encrypt شده شما را در اختیار داشته باشد به آنها براحتی دسترسی داشته باشد برای جلوگیری از این مشکل بعد از اتمام کار باید گواهینامه خود را از سیستم مورد نظر خود حذف کنید، توجه کنید که به اشتباه گواهینامه را از روی سیستم شخصی خود (سیستمی که فایل های خود را روی آن Encrypt کرده اید) حذف نکنید، برای حذف گواهینامه از روش زیر استفاده کنید.

حذف گواهینامه EFS

1. منوی Start را باز کنید و برنامه Run را اجرا کنید در پنجره باز شده mmc.exe را تایپ و بر روی کلید OK کلیک کنید. (عکس شماره 7)

2. در صفحه باز شده منوی File را باز کنید و روی گزینه Add/Remove Snap-In کلیک کنید در این صفحه بر روی کلید Add کلیک نمایید (در ویندوز XP) .
3. در صفحه باز شده از سمت چپ Certificates را انتخاب و بر روی کلید Add کلیک نمایید (عکس شماره 9) .
4. در صفحه جدید گزینه My user account را انتخاب و بر روی کلید Finish کلیک کنید.
5. کلید Close (در ویندوز XP) و سپس کلید OK را کلیک کنید.
6. در پنجره باز شده سمت چپ Certificates – Current User را باز کنید سپس بخش Personal را باز و بر روی Certificates کلیک کنید (عکس شماره 10).
7. سمت راست پنجره، گواهینامه های مربوط به اکانت این کامپیوتر نمایش داده می شود بر روی گواهینامه ی مربوط به Encrypting File System و اکانت خود راست کلیک کنید و از منوی باز شده روی گزینه ی Delete کلیک کنید.
8. برای تایید بر روی Yes کلیک کنید.

حالا می توانید براحتی هارددیسک اکسترنال یا کول دیسک خود را از این سیستم جدا کنید.
توجه : در نگهداری فایل Certificate و Private Key خود دقت کنید در صورتیکه به سیستم اصلی خود دسترسی نداشته باشید و این فایل از بین برود دسترسی به فایل های Encrypt شده غیر ممکن می شود. بنابراین سعی کنید کلمه عبور گواهینامه را بخاطر بسپارید و فایل گواهینامه را چند جای مختلف نگهداری کنید تا در صورت نیاز براحتی بتوانید آن را به سیستم جدید خود Import و به فایل های رمز شده ی خود دسترسی پیدا کنید.

EFS یکی از معتبرترین روش های محافظت از اطلاعات در سیستم عامل های مایکروسافت (بر پایه NT) است، ممکن است استفاده از آن برای بار اول ساده و دوستانه نباشد ولی مطمئنا راهی قابل اعتماد برای محافظت از اطلاعات است و ارزش استفاده کردن را دارد.

August 2008

نویسنده :
فرشاد دشتی
Certified Systems Engineer - Microsoft Certified Systems Microsoft
Messaging : Administrator

منبع اصلی مقاله : http://www.persianforum.net/Topic108344-72-1.aspx

منابع :

کتاب : Reference McGrawHill Windows Vista The Complete

کتاب : Vista MCTS Self-Paced Training Kit : Configuring Windows

کتاب : MCSE Training Kit : Windows XP Professional

وب سایت : www.microsoft.com

گرد آوری : **www.Group-F5.org**