

# Microsoft Windows Encrypting File System (EFS) Certificate Migration from XP to VISTA (also works with Windows 7)

Instruction Guide



Army Information Assurance CAC/PKI Division 2530 Crystal Drive Arlington, VA 22202

July 2009

# **Revision History**

Version Number	Preview Release	Section	Date

# Table of Contents

Table of Contents 3
Introduction4
Purpose4
Requirements4
Exporting EFS Certificates from MS Windows XP (End-User)
Importing EFS Certificates into Windows Vista (End-User)11
CAC Certificate Replacement Procedures for VISTA Encrypting File System (EFS) 15
Recovering your old Encryption Certificate:
Update Existing Files with New Encryption Certificate:17

## Introduction

Microsoft Windows Encrypting File System (EFS) is a file system encryption process that allows users to encrypt and decrypt files or folders on their workstation. Windows XP EFS uses a Microsoft self-signing encryption certificate to encrypt the files or folders on the user's workstation. Windows VISTA can be configured to use either Microsoft's self-signed certificates or public key certificates. When upgrading from Windows XP to Windows Vista, the encryption certificate must be saved so that any encrypted data can be decrypted after the migration process is completed. This instruction guide outlines the procedures that must be followed to ensure a successful migration from Windows XP to Windows Vista. When a user attempts to encrypt or decrypt data, EFS looks in the user's personal certificate store for an EFS certificate.

### **Purpose**

This document provides end-user and administrator guidance on the migration process of exporting user's Windows XP EFS certificates into a Windows VISTA configuration. This instruction guide outlines the procedures that must be followed to ensure a successful migration of your EFS Certificates from Windows XP to VISTA.

## Requirements

For the purposes of EFS Certificate Migration, the following prerequisites apply -

- User Type(s): The end-user and an administrator (with administrator rights) must be available.
- System Requirements:
  - a. One computer configured with Windows XP OS with the end-user's current public/EFS certificates.
  - b. One computer configured with Windows Vista OS.
- Network or Accessible Storage Media: A location for the use of exporting and importing user data that can be accessed by both the XP and Vista systems.

#### Exporting EFS Certificates from MS Windows XP (End-User)

To save the EFS certificate, it is necessary to export the EFS certificates from Windows XP and save it to a network drive or accessible storage media. The following procedures must be followed:

- 1. End-user: Logon to your assigned desktop/laptop (Windows XP)
- 2. From the desktop, click the start button, then click Run



3. In the dialog box, Type mmc and click OK

Run		? 🛛
-	Type the name of a program, fold Internet resource, and Windows v	er, document, or vill open it for you.
Open:	mmc	~
		el Browse

4. From the Main Menu, click File, then click Add/Remove Snap-in



5. In the Add/Remove Snap-in dialog box, click Add

Add/Remove Snap-in
Standalone Extensions
Use this page to add or remove a stand-alone snap-in from the console.
Snap-ins added to: Console Root 💌 💿
Description
Add
OK Cancel

6. Select Certificates, then click Add



7. Underneath "This snap-in will always manage certificates for:" select **My user account** and select **Finish.** 



8. From the Add/Remove Snap-In box, click Close

dd Standalone Snap-in		?		
Snap-in	Vendor	^		
and ActiveX Control	Microsoft Corporation			
Certificates	Microsoft Corporation			
Component Services	Microsoft Corporation			
Computer Management	Microsoft Corporation			
📕 Device Manager	Microsoft Corporation			
😵 Disk Defragmenter	Microsoft Corp, Execut			
👹 Disk Management	Microsoft and VERITAS			
💼 Event Viewer	Microsoft Corporation			
🚞 Folder	Microsoft Corporation			
💐 Group Policy Object Editor	Microsoft Corporation	¥		
Description The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.				
	Add Close	,		

9. From the Add/Remove Snap-In box, Click OK

Add/Remove Snap-in
Standalone Extensions
Use this page to add or remove a stand-alone snap-in from the console.
Snap-ins added to: 🔄 Console Root 💌 💼
🗐 Certificates - Current User
Description
Add Remove About
OK Cancel

- 10. Browse to the Personal\Certificates folder -
  - a. Click the **plus sign** in next to "Certificates Current User"

🚡 Cons	ole1 - [	Conso	le Root\Ce	rtificates	; - C
🚡 File	Action	View	Favorites	Window	He
⇔ ⇒	<b>E</b>	] 🖸	8	▶ I	
Cons	ole Root Certificate	s - Curn	ent User		

b. Click the **plus sign** in next to the "Personal" folder

🚡 Cons	ole1 - [(	Conso	le Ro	ot\Ce	rtificates	- (
🚡 File	Action	View	Fav	orites	Window	н
$\Leftarrow \Rightarrow$	1	0	₿	1	E	
Conse	ole Root					
📄 🐻 C	ertificates	- Curre	ent Us	ser		
÷	🗋 Persona	el				
	Trusted	Root	Iertifi	cation A	uthorities	
1 📅 🖻	Entorne	ico Tru				

c. Click the Certificates folder



- 11. Export the certificate(s) -
  - a. Right-click on the certificate(s) for migration.
  - b. Click All Tasks and then click Export.



12. At the Certificate Export Wizard Welcome screen, click Next



13. At the File to Export screen, click the Browse button

Certificate Export Wizard	
File to Export Specify the name of the file you want to export	
File name:	Browse

14. In the Save As dialogue box, choose a file location (e.g. a network drive or other accessible location or media), give the certificates a File name (e.g. MyPersonalCertificates1) and ensure file type is either \*.p12/\*.pfx or All Files \*.\*Click Save.

Save As	?	×
Save in:	: 📔 My Documents 🔹 🕐 📴 🚥 -	
My Recent Documents	2.1.1.1.3	
Desktop	My Music My Pictures My Videos	
My Documents		
My Computer		>
<b></b>	File name: Save	
My Network	Save as type: All Files (".") Cancel	
	PKCS #7 Certificates (*.p7b) All Files (*.*)	

15. In the File to Export dialogue box, click Next

ertificate Export Wizard
File to Export Specify the name of the file you want to export
File name:
C:\Documents and Settings\Administrator.M50-XP01\My Document Browse
< Back Next > Cancel

16. At the Completing Certificate Export dialogue box, click Finish and then click OK

Certificate Export Wizard		×		
	Completing the Certificate Export Wizard Vou have successfully completed the Certificate Export wizard. You have specified the following settings: The Name C:Ipocuments and SettingsiAdministrator File Format Cryptographic Message Syntax Standard	Cer Tł	Expiration Date 4/23/2010 4/23/2010 4/23/2010 tifficate Export V we export was succes	Intended P <all> <all> Smart Card</all></all>
	< Back Finish Cancel		OK	ł

17. Exit Console1, by clicking **File** and **Exit**, from the console's main menu, then click **Yes** to save

🚡 C	onsole1 - [Console Root\Cert	ificates - Cu	
6	le Action View Favorites '	Window Help	
4	New	Ctrl+N	
	Open	Ctrl+O	
<u> </u>	Save	Ctrl+S	
	Save As		Microsoft Management Console
	Add/Remove Snap-in	Ctrl+M	
	Options		
-	1 C/WINDOWS/system32/apedit		Save console settings to Console1?
	2 CIWINDOWS(system32)compmo	mot	
	3 C:\WINDOWS\system32\devman	anc. at	
	4 C:\WINDOWS\system32\dfra		
	( citing points) sconoriality		Yes No Cancel
	Exit 🕨		
			<b>~</b>

18. At the Save As dialogue box, click Save



19. End-user: Logoff the desktop/laptop

#### Importing EFS Certificates into Windows Vista (End-User)

- 1. End-user: Logon to your assigned, destination desktop/laptop
- 2. From the desktop, click the start button, then click Run
  - Windows Update

    Programs
    Progr
- 3. In the dialog box, Type mmc and click OK

Run		? 🛛
-	Type the name of a program, fold Internet resource, and Windows v	er, document, or vill open it for you.
Open:	mmc	~
		el Browse

4. From the Main Menu, click File, then click Add/Remove Snap-in



5. In the Add/Remove Snap-in dialog box, under the Available snap-ins column, click **Certificates**, then click **Add**, and then click **OK** 

Cono in	Vondor		Concelo Root	Edit Ex
ActiveX Control	Microsoft Cor Microsoft Cor		Console Root	R
Component Services	Microsoft Cor			M
Device Manager	Microsoft Cor		_	Mo
🗃 Disk Management 🛃 Event Viewer	Microsoft and Microsoft Cor	Add		
Folder	Microsoft Cor			
IP Security Monitor	Microsoft Cor			
IP Security Policy Ma	Microsoft Cor			
Local Users and Gro	Microsoft Cor	-		Adv
escription:				

- 6. Importing the certificate(s)
  - a. In the Console1 dialogue window, click the next to **Certificates Current User** to expand the folder list
  - b. Right-Click on the **Personal** folder
  - c. Select All Tasks and then select Import

Console1 - [Console Root]	
File Action View Favorites	Window Help
Þ 🔿 🔚 🔒 🖬 🖬	
Console Root Name	
🗄 🗊 Certificates - Current L 🙀 Ce	ertificates - Current User
★ Find Certificates	
All Tasks	Find Certificates
E New Window from Here	Request New Certificate
E Refresh	Import
	Advanced Operations
± Help	1

7. At the Certificate Import Wizard dialogue box, click Next



- 8. Locate your certificates for importing
  - a. Click the Browse button



- b. Locate your file folder location, by clicking the down arrow and opening the folder or drive of your exported certificate from Windows XP, (See: <u>Step 1.13</u>).
- c. Change the file type to PKCS #12 Certificates (\*.p12/\*.pfx) <u>OR</u> All Files \*.\* Note: Your *MyCertificates1* file should be available.

G 🕞 - 🕨 - Documen	ts • EFSProtected		• 🙀 🖂	arch		2	8
Organize  Viganize  Vigani	New Folder     New Folder     Name *   +  Date     MyCertificates.pfx	V Type	+  Sze	+  Tags	-	0	
Polders				-			
File name	MyCertificates pfx		×	Personal In X 509 Certificate Certificate Microsoft S	Iomation Exchang icate (".cer," crt) omotion Exchang nat List (".sti) levocation List (".c stalized Certificate	• • • • • • • •	(".81

9. From the Open dialogue box, double-click your *Certificates* file and click the **Open** button

Copen			<u> </u>
😋 🗢 📕 « EFS 🕨 M	lyCertificates		arch 🖇
🌒 Organize 👻 🇱 Views	👻 📑 New Folder	_	6
Favorite Links	Name Date modif	Type Siz	te
Computer Co	MyCertificates1		
Folders ^			
File name:	MyCertificates 1	•	PKCS #7 Certificates (*.spc;*. • Open Cancel

10. Click Next

11. Click Next

12. Click Finish



- 13. Exit Console1, by clicking **File** and **Exit**, from the console's main menu, then click **Yes** to save
- 14. At the Save As dialogue box, click **Save** [END OF INSTRUCTIONS]

#### CAC Certificate Replacement Procedures for VISTA Encrypting File System (EFS)

#### **Recovering your old Encryption Certificate:**

1. Insert your CAC into your CAC Reader and from the Window's desktop, double-click the **Internet Explorer** icon to open the browser.

2. User must recover and install his encryption key or certificate from their previous CAC (.p12 file) from the DISA Automated Key Recovery website. Go to the following URL: https://ara-1.c3pki.chamb.disa.mil/

Note: If user is having application issues with IE the user may need to download the .p12 file using another computer and transfer the file to their computer.

<i>0</i>				Window	vs Inte	ernet Exp	plorer	
$\bigcirc$	0	- 🧧	https://ara-:	1.c3pki.c	hamb.d	isa.mil/		_
File	Edit	View	Favorites	Tools	Help			

3. This will prompt you to choose a digital certificate. Select your **ID Certificate** (won't have EMAIL listed under Issuer) and select **OK.** 

Name	Issuer	
First Name	DOD CA-19	
First Name	DOD EMAIL CA-19 DOD EMAIL CA-20 DOD CA-20	
Joe Smith		
Joe Smith		
	More Info View Certificate	

4. You will see the DoD Warning. Select **OK** to continue.



5. The site will come up and show you the keys available for download. You will need to select the key from your previous CAC. Once identified, select **Recover** 



6. You will be prompted with a DoD prompt. Read the conditions carefully and select **OK**.

Microsoft	: Internet Explorer 🔀
?	I acknowledge that I am the DoD subscriber for this escrowed key. I acknowledge that I am attempting to recover this key. Per DOD FORM 2842, I agree to use this key for authorized purposes only, to protect it from use by others, and to destroy it when no longer needed.
	OK Cancel

7. Please wait while Auto Key Recovery takes place. This can take up to 2 minutes.



#### Please Wait.

The Automated Key Recovery Agent is recovering the key you selected. This process can take up to two minutes.

Please do not hit the 'Back' button on your browser toolbar.

If the results do not appear within two minutes,  $\underline{\operatorname{click}\,\operatorname{here}}$ 



8. Once completed, you will get a message saying "**The Automated Key Recovery Agent has recovered your key. To retrieve your key, select the following link**". Select **DOWNLOAD** to download the .p12 file from your previous certificate. You will also receive a one-time password that you will need to use to restore your encryption key or certificate to your system- take note of that password.



9. Open the .p12 file and allow it to install.



10. Select Logout



Once this key is recovered and installed on your system you will be able to view those previously encrypted files and have no problems with applications because you are viewing them with the certificate from your previous CAC.

#### Update Existing Files with New Encryption Certificate:

Perform an update to all your files with your new certificate or encryption key that from your replacement CAC. This is done through use of the executable called rekeywiz.exe. The steps are as follows;

1. Close any open files or applications. Got to command prompt by selecting Start  $\rightarrow$  Run, type in CMD, then enter the command prompt window will appear.

7	Type the nar	me of a progra	im, folder, docur	ment, or Interne
		d windows wi	in open it for you	•
en:	cmd			

2. The command prompt will be displayed on your screen as follows. Ensure you are at the root of your local drive i.e. C:\. To change to a different directory type the directory letter then a colon (C:). To go from a subdirectory to the root directory type cd and a back slash (CD\)



3. Type in **rekeywiz.exe** and then press **enter**.



4. This will take you into the rekey wizard. Select **Next**.

Manage your file encryptic	on certificates	
To encrypt files for addit	ional security, you must have an encryption certificate and i	ts
associated decryption k	ey on your computer or on a smart card. You can't access	your
encrypted files without th	is certificate and key.	
Use this wizard to:		
<ul> <li>Select or create a file e</li> </ul>	ncryption certificate and key.	
Back up the certificate	and key to avoid losing access to your encrypted files.	
- Set Encrypting File Sys	item to use a smart card.	
- Update previously enc	rypted files to use a different certificate and key.	
What is Encrypting File S	System?	

5. You will be taken to another screen that ask whether you are creating a new encryption certificate or selecting an existing certificate. In this case select "**Use this certificate**" as shown. **DO NOT SELECT "CREATE A NEW CERTIFICATE.**" Select **Next.** 

select or create a file encryption certificate	
Select an existing file encryption certificate or create a encrypted files, you can update them to use this certific	new one. If you have already ate.
Vise this certificate If you are using a smart card, select the certificate or	the smart card.
Certificate details: Issued to: NAME_FIRST.A.1111111111	View certificate
Issued by: DOD EMAIL CA-19 Expires: 8/31/2009	Select certificate
Create a new certificate	

6. You will be taken to the **Update Previously Encrypted Files** Screen. Make sure "**All Logical Drives**" is checked, then select **Next**.

Encryp	ting File System
Update yo	ur previously encrypted files
Select the certificate f the previ	folders containing encrypted files that you want to associate with the new and key. Updating now helps you avoid losing access to your encrypted files ous certificate and key are lost.
olders:	
- I'll upda	ate my encrypted files later

7. Select I want to complete this action



8. Press Control + Alt + Delete



9. Enter your PIN and Select OK.

New credents	is: Insert the smart card you want to use for encrypting t	ies.
	FIRST.NAME.A Smart card credential first.nam e @ua.army.ml	
1	PIN	

10. Your files are being updated. This may take a considerable amount of time depending on the number of files being updated.

2 Encrypting File System		
Progress		
Updating your encrypted files	-	

11. Your files have been updated. You should now be able to view the previously encrypted files. Select **Close.** 

encrypted files have been updated		
ssued to: NAME.FIRST.A.1111111111	View certificate	
ssued by: DOD EMAIL CA-19 Expires: 8/31/2009	View log	

# If additional assistance is required, please contact the Army IA CAC/PKI Division Helpdesk.

COMM: (703) 602-7514 TOLL FREE: (866) 738-3222 DSN: (312) 332-7514 Email: <u>iacacpki.helpdesk@us.army.mil</u>